Cisco Prime Network 5.3 User Guide

May, 2020

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

Text Part Number:

CONTENTS

Setting Up Prime Network to Manage Devices, Faults, and the Network

Prime Network Support for Third-Party Devices

Prime Network supports third-party devices through Cisco Advanced Services engagement. As of release 5.1, Prime Network will not natively support third-party devices, and a Cisco Advanced Services contract will be required for their enablement and support.

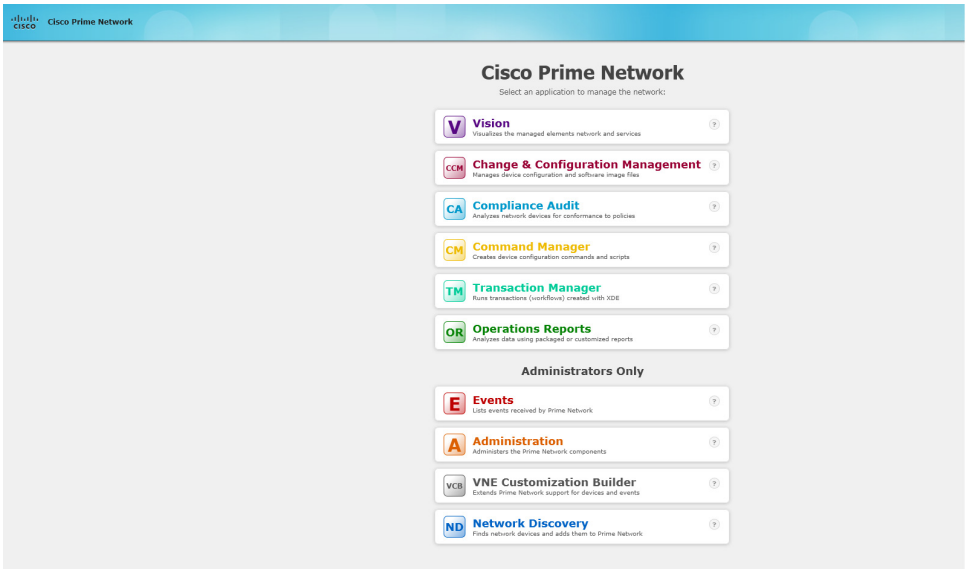
Overview of Prime Network GUI clients

This topic provides an overview of the Prime Network GUI clients, which provide intuitive interface for managing your network and services, and for performing the required system administration activities.

To launch the Webstart page for the Prime Network GUI clients:

Step 1 Open your web browser and type the following address in the Address field: http://<server>:6080/ana/services/install/install/webstart.html. The following Webstart page is displayed:

Figure 1-1 Cisco Prime Network Webstart Page



Step 2 The webstart launch page helps launch the following GUI clients:

GUI client	Description
Vision	The main GUI client for Prime Network using which you can create maps of devices to create a visualization of the network, from the intricacies of a single device physical and logical inventory, to multi-layer topological information on connections, traffic, and routes.
Change & Configuration Management	Helps in management of software images and device configuration files used by the devices in your network.
Compliance Audit	Helps to check compliance of device configurations to deployment policies.
Command Manager	Repository of all configuration commands available in the system. It can be used to create new commands and command sequences, which can then be applied to groups of devices.
Transaction Manager	Helps in management and execution of activation workflows (transactions) that are made up of configuration scripts and designed to execute on devices according to a specific sequence or flow.
Operations Report	An optional add-on component to Prime Network that provides extended reporting functionality. In addition to providing prepackaged, read-only fault, physical inventory, and technology-related reports, it also enables you to create your own reports and to customize some prepackaged reports.
Administrators Only	
Events	The interface used by system managers and administrators for viewing system events that occur in the network.
Administration	The GUI client used to manage the Prime Network system. Administrators use this GUI client to create user accounts, device scopes, polling groups, redundancy settings, and so forth.

GUI client	Description
VNE Customization Builder	Helps you to enable support for unsupported device types, software versions, modules, and events.
Network Discovery	Automatic discovery of network devices.

Setting Up the Prime Network Clients

These topics provide some information about how to set up your devices and get started with the Cisco Prime Network Vision client. These topics assume that the devices have been added to Prime Network using the procedures described in *Cisco Prime Network 5.3 Administrator Guide*.

- Changing Passwords and Using Help in the Prime Network Clients, page 2-5
- Extending Prime Network Features, page 2-6
- Using Prime Network with Prime Central, page 2-7

These topics provide specific instructions for setting up the Vision client and the Events client:

- Workflow for Creating a Map, page 4-2
- Workflow for Setting Up Fault Management, page 6-1

Whether you can perform these setup tasks depends on your account privileges. See Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1for more information.

Changing Passwords and Using Help in the Prime Network Clients

Most Prime Network users run the Vision client. The actions a user can perform depends on how their user account was set up—that is, which operations they can perform using the Vision client and the Events client, and on which devices they can perform those actions. To view permission requirements per function, see Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1.

When you first log into the Vision client or the Events client, Prime Network may require a few extra minutes to download the necessary client files. This will only happen the first time you log in. If you log into a client and Prime Network displays a message that says the client files need to be updated, let the update proceed, and then log in again.

The following table lists some basic Prime Network clients tasks and how to perform them.

To do the following:	Choose from the main menu:
Change your Prime Network client password **Note** Administrators can change the client passwords fro all Prime Network users.	**Tools > Change User Password**
View the icon reference	**Help > Icon Reference**

To do the following:	Choose from the main menu:
Check the version of Prime Network	**Help > About Cisco Prime Network Vision** **Help > About Cisco Prime Network Events**
Launch the Prime Network online help for the Vision client and Events client	**Help > Cisco Prime Network Vision Help** **Help > Cisco Prime Network Events Help**

By default, only advanced users (users with Administrator privileges) can use the Events client. If desired, Prime Network can be configured to allow users with Configurator privileges to run the Events client. For information on how to do this, see the Registry Controller discussion in the *Cisco Prime Network 5.3 Administrator Guide* for more information.

These topics provide setup information for advanced users:

- Setting Up Configuration Management, page 3-5
- Workflow for Creating a Map, page 4-2
- Workflow for Setting Up Regular Reports, page 5-1
- Workflow for Setting Up Fault Management, page 6-1

Extending Prime Network Features

You can download and install new support for NEs, software versions, modules, events, and commands and activation scripts using Prime Network Device Packages (DPs). These can be downloaded from the Prime Network software download site. For more information on how to download and install DPs, see the discussion of DPs in the *Cisco Prime Network 5.3 Administrator Guide*.

In addition, advanced users can also extend the features of Prime Network in the following ways.

To add this extension:	Do the following:
Model and display additional NE properties in the Prime Network clients	Use Prime Network Soft Properties to add these properties to the Prime Network clients.
Add support for unsupported devices, software versions, and modules	Use the Prime Network VNE Customization Builder (VCB) to add support for devices, software versions, and modules that are currently unsupported, so they can be displayed in the Vision client.
Add commands and scripts to perform device configurations	Use Prime Network Command Manager to create scripts and commands that users can launch from an NE's right-click menu in the Vision client. These can range from simple show commands to command scripts containing wizards with multiple pages and input methods, such as check boxes and drop-down lists. See the *Cisco Prime Network 5.3 Customization Guide*.
Create configuration and activation workflows	Use Prime Network Transaction Manager to schedule and run transactions (workflows) that are created using the Cisco XDE Eclipse SDK. See the *Cisco Prime Network 5.3 Customization Guide*.

To add this extension:	Do the following:
Add support for new events	Use the Prime Network VNE Customization Builder (VCB) to add support for traps and syslogs that are currently unsupported so they can be managed by Prime Network. You can also use the VCB to customize the behavior of supported events. See the *Cisco Prime Network 5.3 Customization Guide*.
Add new threshold-crossing alarms	Use Prime Network Soft Properties to create TCAs that are generated when a condition you specify occurs. These TCAs can be viewed in the Prime Network clients. See the *Cisco Prime Network 5.3 Customization Guide*.
Add external launch points to the Vision client	Add a launch point to an external application or URL to an NE's right-click menu using the Prime Network Broadband Query Language (BQL). Launch points can be added to network elements, links, tickets, and events. See the *Cisco Prime Network 5.3 Customization Guide*.
Integrate with northbound applications	Integrate with northbound APIs using BQL to extend the Prime Network Information Model Objects (IMOs), which provide a generic information representation. See the *Cisco Prime Network Integration Developer Guide*.
Support Multi-Technology Operations Systems Interface (MTOSI) and 3GPP northbound interfaces (licensed separately)	Install a Prime Network integration layer that allows Prime Network to expose MTOSI and 3GPP APIs over Service Oriented Access Protocol (SOAP). You can also schedule regular 3GPP inventory reports (by choosing **Tools > Web Service Scheduler** from the Administration client or Vision client). See the *Cisco Prime Network Integration Guide for MTOSI and 3GPP*.
Integrate Cisco Multicast Manager with Prime Network by adding CMM launch points to the Administration and Vision client Tools menus.	Follow the instructions in the *Cisco Prime Network 5.3 Installation Guide* for setting up CMM.

Using Prime Network with Prime Central

Prime Network can be installed as a standalone product or with Cisco Prime Central. When installed with Cisco Prime Central, you can launch Prime Network clients from the Cisco Prime Portal. The right-click menus in the Vision client will include cross-launches for accessing the other Cisco Prime applications. The applications share a common inventory.

The Cisco Prime Portal uses a single sign-on (SSO) mechanism so that users need not reauthenticate with each Prime Network client. All session management features are controlled by the portal (such as client timeouts). If a user tries to log into a standalone Prime Network client, the user will be redirected to the portal login. The only exception is the emergency user, who will still be allowed to log into a standalone Prime Network client.

If Prime Network is installed on Standalone mode and Suite mode with Prime Central client, and if the user launches to NCCM from Prime Network, and allows the Prime Network session to expire, the Prime Network will close and prompts the user to login again while NCCM will not close automatically. The session will remain active until the user logs out of the NCCM.

Prime Performance Manager

If the Cisco Prime Performance Manager application is also installed, the Vision client includes right-click options that allow you to generate device, interface, and VRF-related reports using Prime Performance Manager. Prime Network will receive threshold crossing alarm (TCA) events from Prime Performance Manager components and generate a ticket that you can view in the Prime Network Events client.

Prime Network also receives EPM-MIB traps from the network. By default Prime Network receives EPM-MIB traps from any source in the network. If desired, you can configure Prime Network to only process EPM-MIB traps arriving from a specific Prime Performance Manager server.

Events Client

If you are using Prime Network with Prime Central, launch Prime Network Events from Prime Central. Choose **Assure > Prime Network > Events** in the menu bar. The Prime Network Events application is opened in a separate window.

The following ticket functions are disabled when Prime Network is being used with Prime Central: Acknowledge, Deacknowledge, Add Note, Clear, and Remove.

If Prime Network is being used with Prime Central, both job authorization and credential requirements are enabled.

Vision Client

If you are using Prime Network with Prime Central, launch Prime Network Events from Prime Central. Choose **Assure > Prime Network > Vision** in the menu bar. The Vision client is opened in a separate window.

If Prime Network is installed Prime Central, right-click NE menus will include options for accessing the other Cisco Prime applications.

The following ticket functions are disabled when Prime Network is Prime Central: Acknowledge, Deacknowledge, Add Note, Clear, and Remove.

If Prime Network is being used with Prime Central, both job authorization and credential requirements are enabled.

Setting Up Change and Configuration Management

Cisco Prime Network Change and Configuration Management (CCM) allows you to manage the device configurations and software images used by the devices in your network. These topics explain how to use CCM:

Whether you can perform these setup tasks depends on your account privileges. See Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1 for more information.

Note After installing or upgrading Prime Network, we recommend you to clear the browser cache before using CCM.
If Prime Network is installed on the Standalone mode and Suite mode with Prime Central client, and if you launch the NCCM from Prime Network, and allows the Prime Network session to expire, the Prime Network will close and prompts you to login again while the NCCM will not close automatically. The session will remain active until you log out of the NCCM.

Workflow for Setting Up CCM

The following table provides the basic workflow for setting up CCM.

	Description	See:
Step 1	Make sure Prime Network is set up correctly: • Verify the CCM port on the gateway, make sure the TFTP directory is set up on the gateway or unit, and so forth. • Check the global settings that can impact the CCM functions that users can perform. If necessary, ask your Administrator to adjust the settings.	Configuring Prime Network for CCM, page 3-2 Checking Prime Network Global Settings for CCM Operations, page 3-4
Step 2	Set up your devices so CCM can manage them—for example, make sure devices are reachable and your transfer protocols are set up correctly.	Setting Up Devices to Work With CCM, page 3-4
Step 3	Set up Configuration Management—for example, perform the initial backup of configuration files to the configuration archive, set up the policy for ongoing and event-driven configuration checks, and so forth.	Setting Up Configuration Management, page 3-5
Step 4	Set up Image Management—for example, configure the transport protocol and the staging and storage directories.	Setting Up Image Management, page 3-15
Step 5	Set up device groups for bulk CCM operations.	Setting Up CCM Device Groups, page 3-20

Setting Up Prime Network to Work With CCM

These topics describe how to set up Prime Network to use the CCM features:

- Configuring Prime Network for CCM, page 3-2
- Checking Prime Network Global Settings for CCM Operations, page 3-4

Configuring Prime Network for CCM

Check these settings to ensure Prime Network components are properly configured for CCM operations.

- Verify the gateway port to be used. 8043 is the secure HTTP port enabled by default for CCM, but you can use port 8080 instead using this command:

```
# cd $NCCM_HOME/scripts/
# ./nccmHTTP.csh enable
# dmctl stop
# dmctl start
```

  To disable port 8080, perform the same operation but use the **disable** argument.

- For Image Management, verify that the gateway has sufficient space for the storing and staging directories (see Reference: Image Management Global Settings, page 3-16).
- For file transfers using TFTP, verify that the TFTP directory is set up and available in the Prime Network gateway and/or unit. To modify and verify the TFTP directory, log in as *network-user* and run the following commands from *NETWORKHOME* (the Prime Network installation directory, which is export/home/*network-user* by default). In the following, *IP-address* is the IP address of the unit or gateway.

– To check the TFTP directory:

```
./runRegTool.sh -gs 127.0.0.1 get IP-address avm83/services/tftp/read-dir

./runRegTool.sh -gs 127.0.0.1 get IP-address avm83/services/tftp/write-dir
```

– To change the TFTP directory (optional):

```
./runRegTool.sh -gs 127.0.0.1 set IP-address avm83/services/tftp/read-dir
tftp-dir-name

./runRegTool.sh -gs 127.0.0.1 set IP-address avm83/services/tftp/write-dir
tftp-dir-name
```

Supported TFTP Directory Name Format

The TFTP directory name (*tftp-dir-name*) must be a single word and should not include any absolute path from the root directory.

The following example represents the supported TFTP directory formats:

```
./runRegTool.sh -gs 127.0.0.1 set 10.81.87.25 avm83/services/tftp/write-dir
tftpnew1
./runRegTool.sh -gs 127.0.0.1 set 10.81.87.25 avm83/services/tftp/read-dir
tftpnew1
```

TFTP Directory Name Formats that are not Supported

Follow these restrictions while specifying the TFTP directory name (*tftp-dir-name*) in the registry settings:

Do not use the forward slash (/) at the beginning and the end of the TFTP directory name.

Specify the directory name without using the sub directories.

The following example represents that the sub directories *tftpnew/tftpinner* are used and this naming format is not supported:

```
./runRegTool.sh -gs 127.0.0.1 set 10.81.87.25 avm83/services/tftp/write-dir
tftpnew/tftpinner
./runRegTool.sh -gs 127.0.0.1 set 10.81.87.25 avm83/services/tftp/read-dir
tftpnew/tftpinner
```

Specify the same TFTP directory name in the registry settings for both the read directory *avm83/services/tftp/write-dir* and write directory *avm83/services/tftp/read-dir*:

The following example represents that the TFTP directory name *tftpnew1* is used for both the read and the write directories:

```
./runRegTool.sh -gs 127.0.0.1 set 10.81.87.25 avm83/services/tftp/write-dir
tftpnew1
./runRegTool.sh -gs 127.0.0.1 set 10.81.87.25 avm83/services/tftp/read-dir
tftpnew1
```

– Restart AVM 83:

```
networkctl -avm 83 restart
```

Note Do not block the port number 1069. Prime Network uses this port to listen the TFTP traffic flow.

- If the *gateway* is behind a firewall, you must open special ports for CCM. This is not required for units that are located behind firewalls and use Network Address Translation (NAT) because the unit will not require a publicly-available IP address in order for the gateway to contact it.

- For IPv6, CCM functions run smoothly when the network and devices have IPv6 addresses.
- Prime Network's information must be consistent with the device configuration.
  - The SCP port configured on the device VNE (Prime Network's model of the device) must match the SCP port used by the device. If a device is not using the default SCP port, the VNE must also be configured with the non-default port. VNE properties are controlled from the Administration client. See the *Cisco Prime Network 5.3 Administration Guide* for more information.
  - The SNMP read-write community configured on the device VNE must match the read-write community configured on the device.
- You can configure timeout for the Command-line interface used for Image distribution jobs. In Prime Network Administration, click **Tools** > **Registry Controller** > **Image Management Settings** > **Image Distribution** to configure timeout for image distribution. The default timeout value is 5400000 ms. You can enter a timeout value between 3600000 ms and 7200000 ms.

Checking Prime Network Global Settings for CCM Operations

The following default CCM behavior is controlled from the Administration client.

- The CCM actions that you can perform, and the devices you can view and manage. When a user account is created the administrator assigns a user access level to the user account.
  - The user access level controls what actions the user can perform using CCM.
  - The device scope determines which devices a user has permission to access, and what the user is allowed to do on those devices.

  For a matrix of actions users can perform depending on their user access level and device scope assignments, see Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1.
- Whether users have permission to run CCM jobs. If global per-user authorization is enabled, a user can only run CCM jobs if they have been granted this permission in their user account settings. Global per-user authorization is disabled by default.
- Whether users are required to enter their credentials when they run CCM operations. This is disabled by default.

Note If Prime Network is being used with Prime Central, both, job authorization and credential requirements are enabled.

Users with Administrator privileges can change these settings. They can also configure Prime Network to generate a warning message whenever a user executes a command script. For more information, see the *Cisco Prime Network 5.3 Administrator Guide*.

Setting Up Devices to Work With CCM

Check these device settings to ensure your devices can communicate with Prime Network:

- Verify that the device is supported. See *Cisco Prime Network 5.3 Supported Cisco VNEs*.
- Make sure you have performed all of the CCM-specific device configuration prerequisites for adding VNEs. These commands are described in the *Cisco Prime Network 5.3 Administrator Guide*. For device configuration files, verify that devices are configured to forward configuration change

notifications to Prime Network. If you will be using event-triggered archiving, make sure the **logging *gateway-IP*** command is configured on all devices. For CPT devices, the TL1 protocol must be enabled in the VNE Properties, and the default TL1 port is 3082.

- The SNMP read-write community configured on the device must match the SNMP read-write community on the device VNE.
- Verify the reachability between devices and their hosting units.
- Verify the FTP settings. CCM supports FTP for all file and image transfers. Although you can configure a username and password on the device using the **ip ftp** command, this may not be safe if the network is not secure. Before using FTP, do the following:
  - Configure the network device to add the Prime Network *unit user* credentials of the unit that manages the device. (You do not need to add Prime Network *unit server super-user* credentials of the to the device configuration.)
  - Restrict the FTP configuration such that the Prime Network *unit user* has read-write access only to the *NETWORKHOME*/tftp directory and therefore does not have access to unwanted files outside the home directory.
- For IPv6, CCM functions run smoothly when the network and devices have IPv6 addresses.

Setting Up Configuration Management

These topics provide information on how to set up the Configuration Management feature:

- Steps for Setting Up Configuration Management, page 3-5
- Reference: Global Settings for Configuration Management, page 3-7
- Notes on Exclude Commands, page 3-15

Note CCM does not support the following special characters on its Settings pages:

- For Password fields—>, <, ', /, \, !, :, ;, and "
- For all other fields—`, ~, @, #, $, %, ^, &, *, (,), +, =, |, {, }, [,], ', ?, >, <, /, \, !, :, ;, and "

Steps for Setting Up Configuration Management

Many Configuration Management features are disabled by default so that you do not encounter unexpected processing loads on your server—for example, how often CCM checks devices and backs up their configurations to the archive. The following steps explain what you must do to set up Configuration Management. All of these items are configured from the Configuration Management Settings page (**Configurations > Settings**). Many of these settings can be overridden when you create specific jobs.

1. Configure the transport protocol that Prime Network will use between the device and the gateway. These are controlled from the Transport Protocol area. The options are TFTP, SFTP/SCP, and FTP (TFTP is the default). To use FTP as the transfer protocol, you must install FTP on the gateway and the unit servers that manage the VNEs. Note the following:

   Note FTP is not a secure mode of transfer. Use SCP/SFTP instead, for secure config and image transfers.

- The TFTP source interface on the devices must be able to reach the unit. Otherwise, the configuration management jobs that require TFTP may fail.
- To use SFTP/SCP for configuration file transfers from a device to a unit, ensure that an SSH server is configured and running on the device (so that during the transfer, the device acts as a server and the unit as a client).
- For Cisco IOS, Cisco IOS XR, and Cisco IOS-XE devices, configure the device with K9-security-enabled images so that the SSH server is up and running on the device.
- To use SCP as the protocol to retrieve configuration files, execute the following command on the device:

```
# ip scp server enable
```

2. Enable the initial synchronization of the archive files with the configurations that are running on the network devices. Whenever the gateway is restarted, CCM will perform this synchronization. By default, synchronization is disabled. To enable it, activate **Enable Initial Config Syncup**.
3. Configure the policies that control how often CCM retrieves information from devices and copies (backs up) configuration files to the archive. By default, all of these settings are disabled. Consider these questions when configuring your settings:
   a. How much disk space is available? Smaller space may require more frequent purging.
   b. Should new configuration files be copied (backed up) to the archive on a periodic basis or on an event-driven basis?

      If configurations are changing frequently and the changes are not of immediate importance, use periodic backups by selecting **Enable Period Config Backup**. This will minimize server workload.

      Note The periodic setting is recommended.

      If every change is considered significant, use event-driven backups (**Enable Event-Triggered Config Archive**).
   c. For event-driven archiving, should information be copied to the archive immediately upon receiving a change (**Sync archive on each configuration change**)? Or should changes be queued and then copied at a certain interval (**Sync archives with changed configurations every ___ hours and ___ minutes**)? If information needs to be copied to the archive immediately, synchronize the archive on each configuration change. Otherwise, you can synchronize the archive at regular intervals (every 1-24 hours).

   While scheduling automatic backup operations, you might be prompted to enter your device access credentials. The device credentials are taken from the Configuration Settings. (See Setting Up Prime Network to Work With CCM, page 3-2.).

   In Prime Network 5.3, as part of Prime Network CCM configurations, to prevent a backup failure you can permit backup configuration operations as a text format commit label in IOS XR devices instead of auto generated numeric value commit label.
4. Configure CCM to perform periodic synchronization of out-of-sync devices by selecting **Enable Periodic Sync for Out of Sync Devices (24Hours)**. The configmgmt-synchronize-sysjob system job is scheduled. You can view the scheduled job in the Configuration Management Jobs (**Configurations > Jobs**) page.

5. Configure CCM to export archived configuration to an export server on a periodic basis by selecting **Enable Periodic Config Export** and **Export Settings.** This allows you to free up disk space while keeping a permanent record of historical archives.
6. Configure when files should be purged from the archive using the **Archive Purge Settings**. Consider these questions when configuring the purge settings:
   - How big are the configuration files?
   - How often are changes made to devices?
7. Specify the default mode of restoring configuration files to the devices using **Restore Mode**.
8. Configure the SMTP server and e-mail IDs so that regular configuration management job status e-mails are sent. (You can also specify e-mail settings when you create a job.)
9. Specify the commands that should be excluded when CCM compares device configuration files. A set of common exclude commands is provided by default (for example, ntp-clock-period). These are controlled in the **Exclude Commands** area (see Notes on Exclude Commands, page 3-15).

Note Configuring exclude commands is especially important if you are using event-driven archiving. Doing so avoids unnecessary file backups to the archive.

Reference: Global Settings for Configuration Management

Note In the Configuration Management and Image Management Settings pages, CCM does not support the following special characters:

- For Password fields—>, <, ', /, \, !, :, ;, and "
- For all other fields—`, ~, @, #, $, %, ^, &, *, (,), +, =, |, {, }, [,], ', ?, >, <, /, \, !, :, ;, and "

The following table describes all of the settings in the Configurations global settings page. To open the page, choose **Configurations > Settings**.

The backup settings you enter here do not affect the manual backups you can perform by choosing **Configurations > Backup**. The backups you perform from that page and the backups you configure on this Settings page are completely independent of each other.

Table 3-1 Configuration Archive Global Settings

Field	Description
Export Settings	
Server Name	DNS-resolvable server name. **Note** CCM supports export servers with IPv4 or IPv6 address.
Location	The full pathname of the directory to which Prime Network should copy the file on the server specified in the Server Name field.
Username	The login username that Prime Network should use when connecting to the server specified in the Server Name field.
Password	The login password that Prime Network should use when connecting to the server specified in the Server Name field.

Table 3-1 Configuration Archive Global Settings (continued)

Field	Description
Export Protocol	Default export protocol that Prime Network should use when exporting configuration files to another server. The choices are FTP and SFTP. The default is FTP. You can override this protocol while scheduling an export job, if required.
Archive Purge Settings	
When you set the Archive Purge Settings, the configmgmt-archivepurge-sysjob system job is scheduled. You can view the scheduled job in the Configuration Management Jobs (**Configurations > Jobs**) page.	
Minimum Versions to Retain	Minimum number of versions of each configuration that should be retained in the archive (default is 2).
Maximum Versions to Retain	Maximum number of versions of each configuration that Prime Network should retain (default is 5). The oldest configuration is purged when the maximum number is reached. Configurations marked **do not purge** are not included when calculating this number. The minimum number of versions to be retained is 5. The maximum number of versions that can be retained is 2147483647.
Minimum Age to Purge	Age (in days) at which configurations should be purged (between 5-360).
Configuration Change Purge Settings	
Purge Change Logs after	Age (in days) at which to purge Change Logs. (Change Logs contain configuration change notifications from devices.) The default is 30 days and the range is 5-360. When you set the Configuration Change Purge Settings, the configmgmt-changeadtprg-sysjob system job is scheduled. You can view the scheduled job in the Configuration Management Jobs (**Configurations > Jobs**) page.
Global Settings	
Transport Protocol	Default transport protocol that Prime Network should use when copying configuration files to and from a device. The options are TFTP, SFTP/SCP, and FTP. The default is TFTP. To use FTP as the transfer protocol, you must install FTP on the gateway and the unit servers that manage the VNEs. Note the following: • The TFTP source interface on the devices must be able to reach the unit. Otherwise, the configuration management jobs that require TFTP may fail. • To use SFTP/SCP for config transfers from a device to a unit, you need to ensure that an SSH server is configured and running on the device, such that the device acts as a server and the unit as a client during the transfer. For Cisco IOS, Cisco IOS XR, and Cisco IOS-XE devices, configure the device with K9-security-enabled images so that the SSH server is up and running on the device. For information on the transfer protocol that CCM supports for each device, see the *Cisco Prime Network 5.3 Supported VNEs - Addendum*. For its Supported Protocols see the *Support for Change and Configuration Management in 5.3 tables*.

Table 3-1 Configuration Archive Global Settings (continued)

Field	Description
Enable Periodic Config Backup	Detect ongoing configuration changes by performing a periodic collection of device information. Use this method if configurations change frequently but those changes are *not* important to you. CCM compares the timestamp for the last configuration change on the version in the archive with the timestamp on the newer version. If they are different, CCM backs the new file to the archive immediately. By default, this is not enabled. The start time and repeat interval are configurable (4-100 hours). The default start time is 12:00 AM and the default repeat interval is 72 hours. **Note** This CCM collection is independent of the Prime Network inventory collection. When you enable this option, the Configmgmt-backup-sysjob system job is scheduled. You can view the scheduled job in the Configuration Management Jobs (**Configurations > Jobs**) page.
Enable Periodic Sync for Out of Sync Devices (72 Hours)	(For Cisco IOS only) Enables automatic synchronization of the out-of-sync devices on a periodic basis. Prime Network adds a device to the list of out-of-sync devices whenever the latest version of the startup configuration is not in sync with the latest version of the running configuration file on the device. The start time and repeat interval are configurable (4-100 hours). The default start time is 12:00 AM and the default repeat interval is 72 hours. When you enable this option, the configmgmt-synchronize-sysjob system job is scheduled. You can view the scheduled job in the Configuration Management Jobs (**Configurations > Jobs**) page.

Table 3-1 Configuration Archive Global Settings (continued)

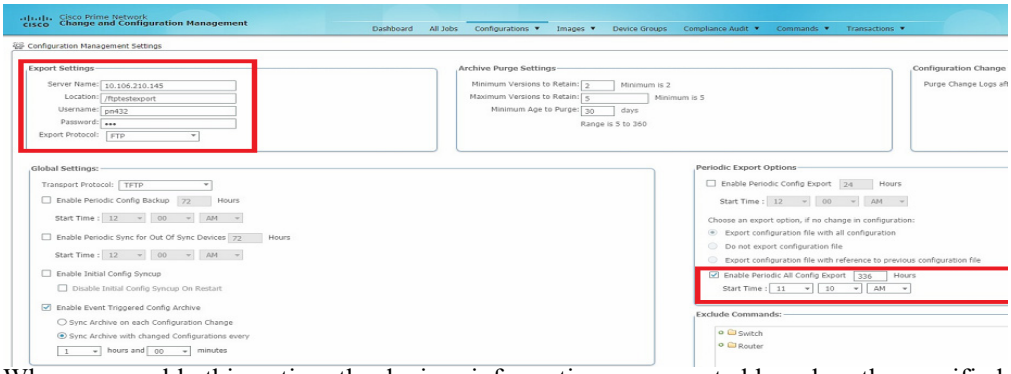
Field	Description
Periodic Export Options	
Enable Periodic Config Export	Allows CCM to periodically export configurations from the archive to the export server. You can set up an interval in the range of 4-100 hours. The default value for export interval is 24 hours. You can also specify the start time for the periodic export operation. Choose one of the following to specify how the export job should be performed when a copy of an archived configuration already exists on the export server: • Export configuration file with all configurations—Overwrite the existing configuration on the export server. • Do not export configuration file—Do nothing. • Export configuration file with reference to previous configuration file— Create a new file that only contains a reference to the previous file. Refer to Copying the Device Files to the Archive (Backups), page 9-42, to learn more about the type of configuration files exported for different devices. When you enable this option, the configmgmt-export-sysjob system job is scheduled. You can view the scheduled job in the Configuration Management Jobs (**Configurations > Jobs**) page. • Enable Periodic All Config Export — Check the **Enable Periodic All Config Export** check box to: – Specify the Start and End time to 4hrs and 336 hours (2 weeks time) for creating or exporting all configuration data, irrespective of the last modification on the Archive whenever the Job is run. – Set the start time to export the configured data of the new system job. *Figure 3-1 Enable Periodic Options*  When you enable this option, the devices information are exported based on the specified interval, irrespective of the last modification on the Archive. You can view the newly created “configmagmt-exportall- system job” in the Configuration Management Jobs page and the job details by clicking the Lastrun Results link.

Table 3-1 Configuration Archive Global Settings (continued)

Field	Description	
Enable Initial Config Syncup	Allows CCM to fetch the configuration files from the network devices and archive it whenever a new device is added to Prime Network. This populates the Configuration Sync Status dashlet on the dashboard. If this setting is enabled, CCM will *not* perform a syncup when the gateway is restarted (to protect performance), and the Disable Initial Config Syncup on Restart is checked by default. If you *do* want CCM to fetch the configuration files when the gateway restarts, uncheck the Disable Initial Config Syncup on Restart check box. **Note** The "sync up" described here pertains to making sure the archive correctly reflects the network device configurations. This is different from the Synchronize operation, where devices are checked to make sure their running and startup configurations are the same.	
	Disable Initial Config Syncup on Restart	Do not fetch configuration files when the gateway restarts.

Table 3-1 Configuration Archive Global Settings (continued)

Field	Description
Enable Event-Triggered Config Archive	Detect ongoing configuration changes by monitoring device configuration change notifications. This setting also controls whether Prime Network populates the Configuration Changes in the Last Week and the Most Recent Configuration Changes dashlets (on the dashboard). When you enable this option, the configmgmt-chngprdcsync-sys job system job is scheduled. You can view the scheduled job in the Configuration Management Jobs (**Configurations > Jobs**) page. Use this method if you consider every configuration file change to be significant. When a notification is received, CCM backs up the new running configuration file to the archive using one of the following methods: • Sync archive on each configuration change—Upon receiving a change notification from a device, immediately backs up the device configuration file to the archive. For each configuration change, a new archive version is created in the Configuration Archives page (Configurations > Archives) and the archive version ID is updated in the Configuration Change Logs page (Configurations > Change Logs). If the archive version is not created in the Configuration Archives page, the Version column in the Configuration Change Logs page displays “N/A”. • Sync archives with changed configurations every ___ hours and ___ minutes—Upon receiving a change notification from a device, queue the changes and backs up the device configuration files according to the specified schedule. When a change is queued, the configuration change is updated in the Configuration Change Logs page but the Version column displays “N/A”. The backup operation starts to execute and based on the time that the device takes to respond, CCM fetches the running configuration from the device. When the backup operation is successful, a new archive version is created in the Configuration Archives page and the version ID is updated in the Version column in the Configuration Change Logs page. Following are the scenarios when the version ID is not updated in the Configuration Change Logs page: • If you change any configuration using the Exclude Command, CCM ignores the change and will not create any new archive version in the Configuration Archives page. Therefore, version ID is not updated in the Configuration Change Logs page. Make sure you check the Excluded Commands area in the Configuration Management Settings page. • When the backup operation fails and a new archive version is not created in the Configuration Archives page. **Note** Make sure that the configuration change detection schedule does not conflict with purging, since both processes are database-intensive. **Note** If you are using event-triggered archiving, you should also make sure that exclude commands are properly configured. Exclude commands are commands that Prime Network ignores when comparing configurations, and they are controlled from the Settings page. Using this mechanism eliminates unnecessary file backups to the archive. When a configuration change occurs for Cisco ASR 5000, Cisco ASR5500, and Cisco OLT devices, the relevant trap does not include the information about the user who initiated the configuration change. Therefore, the User column in the Configuration Change Logs page displays “N/A”.

Table 3-1 Configuration Archive Global Settings (continued)

Field	Description
	Enabling the Enable Event-Triggered Config Archive will start the CCM TFS registration and disabling this option will stop the CCM TFS registration. If you stop the CCM TFS registration in the Event Notification Services page of Prime Network Administration, when the Enable Event-Triggered Config Archive option is enabled, CCM will not receive any change notifications. Similarly, if you start the CCM TFS registration in the Event Notification Services page of Prime Network Administration, when the Enable Event-Triggered Config Archive option is disabled, the count of notifications will increase in the Event Notification Service page, but CCM will not receive any change notifications. Hence, change logs will not be created.
Device Access Credentials	For enhanced security, and to prevent unauthorized access to devices, you might be asked to enter device credentials. This option is enabled if, from the Administration client, **Global Settings > Security Settings > User Account Settings > Execution of Configuration Operations**, you checked the option **Ask for user credentials when running configuration operations**. By default, the device credentials field is populated with the default VNE credentials. You must change the credentials to the device credentials before you save the settings. System jobs will fail, if the credentials entered are incorrect. If you checked the option **Ask for user credentials when running configuration operations** from the Administration client, and did not change the settings from the Settings page after making the change, all system jobs that are scheduled to run will fail. If the option **Ask for user credentials when running configuration operations** (from the Administration client) is not enabled, the default VNE credentials are used. Also, if device credentials are entered in the Settings page, and the option **Ask for user credentials when running configuration operations** is not enabled from the Prime Network Administration client (the Administration client), the device credentials you have entered in the Settings page are ignored and the default VNE credentials are used.
Restore Mode Settings	
Restore Mode	Mode for restoring configuration files to a device: • Overwrite—Prime Network overwrites the existing configuration on the device with the file you selected from the archive. Check the **Use Merge on Failure** check box to restore configuration files in merge mode, if overwrite mode fails. • Merge—Prime Network merges the existing running or startup configuration on the device with the configuration present in the version you selected from the archive.
E-mail Settings	
SMTP Host	SMTP server to use for sending e-mail notifications on the status of configuration management jobs to users. If an SMTP host is configured in the Image Management Settings page, the same value will be displayed here by default. You can modify it, if required.

Table 3-1 Configuration Archive Global Settings (continued)

Field	Description

From E-mail Id	E-mail address of the user to receive e-mail notifications after the scheduled job is complete. This email ID will be used across all the jobs and across all the users. This field can contain only one e-mail address and is initially populated with the following default value:
	`ChangeAndConfigManagement@<PN-GW-HOSTNAME.DOMAINNAME>`
	Note Any changes made to this field under Configuration Archive Global Settings will also reflect in Image Management Global Settings and vice versa.
	Make sure the /etc/hosts file lists the fully qualified domain name (FQDN). FQDN can be listed before or after hostname.
	For example,
	`172.16.17.127 cvldprimegate1.cscdev.com cvldprimegate1`
	or
	`172.16.17.127 cvldprimegate1`
	`cvldprimegate1.cscdev.com`

To E-mail Id(s)	E-mail addresses of users to send a notification to after a scheduled job is complete. For more than one user, enter a comma-separated list of e-mail IDs. For example: `xyz@cisco.com,abc@cisco.com` The e-mail IDs configured here will appear by default while scheduling all jobs. However, you can add or modify the e-mail IDs then. This field is optional.
SMTP Port	SMTP port ID to connect to the host server. The default port is 25.
Email Option	Send an e-mail notification for Configuration Management jobs: • All—To send a notification e-mail irrespective of the job result. • Failure—To send a notification e-mail only when the job has failed. • No Mail—Do not send a notification e-mail on the job status. The selected option will appear by default while scheduling Configuration Management jobs. However, you can modify the option then.
Exclude Commands	
(Device Selector)	Devices to which the exclude commands should be applied (meaning the exclude commands will not be considered when comparing device configuration files). The current selection is highlighted in green. All exclude commands applied to that selection will be listed below the device selector. See Notes on Exclude Commands, page 3-15.
Category Commands	Comma-separated list of commands to be excluded when comparing device configurations for any devices in this category (for example, all Cisco routers).
Series Commands	Comma-separated list of commands to be excluded when comparing device configurations for any devices in this series (for example, all Cisco 7200 series routers).
Device Commands	Comma-separated list of commands to be excluded when comparing device configurations for any devices of this same device type (for example, all Cisco 7201 routers).

Notes on Exclude Commands

Exclude commands are inherited; in other words, if three exclude commands are specified for Cisco routers, all devices is any of the Cisco router families will exclude those three commands when comparing configuration files.

Caution Exclude commands configured for a device family (such as Cisco 7200 Routers) will be applied to all device types in that family (Cisco 7201, Cisco 7204, Cisco 7204VXR, and so forth).

When you are working in the Exclude Commands page, your current selection will be highlighted in green. All exclude commands applied to that selection will be listed below the device selector. When Prime Network compares the router configuration files, it will exclude all of the commands listed in the Device Commands field. If a series is selected (example, Cisco 7200 Series), the commands listed in the Series Commands field will be excluded and so on.

The following procedure describes how to configure exclude commands.

Step 1 Choose **Configurations > Settings**.

Step 2 In the Exclude Commands area, navigate and choose one of the following (your selection is highlighted in green):

- A device category
- A device series
- A device type

Step 3 Enter a comma-separated list of commands you want to exclude when comparing configuration files for that device category, series, or type. You can also edit an existing list of commands.

Your entries change to red until they are saved, and all affected device types, series, or categories are indicated in bold font.

Step 4 If you want a device type to ignore the parent commands (that is, the series and category commands), check the **Ignore Above** check box.

Step 5 Click **Save** to save your changes.

Setting Up Image Management

These topics provide information on how to set up the Configuration Management feature:

- Steps for Setting Up Image Management, page 3-16
- Reference: Image Management Global Settings, page 3-16

Note In the Configuration Management and Image Management Settings pages, Change and Configuration Management does not support the following special characters:

- For Password fields—>, <, ', /, \, !, :, ;, and "
- For all other fields—`, ~, @, #, $, %, ^, &, *, (,), +, =, |, {, }, [,], ', ?, >, <, /, \, !, :, ;, and "

Caution FTP is not a secure mode of transfer. For secure config and image transfers, use SCP/SFTP.

Steps for Setting Up Image Management

The following prerequisites are controlled by the Image Management Settings page (**Images > Settings**). All of the fields in the settings page are described in xxxx.

Many of these settings can be overridden when you create specific jobs.

1. Configure the transport protocol that Prime Network will use between the device and the gateway/unit that manages the device; these are controlled from the **Transport Protocol** area. The options are TFTP, SFTP/SCP, and FTP. The default is TFTP. Note the following:
   - The TFTP source interface on the devices must be able to reach the unit. Otherwise, the configuration management jobs that require TFTP may fail.
   - To use SFTP/SCP for image file transfers from a device to a unit, ensure that an SSH server is configured and running on the device (so that during the transfer, the device acts as a server and the unit as a client). For Cisco IOS, Cisco IOS XR, and Cisco IOS-XE devices, configure the device with K9-security-enabled images so that the SSH server is up and running on the device.
2. Configure the gateway *staging* directory to use when transferring images from Prime Network out to devices in the **File Locations** area. The default is *NETWORKHOME*/NCCMComponents/NEIM/staging/.
3. Configure the gateway *storing* directory to use when transferring images from an outside source into the image repository (from Cisco.com or from another file system). This is controlled from the **File Locations** area. The default is *NETWORKHOME*/NCCMComponents/NEIM/images/.
4. In case of insufficient memory, use the **Clear Flash** option (under **Flash Properties**). This deletes any one file (other than the running image) and recovers the disk space occupied by the file. This procedure is repeated until adequate space is available in the selected flash.
5. Enable the warm upgrade facility to reduce the downtime of a device during planned Cisco IOS software upgrades or downgrades (in the **Warm Upgrade** area).
6. Configure the SMTP server and e-mail IDs so that regular software image management job status e-mails are sent. (You can also specify e-mail settings when you create a job.) This is controlled in the **E-Mail Settings** area.
7. If you plan to download files from Cisco.com, configure the necessary vendor credentials to connect to Cisco.com. These are set in the **Vendor Credentials** area. If you do not have login privileges, follow the procedure in Reference: Image Management Global Settings, page 3-16.
8. Configure the proxy server details to use while importing images to the repository from Cisco.com (in the **Proxy Settings** field).
9. If you plan to download images from an external repository, set up the details of the external server to import images to the Prime Network image repository (in the **External Server Details** area).

Reference: Image Management Global Settings

Note In the Configuration Management and Image Management Settings pages, CCM does not support the following special characters:

- For Password fields—>, <, ', /, \, !, :, ;, and "

- For all other fields—`, ~, @, #, $, %, ^, &, *, (,), +, =, |, {, }, [,], ', ?, >, <, /, \, !, :, ;, and "

The following table describes all of the settings in the Image Management global settings page. To open the page, choose **Images > Settings**.

Table 3-2 Image Management Global Settings

Field	Description	
Transfer Protocol	Default transfer protocol to use when copying images to and from a device. This setting can be overridden when creating a distribution job (for example, if you know that a device does not support the default protocol), FTP and TFTP are unsecured. The TFTP source interface on the devices must be able to reach the unit. Otherwise, the image management jobs that require TFTP may fail. To use SFTP/SCP for image transfers from a device to a unit, you need to ensure that an SSH server is configured and running on the device, such that the device acts as a server and the unit as a client during the transfer. For Cisco IOS, Cisco IOS XR, and Cisco IOS-XE devices, configure the device with K9-security-enabled images so that the SSH server is up and running on the device.	
Flash Properties	In case of insufficient memory, use the **Clear Flash** option (under **Flash Properties**). This deletes any one file (other than the running image) and recovers the disk space occupied by the file. This procedure is repeated until adequate space is available in the selected flash.	
Warm Upgrade	If checked, a Cisco IOS image can read in and decompress another Cisco IOS image and transfer control to this new image. This functionality reduces the downtime of a device during planned Cisco IOS software upgrades or downgrades. This can be overridden when creating the job. **Note** You can perform a warm upgrade only on Cisco IOS devices 12.3(2)T or later, such as 12.4T, 15.0, 15.1T, and for ISR 800/1800/2800/3800 series and 1900/2900/3900 series.	
File Locations	Full pathname of directories where images are stored when they are being imported into the Prime Network image repository, or when they are being transferred out of the repository to devices. New directories must be empty and have the proper permissions (read, write, and execute permissions for users). The entries must be full pathnames. In the following default locations, *NETWORKHOME* is the Prime Network installation directory.	
	Staging Directory	Location where images from the Prime Network image repository are placed before transferring them out to devices. The default is *NETWORKHOME*/NCCMComponents/NEIM/staging/.
	Storing Directory	Location where images from an outside source are placed before importing them into the Prime Network image repository (from Cisco.com, from existing devices, or from file system). The default is *NETWORKHOME*/NCCMComponents/NEIM/images/.

Table 3-2 Image Management Global Settings (continued)

Field	Description	
External Server Details	Details about external server from which images can be imported into repository.	
	Server Name	IP address of the external server (IPv4 or IPv6 addresses supported).
	Image Location	Path where the image is located on the server.
	User Name	Username to access the external server. **Note** Username is not displayed for Cisco OLT devices.
	Password	Password to access the external server.
	SSH Port	SSH port ID to connect to the server.

Table 3-2 Image Management Global Settings (continued)

Field	Description	
E-mail Settings	Settings for automatic e-mail notifications about the status of jobs.	
	SMTP Host	SMTP server to use for sending e-mail notifications on the status of image management jobs to users. If an SMTP host is configured in the Configuration Management Settings page, the same value will be displayed here by default. You can modify it, if required.

	From E-mail Id	E-mail address of the user to receive e-mail notifications after the scheduled job is complete. This email ID will be used across all the jobs and across all the users. This field can contain only one e-mail address and is initially populated with the following default value:
		`ChangeAndConfigManagement@<PN-GW-HOSTNAME.DOMAINNAME>`
		Note Any changes made to this field under Image Global Settings will also reflect in Configuration Archive Management Global Settings and vice versa.
		Make sure the /etc/hosts file lists the fully qualified domain name (FQDN). FQDN can be listed before or after hostname.
		For example,
		`172.16.17.127 cvldprimegate1.cscdev.com cvldprimegate1`
		or
		`172.16.17.127 cvldprimegate1 cvldprimegate1.cscdev.com`

	To E-mail Id(s)	E-mail addresses of users to send a notification to after a scheduled job is complete. For more than one user, enter a comma-separated list of e-mail IDs. For example: `xyz@cisco.com,abc@cisco.com` The e-mail IDs configured here will appear by default while scheduling all jobs. However, you can add or modify the e-mail IDs then. This field is optional.
	SMTP Port	SMTP port ID to connect to the host server. The default port is 25.
	Email Option	Controls when e-mail notifications for Imange Management jobs are sent (can be overridden when creating the job): • All—Send a notification irrespective of the job result. • Failure—Send a notification e-mail only when the job has failed. • No Mail—Do not send a notification e-mail on the job status.
Proxy Settings	Details about proxy server to use when importing images from Cisco.com	
	HTTP Proxy	HTTP proxy server to use for downloading images from Cisco.com.
	Port	Port address to use for downloading images from Cisco.com.

Table 3-2 Image Management Global Settings (continued)

Field	Description
Vendor Credentials	Usernames and passwords that can be used to download images from Cisco.com. (See the procedure described in Reference: Image Management Global Settings, page 3-16.)

Obtaining Cisco.com Login Privileges for Image Management

Login privileges are required for all images operations that access Cisco.com. To get access, you must have a Cisco.com account. If you do not have a user account and password on Cisco.com, contact your channel partner or enter a request on the main Cisco website.

You can register by going to the following URL:

http://tools.cisco.com/RPF/register/register.do

To download cryptographic images from Cisco.com, you must have a Cisco.com account with cryptographic access.

To obtain the eligibility for downloading strong encryption software images:

Step 1 Go to the following URL:

http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y&return_url=http://www.cisco.com

Step 2 Enter your Cisco.com username and password, and click **Log In**.

Step 3 Follow the instructions provided on the page and update the user details.

Step 4 Click **Accept** to submit the form.

Step 5 To verify whether you have obtained the eligibility to download encrypted software:

a. Go to the following URL:

http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y&return_url=http://www.cisco.com

b. Enter your username and password, and click **Log In**.

The following confirmation message is displayed:

```
You have been registered for download of Encrypted Software.
```

Setting Up CCM Device Groups

User-defined device groups allow you to apply changes to devices in bulk. You can choose specific devices as you perform CCM operations, but having predefined device groups can save you time. There are two types of device groups:

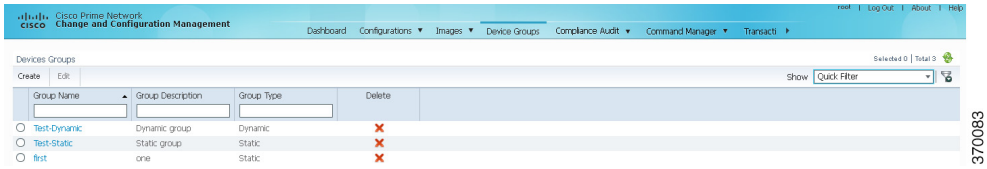
Group Type	Description
Static	Devices are never automatically added to these groups; new devices must be added manually.
Dynamic	Devices are automatically added to a group if they match membership rules.

If a device group's members changes during a CCM operation, the CCM operation is applied to the devices that belong to the group *at the time of execution*.

To view the existing device groups and create new user-defined device groups:

Step 1 Click the **Device Groups** tab. The Device Groups page appears as shown in Figure 3-2.

Figure 3-2 Device Groups Page



The Device Groups page displays the name, description, and whether the membership is static or dynamic. To delete a group, click the red X next to the group name.

To view the devices in a group, click the hyperlinked group name. The Group Members page displays the device status, IP address, and element type. To display additional device properties, click the Device Name hyperlink. The status icons are illustrated in the following.

Symbol	Description
	Device is in operational state.
	Device is not in operational state (the device is most likely in the Maintenance or Unreachable state). Click the device hyperlink and open the device properties popup to see details about the device.

Step 2 To create a new group, click **Create** and enter the required information. Names must be unique. Do not use the reserved names **adminGroup** and **ROOT-DOMAIN.**

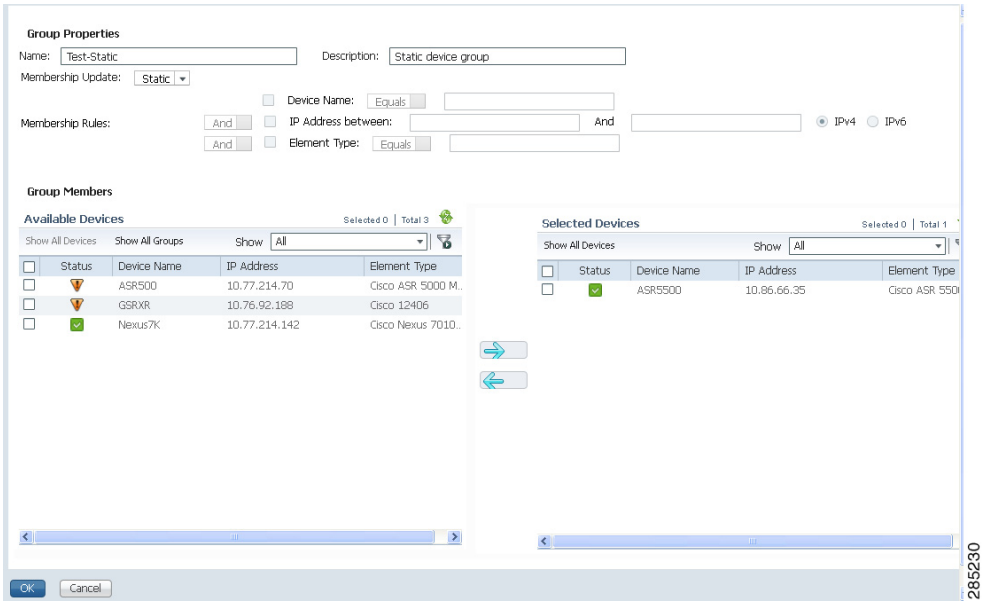
Step 3 In the Membership Update drop-down list box, choose Static or Dynamic.

- Dynamic device group—If you choose Dyamic, set up a membership rule to control which devices are added to the group. You can use rules with parameters such as device name, range of device IP addresses, and device element type. For example:

```
Device Name    equals    1800
IP Address between    10.77.214.107    And    10.77.214.171    IPv4
Element Type    equals    Cisco 1801
```

Note You can choose a combination of parameters by using the And/Or operator. You can also use a comma-separated list to provide multiple values for the Device Name and Element Type parameters.

- Static device group—If you choose static, select the devices from the Group Members list.



Step 4 Click **OK** to save the group.

Setting Up Image Distribution Servers

Cisco Prime Network provides solution for distributing software images in a network based on the network architecture that contains CCM GUI, gateways, units, and direct network elements with distribution servers placed between the units and network elements. Using the distribution servers for storing software images facilitates efficient bandwidth utilization within a network. The distribution server works with the secure protocol, for example, SCP or SFTP.

In the distribution server, you can copy the software image to the network element.

Note Using Distribution servers you can perform only the Distribution operation. Install Add operation must be performed as a separate operation.

Prerequisites for Using Distribution Server

- Distribution server is a Linux server with minimal installation of RHEL with expect, PERL, and OpenSSL packages (to provide SSH, SCP, SFTP, and rsync functionalities). The Prime Network software must not be installed on it.
- Distribution server should be ready with a user account created to be used as a part of this solution.
- Distribution server credential configuration file should be created, at the time of solution installation, using a script provided as a part of the solution.
- Location of the directory where the images are stored on the distribution server should be identified and added to the mapping file.

- Initial configuration of tool or solution after installation includes executing the script to fetch distribution server username, SSH keys of the unit, and creating or saving it to a configuration file. You can test connectivity to distribution server at this time using a utility which is a part of the solution.

Required Settings for Using Distribution Server

- VNE device to distribution servers mapping in Units—External file, for example file in CSV format must be available in the units. The CSV file contains information that describes about the mapping between the VNE devices and corresponding distribution servers, for example, distro_scp.csv and distro_sftp.csv. This file is maintained as a part of the new device add process to ensure that it is in sync with the Prime Network inventory.
- Certified Software Image on the Gateway—A certified image is made available in a predefined directory on the gateway. The image is imported into the Prime Network repository. Then, the image is copied to the distribution servers using rsync mechanism.
- SSH connection between unit and distribution server—Login as a Prime Network user and execute the following commands to setup SSH keys between the unit server and distribution server:

```
ssh-keygen -t rsa
ssh-copy-id -i /export/home/pn422/.ssh/id_rsa.pub root@10.76.82.171
```

- Execute image distribution configuration script—Execute the image distribution configuration script (imagedistributionconfig.pl) on units to provide the distribution server access credentials username and SSH keys. After which, a configuration file (.distroCreds.conf) is created.
- Copy the software image to the distribution server—Copy the image to be copied to the distribution server and configure the image directory and distribution mappings in the CSV file on unit.
- Copy the Bulkstat file along with the images to StarOS devices during distribution operation.
- Test the connectivity to distribution server—Execute the script (testDistroSSHaccess.pl) to test the connectivity. The script is available in the following location: $ANAHOME/Main/scripts/configuration/cisco/NEIM.

Note The required PERL modules should be installed.

- You can use distribution server in the IPv4 environment only.

Setting Up Distribution Servers

To set up distribution servers:

Step 1 Choose **Tools** > **Registry Controller** > **Image Management Settings** > **Image Distribution**.

Step 2 In the **Image Distribution** window, select the **True** option to use distribution server.

Note You can also copy the software image without using the distribution server. Choose the **False** option in the **Image Distribution** window. The **False** option is the default value in the **Image Distribution** window.

Enabling SSH Resync on VNE and CCM

SSH key is the common way to securely connect to remote machines. It is used to identify trusted computers, without using passwords. SSH enables connecting to a virtual private server in a highly secured manner than using a password.

In Cisco Prime Network, the SSH key synchronization is created to handle device disconnections due to SSH key mismatch. Prime network uses SSH keys to communicate with the devices.

Synchronization of SSH Key with VNE

Based on user configuration, when the device reboots, a new SSH key is generated to serve the internal security purposes. Prime Network tries to connect to a device with the key which was used at the first communication. In case of any key mismatch, the VNE synchronizes with the device automatically, fetches the new SSH key from the device, updates in Prime Network, and re-connects to the device using the updated key. The new SSH key synchronization happens only if the server authentication is enabled as 'save-first-auth' and automatic key synchronization feature is enabled via the registry controller.

Synchronization of SSH Key in CCM

When communicating with the device, Cisco Prime Network CCM operations use the SSH keys that are stored in the **known_hosts** file. This file is available in the ***<Prime Network HOME>/.ssh/known_hosts*** directory. If there is a mismatch in the SSH key and if the automatic key synchronization feature is enabled, then the Cisco Prime Network CCM script synchronizes with the device automatically. After which, the CCM script connects without server-side authentication, learns the new SSH keys, and updates the new keys in the **known_hosts** file for further communication. If there is a mismatch, then the automatic key synchronization feature should be enabled to synchronize with the SSH keys.

Common Settings for Key Resync for SSH-VNE and CCM

Follow the prerequisites to enable key resync for SSH VNE and CCM:

- Enabling Server Authentication Settings, page 3-24
- Enabling SSH key synchronization, page 3-25

Enabling Server Authentication Settings

To enable SSH settings, follow the steps provided below:

Step 1 Log on to the **Administration** client.

Step 2 Click **New** to open the **New VNE** window.

Step 3 Click the **Telnet/SSH** tab and check the **Enable** check box.

In the **Telnet/SSH** window, once the **Enable** option is checked, the other options such as **Protocol**, **Port**, **Prompt**, and **Mask** are also enabled.

Step 4 From the **Protocol** drop-down list, choose the **SSHv2** option to open the **SSHv2** pane.

Step 5 In the **Server Authentication** drop-down list of the **SSHv2** pane, choose **save-first-auth mode**.

The server authentication is set.

Enabling SSH key synchronization

SSH key synchronization is defined in device protocol reachable settings.

To enable the SSH key synchronization, follow the steps provided below:

Step 1 Log on to the **Administration** client.

Step 2 From the **Tools** menu, choose **Registry Controller** to open the **Registry Controller** window.

Step 3 In the **Registry Controller** window, expand the **Device Protocol Reachability** node.

Step 4 Click **Telnet** to open the **Telnet** pane.

Step 5 Choose **True** from the **Enable Re-Sync SSH Keys** drop-down list. The SSH key synchronization is enabled.

By default, the **Enable Re-Sync SSH Keys** option is set to **False**.

Verifying SSH key Resync on VNE

To verify SSH key resync on VNE, follow the steps provided below:

Step 1 Model the VNE using SSHv2. Refer Enabling Server Authentication Settings, page 3-24.

Step 2 Enable resync on the device. Refer Enabling SSH key synchronization, page 3-25.

Step 3 Log into the device, and change the key in the device.

Note For **VNE**, a **DSA key** change is to be performed by using the **crypto key generate dsa** command. Refer the Configuring SSH topic (Steps 5 and 6 under the Detailed Steps section) of the Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide.

Step 4 In the PN Admin/Vision client, right-click the VNE and restart by selecting **Stop VNE** followed by **Start VNE** options to reflect the actual state of the VNE.

To ensure the key resync on VNE

- If the device key is changed and the resync is set to **true**, after restart-In the **VNE status** tab, the **Investigation State** would be **Operational** and the **CLI state** under **Telnet/SSH Connectivity** also would be **Operational**.
- If the key is changed and resync is set to the default value of **false**, after restart-The **VNE status** tab would update the **Investigation State** to **Currently Unsychronized,** and the **Telnet/SSH Connectivity CLI State** to **Down** and **Description** as '**Protocol failed to connect to host**'.

Verifying SSH key Resync on CCM

To verify SSH key resync on CCM, follow the steps provided below:

Step 1 Model the VNE using SSHv2. Refer Enabling Server Authentication Settings, page 3-24.

Step 2 Enable resync on the device. Refer Enabling SSH key synchronization, page 3-25.

Step 3 Login to the device, and change the key in the device.

Note For **CCM**, an **RSA key** change is to be performed using the **crypto key generate rsa** command. On setting the resync value to true, the **RSA key entries** sync with the device and are updated in the **known_host** file so that the CCM operations become successful. On setting the resync value to false, the CCM operations would fail.

Step 4 Login to the CCM Dashboard, navigate to the **CCM** page, and choose any CCM operation such as Backup/Restore.

Step 5 From the VNEs listed, select the required VNE on which the operation needs to be performed.

To ensure the key resync on CCM

- If the resync value is set to false, then any CCM operation performed would fail.
- If the resync value is set to true, then any CCM operation performed would succeed.

Known Limitation for CCM

On performing a **DSA key change**, the **DSA key entries** are not updated in the **known_host** files. However, this does not impact any CCM operation. In other words, irrespective of the resync value (true or false), the CCM operations are always successful.

Setting Up Vision Client Maps

Vision client maps display devices and their physical and logical relationships, including relationships with logical NEs such as services. From a map, users can drill down into both the physical and logical NE details and perform other operations, such as launching command scripts and external applications. These topics explain how to set up maps:

Whether you can perform these setup tasks depends on your account privileges. See Vision Client Permissions, page B-1 for more information.

Workflow for Creating a Map

Use maps to highlight different segments of your environment. For example, you could create one map to display the BGP architecture and relationships between NEs, and another map to display the physical connectivity of the network. You can create maps that cover specific network segments, customer networks, services, or any other mix of network elements required. Network maps provide a graphic display of active faults and alarms and serve as access points for activating services. When you create a map, it is saved in the database and made available to other users if they have sufficient access and security privileges. When you delete a map, it is removed from the database.

You can only perform these tasks if you have the required privileges. See Vision Client Permissions, page B-1.

The following table provides the basic workflow for setting creating maps.

	Description	See:
Step 1	Launch the Vision client and create an empty map using a name that reflects the map purpose, and add elements or services to the map.	Creating a New Map and Add NEs to the Map, page 4-3
Step 2	Apply optional customizations to the map:	
	Group NEs into aggregations, which are displayed as a single entity by default (but can be opened for NE details).	Grouping Network Elements into Aggregations, page 4-7
	Apply a layout or drag NEs to a desired layout	Applying a Layout to a Map, page 4-7
	Label important NEs by creating and applying business tags, allowing users to search for NEs using labels created for your deployment's needs.	Labelling NEs to Associate Them with Customers (Business Tags), page 4-9
	Apply background images to maps.	Applying a Background Image To a Map, page 4-12
Step 3	Create logical links to ensure that correlation flows are not interrupted.	Adding a Static Link When a Network Link is Missing, page 4-13
Step 4	Adjust Vision client settings that affect maps (audio alarms, display defaults, and so forth).	Changing Vision Client Default Settings (Sound, Display, Events Age), page 4-15
Step 5	(Optional) Create ticket (or event) filters and save them so you can use them as needed.	Table 11-2Regular and Resynced Events Processing, page 11-6
Step 6	Check the global settings that can impact map operations (for example, whether users can view maps created by others).	Check Global Settings for Vision Client Maps, page 4-14
Step 7	(Optional) Extend the Vision client to model and display additional NE properties; support new devices, software versions, and modules; display commands that users can launch from an NE's right-click menu; launch external applications; integrate with northbound applications; and many other customizations.	Extending Prime Network Features, page 2-6

After creating a map and adding devices to it, you can view the NE properties as described in Opening Maps, page 7-2.

Creating a New Map and Add NEs to the Map

Naming Your Maps

The name you assign a map is a significant way to organize the NEs in your network. Use these steps when naming maps:

- Give each map a specific function. For example, do not mix network and service elements together in a map.
- Give each map a name that reflects the map function, such as:
  - **Core Devices** for a network map named
  - **MPLS** for a service map named

Step 1 Launch the Vision client.

If You Are Using Prime Network:	Launch the Vision client by choosing:
As part of suite	**Assure > Prime Network > Vision** from the REPLACE main menu bar
As a standalone application	**Start > Programs > Cisco Prime Network > Cisco Prime Network Vision** from your local machine

Step 2 To create a new map, choose **File > New Map** in the Vision client main menu and enter a map name that reflects the map function. To add elements to the map, do one of the following:

For this map function:	Examples	See:
A map of services in the network	Cross connects, Ethernet services, MPLS-TP tunnels, pseudowires, unassociated bridges, VLANs, VPLs, VPNs	Creating a Service Map, page 4-3
A map of the network's physical topology	Core devices with their physical links	Creating a Physical Topology Map, page 4-4
A map of NEs that are connected using a specific type of link	Data links: ATM, Frame Relay Tunneling: GRE, Layer 2 TP, pseudowires, MPLS-TE, GRE Tunnels Protocol architectures: BGP	Creating a Special-Purpose Map, page 4-5

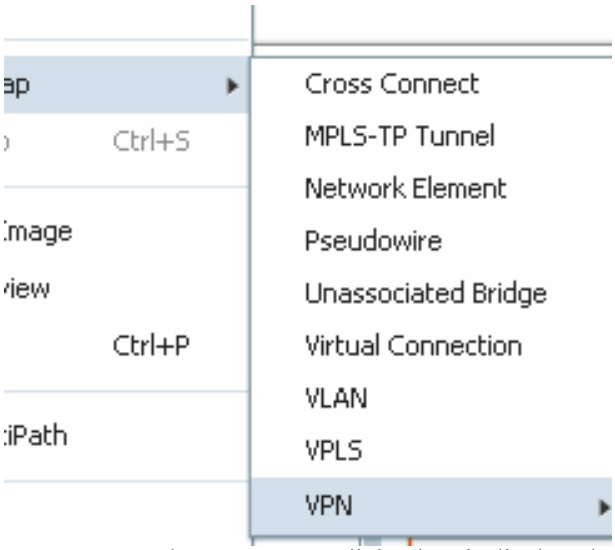
Creating a Service Map

This procedure explains how to locate services in the network so you can add them to a map. When Vision client users open the map, they will only be permitted to view a service if the NE associated with the service is in their device scope.

If you have a very large network, you can alternatively generate a service report by choosing **Reports > Run Report > Network Service Reports** and choosing Ethernet Services, Pseudowire, or VPLs.

Step 1 Choose **File > New Map**, and enter a map name that reflects the service.

Step 2 Click the tab for your new map and choose **File >Add to Map**. The following figure shows the service types you can choose.



If you choose **VPN > New**, the Create VPN dialog box is displayed. For information on creating a VPN, see Creating a VPN, page 17-22.

Step 3 Choose a service (such as **VPLS**) and Prime Network displays all services of that type.

Step 4 If you are working with a very large number of NEs that are affected by the services, click **Search**. The search criteria depends on the entity type. For example, you can search for Ethernet Services by the system name, pseudowires by their role, and so forth.

Step 5 Choose the services and click **OK**.

Creating a Physical Topology Map

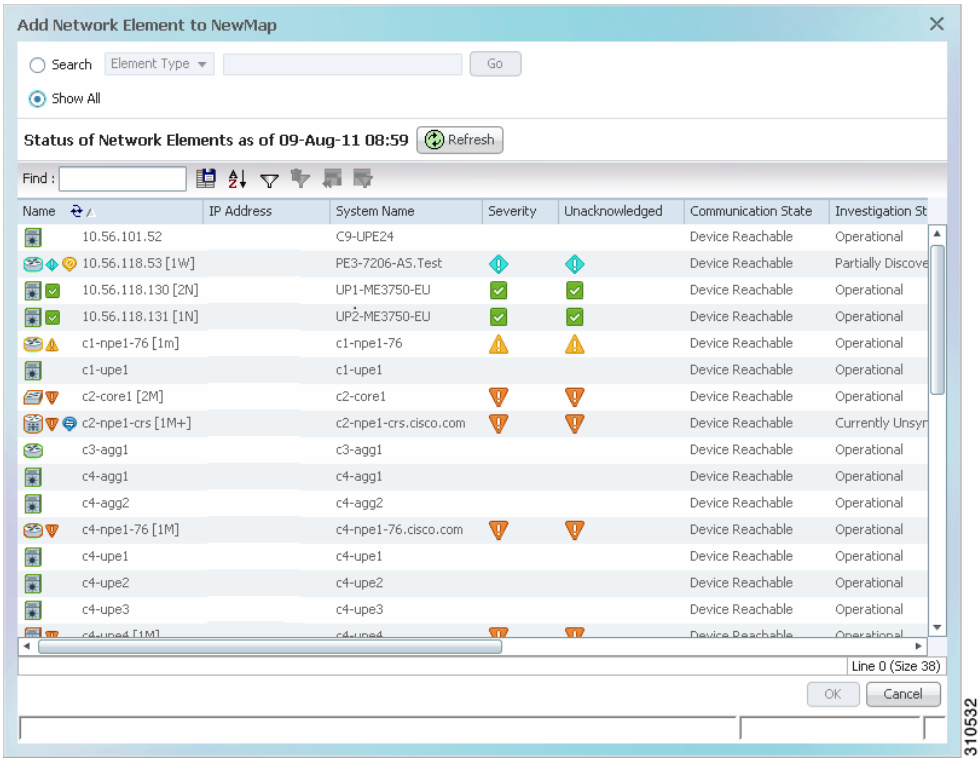
This procedure explains how to locate physical NEs in the network so you can add them to a map. When a Vision client user opens the map, they will be able to see the map devices, but devices outside their device scope will be displayed with a lock icon.

If you have a very large network, you can alternatively generate a service report by choosing **Reports > Run Report > Inventory Reports** and choosing a hardware report.

Step 1 Choose **File > New Map**, and enter a map name that reflects the map purpose (such as **Core Devices**).

Step 2 Choose **File >Add to Map > Network Elements**.

Step 3 Click **Search** to find NEs by their vendor, element type, IP address, and so forth; or click **Show All** to list all NEs. A locked device icon means the device is not in your scope. For example, to find all Cisco 7600 series routers, click the Filter button, choose Element Type as your filter criteria, and enter **76** in the text box.



Step 4 Choose the NEs and click **OK**.

Creating a Special-Purpose Map

You can create a special-purpose map by selecting specific link types for your map, such as a map that shows all the BGP links in the network.

Tip Do not mix logical and physical links into one map because they can be displayed the same way. Link types can only be ascertained by hovering the mouse over the link.

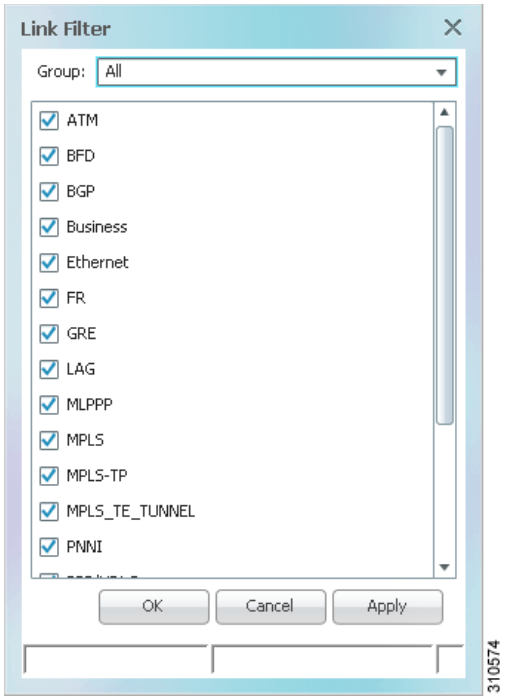
By default, Vision client users will only be able to view links if both link endpoints are in their device scope. (This can be changed using the Registry Controller; see the *Cisco Prime Network 5.3 Administrator Guide*.)

Keep in mind that this procedure effectively filters in or filters out certain link types. If subsequent users want to filter the map, the links offered for filtering are limited to what you specify in this procedure.

Step 1 Choose **File > New Map**, and enter a map name

Step 2 In the Create Map dialog box, and click **Advanced**. The Link Filter dialog displays link types, as shown in Figure 4-1.

Figure 4-1 Link Filter Dialog



These are some examples of what you can create using the various link types:

- Process map with all BFD links
- Traffic map with all Frame Relay links
- Tunnel map with all GRE tunnels

The link type also determines the algorithm Prime Network will use for the may layouts (symmetrical, orthogonal, and so forth).

Step 3 Check the link type you want to include in your map and click **Apply** to apply the defined link filter settings and continue with more selections.

Step 4 Click **OK** when you have completed your selections.

Step 5 In the Create Map dialog box, enter a name for the new map and click **OK**. An empty new map is displayed in the navigation pane and content area, and the map toolbar displays the Link Filter Applied button, which indicates that a link filter is currently applied to the map.

	Indicates a link filter is currently applied to the map. If you want to clear the filter, click this icon and choose **None** from the Group drop-down list.

Step 6 Add the required elements to the map by choosing Choose **File >Add to Map**.

Grouping Network Elements into Aggregations

An aggregation is a group of NEs. You specify the NEs to add to the group, and then name the aggregation as needed. These are some examples of ways to use aggregations:

- Group NEs that are in a logical segment of the network
- Group NEs located in a geographical fragment of the network.
- Group NEs that have the same device type or role

Note You cannot aggregate service entities that exist within a service. For example, you cannot aggregate VRFs that exist within a VLAN.

To aggregate network elements, follow this procedure. The aggregation name can include Chinese characters.

Step 1 Select multiple NEs by pressing **Ctrl**.

Step 2 Aggregate the network elements by choosing **Node > Aggregate**.

Step 3 In the Aggregation dialog box, enter a unique name for the aggregation and click **OK**. The aggregation is displayed in the navigation pane and the map pane. The aggregation icon changes color according to the alarm severity. For more information about severity colors, see Severity Icons and Colors for Events, Tickets, and NEs, page A-15.

Applying a Layout to a Map

The Vision client provides four standard layouts that you can apply to your map. The layout determines how the topology should be displayed: Circular, hierarchical, orthogonal, or symmetric. By default, maps use a circular topology. To select a layout, choose **View > Layout** from the main menu. You can also move individual NEs as desired. When you have finished, choose **File > Save Map**.

The following screen shots provide examples of the same map using the different layouts.

Figure 4-2 Hierarchical Map Layout

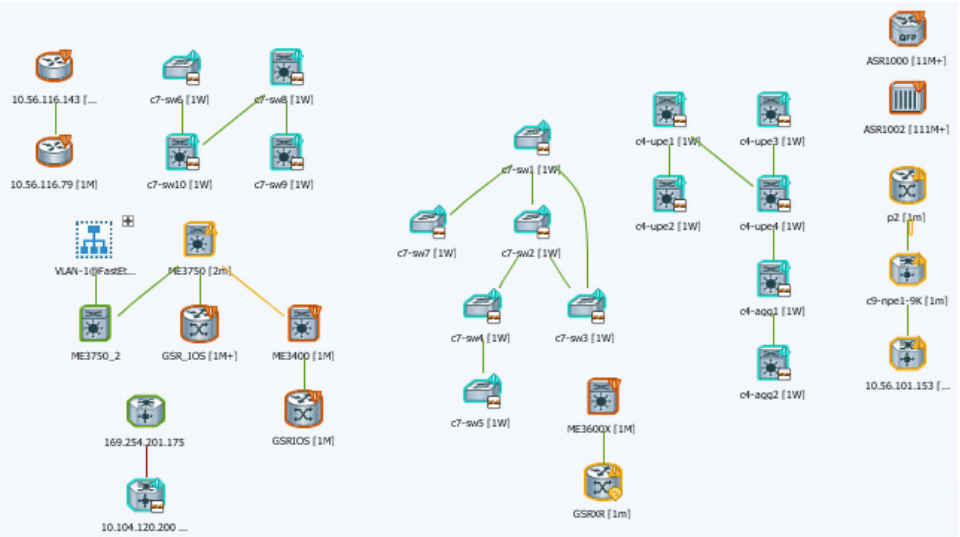


Figure 4-3 Circular Map Layout (The Default Layout)

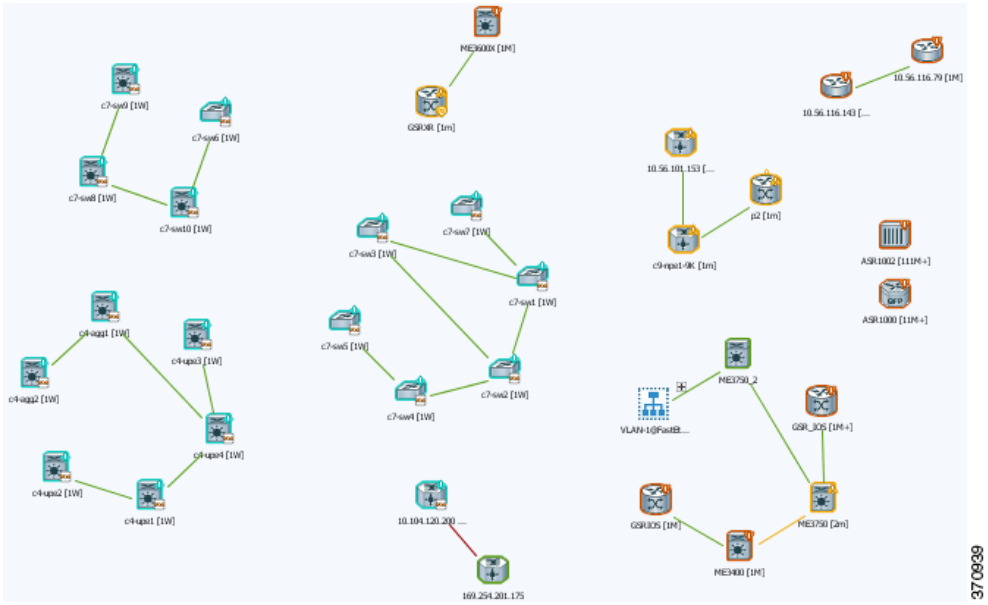


Figure 4-4 Orthogonal Map Layout

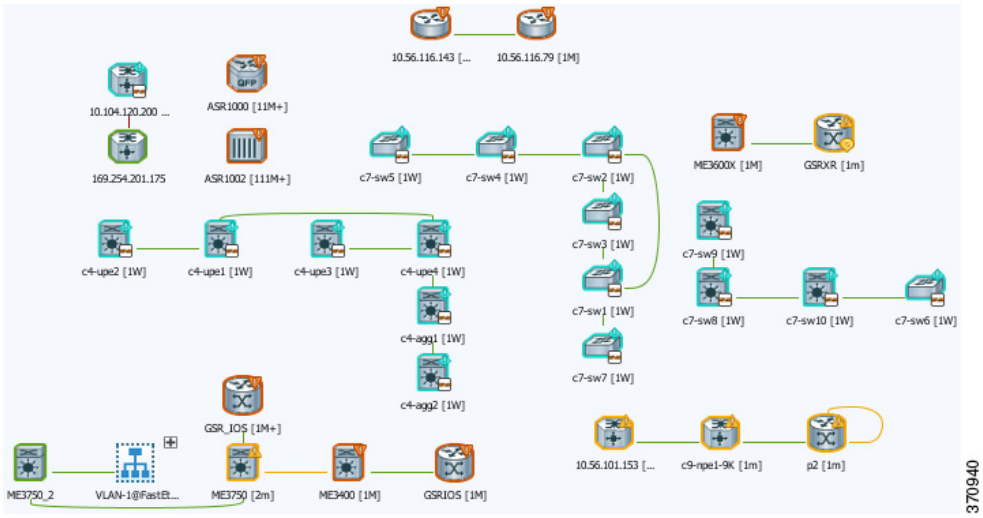
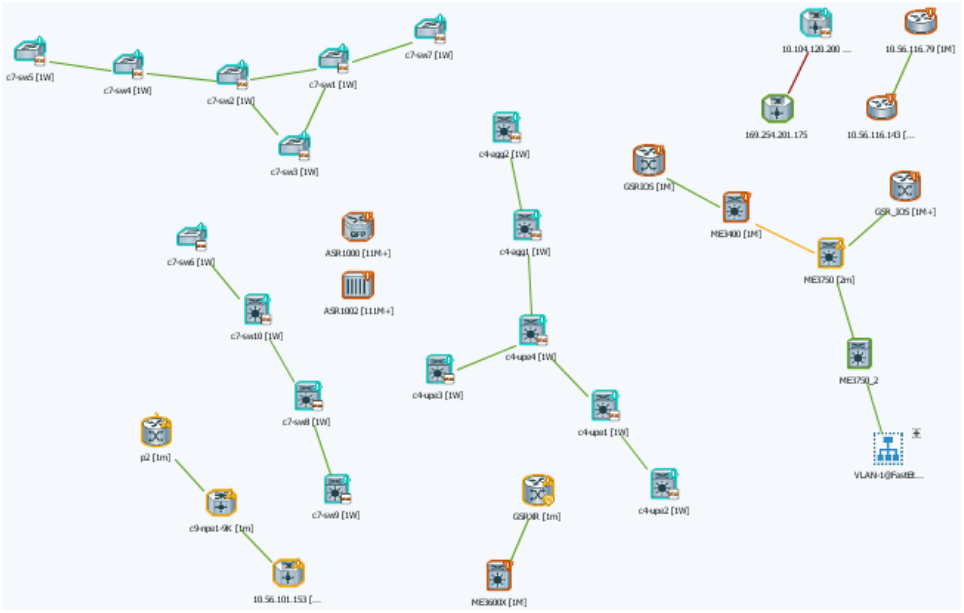


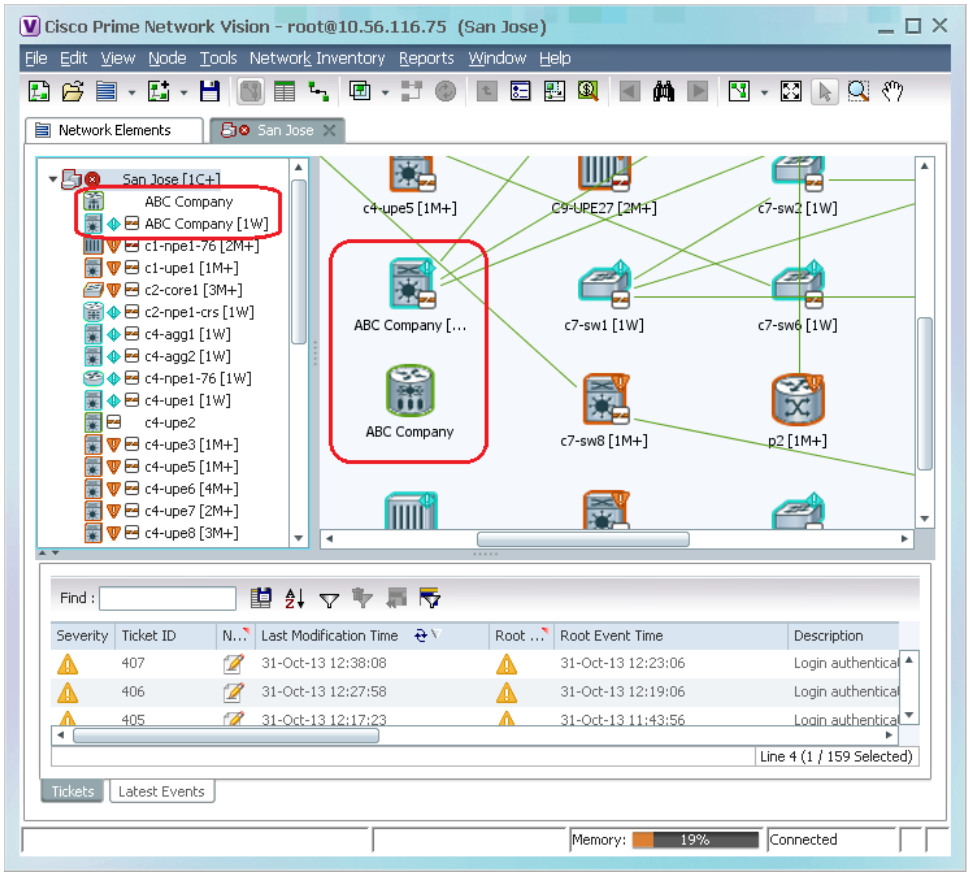
Figure 4-5 Symmetrical Map Layout



Labelling NEs to Associate Them with Customers (Business Tags)

A *business tag* is a string that is meaningful to the business, and which can be used to label a component of a network element for use in Prime Network screens and reports. Figure 4-6 shows two devices with a business tag named **ABC Company**.

Figure 4-6 Find Business Tag Dialog Box With Results



Business tags are normally applied to *business elements*, which are constructions or organizations of certain network elements and their properties into a logical entity (such as Layer 2 VPNs, Layer 3 VPNs, and virtual routers). You can also apply business tags to individual entities, such as a single port or interface. Business tags allow you track business elements and individual entities in a way that makes sense from your business perspective. For example, a business tag might identify a new subscriber to a port, or other information that is relevant in your environment.

Note Business tags support Chinese characters, but your system must be properly configured to support this. See the *Cisco Prime Network 5.3 Installation Guide*.

By default, business tags replace the NE name. If you want to change this setting, or disable business tags completely, see Changing Vision Client Default Settings (Sound, Display, Events Age), page 4-15.

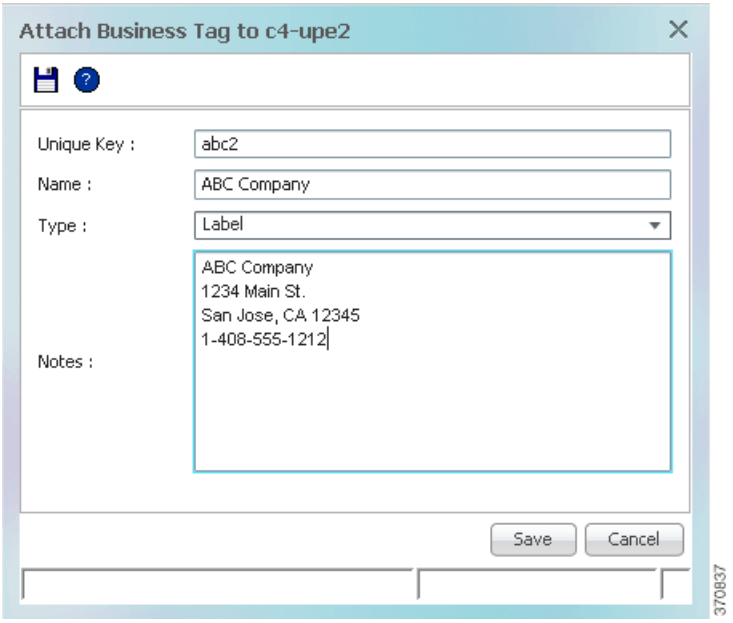
Step 1 Right-click the required network object and choose **Attach Business Tag**.

Step 2 Enter the information for the business tag in the Attach Business Tag dialog box:

Field	Description
Unique Key	A letter or number string that identifies the entity throughout the deployment. For example, if three devices have the ABC Company business tag, you could use abc1, abc2, and abc3.
Name	Name that is displayed in the clients. Names are case-sensitive.
Type	Subscriber, Provider Connection, or Label. **Note** If you select Label, the name of the network object changes to display the business tag name if the Replace name with Business Tag option is selected in the Options dialog box (**Tools > Options**). For more information about display options, see Changing Vision Client Default Settings (Sound, Display, Events Age), page 4-15.
Notes	Text-free message.

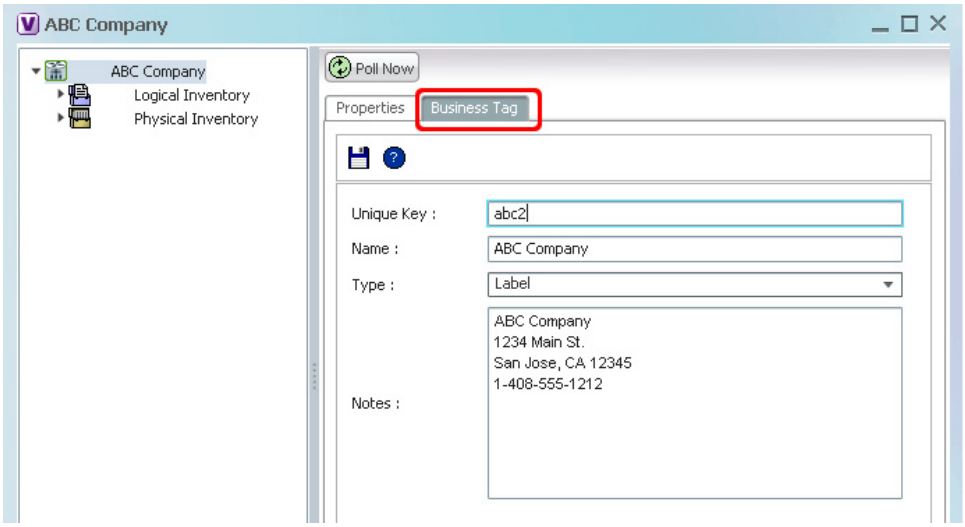
Step 3 Figure 4-7 provides an example. (After the tag is attached, the Vision client allows you to search for business tags based on type or on partial strings that appear in the Unique Key, Name, and Notes fields.

Figure 4-7 Attach Business Tag Dialog Box



Step 4 Click **Save**. The business tag is attached to the network object and displayed throughout the Vision client. A new Business Tag tab is also added to the device's inventory window, as shown in Figure 4-8. (The tab is displayed when you select the entity that contains the business tag.)

Figure 4-8 Vision Cllient Device Inventory—Business Tag Tab



You can edit or delete business tags by right-clicking them and using the appropriate command.

Applying a Background Image To a Map

You can apply GIF, JPG/JPEG, and PNG images as a map background. Subordinate windows (such as a detailed view of an aggregation) can use the same or a different image.

Step 1 Navigate to the required map in the Vision client.

Step 2 Right-click the map background and choose **Set Map Background**.

Step 3 In the Manage Map Background dialog box, provide the following information.

Table 4-1 Manage Map Background Options

Field	Description
Select Image	Applies the selected image to the current map background: 1. Choose **Select Image**. 2. Click **Browse**. 3. In the Open dialog box, select the desired image and click **OK**. 4. Click **OK** in the Manage Map Background dialog box.
Use Image From Upper Level	Indicates whether the selected subordinate map should use the same image as the parent map or a different image: • To use the same image, choose **Use Image from Upper Level**. • To use a different image, choose **Select Image** and complete the steps.
Remove Image	Removes the current image from the map background.

Step 4 Click **OK**. The current map background is updated as specified.

Step 5 To retain the background image for subsequent logins, choose **File > Save**.

Adding a Static Link When a Network Link is Missing

If Prime Network does not discover a link that you know exists in the network, you can create a static link that will be displayed in the map, but exists only at the model level. This allows correlation flows to go through the links, as if they were real physical or logical links. Static link properties are not updated because the links do not really exist in the network, but the link will change color under certain conditions, such as when a port is down.

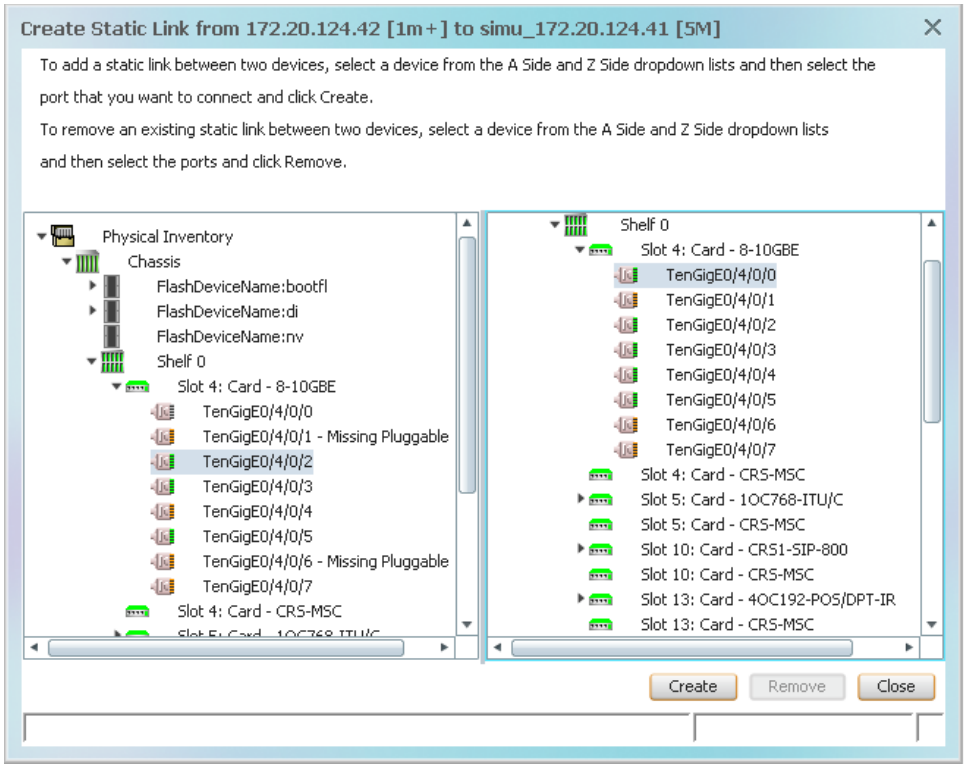
You can also use static links to create a link between a device and an unmanaged network, or to connect a tunnel to a VPN.

Static links are created between a device or port on the A side, and a device or port as the Z side. Prime Network validates the new link by checking the consistency of the port types (for example, RJ45 on both sides), and Layer 2 technology type (for example, ATM OC-3 on both sides). You can also create static links between Ethernet Link Aggregation Groups (LAGs) by choosing a LAG and the desired port channel for the A or Z side as described in the following procedure.

Step 1 Right-click the required A Side device in the navigation pane or in a map, and choose **Topology > Mark as A Side**. (You can also perform this operation from the inventory window.)

Step 2 Right-click the required Z Side device or LAG in the navigation pane or properties pane to display the right-click menu and choose **Topology > Mark as Z Side**. The Create Static Link window is displayed as shown in Figure 4-9, so that you can select the ports to connect.

Figure 4-9 Create Static Link Window



Step 3 Select the required port on both the A Side device and the Z Side device.

Step 4 Click **Create** to validate the connection and create the new link.

For information about removing a static link, see the *Cisco Prime Network 5.3 Administrator Guide*.

Check Global Settings for Vision Client Maps

The following map behavior is controlled from the Administration client:

- The Vision client actions users can perform, and the devices users can view and manage. When a user account is created, the administrator assigns:
  - A user access level to the user account (Viewer, Operator, Operator Plus, Configurator, or Administrator). It controls what actions the user can perform using the Vision client, such as adding and removing NEs from a map, or applying a background image to a map.
  - One or more device scopes. Device scopes determine which devices a user has permission to access, and the actions a user can perform on those devices. For example, a user might have sufficient privileges to add a device to a map, but the user can only do so if the device is in their device scope.

  For a matrix of actions users can perform depending on their user access level and device scope assignments, see Vision Client Permissions, page B-1.

- Which maps users are permitted to use. By default, Vision client users can view all maps made by other users. Administrators can instead control which maps users can see using the Registry Controller.
- Whether users can view links with only one endpoint in their device scope. By default, users will be permitted to see links only if both link endpoints are in their scope.

Users with Administrator privileges can change these settings by following the directions in the *Cisco Prime Network 5.3 Administrator Guide*. For information on fault-related settings that affect all of the Prime Network clients, see Changing Vision Client Default Settings (Sound, Display, Events Age), page 4-15.

Changing Vision Client Default Settings (Sound, Display, Events Age)

All map users can adjust these Vision client options. Changing these options applies only to the client machine (that is, the machine from where the client is launched).

These options control which items are displayed in maps, how items are displayed in maps, whether to use audio sounds, and when to remove NE tickets and events from the map. To change them, choose **Tools > Options** from the main menu.

To Do the Following:	Select the following from Tools > Options	Default
When Vision client starts, display Open Map dialog with last maps viewed	Startup tab—Load Workspace on Startup	Enabled
Change NE Label Font Size	Display tab—Map Labels Font Size	30pt
Change what severity information is displayed with NE icons	Severity tab—Show Severity Text	Enabled
	Severity tab—Show Acknowledged	Enabled
	Severity tab—Show Propagated	Enabled
Change how labels (business tags) are displayed (choose one)	Display Name tab—Do not use business tags	Disabled (tags are enabled)
	Display Name tab—Add business tags to name	Disabled (tag replaces name)
	Display Name tab—Replace name with business tag	Enabled

To Do the Following:	Select the following from Tools > Options	Default
Enable or disable audio alerts and control audio sounds	Audio tab—Enable Audio Response for Alarm	Disabled
	Audio tab—Critical, Major, Minor If audio is enabled, specifies .wav file for sound.	(see client)
	Audio tab—Loop Sound on Critical Alarm If audio is enabled, continuously plays .wav file for critical event.	Disabled
Control how long events are displayed in inventory window	Maximum age of events to display in the Tickets and Latest Events tabs. To only display active events, enter 0 (zero). The default (6 hours) is controlled from the Administration client client. **Note** Prime Network also has a limit of 15,000 events that can be sent from the server to clients. Older events are purged when either the maximum age or the maximum number of events is exceeded. The purging mechanism runs once per minute.	6 hours

Changing You Vision Client Password

Users can change their own Vision client passwords at any time by selecting **Tools > Change User Password** from the Vision client main menu. You may be required to change your password on a regular basis according to the password rules set by the Administrator.

Setting Up Native Reports

Prime Network provides two reporting functions. The native reports feature is launched from the Reports menu in the Vision client, Events client, or Administration client; this reporting tool is described in the following topics. The Operations Reports feature is an optional application and is described in *Cisco Prime Network 5.3 Operations Reports User Guide*.

These topics describe how to set up the native reports feature:

Whether you can perform these setup tasks depends on your account privileges. See Permissions Required to Perform Tasks Using the Prime Network Clients for more information.

Workflow for Setting Up Regular Reports

This workflow shows the steps required to set up regular, scheduled reports. If you simply want to run an existing predefined report, see:

- Inventory Hardware and Software Reports, page 5-7
- Network Service Reports, page 5-10

The following table provides the basic workflow for setting up scheduled reports.

	Description	See:
Step 1	If necessary, adjust the global settings that affect reports (for example, whether users can create shared reports which others can view).	Checking Global Settings for Report Operations, page 5-2
Step 2	Set up your report folder structure in Report Manager.	Setting Up Your Report Folders, page 5-2

	Description	See:
Step 3	Choose the report you want to customize: • Event reports—Tickets, Service events, Syslogs, and Traps; Audit, Provisioning, System and Security events; database-related information • Hardware and software reports • Ethernet service, network pseudowire, VPLS/H-VPLS reports	• Event Reports, page 5-3 • Inventory Hardware and Software Reports, page 5-7 • Network Service Reports, page 5-10
Step 4	Create a customized report based on any of the predefined reports that are packaged with Prime Network.	Creating Your Customized Report, page 5-11
Step 5	Test your customized report.	Entering Report Criteria and Testing Your Report, page 5-13
Step 6	Schedule your recurring report.	Entering Report Criteria and Testing Your Report, page 5-13

Checking Global Settings for Report Operations

The following default report behavior is controlled from the Administration client and will affect report users:

- The report actions users can perform, and the devices users can view and manage. When a user account is created the administrator assigns a user access level to the user account (Viewer, Operator, Operator Plus, Configurator, or Administrator).
  - The user access level controls which reports a user can generate.
  - The device scope determines which devices a user has permission to access, and which devices they can run reports against.

  For a matrix of actions users can perform depending on their user access level and device scope assignments, see Permissions Required to Perform Tasks Using the Prime Network Clients.
- Whether users can create public (shared) reports. By default, users cannot create shared reports.

Users with Administrator privileges can change these settings. They can also configure Prime Network to generate a warning message whenever a user executes a command script. For more information, see the *Cisco Prime Network 5.3 Administrator Guide*.

Setting Up Your Report Folders

Create nested folders to organize your reports under the existing Report Manager categories: Events Reports, Inventory Reports, and Network Service Reports. You can then place your customized reports under these folders (by specifying the Location field when you create the report).

Step 1 Choose **Reports > Report Manager** from the Prime Network client main menu.

Step 2 In Report Manager, choose **Events Reports > New Folder**.

Step 3 In the New Folder dialog, enter a folder name. The new folder appears under the Events Reports.

You can also move folders and reports to new locations from the Report Manager.

Event Reports

These event reports can be run from the Vision client, Events client, or Administration client:

Generalized Network Event Reports (Tickets, Service Events, Traps, Syslogs)

To get this network event information:	Use this report:	Can you choose devices?	Can you specify a time period?
Devices with most severe events (Pie chart shows device percentages)	Events Reports > Devices with the Most Events (By Severity)	Yes	Yes
Devices with most frequent events Pie chart shows device percentages	Events Reports > Devices with the Most Events (By Type)	Yes	Yes
Devices with most syslogs Devices with most traps Devices with most Service events (up to 1,000 devices):	Detailed Event Count (By Device)	Yes	Yes

Ticket Event Reports

To get this ticket information:	Use this report:	Can you choose devices?	Can you specify a time period?
Most common tickets for all managed devices Pie chart shows type percentages	Events Reports > Most Common Daily Events	No; all devices chosen by default	Yes
Details about tickets by their severity: • Alarm cause and the root event time • Affected devices • Whether ticket was acknowledged • Other event details: Duplication count, reduction count, alarm count, last modification, etc.	Detailed Tickets	Yes	Yes
Ticket details for specific devices (up to 1,000 devices): • Number of tickets per severity • Number of tickets per ticket type	Detailed Event Count (By Device)	Yes	TBD
Tickets with highest number of associated events with details such as: • Root cause • Ticket creation time	Events Reports > Event Reduction Statistics	Yes	Yes
Ticket MTTR[1] (mean time to repair information): • Number of tickets cleared manually • Number of tickets cleared automatically (by system) • MTTR • Ticket root cause and creation time	Events Reports > Mean Time to Repair	No; all devices chosen by default	Yes

1. MTTR is based on time of ticket creations, and time the ticket was last modified. (Acknowledging a cleared ticket can therefore affect the MTTR for the ticket.)

Service Event Reports

To get this network event information:	Use this report:	Can you choose devices?	Can you specify a time period?
Most common Service events, tickets, syslogs, traps Pie chart shows type percentages	Events Reports > Most Common Daily Events	All chosen by default	Yes
Most severe Service events with details	Detailed Service Events	Yes	Yes

Syslog-Specific Event Reports

To get this Syslog information:	Use this report:	Can you choose devices?	Can you specify time period?
Most common syslogs, and how many of each type? Pie chart shows type percentages	Events Reports > Most Common Syslogs	No; all devices chosen by default	Yes
Devices with most syslogs **Note** This report can also be generated from generic (non-actionable) events. Pie chart shows device percentages	Events Reports > Devices with the Most Syslogs	No; all devices chosen by default	Yes
Time frame when most syslogs occurred	Events Reports > Daily Average and Peak	No; all devices chosen by default	Yes
Syslog details (up to 250,000): • IP address time, description • Syslog raw data (generic events) or description (actionable events) **Note** This report can also be generated from generic (non-actionable) events.	Detailed Syslogs	Yes	No
For specific syslogs, their count and first and last time they occurred Pie chart show s syslog percentages	Events Reports > Syslog Count	No; all devices chosen by default	Yes
For specific syslogs, the devices they occurred on Pie chart show s syslog percentages	Events Reports > Syslog Count (By Device)	Yes	Yes
For specific syslogs and specific devices, a graph of syslogs with their priority	Events Reports > Syslog Trend (By Severity)	Yes	Yes

Trap-Specific Event Reports

To get this trap information:	Use this report:	Can you choose devices?	Can you specify a time period?
Most common traps for all managed devices Pie chart shows type percentages	Events Reports > Most Common Daily Events	Yes	No; all devices chosen by default
Time frame when most traps occurred	Events Reports > Daily Average and Peak	Yes	No; all devices chosen by default

To get this trap information:	Use this report:	Can you choose devices?	Can you specify a time period?
Traps generated by specific devices: • Number of traps per severity • Number of traps per ticket type **Note** This report can also be generated from generic (non-actionable) events. Pie chart shows device percentages	Events Reports > Devices with the Most Traps	Yes	Yes
Trap details for specific devices: • IP address, time, description (long description if report is generated from actionable events) • SNMP and trap version • Generic or device-specific trap OID, if the event is generic The maximum number of traps retrieved for this report depends on whether the Long Description check box is selected. When checked, a maximum of 30,000 traps are retrieved. When this check box is not checked, a maximum of 100,000 traps are retrieved for this report. **Note** This report can also be generated from generic (non-actionable) events.	Detailed Traps	No	Yes

Database-Related Event Reports

For this database-related information:	Use this report:	Can you choose devices?	Can you specify time period?
For specific period, the number of active tickets, alarms, and events stored in DB Tickets with most number of events Events-per-second rate	Events Reports > Database Monitoring	N/A	Yes
For specific period, the number of generated tickets with these details: • Ticket type and count • Root cause and ticket creation time • Number of correlated events per ticket (largest, smallest, average)	Events Reports > Event Reduction Statistics	Yes	Yes
For a specific period, total number of actionable and generic events added to the Oracle database by type (Syslogs, Traps, Tickets, correlated/uncorrelated events, network/non-network events)	Events Reports > Fault DB vs. Event Archive Statistics	N/A	Yes

Audit, Provisioning, System, Security Event Reports (Non-Network Reports)

For this non-network event information:	Use this report:	Can you choose devices?	Can you specify a time period?
Audit event details: • Severity, timestamp, description • Username, originating IP address • Command details: name, parameters, signature	Detailed Audit Events	No	Yes
Provisioning event details • Severity, timestamp, description, username • Status	Detailed Provisioning Events	No	Yes
Security event details: • Severity, timestamp, description, location • Username, originating IP address	Detailed Security Events	No	Yes
System event details: • Severity, timestamp, description, location	Detailed System Events	No	Yes

Inventory Hardware and Software Reports

For all inventory reports, Prime Network retrieves the inventory information from the network element. These inventory reports can be run from the Vision client, Events client, or Administration client:

- Hardware Reports, page 5-8
- Software Reports, page 5-10

Hardware Reports

Hardware inventory information:	Type of report:	Can you choose devices?
Hardware details (you can filter this report using a string from the device, chassis, module, or port name): • Chassis—Description and serial number; shelf description, serial number, and status **Note** When the last Virtualized Services Module (VSM) blade is removed from the chassis, a notification stating that the data center has been removed is sent by the Prime Network. When this notification is received and transformed by Prime Network Integration Layer to the Operations Support Systems (OSS) client, the client is expected to delete all objects (Hosts, VM) under this specific virtual device context (VDC). • Module—Module and sub module name; module status, hardware type, and version • Port—Port location, type, and status; port alias, if port is sending alarms, if port is managed, PID, pluggable type serial number.	Hardware Detailed	Yes
Hardware details you can optionally group (the report also provides the device IP address and serial number): • Device name or system name • Vendor, product, device series, element type, or chassis	Hardware Summary	Yes

Hardware inventory information:	Type of report:	Can you choose devices?
Module details (you can filter this report using a string from the module name): • Device • IP Address • Serial Number • Hardware Version • Software Version Pluggable Transceiver properties: **Note** For a module which contains ports but no pluggable transceiver ports, these properties will be marked as N/A. • Interface Name • Connector Type • Connector Description • Connector Serial Number • Pluggable Type • Pluggable Transceiver ID • Pluggable Port State	Modules SFP Summary (By Type)	Yes
Module details (you can filter this report using a string from the module name): • Device • IP Address • Serial Number • Hardware Version • Software Version	Modules Summary (By Type)	Yes

Software Reports

Software information:	Type of report:	Can you choose devices?
Software sorted by devices: • Software version and image file name • Device name, type, IP address, and serial number	Software Summary (By Device)	Yes
Software sorted by version: • Number of software versions being run • Image file name and number of devices running that image	Software Summary (By Version)	Yes
Cisco IOS-XR software sorted by devices: • Cisco IOS XR software version • For each package installed on device: – Package name and state (active or inactive) – Storage location – Module name • Device name, type, IP address, and serial number	IOS-XR Software Package Summary	Yes

Network Service Reports

The following network service reports can be run from the Vision client, Events client, or Administration client.

Table 5-1 Standard Network Service Report Types

For this service information:	Use this report:
Ethernet service information which you can filter using a service, EVC, or map name: • Ethernet service or Layer 2 VPN name, including the customer label (business tag) • EVC name and customer label • Maps containing the Ethernet service or Layer 2 VPN instance	Ethernet Service Summary
Ethernet service summary with the following additional details: • Edge EFPs associated with the EVC or Layer 2 VPN • EFT fragment name and type	Ethernet Service Detailed
Network pseudowire information which you can filter using a pseudowire name, type, or map name: • Pseudowire name and type, including any customer labels (business tags) • Maps containing the pseudowire instance	Network Pseudowire Summary
Network pseudowire summary with the following additional details: • Pseudowire details and type, such as pseudowire edge, Ethernet flow point, or switching entity	Network Pseudowire Detailed

Table 5-1 Standard Network Service Report Types (continued)

For this service information:	Use this report:
VPLS/H-VPLS information which you can filter using a VPLS/H-VPLS name or map name: • VPLS or H-VPLS name, including any customer labels (business tags) • Maps containing the VPLS/H-VPLS instance	VPLS Summary
VPLS/H-VPLS summary with the following additional details: • Type of VPLS service, such as VPLS forward, access EFP, or core pseudowire	VPLS Detailed

Creating Your Customized Report

Customized reports can be added to Report Manager so that other users can run them using their own criteria (depending on their user access level and device scopes). If you created new report folders as described in Setting Up Your Report Folders, page 5-2, customized reports can be organized under that folder (using the Location field).

This example shows how to create a report called 24-Hour Critical Tickets. The customized report will be stored under a user-created folder called Critical Tickets - Daily Report - August 2014.

Step 1 Right-click **Events Reports > Detailed Network Events > Detailed Tickets > Define Report of This Type**.

Step 2 In the Create Report dialog, enter the required information, such as:

- Report Settings
  - Name—**24-Hour Critical Tickets**
  - Location—Click **Browse** and navigate to **Events Reports > Critical Tickets - Daily Report - August 2014** in the Move To dialog box.
- Date Selection—**Last 1 days**
- Device Selection—**All Devices**
- Filter Events/Tickets By Severity—**Critical**

Step 3 Click **OK**.

Creating Detailed Standard Events Report

This example shows how to create a Detailed Standard Events report for devices from Prime Network Vision client, using the Report Manager. When you create a Detailed Standard Events you can schedule, according to the severity and events you can filter the reports. After creating the report you can view the job and export Job details in a report format that are managed by Prime Network. You can save the reports in any one of the following formats PDF, XM,.CSV, HTML, and XLS.

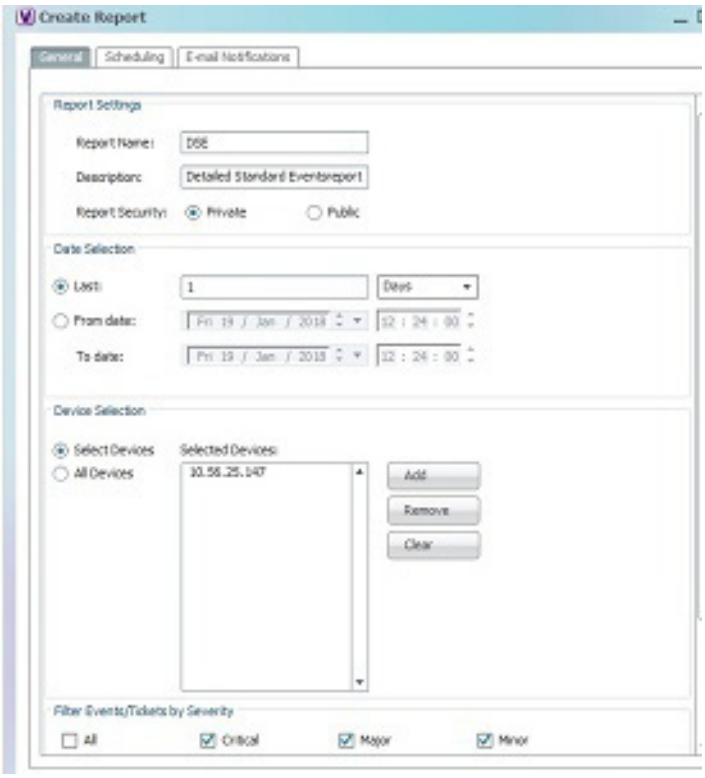
You can export these Standard events report through Prime Network Vision client, schedule and send email notification automatically. Also, you can use the Prime Network Administrator and Events clients to generate the Detailed Standard Events report.

To create a detailed standard events report in Prime Network Vision client:

Step 1 Log in to the Prime Network Vision.client.

Step 2 Select **Reports > Reports Manager > Events Reports > Detailed Network Events > Detailed Standard Events.**

Step 3 Right-click the **Detailed Standard Events > Run**. The Create Report window appears.



Note You can also choose **Reports > Run Report > Events Reports > Detailed Network Reports > Detailed Standard Events.**

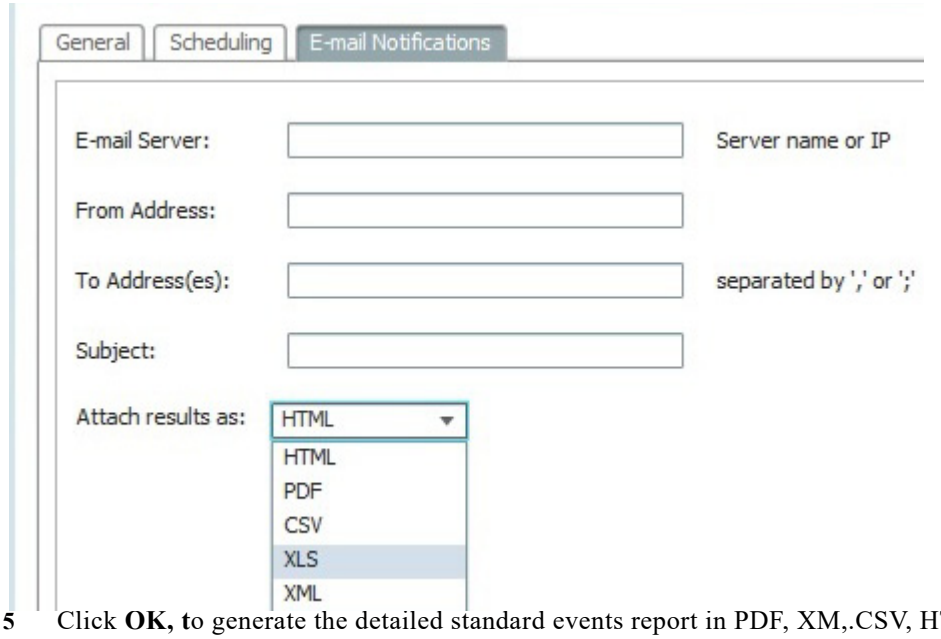
Step 4 In the **Create Report** window, on the **General** tab, enter the required information:

- Report Settings
  - Name—Specify the name of the report.
  - Description—Enter the description of the report.
  - Report Security—Click the **Private** or **Public** radio button to set the security.
- Date Selection—**Last 1 days**
- Device Selection—**Select Devices** or **All Devices**

Note You can also click **Add** to add a network element to create a report.

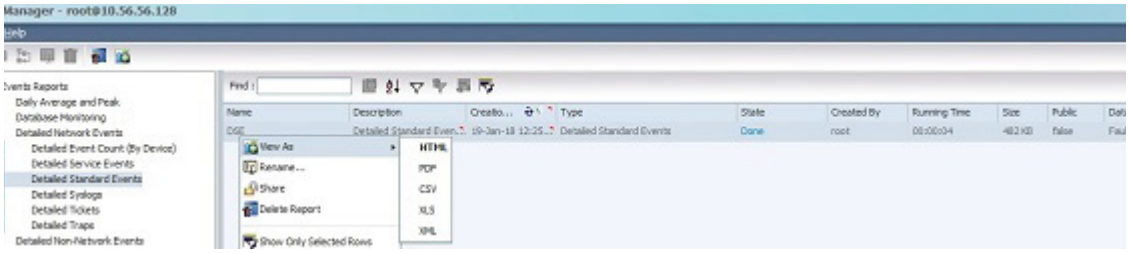
- Filter Events/Tickets By Severity—**Critical**
- Filter Events—Click the **Syslogs** or **Traps** or **All** radio button
- Additional Report Specifications—Enter the additional description, if required.
- On the **Scheduling** tab, enter the required information:

  - Run Now—Click the radio button to run the report
  - Schedule Job—Click the radio to specify all job criteria.
- On the **E-mail Notifications** tab, enter the required information.



Step 5 Click **OK, t**o generate the detailed standard events report in PDF, XM,.CSV, HTML, or XLS format.

Step 6 In the **Reports Manager** window, the created report details will be displayed and you can click **View As** to select the format, save and download the report in the specified format.



Entering Report Criteria and Testing Your Report

To enter criteria and test a customized report:

Step 1 Select **Reports > Report Manager > Run Report** and navigate to your customized report.

Step 2 Right-click the report and choose **Run Now**.

Step 3 Supply your report criteria. What you must supply depends on the report type. Most criteria is self-explanatory, but the following provides some additional details on the choices.

Note The settings that are displayed depend on the report type.

- General Criteria:

Report Settings	
Report Security	**Note** This field is displayed only if report sharing is enabled. See Checking Global Settings for Report Operations, page 5-2. • Private—Can only be viewed by creator. • Public—Can be viewed by all users, even if the devices are outside their scope. If sharing is enabled, this setting can be changed after the report is created (by right-clicking the report and selecting **Share** or **Unshare**).
Display *n*	Number of items to be displayed in report.
Data Source	Run report based on actionable or generic events
Include pie charts in report output	Also generate pie chart.
Device Selection	
Select Devices	To select specific devices: 1. Click **Select Devices**. 2. Click **Add**. 3. In the Add Network Element dialog box: – Click **Search** to find NEs based on your criteria. – Click **Show All** to choose from a list of all NEs. 4. Select the NEs and click **OK**.

- Special Criteria for Traps:

Traps Detailed Description	Include traps with descriptions that match *string*.	
Long Description	(Actionable events) Include traps that have *string* in their long description. 1. Check Show Long Description check box. 2. Enter the string that the trap long description must contain.	
SNMP Version	(Generic events) SNMP versions to include in the report: All, 1, 2, or 3.	
Generic	Include generic (non-actionable) traps:	
	All	All generic traps
	0	coldStart
	1	warmStart
	2	linkDown
	3	linkUp
	4	authenticationFailure
	5	egpNeighborLoss
	6	enterpriseSpecific (enter comma-separated OIDs, up to 125 digits, in Vendor Specific field)

Step 4 Click the Scheduling tab and choose **Run Now**.

Step 5 Verify the results in Report Manager or when the report is displayed in the web browser.

Scheduling a Recurring Report

To schedule a recurring customized report, use the Report Manager. If you want to schedule a predefined report, you can run it from Report Manager or directly from the Prime Network client Reports menu. To run a report immediately, click the Schedule tab and choose **Run Now**.

To schedule a report:

Step 1 Select the report you want to schedule.

Report Type	Run From Main Menu:
Predefined reports that come with Prime Network	**Reports > Run Report**
Customized reports (reports you modified and saved)	**Reports > Report Manager > Run Report**

Step 2 Supply your report criteria.

Step 3 Click the Scheduling tab and give the job a meaningful title (for example, 24-Hour Ticket Report Job).

Step 4 Enter the schedule criteria—for example: Recurring, Daily, Run Indefinitely, and from the current time for 30 days.

Once you schedule a job, the job information can only be edited from the Job Manager by choosing **Tools > Schedule Job** from the Vision client main menu. You can also rerun the job and clone the job using the Job Manager.

Sending a Report Through E-mail Notification

To send a report, you can enter the e-mail notification criteria in the Create Report window. If e-mail notification details are provided, you can run the report and automatically the report is mailed as an attachment in a desired format. You can attach reports in the XML, PDF, CSV, XLS, or HTML format.

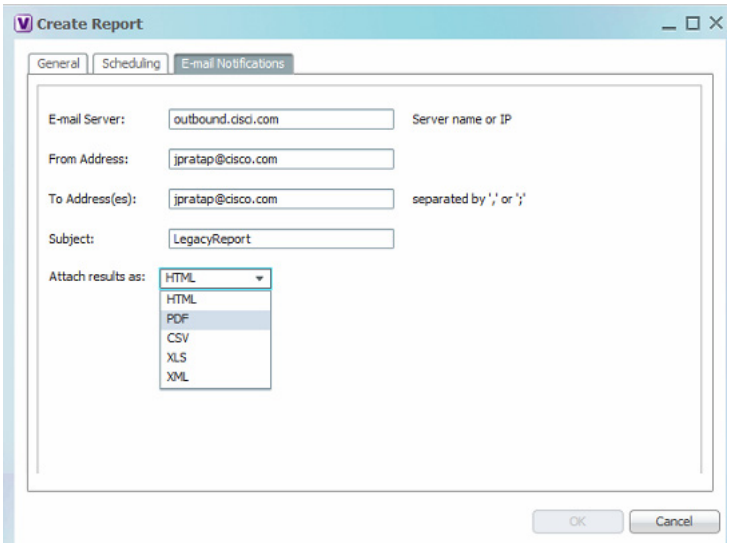
To enter criteria and send a report through e-mail notification:

Step 1 Select **Reports > Report Manager. I**n the Reports Manager window, expand either one of the Events Reports, Inventory Reports, or Network Service Reports node.

Note You can also create and send a report by using the following navigation path:
Select **Reports >Run Report >Events Reports >** click a report
Select **Reports >Run Report >Inventory Reports >** click a report.
Select **Reports >Run Report >Network Service Reports >** click a report.

Step 2 Choose a report > right-click a selected report > click **Run**. The Create Report page appears.

Figure 5-1 E-mail Notification Tab



Step 3 Click the **E-Mail Notifications** tab, enter a valid Email Servers, To-Address, From-Address (es), and Subject details.

Note If you have configured the **Email Server** and **From Address** in the **Global Report Settings** then those details will be displayed by default.

Step 4 From the **Attach results as** drop-down list, choose a report format to attach in an email.

Step 5 Click **OK** to create a report and to send the report as an attachment.

Saving Reports

Use the Prime Network **Report Manager** to specify a report format (default format is XML) and save all reports in the path specified by you as soon as the reports are generated. You can also change the save location while generating a report. The following actions are also available:

- View the saved report location path on the **Save Report** tab in the **Create Report** window for all reports.
- Check AVM 11 logs if report is not saved in the provided location.
- If you save two reports with the same name in the same location, and completing on the same time it will override the other one.

Note If you want to purge reports you must do it manually.

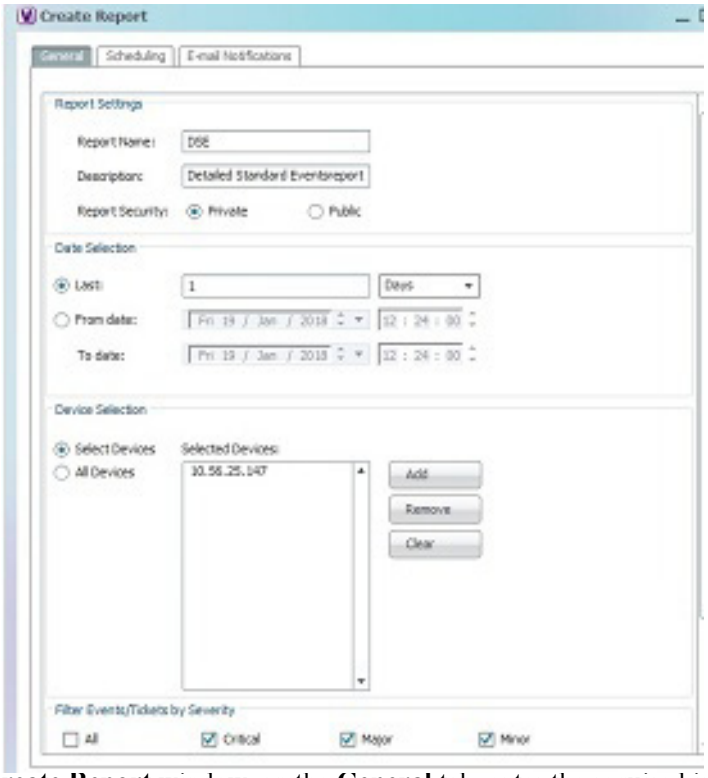
Prerequisites

- The location for saving reports must be created.
- Read-write permission must be enabled before generating reports.

This example shows how to save a report.

Step 1 Select **Reports > Report Manager. I**n the Reports Manager window, expand either one of the Events Reports, Inventory Reports, or Network Service Reports node.

Step 2 Choose a report > right-click a selected report > click **Run**. The Create Report page appears.



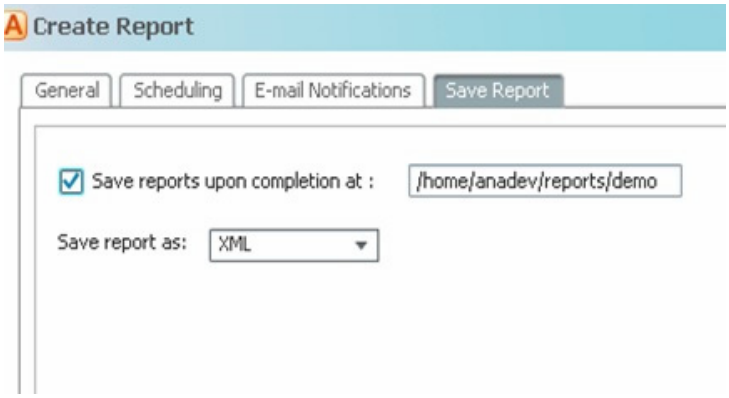
Step 3 In the **Create Report** window, on the **General** tab, enter the required information:

- Report Settings
  - Name—Specify the name of the report.
  - Description—Enter the description of the report.
  - Report Security—Click the **Private** or **Public** radio button to set the security.
- Date Selection—**Last 1 days**
- Device Selection—**Select Devices** or **All Devices**

Note You can also click **Add** to add a network element to create a report.

- Filter Events/Tickets By Severity—**Critical**
- Filter Events—Click the **Syslogs** or **Traps** or **All** radio button

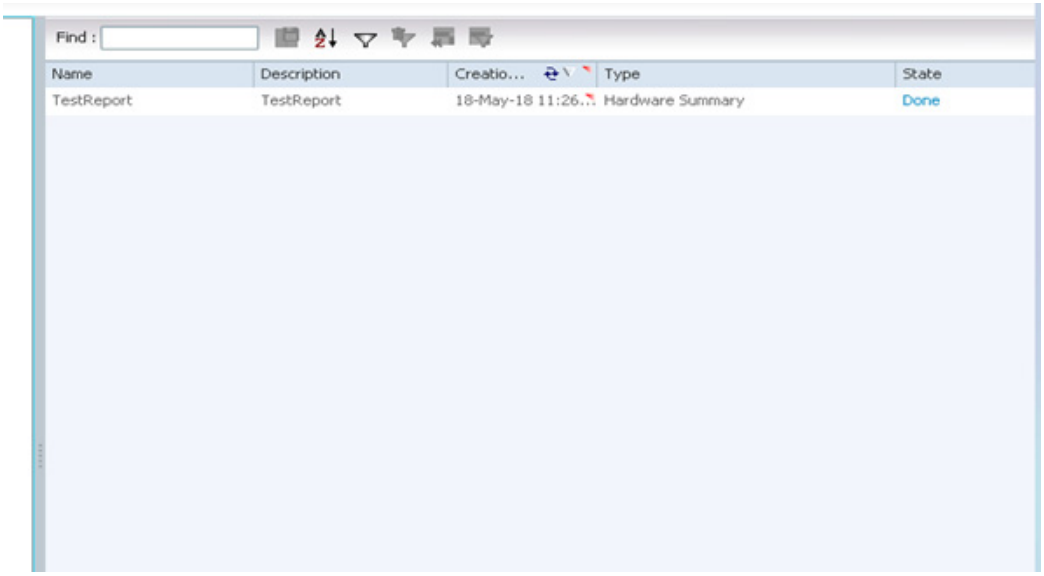
- Additional Report Specifications—Enter the additional description, if required.
- On the **Scheduling** tab, enter the required information:
  - Run Now—Click the radio button to run the report
  - Schedule Job—Click the radio to specify all job criteria.
- On the **E-mail Notifications** tab, enter the required information.
- On the **Save Report** tab, in the **Save reports upon completion** field the location path that you have specified in the Report Manager window is displayed. You can modify the path if required.



  - From the **Save report as** drop-down list, choose a format to generate and save the report.

Step 4 Click **OK, t**o generate and save a report in the desired format.

In the **Reports Manager** window, the created report details with the save location is displayed.



In the **Location** field, either one of the following detail is displayed:

- The location of the report saved when the provided location is available and if it has read/write permission
- NA— Displayed as “NA” when save report option is disabled
- Saving failed:Path not exists—Displayed as “Saving failed:Path not exists” when the location path does not exists and when the location provided does not exist.
- Saving Failed Permission denied —Displayed as “Saving failed: Permission Denied” when the location exist and it does not have write permission.

Setting Up Fault Management and the Events Client Default Settings

The following topics describe how to use the Events client to view and manage faults:

Whether you can perform these setup tasks depends on your account privileges. See Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1 for more information.

Workflow for Setting Up Fault Management

Most of the fault management setup tasks are documented in the *Cisco Prime Network 5.3 Administrator Guide* and should already be completed. The following table provides the basic workflow for the remaining fault management setup tasks.

	Description	See:
Step 1	Check the global setting that control when tickets are auto-cleared and auto-archived, when a cleared ticket can no longer be reopened, whether raw events are saved, and when data is purged from the Oracle database	Check Global Settings for the Events and Vision Clients, page 6-2
Step 2	Check the device setup tasks to see if there are any changes you need to make, such as enabling SNMP traps	Making Sure Devices Are Configured Correctly, page 6-3
Step 3	Adjust the Events client settings (client refresh interval, age of events to display, number of events to display)	Setting Up Your Events View, page 6-4
Step 4	(Optional) Create event filters and save them so you can use them as needed	Creating Ticket and Event Filters for Vision and Events Client Users, page 6-5

	Description	See:
Step 5	(Optional) Extend Prime Network: • Download and install new events support using Prime Network Device Packages (DPs) • Add support for customized events and threshold-crossing alarms	• *Cisco Prime Network 5.3 Administrator Guide* • *Cisco Prime Network 5.3 Customization Guide*

Check Global Settings for the Events and Vision Clients

The following fault-related actions are controlled from the Administration client:

- The Vision client and Events client operations users can perform, and the devices users can view and manage. When a user account is created, the administrator assigns:
  - A user access level to the user account (Viewer, Operator, Operator Plus, Configurator, or Administrator). It controls what actions the user can perform using the Vision client, such as clearing or adding notes to tickets).
  - One or more device scopes. Device scopes determine which devices a user has permission to access, and the actions a user can perform on those devices. For example, a user might have sufficient privileges to clear a device ticket, but the user can only do so if the device is in their device scope.

  For a matrix of actions users can perform depending on their user access level and device scope assignments, see Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1.

The following default settings are configured from the Administration client:

Options	Description	Default Setting
Events client login	User access role that is required to log in to the Events client (the Events client is for advanced users).	Administrator
Locking cleared tickets	Age at which a cleared. ticket can no longer be reopened or have new events added to it.	Disabled
Auto-clearing tickets	Auto-clear tickets if they meet the following criteria: • Is the specified severity (or lower), and • Has not been modified for a specified period of days.	Disabled
Auto-archiving cleared tickets	Move the ticket from an active to an archive partition in the Oracle database and it begins aging. • When the total number of cleared tickets exceeds a specified number. • When a single ticket contains more than a specified number of associated events.	 16,000 150
Saving raw traps and syslogs	Whether raw traps and syslogs received from devices are saved to the Oracle database. It can also store information from unmanaged devices if notification from unmanaged devices is enabled.	Enabled

Options	Description	Default Setting
Viewing standard events	Whether standard events can be viewed in the clients. Standard events are events for which Prime Network only does very basic parsing; they are not examined for correlation or used as a basis for generating tickets. If enabled, these events are displayed in: • Vision client—Latest Events tab (map view) • Events client—Standard tab **Note** For large deployments, enabling this is not recommended so that Prime Network performance is not negatively impacted.	Disabled
Purging data from Oracle database	When data is purged from the Oracle database: • Actionable events begin aging when they are archived (moved to an archive partition in the Oracle database). • Generic (non-actionable) events begin aging as soon as they are saved.	14 days

For more information on how Prime Network responds to incoming events, see How Prime Network Handles Incoming Events, page 10-1.

Users with Administrator privileges can change these settings by following the directions in the *Cisco Prime Network 5.3 Administrator Guide*.

Making Sure Devices Are Configured Correctly

In order for Prime Network to fully model and manage faults on your devices and network, the NEs must be configured correctly so that Prime Network can get the information it needs. A complete list of required and recommended configurations is provided in an appendix to the *Cisco Prime Network 5.3 Administrator Guide*.

You can make most required configuration changes using commands that are packaged with Prime Network. To launch these commands, right-click an NE and choose **Commands**. Whether or not you can run these commands depends on your user privileges. See these topics for information on how to use these packaged commands:

- Changing the SNMP Configuration and Managing SNMP Traps, page 8-27
- Changing Device Port Properties and Disabling Ports, page 8-29
- Changing Device Interface Properties and Disabling Interfaces, page 8-30
- Changing Server Settings for DNS, NTP, RADIUS, and TACACs, page 8-31

Other commands are described throughout this document with the services and technologies they apply to.

Configuring Prime Network to Support Unmanaged Devices

You can configure Prime Network to also support events from unmanaged devices. Prime Network can then include these devices in its reports, and you can configure an Event Notification Service to forward these events to northbound clients.

To enable support for unmanaged devices, you must configure the support using the Prime Network Broadband Query Language (BQL) as described in the Cisco Prime Network Integration Developer Guide.

An Event Notification Service can be configured using the Administration client as described in *Cisco Prime Network 5.3 Administrator Guide*.

Setting Up Your Events View

The Events client Options dialog box enables you to change various aspects of the event display in Events client.

If You Are Using Prime Network:	**Launch the Events client by choosing:**
As part of suite	**Assure > Prime Network > Events** from the REPLACE main menu bar
As a standalone application	**Start > Programs > Cisco Prime Network >** *gateway-IP-address* **> Cisco Prime Network Events** from your local machine

To set up your events view, choose **Tools > Options** from the main menu. Table 6-1 lists the available options.

Table 6-1 Options for Changing Events client Client

Option	Description	Default
Save last filter	Saves a filter and its criteria so it is available the next time you log into Events. Events are not filtered automatically when you next log into Events client unless the *Open Events with saved filter* option is also selected.	Enabled
Open Prime Network Events with saved filter	When enabled, applies the previous filter to the events as soon as you log into Events. While this option is enabled, a filter remains on until you manually disable it.	Disabled
Display *n* records per page	Specifies the number of events to be displayed per page.	50
Export *n* records in total	Sets the maximum number of events to be exported to a file.	1000
Run auto refresh every *n* secs	Automatically refreshes the Events client display after the specified number of seconds. **Note** This option uses rapid refresh from the database, which can affect the performance of other vital database options.	60

Table 6-1 Options for Changing Events client Client (continued)

Option	Description	Default
Display data for the last *n* hours	Displays past events for the number of hours specified here. For example, if you specify 4 in this field, then events received over the past 4 hours are displayed in the Events client. The default value is two hours, but you can specify up to 10 hours. The higher the value, the longer it takes for the events to be displayed.	2
Find mode (No automatic data retrieval)	Operates the Events client window in Find mode. In this mode, no events will be retrieved from the Oracle database when you open the application or switch between tabs. You can click the Find button in the toolbar to search for the events you need. When in Find mode, the status bar in the Events client window shows "Find Mode (no automatic data retrieval)."	Disabled

Creating Ticket and Event Filters for Vision and Events Client Users

The Vision client and Events client both support a filtering mechanism that lets you create filters and save them for later use. Filters created in a client can be shared, which means other users of the same client can access and run the filters. The following table describes the filters you can create from the two clients and where to get more information.

Client	To create a filter that uses this criteria:	See:
Vision client	All devices in a map: • Tickets • Incoming syslogs and traps • Service events generated by Prime Network	Viewing Tickets and Latest Events for All Devices in a Map, page 11-3
	A specific device: • Tickets • Incoming syslogs and traps (including events not handled by Prime Network, if enabled) • Service events generated by Prime Network • Configuration changes	Viewing Tickets and Events for a Specific Device, page 11-4

Client	To create a filter that uses this criteria:	See:
Events client	All devices managed by Prime Network: • Active and archived Tickets • Active and archived Trap, Syslog, and Service events • Active and archived Trap and Syslog events (standard events) not handled by Prime Network (if enabled) • Device configuration changes (including who made the changes)	Creating and Saving Filters for Tickets and Events, page 12-6
	Trap events and Syslog events from unmanaged devices (if enabled)	
	Prime Network internal system and security events	

Viewing Investigation Ticket Information

Prerequisite

The information ticket is generated only when the **investigation-state-update-ticket** option is enabled. By default, this option is enabled.If you require to disable the option, the below **run registry tool** command is given:

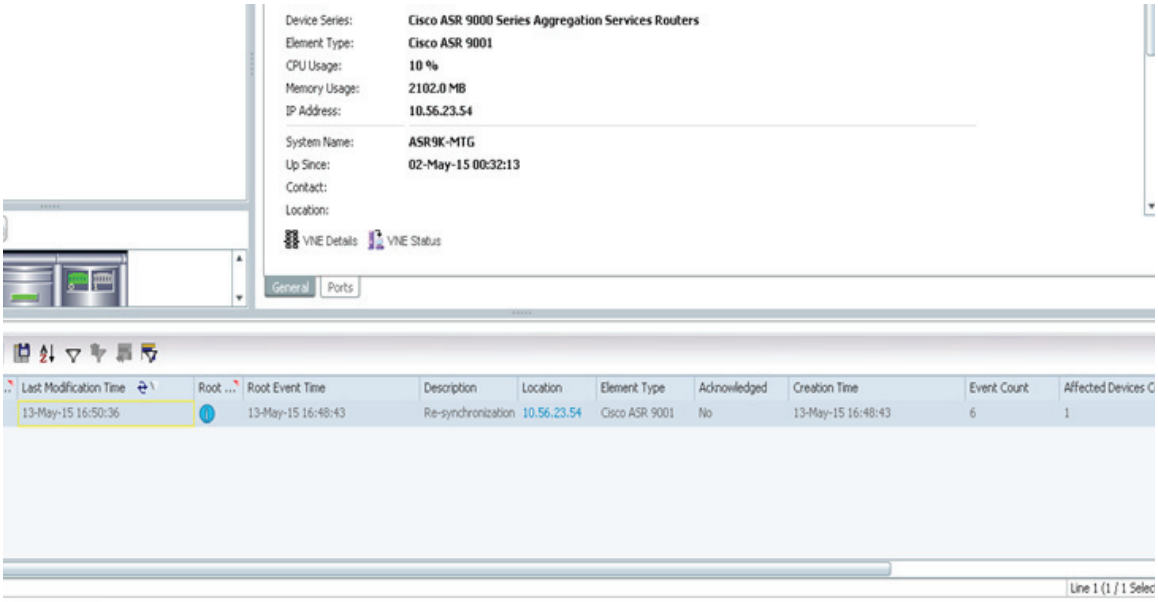
runRegTool.sh -gs localhost set 0.0.0.0 agentdefaults/da/investigation-progress/investigation-state-update-ticket false

VNEs undergo multiple investigation states in its lifecycle. The tracking of information is enabled as **Information** tickets. Using these tickets, you can receive notification if the state of the VNEs is changed.

The information ticket is generated once the VNE is started and the same ticket is updated whenever the VNE state changes in its lifecycle. Once the VNE comes to the **Operational** state, the ticket is cleared.

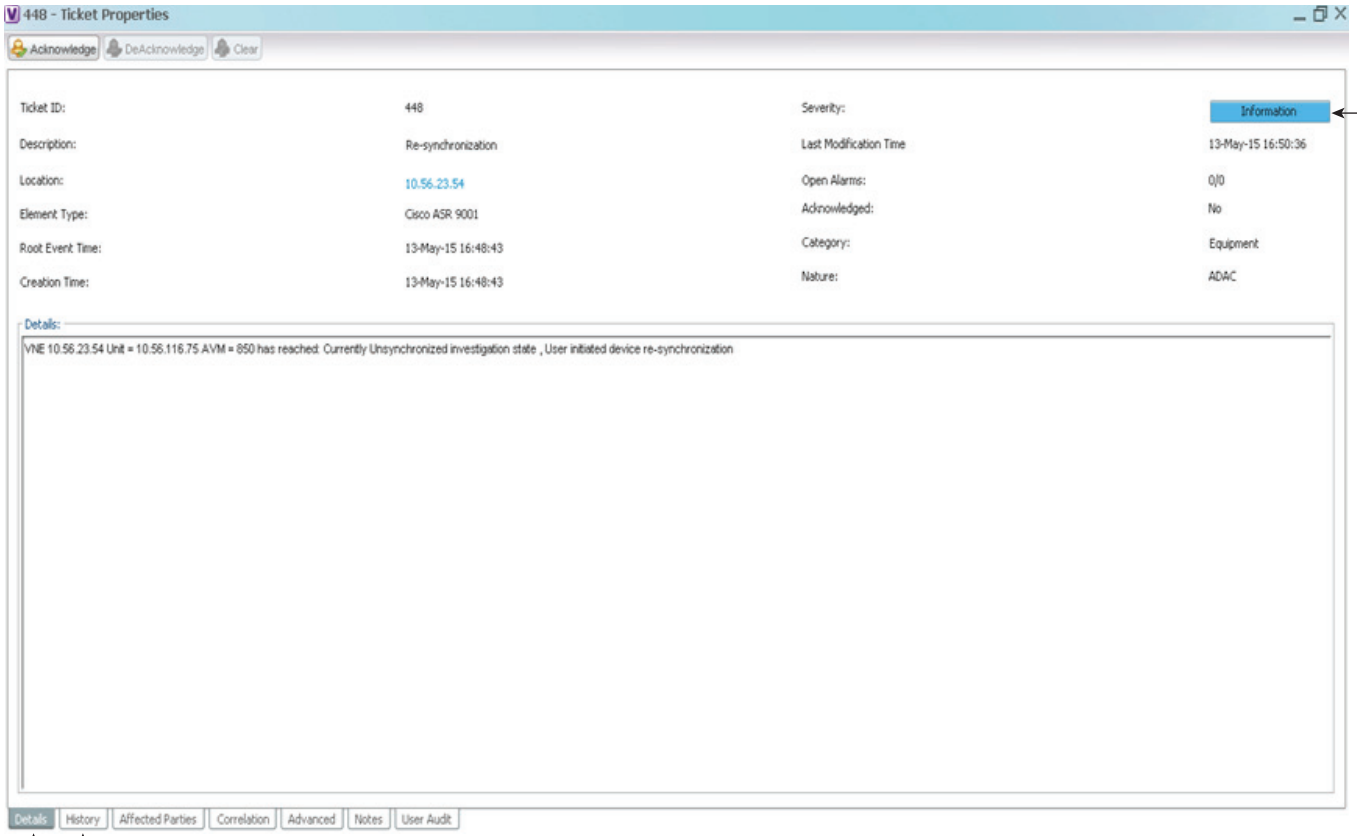
Once a ticket is opened, you can view the reason for each state in the **Details** pane. You can view the history details of a particular ticket with information on various states of the ticket in the **History** window. Figure 6-1 provides the details of ticket information

Figure 6-1 Viewing Investigation Ticket Information



Once a ticket is opened, you can view the reason for each state in the **Details** pane. You can view the history details of a particular ticket with information on various states of the ticket in the **History** window. Figure 6-2 displays the information ticket in **Details** pane.

Figure 6-2 Viewing the Investigation Ticket Information in Details Pane



Monitoring Alarms/Events in Prime Network (Event Manager)

In the devices like ASR 903 or ASR 9K, we have monitored service alarms/events to find out the time taken by Prime network to generate the service alarms/events whenever changes on devices such as interface/port/link down or vice versa. Prime Network has the option of monitoring the time taken to generate the alarms /events for the following:

- Admin
- Operational

The Status of the device will be in **Disabled** when there is any interface /port /link is down in physical inventory and the status will be in **OK** state if the same is up. Refer Figure 6-3.Whenever there is change in status in physical inventory, the Prime Network event manager generates the events.

Figure 6-3 Viewing the Status of the device

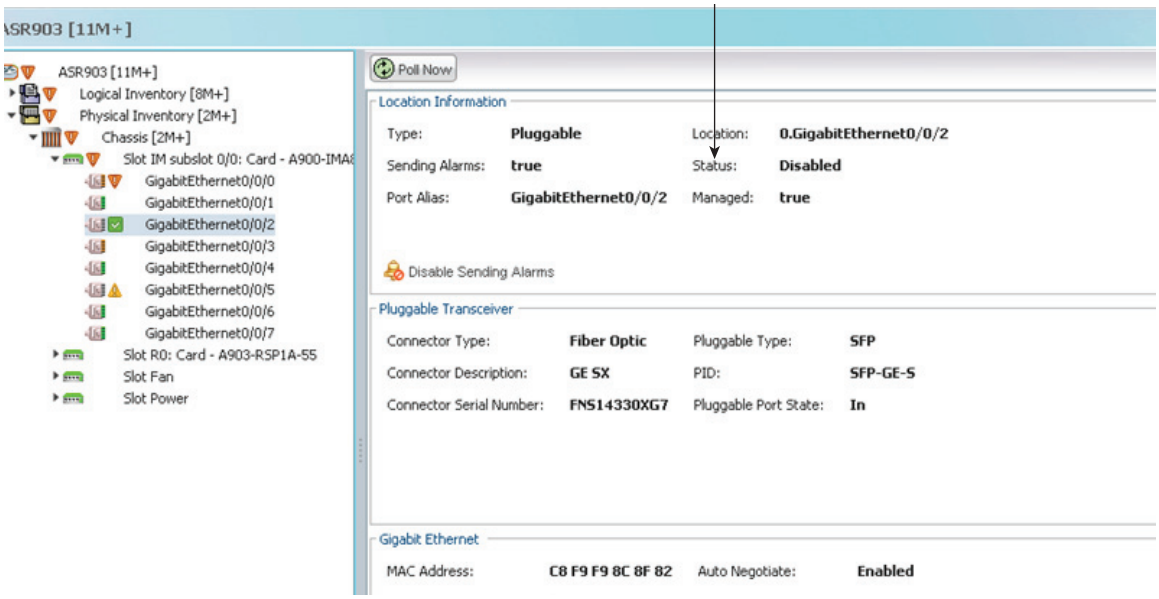
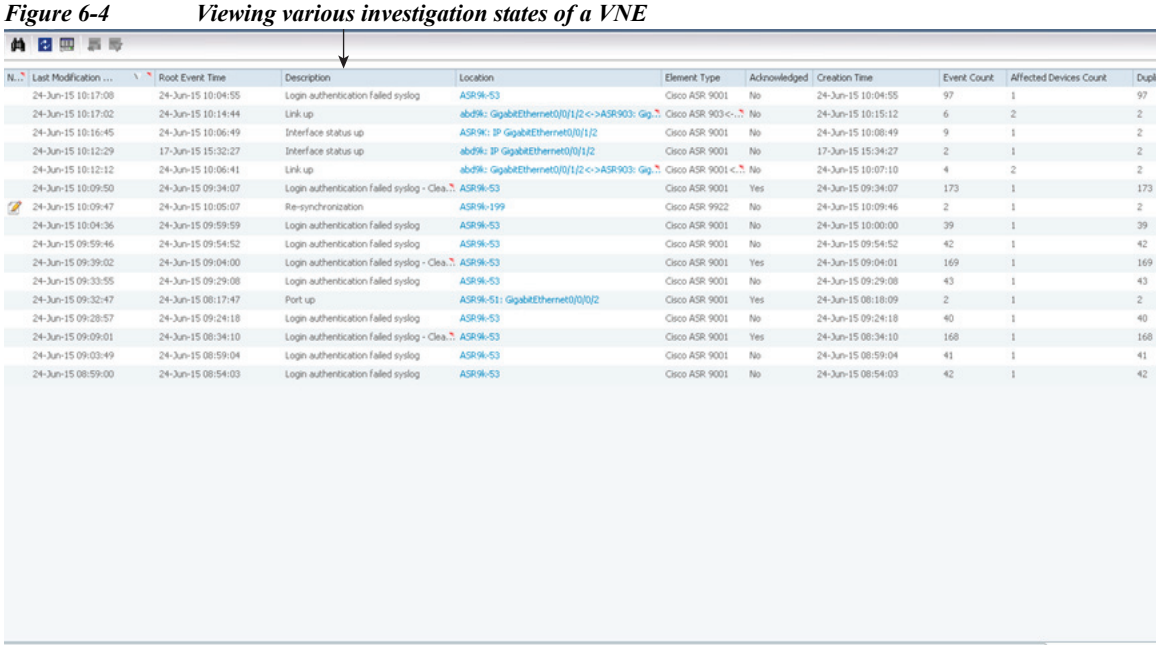


Figure 6-4displays the various investigation states of VNEs

Figure 6-4 Viewing various investigation states of a VNE



The monitoring of alarms /events has been carried out using two types of polling:

Reduced Polling—It is a default polling which provides the time taken by Prime Network for checking any change in the device.

Regular Polling— In regular polling, the time taken by Prime Network for checking any change in device will be more than Reduced Polling.

Viewing Devices, Links, and Services in Maps

Vision client maps display a variety of information in a topological view, such as devices, physical and logical connections, network services, and so forth. Whenever you open a map, Prime Network refreshes the map information. How to create a map is described in Workflow for Creating a Map, page 4-2. These topics describe how to use maps to get the information you need about your network:

Opening Maps

You can work on a maximum of five maps at any given time. Like all Prime Network clients, the Vision client is password-protected. When you log in, client updates (if any) are automatically applied.

Note You can change your password at anytime by choosing **Tools > Change User Password** from the main menu.

Step 1 Launch the Vision client.

If You Are Using Prime Network:	Launch the Vision client by choosing:
As part of suite	**Assure > Prime Network > Vision** from the REPLACE main menu bar
As a standalone application	**http://***gateway-ip***:6080/ana/services/install/install/webstart.html**
	Start > Programs > Cisco Prime Network > Cisco Prime Network Vision

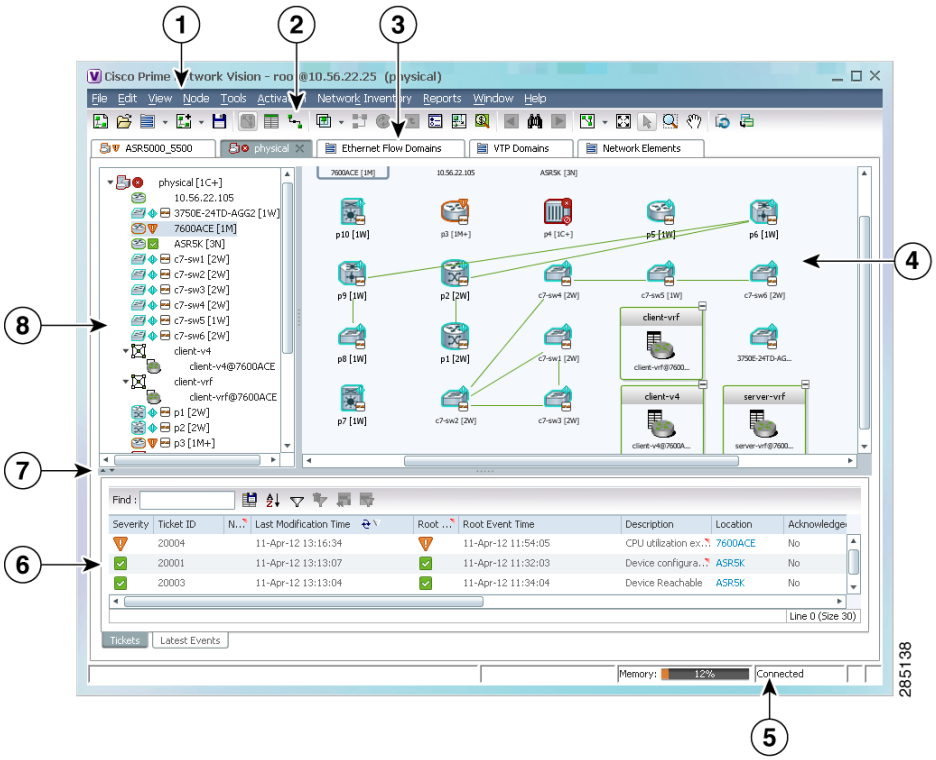
If you want the Vision client to prompt you to open the last map you used, you can configure it to do so as described in Changing Vision Client Default Settings (Sound, Display, Events Age), page 4-15.

Step 2 Select **File > Open Map** from the Vision client menu bar.

Step 3 Select a map and click **OK**.

Figure 7-1 provides an overview of the Vision client with an open map, followed by a description of the map window.

Figure 7-1 Vision Client Window with Map View



1	Main menu—Opening, closing, and changing map layouts, launching CCM, online help and icon reference, etc.	**5**	Status bar (shows commands sent to gateway, memory used by client, and gateway connection status).
2	Toolbar—Map tools, overlays, links, filters, NE labels, and zoom controls.	**6**	Tickets and latest events related to all NEs in the map.
3	Tabs for active maps, lists of managed NEs, and views for Ethernet Flow and VTP Domains, and Compute Services.	**7**	Toggle for hiding/displaying ticket pane.
4	Content pane showing map view—Shows the map NEs and their relationships. Colors such as red and orange indicate problems on the NE. See Troubleshooting a Ticket, page 11-12.	**8**	Inventory window—Displays all NEs in the map. Double-clicking an NE opens the physical and logical inventory for the NE in the content pane.

Why You Cannot See Everything in a Map or Perform All Actions in a Map

What you can see and do in maps is determined by your user account settings. If you try to view an NE but you do not have the required permissions, the Vision client will display an error message.

- NEs—If you do not have permission to view an NE, it is displayed with a lock. The Vision client will also not display tickets for those NEs.
- Links—If one of a link's endpoints is outside your permissions, the link is greyed-out.

- Vision client choices—If you do not have permission to execute a menu choice, button, and so forth, they are greyed-out.

These guide also apply when you view an NE's physical or logical inventory, or perform any actions from the inventory windows. Permissions are described in Permissions for Vision Client Maps, page B-2.

Saving a Changed Map Layout and Changing Map Display Defaults

When you close a map, Prime Network automatically saves most of your changes. If you made a change that Prime Network will not automatically save, the Vision client prompts you to manually save the map by clicking **Save Map Appearance** from the main toolbar.

You can also customize which items are displayed in maps, how items are displayed in maps, whether to use audio sounds, and when to remove NE tickets and events from the map. To change these settings, choose **Tools > Options** from the Vision client main menu. For more information, see Changing Vision Client Default Settings (Sound, Display, Events Age), page 4-15.

Interpreting NE Icons, Badges, and Colors

Tip To view an icon reference, choose **Help > Icon Reference** from the main menu.

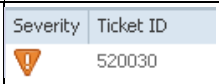
Are There Problems That No One Is Aware of?

The Vision client conveys critical information using colors and alarm badges. These can indicate a problem, its severity, and whether anyone is aware of the problem.

Alarm Badge	Color	Severity
	Red	Critical
	Orange	Major
	Yellow	Minor
	Light Blue	Warning
	Medium Blue	Information

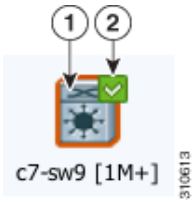
Alarm Badge	Color	Severity
	Dark blue	Indeterminate
	Green	Cleared, Normal, or OK

These examples show how an NE with a major ticket is displayed, depending on where you are in the Vision client.

Value	Navigation Pane	Map	Ticket Pane
Element with ticket of Major severity			

The alarm badge is displayed on top of a managed NE icon. In Figure 7-2 the NE icon is for a Cisco MDS device.

Figure 7-2 What NE Icon Badges Signify

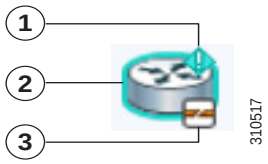


	Description	What this example shows:	Conclusion:
1	Network element icon and color: • Icon represents NE type • Color represents NE's most serious ticket that has *not been cleared* (*cleared* means it is no longer a problem)	NE is a Cisco MDS device. Orange means the NE has at least one *uncleared* ticket, and its severity is Major.	The NE still has a Major uncleared ticket.
2	Color represents NE's most serious ticket that is *unacknowledged* (*acknowledged* means someone is aware of the problem)	Green means the NE has no *unacknowledged* tickets.	Someone is aware of the NE's Major uncleared ticket.

Is The Device Working Properly?

A badge displayed at the bottom right of the icon signals a reachability problem between Prime Network and the device, as shown in Figure 7-3.

Figure 7-3 Element with Overlay Badges



	Description	What this example shows:	Conclusion:
1	Color represents NE's most serious ticket that is *unacknowledged*	Light blue means the NE still at least one *unacknowledged ticket*, and its severity is Warning.	No one is aware of the NE's uncleared Warning ticket.
2	Network element icon and color: • Icon represents NE type • Color represents NE's most serious ticket that has *not been cleared* (that is, the problem no longer exists)	NE is a Cisco 7600 router. Light blue means the NE still at least one *uncleared* ticket, and its severity is Warning.	The NE still has an uncleared Warning ticket.
3	Icon represents the state of the device	The Cisco 7600 router is only partially reachable.	There may be a communication problem between Prime Network and the 7600 router.

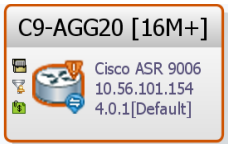
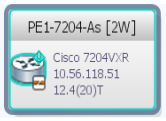
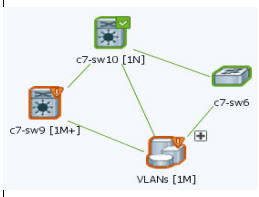
A complete list of all NE icons, severity icons, and device reachability icons is provided in Icon Reference, page A-1. For information on how to respond to NE tickets, see Managing Tickets with the Vision Client, page 11-1.

Zooming In and Out To Get More Details

Use these menu choices to manipulate a map:

From Vision Client Main Menu	To do the following
View > Zoom In	Zoom in on the map
View > Zoom Selection	Select an area in a map to zoom in on by clicking and dragging
View > Fit In Window	Fit the entire map in the display area
View > Pan	Move around in a map by clicking and dragging
View > Zoom Out	Zoom out of the map.

As you zoom in, the Vision client displays more NE detail. As you zoom out, the Vision client displays the NE's topological relationships, as shown in the following examples.

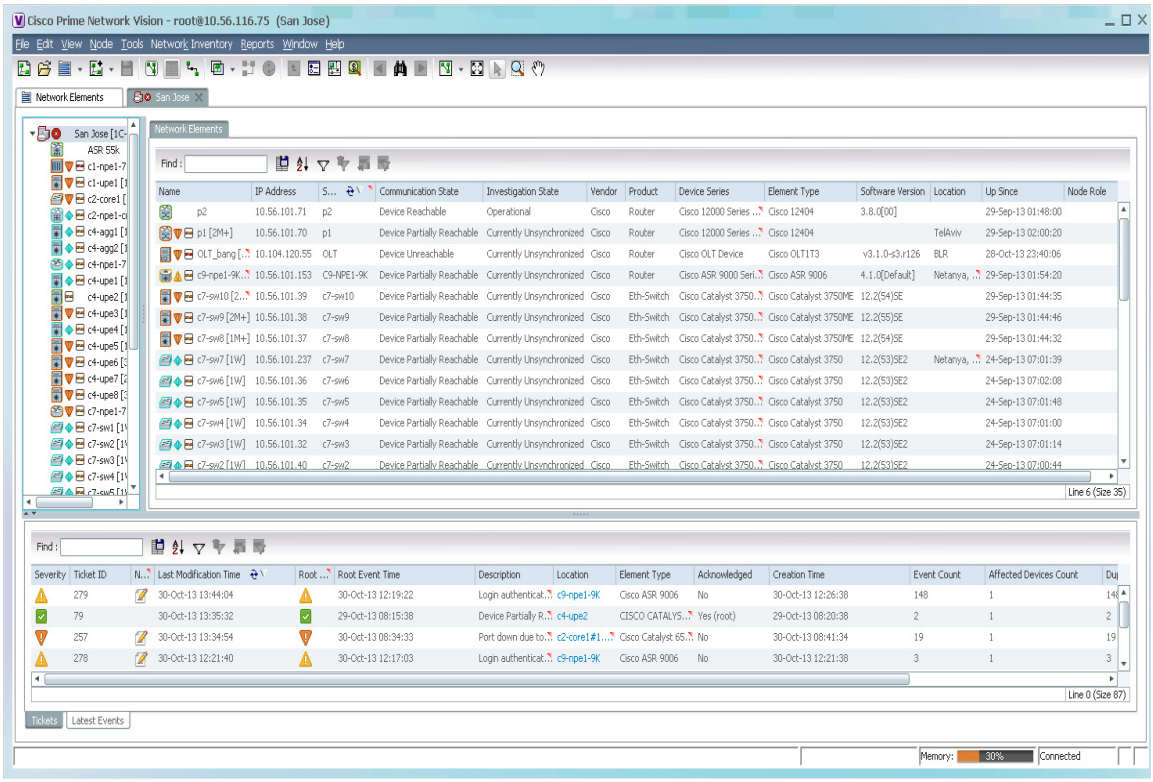
Huge	Large	Normal	Tiny (Overview)
			

Viewing a Table of NEs and Their Properties (List View)

To get a quick look at the properties of devices in a map, change to a list view by clicking **Show List View** from the Vision client toolbar. This view provides a table of all NEs with details about IP addresses, the device model and software image it is running, how long it has been up, and virtualization information.

Note If a cell's contents do not fit in the table, hover your mouse cursor over the table cell.

Figure 7-4 Vision Client Window with List View



The Network Elements tab lists all NEs in the map which you have permission to view. If you do not have permission to view a map's NE, it is listed under the Restricted Elements tab and displayed with a lock icon. From here you can perform the following operations:

To perform this table operation:	Click this toolbar button from List View:	Button Name
Searches for the string you enter		Find
Exports the selected information to a CSV file		Export to CSV
Arrange existing data according to sort operations that you specify (see Sorting Tables, page 7-9)		Sort Table Values
Only display information that matches the filter (see Filtering Tables, page 7-10)		Filter
Clear the existing filter		Clear Filter

To perform this table operation:	Click this toolbar button from List View:	Button Name
Display all table rows that meet the current filtering criteria		Show All Rows
Display only selected table rows		Show Only Selected Rows

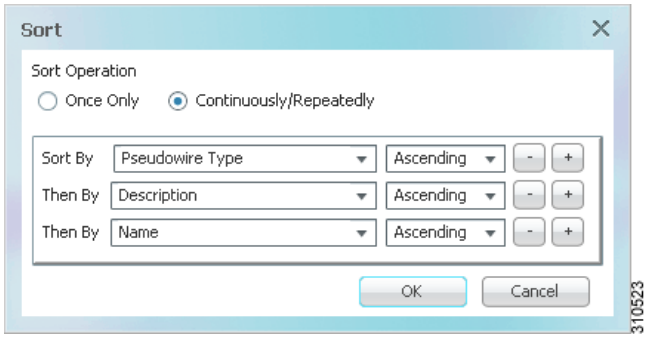
These topics explain how to sort and filter tabular information.

Sorting Tables

Sorting a table lets you arrange existing data in various ways, while filtering a table only displays the information that matches the filter.

Step 1 In the table toolbar, click **Sort Table Values**. The Sort dialog box is displayed.

Figure 7-5 Sort Dialog Box



Step 2 In the Sort Operation field, specify the frequency of the sort operation:

- Only Once—Sorts the information in the table only once according to the specified criteria. When this option is selected, newly added rows will always be listed at the bottom of the table, regardless of their sort criteria value. Also, if an existing row's value changes, the row will remain where it is.
- Continuously/Repeatedly—Sorts the information in the table continuously according to the specified criteria.

  If you select this option, the  icon is displayed next to the selected column heading.

Step 3 In the Sort By field, specify the first sort criterion:

a. In the first drop-down list, choose the column to use for the first sort criterion.

b. In the second drop-down list, choose **Ascending** or **Descending** to indicate the sort order.

Step 4 Add and adjust the criteria as needed, and click **OK**. The table data is sorted.

Filtering Tables

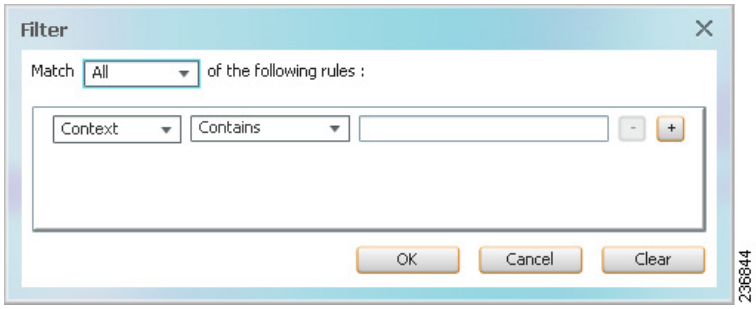
Use filters for tables that contain many entries. You cannot apply a filter until the table has loaded; for tables with many entries, this can take a while. Once the entries are populated, the filter tool becomes available.

You can check whether a filter is applied by hovering your mouse cursor over the filter button.

Note These operations are performed from the table of NEs in a List View. These filters are different from filters that can be configured, saved, and used at a later time. For information on those filters, see Viewing Tickets and Latest Events for All Devices in a Map, page 11-3

Step 1 In table toolbar, click **Filter**. The Filter dialog is shown in Figure 7-6.

Figure 7-6 Table Filter Dialog Box



Step 2 In the Match drop-down list, choose **All** or **Any**.

Step 3 For each criterion, specify the following:

a. In the first drop-down list, choose the primary match category (the drop-down list contains all table columns).

b. In the second drop-down list, choose a rule.

c. In the third field, choose from the available values, or enter text (using a drop-down list or free text).

Tip You can use the "Greater than" or "Less than" rule with a string for filtering. For example, if you want to include all interfaces above Ethernet0/0/3, you can select **Greater than** and enter the string `Ethernet0/0/3` to view interfaces Ethernet0/0/4, Ethernet0/0/5, and so on.

Step 4 Click + to add another criterion.

Step 5 Add and adjust the criteria, then click **OK**. The table data is displayed using the defined filter.

How to Find Entities Inside and Outside Of Maps

The Vision client provides a variety of ways to locate the NEs, technologies, and services you are interested in by using search, filters, business tags, and overlays. If you do not have sufficient permissions to view an NE, it is displayed with a lock icon. If you try to view the NE details, the Vision client displays a warning message.

To search for:	See this section or use this method:
NEs by name or IP address	Finding NEs Using Basic NE Information (Name, Vendor, IP address), page 7-12
NEs by vendor	
NEs by model number (12404) or device type (router)	
NEs by device series (Catalyst, Nexus, 3750)	Finding NEs Using Advanced Filters, page 7-12
NEs by software version	
NEs with tickets of certain severities	
NEs with unacknowledged tickets	
NEs by connectivity state (down, up	
NEs with Data Center virtual devices and associated virtual machines	
NEs with Data Center associated compute servers	
NEs affected by a ticket	Right-click ticket and choose **Find Affected Elements**
NEs by their label (customer or subscriber names, provider connections)	Finding NEs By Searching for NE Labels, Subscribers, and Provider Connections, page 7-13
NEs in current map, using a search string	**Edit > Find in Map**
Maps that contain specified NEs	Right-click the NE and choose **Open Relevant Maps**
Link types: Data links, physical links, VPN links	Using Link Filters to Find Links, page 7-21
Links by their level	Table 7-1 on page 7-25
Ethernet Flow Domains	**Network Inventory > Ethernet Flow Domains** from Vision client main menu
VTP Domains	**Network Inventory > VTP Domains** from Vision client main menu
Services: Ethernet, MPLS-TP tunnels, network clock, pseudowire, VLAN, VPLS, VPNs	Finding Services Using Map Overlays, page 7-17
Network TP tunnels	Click **Show List View**, then click TP Tunnels tab

Finding NEs Using Basic NE Information (Name, Vendor, IP address)

Use this method when you have a large number of NEs to find the NEs that match your criteria.

Note You do not have to clear the results to start a new search. The Vision client always starts the search using all managed NEs.

Step 1 From the Vision client, click the Network Elements tab.

Step 2 Click **Search**.

Step 3 Enter the search criteria. It is not case sensitive, and you can enter fragments.

Criteria	Examples	Example Search Strings
Element type—NE model	Cisco 12404	12404, 124, 12
IP address	198.51.100.1	198, 51, 198.51
Name—Name assigned when NE was added using the Administration client	c7-sw6	c7, sw, c7-
Product—NE family	Eth-switch	Eth, switch
System name—Name from NE MIB	p1	p1, p, 1
Vendor	Cisco	cisco, cisc, Cis

Click **Go**. The Vision client lists all devices that match your criteria, and which you have permission to view.

To start a search using different criteria, you do not have to clear the results. Just select your new choice from the drop-down list and enter your criteria.

Step 4 To open the NE's inventory, double-click the NE from the list.

Finding NEs Using Advanced Filters

Use this method to search for NEs by advanced criteria, such as communication state, ticket severity, and similar detailed criteria. Some of the criteria provide drop-down lists for choices.

These filter buttons are listed above the table of NEs.

	Filter—Turn on filter. If a filter is currently applied to the table contents, hover over this button to display the filter rules (such as **'Name' Contains Cisco**).
	Clear Filter—Turn off filter and revert to original list. If this button is enabled, a filter is currently applied to the table contents.

Step 1 From the Vision client, click the Network Elements tab.

Step 2 Click **Show All**. (Depending on the number of NEs, the table may require a few minutes to load.) Devices that you do not have permission to view are displayed with a lock.

Step 3 Click the **Filter** button and enter the search criteria using the logical operators to create rules.

Criteria	Example Search Strings
Severity	N/a; drop-down list
Unacknowledged	
Device communication state Device investigation state	
Vendor	
Product	
Device software versions	12.2, SG2, 3.8
Device series	Nexus, Catalyst, CRS, 3750
Location	Bangalore, Bang, Jose, San Jose, San
Up Since (dd-mm-yyyy)	3-May, 2013, Aug
Node role	primary, standby, secondary

Step 4 Click **OK**. To start a search using different criteria, clear the results by clicking the **Clear Filter** button.

Step 5 To open the NE's inventory, double-click the NE from the list.

Finding NEs By Searching for NE Labels, Subscribers, and Provider Connections

A *business tag* is a string that is meaningful to the business, and which can be used to label a component of a network element for use in Prime Network screens and reports. Business tags allow you to label NEs in the manner that best fits your deployment.

Business tags are normally applied to *business elements*, which are constructions or organizations of certain network elements and their properties into a logical entities (for example, Layer 2 VPNs, Layer 3 VPNs, and virtual routers).

To search for a business tag:

Step 1 Choose **Edit > Find Business Tag** from the main menu.

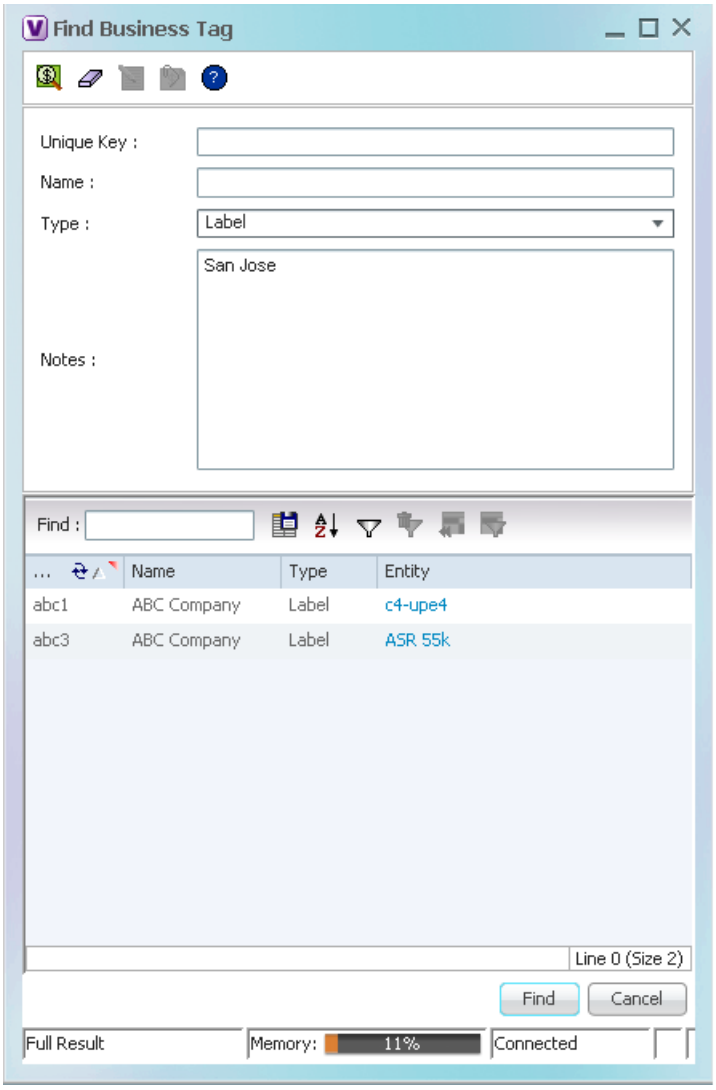
Step 2 In the Find Business Tag dialog box, enter the search criteria.

These are some examples of the criteria you can enter:

Field	Enter:	Vision client will search for NEs with business tags that:
Unique Key	Letter or number string	Have a unique key that contain the string
Name		Have a business tag name that contains the string
Notes		Have notes that contain the string
Type	From drop-down list	Have a business tag of that type (Label, Subscriber, Provider Connection, All types)

Step 3 Click **Find Business Tag**. Figure 7-7 shows the results of a search for any label type business tags with notes that contain the string **San Jose**.

Figure 7-7 Find Business Tag Dialog Box With Results



Double-click the entity hyperlink to open the NE's inventory window. If the results display an NE with a lock icon, it means you do not have sufficient permissions to view it.

Finding Out Which Maps Include an NE

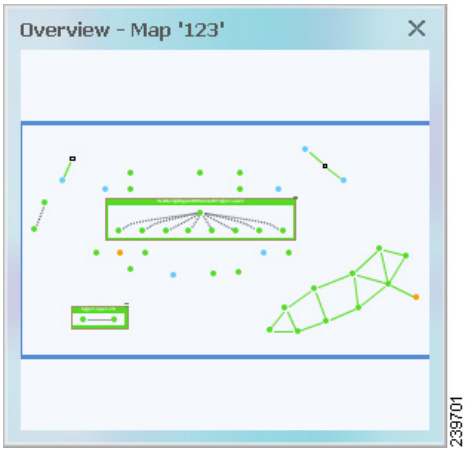
If you have a problematic NE, you may want know all other maps that include the NE to get an overall view of the impact of the NE's ticket. To find out which maps include a specified NE, right-click the NE in a map and choose **Open Relevant Maps**. The Vision client will display the Open Map dialog box with a list of all maps that include the selected element. From there, you can open the maps in which you are interested.

Viewing Very Large Maps Using an Overview Window

The Overview window provides a condensed view of all elements in a map. This is especially useful for large maps.

Step 1 To open the Overview window, choose **View > Overview** from the main menu. Figure 7-8 shows an example of the Overview window. If you do not have permission to view an NE, it is displayed with a lock icon or greyed-out.

Figure 7-8 Overview Window



Note To view an icon reference, choose **Help > Icon Reference** from the main menu.

Dots represent elements, lines indicate links, and the blue rectangle represents the current selection area. In other words, when you open the map named 123, it displays all of the items inside the blue rectangle.

Step 2 To change the overview:

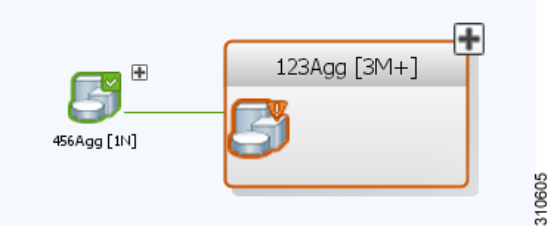
a. Click inside the blue window and drag the rectangle to the desired map area.

b. Use the corner handles to resize the selection area.

Drilling Down Into NE Groups (Aggregations)

Tip To view an icon reference, choose **Help > Icon Reference** from the main menu.

Aggregations are groups of NEs. An aggregation can contain network elements, services, and other aggregations. Aggregations are displayed as a single entity, as shown in the following figure.



If you cannot create an aggregation, it is because you do not have a sufficient user access level, or you do not have permission to manage the NE.

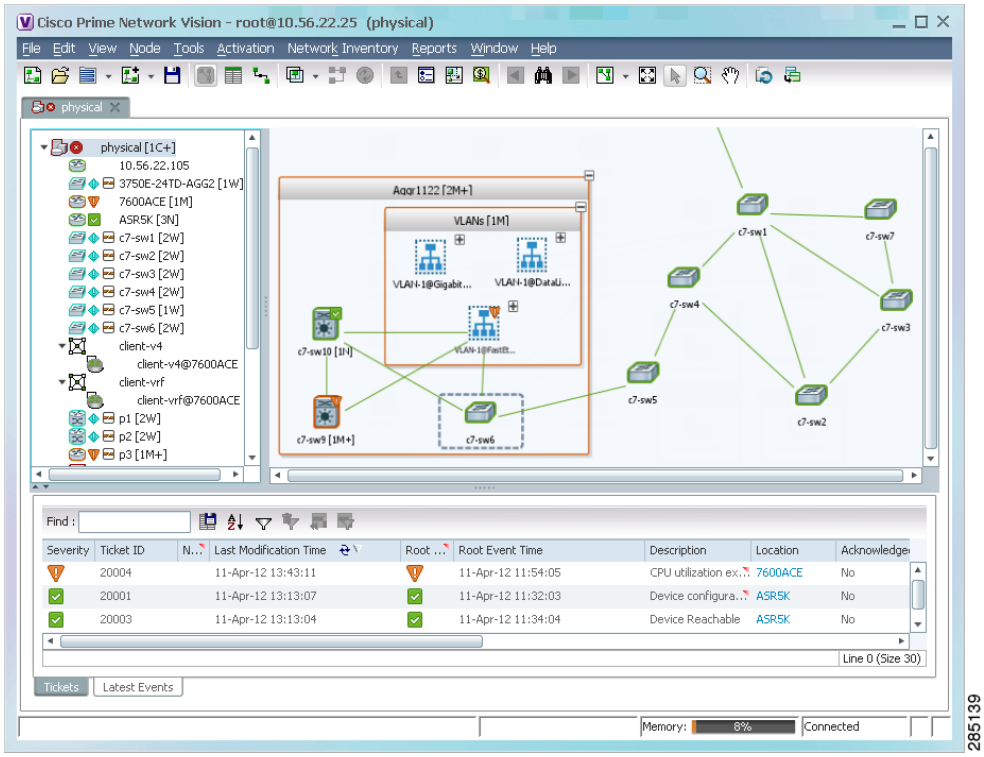
To view an aggregation's contents, expand (open) it by right-clicking the aggregation and choosing **Show Thumbnail**. A thumbnail is an aggregation that has been opened. The Vision client will adjust the location of other NEs in the map so you can view the thumbnail contents, and then move them back when you close the thumbnail. As you traverse an aggregation, you will need to know the meaning of these terms:

- The aggregation *parent* is the next level up.
- The aggregation *root* is the map that contains the aggregation.

Figure 7-9 provides an example of two aggregation thumbnails— **Aggr1122** and **VLANs**. In this example, the Aggr1122 aggregation contains the VLANs aggregation. The dashed gray border around c7-sw6 indicates that c7-sw6 resides inside the **Aggr1122** thumbnail but not at the current map level.

Note Multi-chassis devices are also displayed as aggregations.

Figure 7-9 Aggregation Thumbnails



This table lists the ways to move between aggregations and parent maps.

If you want to...	Do this...
View and drill into only the aggregation (not other NEs in the map)	Double-click the *thumbnail frame* (or the aggregation itself, if it is closed)
From an aggregation, go up one level (parent level)	Double-click the *inner level background*
Open and close thumbnail	Click the plus/minus sign at the top right of the aggregation

Finding Services Using Map Overlays

When you apply an overlay to a map, you can isolate the parts of a network that are being used by a specific service such as VPLS, network pseudowire, MPLS-TP tunnels, and so forth. Prime Network models and manages many more technologies and services which you can view from a device's inventory window. Those technologies and services are described in other topics in this guide.

Applying a Map Service Overlay

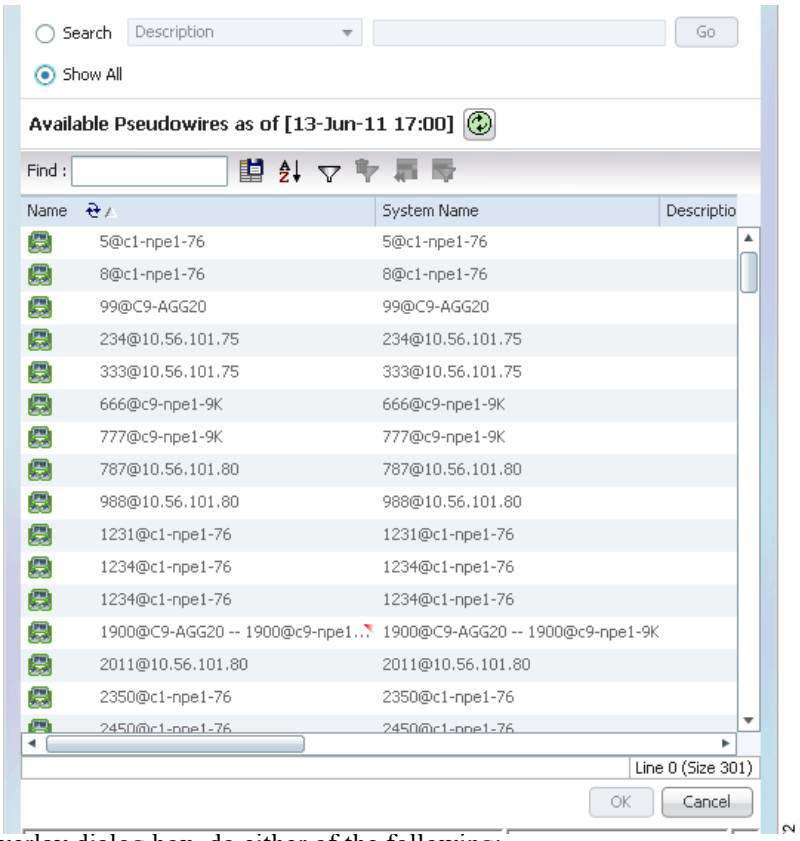
Step 1 From the map toolbar, choose **Choose Overlay Type >** *overlay-type*, where *overlay-type* is one of the following.

Overlay Option	Search Criteria
Ethernet Service	EVC Terminating EFPs, ethernet service name, system name. See Applying Ethernet Service Overlays, page 18-126.
MPLS-TP Tunnel	Description, MPLS-TP tunnel name, system name. See Applying an MPLS-TP Tunnel Overlay, page 17-17.
Network Clock	Name. See Applying a Network Clock Service Overlay, page 26-48.
Pseudowire	Description, Is Multisegment Pseudowire, pseudowire name, pseudowire role, pseudowire type, system name. See Applying Pseudowire Overlays, page 18-115.
VLAN	EFD name, EFD system name, VLAN ID, VLAN name, system name. See Displaying VLANs By Applying VLAN Overlays to a Map, page 18-77; Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 18-80; and Viewing STP Information in VLAN Domain Views and VLAN Overlays, page 18-83.
VPLS	Name, system-defined name, VPN ID. See Applying VPLS Instance Overlays, page 18-98 and Viewing Pseudowire Tunnel Links in VPLS Overlays, page 18-99.
VPN	Description, VPN name. See Applying VPN Overlays, page 17-25.

The dialog box also displays the date and time at which the list was generated. To update the list, click **Refresh**.

Step 2 Select the overlay that you want to apply to the map. Figure 7-10 shows an example of the Select Pseudowire Overlay dialog box.

Figure 7-10 Select Pseudowire Overlay Dialog Box



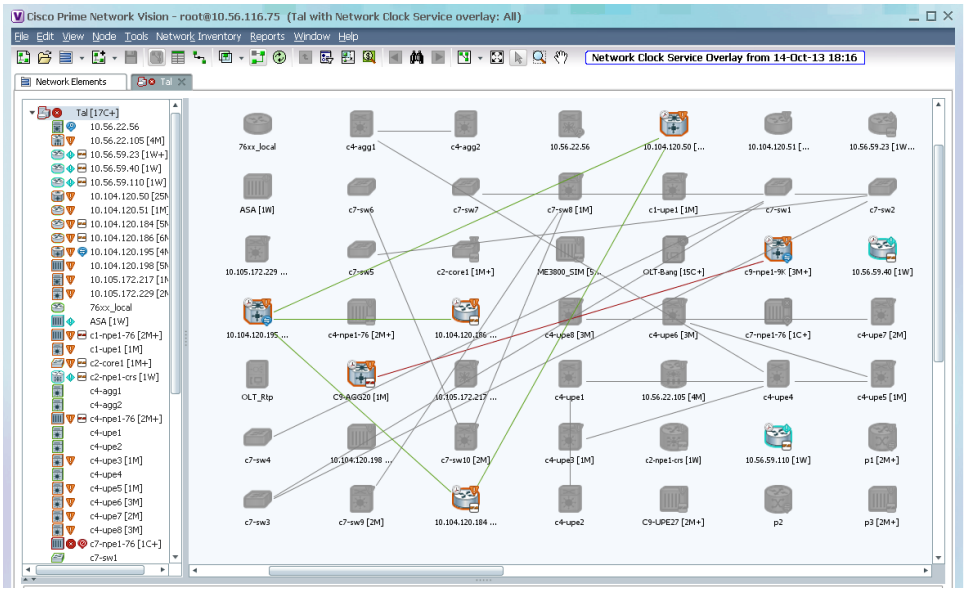
Step 3 In the Select Overlay dialog box, do either of the following:

- Choose **Show All** to list all overlays of that service type.
- Choose **Search** to find the service using the following criteria. (Search strings are case-sensitive.)

Step 4 Click **OK**, and the elements and links that are used by the overlay are displayed in the map, and the overlay name and date are displayed in the toolbar.

Note The overlay is a snapshot taken at a specific point in time. To update the overlay, click **Refresh Overlay** in the toolbar.

Figure 7-11 Clock Service Overlay Example



Hiding and Removing Service Overlays from a Map

To temporarily hide an overlay or remove it completely:

- Temporarily hide a map overlay by clicking **Hide Overlay/Show Overlay** in the toolbar. The button toggles depending on whether the overlay is currently displayed or hidden.
- Delete an overlay from the map by choosing **Choose Overlay Type > None**.

Viewing and Managing Links

Links are the physical and logical connections that exist between elements in the network. You can get link property information for links that are:

- Between two devices.
- Between a device (Device A) and an aggregation, where a device inside the aggregation is connected to Device A.
- Between two aggregations that contain devices that cross the aggregations.

In Vision client maps, a single link can actually represent multiple links—for example, a physical ethernet link and an MPLS link. Drill down into the link to get this information. These topics explain how to manage links using the Vision client:

- Using Link Filters to Find Links, page 7-21
- Interpreting Link Colors, Widths, and Symbols, page 7-21
- Viewing Link Details, page 7-22
- Checking the Impact of Link Problems (Impact Analysis), page 7-27
- Managing Missing Links (Static Links), page 7-29

Using Link Filters to Find Links

Use a link filter when you want to locate specific link types, such as physical links, VPN links, data links, and so forth. Sometimes it may not be clear if a link filter is already applied to a map. To verify whether a map is using a link filter, check the map toolbar.

	A link filter is applied to the map. To clear the filter, click this icon and choose **None** from the Group drop-down list.
	A link filter is not applied. To apply a link filter, see Using Link Filters to Find Links, page 7-21.

To create a link filter:

Step 1 Click **Link Filter** in the main toolbar.

Step 2 Select the specific links you want to view, or select a links group from the drop-down list.

To display these links:	Choose
Data links (ATM, Frame Relay)	Data
Physical layer links	Physical
VPN links (GRE, Pseudowire, VPN, VPN IPv6)	VPN
Link types that you want to choose (your choices will be saved for the next time you open the link filter)	Custom
All links	All

Step 3 Click **Apply** and **OK**. If any links are grey, it means you do not have sufficient permissions to view them. By default, the Vision client only displays a link if you have permission to view both of the link's end points.

If you want to remove the filter later (and show all links), repeat the previous steps but choose **All** from the group drop-down list.

Step 4 To interpret the information displayed by the Vision client, see Viewing Link Information Displayed at the Map Level (Tool Tips and Quick View), page 7-23.

Interpreting Link Colors, Widths, and Symbols

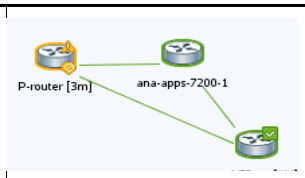
The following tables provide keys for understanding the link information displayed by the Vision client.

Link Colors:

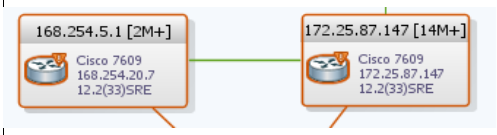
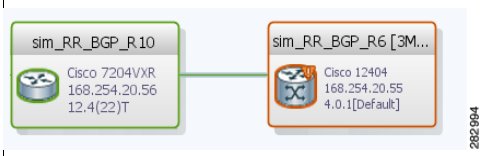
Link has a critical alarm	Red	
Link has a major alarm	Orange	
Link has a minor alarm	Yellow	

Link is operating normally	Green	
Link is selected	Blue	

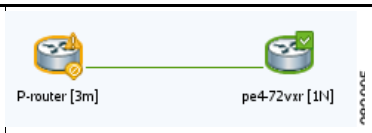
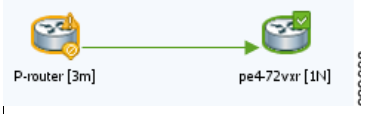
Solid or Dashed Link 5.3

Physical, topological, or service link, such as a link between two devices.	Solid line	
Association or *business link* between such elements as EVCs, VPLS service instances, or VPN components.	Dashed line	

Link Widths

Link represents multiple links of the same group (business, GRE, MPLS-TP, Pseudowire, VLAN, all others)	Normal width	
Line represents an *aggregated link* that contain links of different groups. Use high zoom level to view aggregated links.	Wide width	
Line represents a tunnel, with the center color representing the severity of any alarms on the link.	Tunnel	

Arrowheads

Bidirectional link	No arrowhead	
Unidirectional link, with the flow in the direction of the arrowhead	Arrowhead	

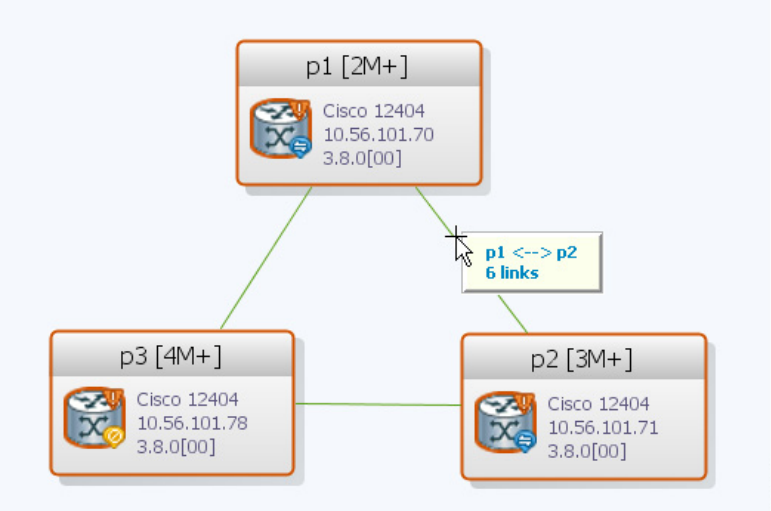
Viewing Link Details

These topics explain how to traverse from the map level down to the link property details:

Viewing Link Information Displayed at the Map Level (Tool Tips and Quick View)

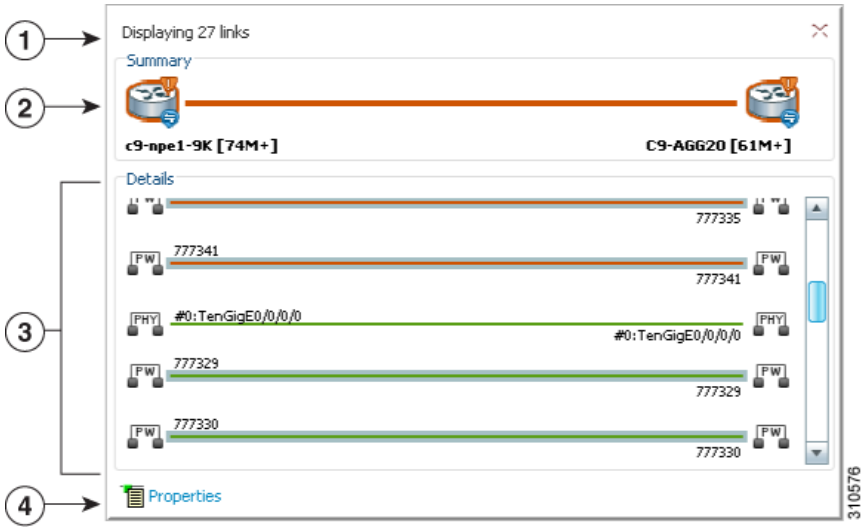
To view the link count and end points, hover your mouse cursor over the link to display the link tool tip, as shown in the following figure.

Figure 7-12 Vision Client Window with Link Tooltip



To display the link quick view, click the tooltip.

Figure 7-13 Link Quick View Example



The link quick view in Figure 7-13 provides the following information.

1	Number of links represented by the single link in the map (in this example, 27 links).
2	Link endpoints.
3	List of all links represented by the link, including the link type, detail, and alarm status (color). This example shows 3 pseudowire links and one physical link.
4	Hyperlink to the link properties window. The Properties button is available for physical, topographical, and service links, but is not available for business links (dashed links). See Viewing Link Status and Detailed Link Properties, page 7-25.

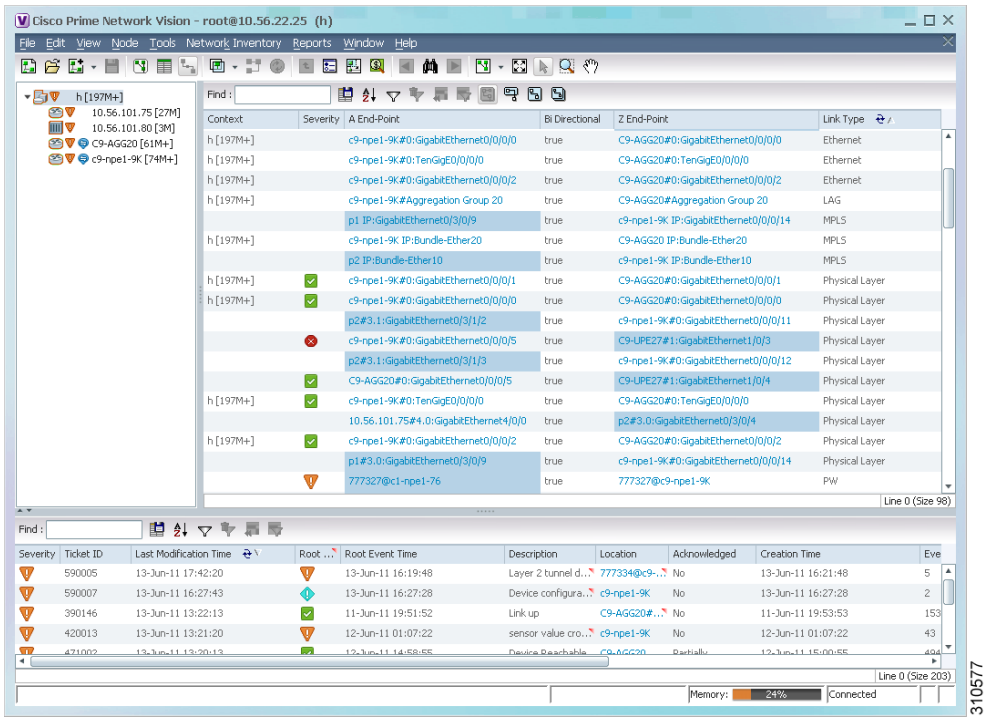
View Links at Different Levels in Aggregations and Maps (Links View)

You can launch a links view from a map or from an aggregation thumbnail. When you open the links view, it shows links at the current level and for all nested aggregations (all links must have both endpoints in the map or aggregation).

To open a links view, click **Show Links View** from the main toolbar. Figure 7-14 shows an example of the links view launched from a map view.

Note If some links are missing, your map may be using a link filter. To clear a link filter, click Link Filter, choose **All** from the group drop-down box (to display all links), and click **Apply** and **OK**.

Figure 7-14 Links View



Note the following:

- The context field may be empty if one side of the link is not included in the map, or the link is filtered out of all contexts. A blue background indicates an external link (a link with only one endpoint in the map or aggregation).
- The A End-Point is the element or site that is the source of the link; The Z End-Point is the destination. For unidirectional links, traffic is from A to Z.

Note If you load a map with many links (for example, thousands of links), it can take a while for the complete list of links to load. The filtering options in the table are unavailable until the table has completely loaded.

The links view provides buttons that allow you to traverse among link levels, as follows:

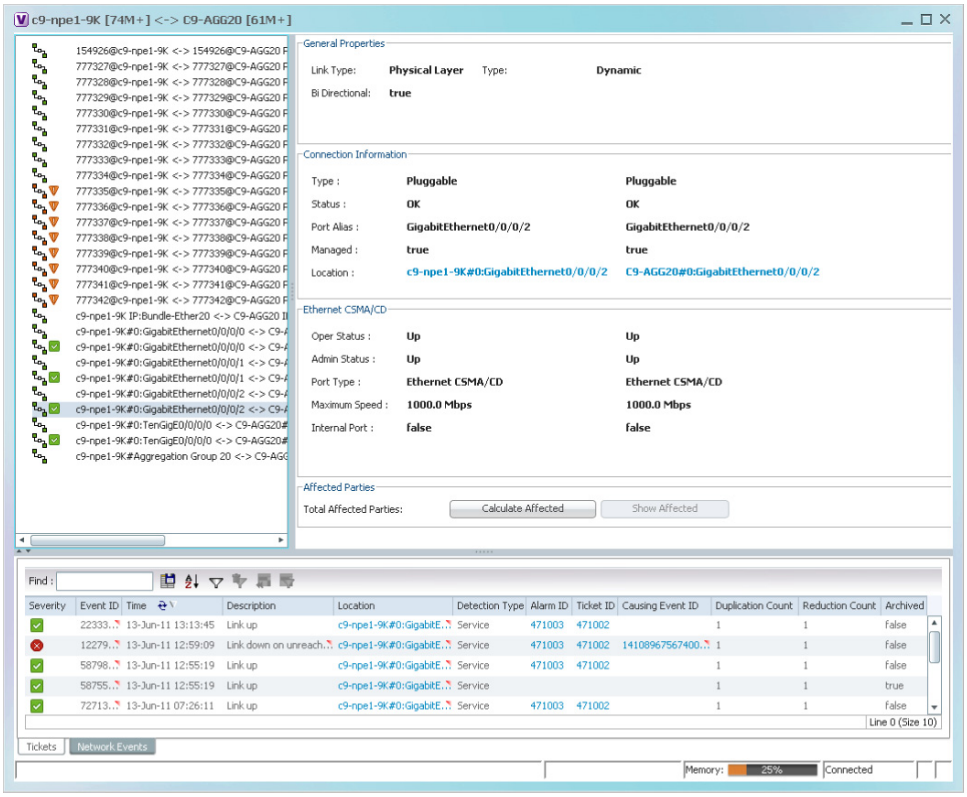
Table 7-1 Ways to Traverse Link Levels

To do the following:	Do the following, or click icon:
View a link in a map	Right-click link and choose **Select Link in Map** (link will be blue)
View all link properties (see Viewing Link Status and Detailed Link Properties, page 7-25)	Right-click link and choose **Properties**
Display all links the map or selected aggregation, including external links (All Links icon).	
Display links that have only one side in the selected map or aggregation (External Links). (These are indicated with the blue background in the previous figure.)	
Display links in the selected map or aggregation, excluding links in any closed aggregations (Flat Links).	
Display for the selected aggregation and any nested aggregations with both endpoints in the map or aggregation (Deep Links). This is the default.	

Viewing Link Status and Detailed Link Properties

To view link details, click the link (it will turn blue), then right-click the link and choose Properties. As shown in Figure 7-15, the link properties window provides general information about the selected link, details of the link connection, and technology-specific information appropriate for the link. If multiple links exist between the elements or aggregations, the link properties window displays information for all the links.

Figure 7-15 Link Properties Window



The links listed on the left display the left and right link identifiers between the two nodes, the device alias, and the Connection Termination Point (CTP). When you select a link, the properties area is populated with extensive information about the selected link, most of which is self-explanatory. These items are especially important:

- Under General Properties, the type can be either dynamic or static.
  - Dynamic links are real links between devices or aggregations.
  - Static links are not real links, but are created by Prime Network advanced users to represent a real link (for example, when a real link is not discovered). Static links provide allow Prime Network to perform correlation flows through the link.
- Link status is displayed under the Connection Information.

Speed, port type, port admin and operational status, and other information is displayed for connections of types such as Ethernet CSMA/CD, Gigabit Ethernet, LAG, MLPPP, MP-BGP, MPLS Link Information, PPP, Pseudowire, T1, and VRF.

Users with advanced privileges can click **Calculate Affected** to see which resource pairs would be impacted by a problem with the link. (If the link had a ticket, the same information would be automatically generated and displayed in the ticket under the Affected Parties tab.) See Checking the Impact of Link Problems (Impact Analysis), page 7-27.

These tools are provided for working with specific technologies:

- **Labels**—For Ethernet links, lists all LSPs and their source and destination labels. For more information, see Viewing LSPs Configured on an Ethernet Link, page 17-13.
- **VCs**—For ATM links, lists configured and misconfigured VCs. For more information, see Viewing ATM VPI and VCI Properties, page 26-10.

Checking the Impact of Link Problems (Impact Analysis)

The Vision client provides a feature that, for a selected network link, calculates the elements that might be affected if the link were to go down.

Note Impact analysis applies only to physical links.

To calculate impact analysis:

Step 1 Select a map or aggregation in the navigation pane, and click **Show Links View** in the main toolbar. The links view is displayed in the content pane.

Step 2 In the table toolbar, click **Link Filter**. The Link Filter dialog box is displayed. For information about the Link Filter dialog box, see Using Link Filters to Find Links, page 7-21.

Step 3 In the Filter dialog box:

a. In the Match drop-down list, choose **All**.

b. In the field drop-down list, choose **Link Type**.

c. In the operand drop-down list, choose **Equals**.

d. In the matching criteria drop-down list, choose **Physical Layer**.

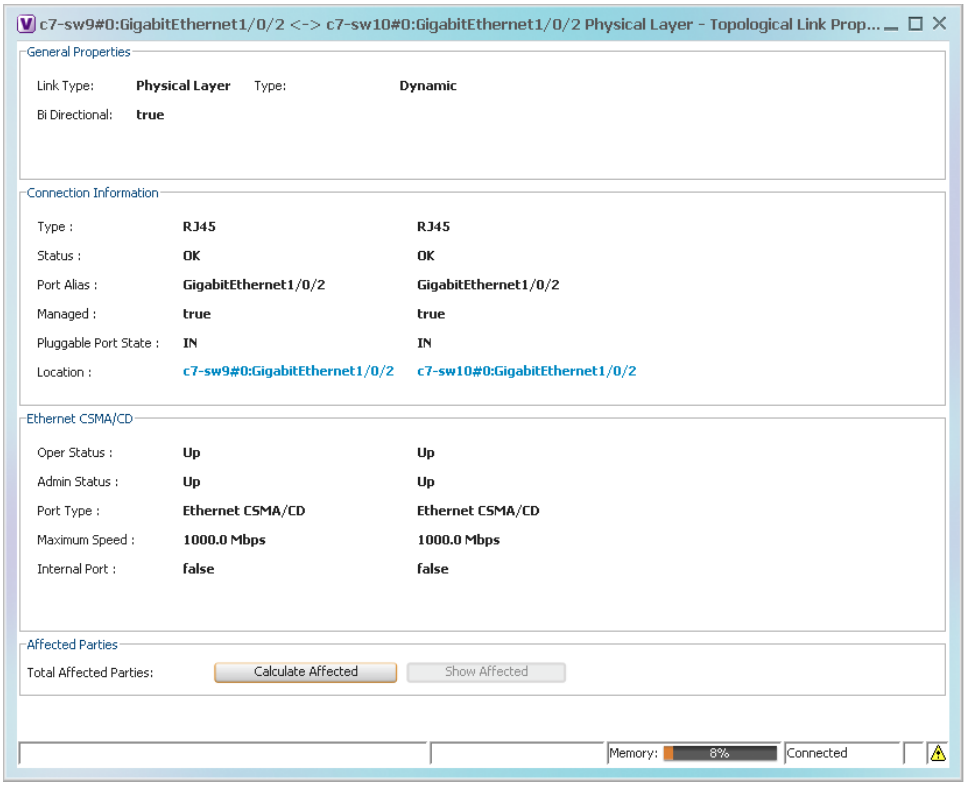
e. Click **OK**.

Only physical links are displayed in the links view.

Step 4 In the links view, right-click the required link and choose **Properties**. The Topological Link Properties window is displayed.

Note Resize the window as needed to view all the information.

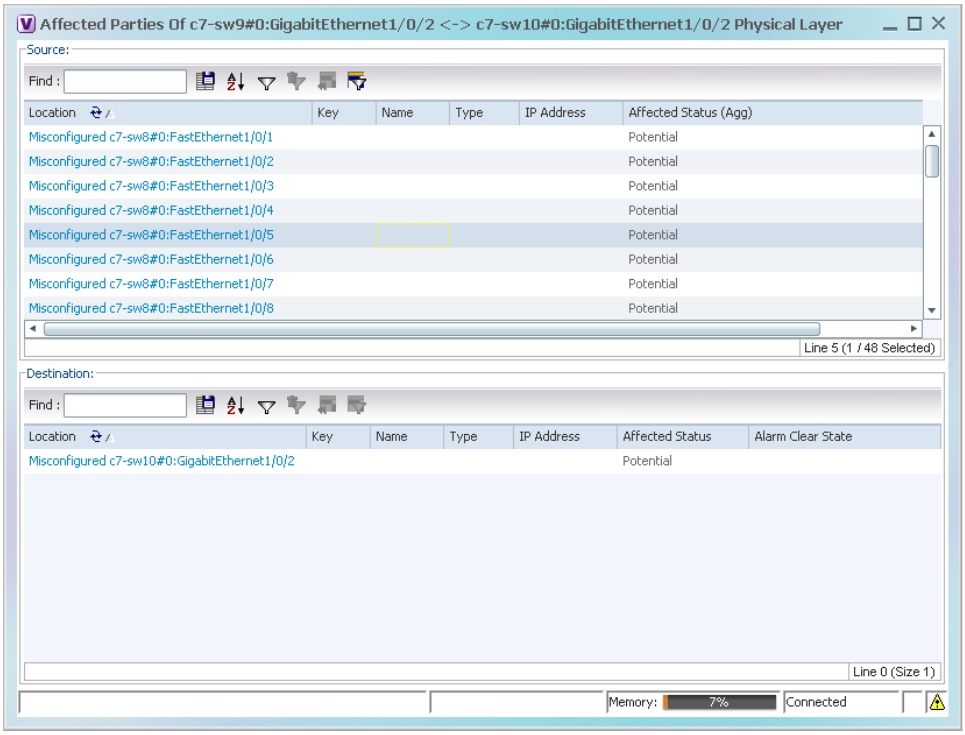
Figure 7-16 Topological Link Properties Window



Step 5 Click **Calculate Affected**. The total number of potentially affected parties is displayed in the Affected Parties area.

Step 6 Click **Show Affected**. The Affected Parties window is displayed as shown in Figure 7-17. For information on the status (Potential, Real, Recovered), see Viewing a Ticket's Affected Parties Tab (Resource Pairs), page 11-15.

Figure 7-17 Affected Parties Window



Step 7 To view the potentially affected destinations if a link were go to down, click an entry in the Source table. The potentially affected destinations are displayed in the Destination table.

Step 8 To view source or destination properties in inventory, click the required hyperlinked entry.

Managing Missing Links (Static Links)

Prime Network allows you to create *static links* that do not perform any configuration or provisioning on a device or in the network. Static links are created in the Prime Network model and are not updated. Static links are useful for map visualization and network correlation; for example, if Prime Network does not discover a link that you know exists in the network, you can create a static link that is displayed in the map. For correlation purposes, Prime Network treats the static link as if it were a physical or logical link and allows correlation flows to go through the static link. Prime Network supports 10 or 100 Gigabit Ethernet link between an ASR9K device and Cloud VNE. Only advanced users can create static links; see Permissions for Vision Client Links, page B-6. For information on creating static links, see Managing Missing Links (Static Links), page 7-29.

Link Discovery and Flickering Ethernet Topology Links

Prime Network discovers topology links using various protocols, such as STP, CDP, and LLDP. In some situations, the link configurations themselves can prevent Prime Network from discovering the correct information. For example, if Layer 2 protocol tunneling is configured and the discovery protocols are tunneled, Prime Network can create an incorrect link. This scenario results in a flickering link that is

first created incorrectly due to tunneled discovery information, and then disconnected when the Prime Network counters test discovers that the counters on the edges of the link do not match. During the next topology cycle, Prime Network recreates the link, which is disconnected again during the counters test.

A link is considered flickering when it is connected, disconnected, and reconnected when using the same connection technique because the topology information is conflicting. When this situation occurs, Prime Network generates a system event with the message "Physical Link discovery inconsistent."

To prevent an ongoing cycle of link creation and disconnecting, Prime Network detects such case of flickering links, creates a system event with the message "Inconsistent Physical Link Discovery between *system:interface1* and *system:interface2*, and stops the link from flickering by disconnecting it.

To remedy the situation, we recommend that you wait until the link disappears from the map and then create a static link.

In addition, you can add a new link using the Administration client. For more information, see the *Cisco Prime Network 5.3 Administrator Guide*.

Adding a Static Link to a Map

Note Only advanced users can create static links. See Permissions for Vision Client Links, page B-6.

To create a static link, select a device or port and define it as the A side. Then define a second device or port as the Z side. Prime Network validates the new link after the two ports are selected. Validation checks the consistency of the port types (for example, RJ45 on both sides), and Layer 2 technology type (for example, ATM OC-3 on both sides).

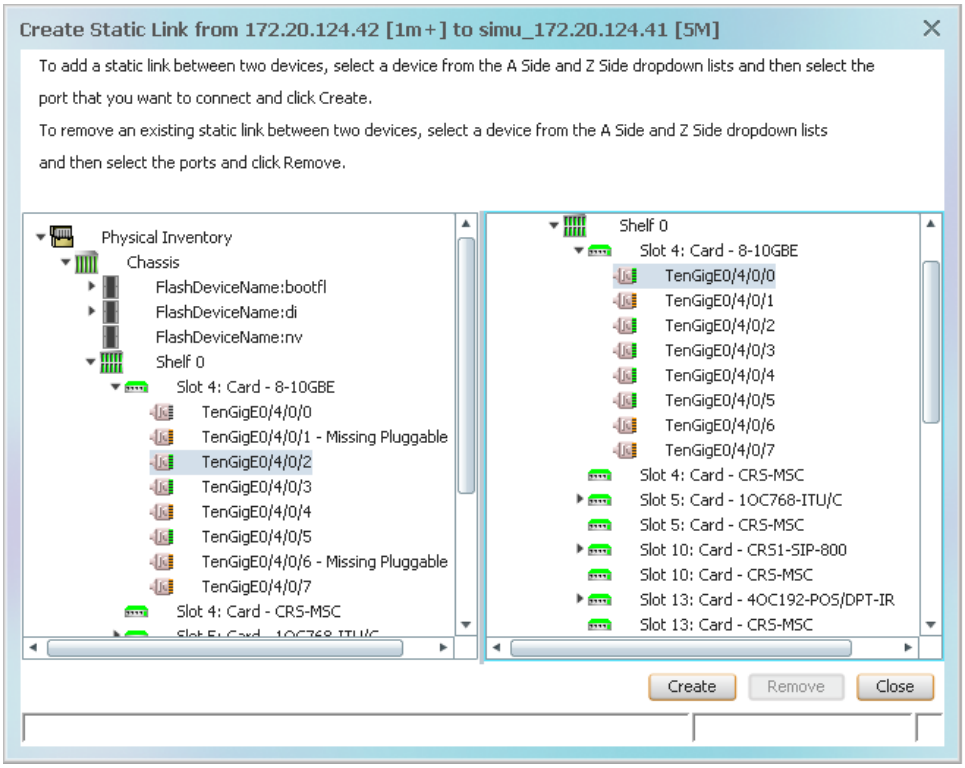
You can also create static links between Ethernet Link Aggregation Groups (LAGs) by choosing a LAG and the desired port channel for the A or Z side as described in the following procedure.

When you add a new link, the color of the link reflects its current state. For example, if the operation status of a port is down, the link is colored red. You can add links from either a map or from an NE's inventory window.

Step 1 Right-click the required A Side device in the navigation pane or in a map, and choose **Topology > Mark as A Side**.

Step 2 Right-click the required Z Side device or LAG in the navigation pane or properties pane to display the right-click menu and choose **Topology > Mark as Z Side**. The Create Static Link window is displayed as shown in Figure 7-18, so that you can select the ports to connect.

Figure 7-18 Create Static Link Window



Step 3 Select the required port on both the A Side device and the Z Side device.

Step 4 Click **Create** to validate the connection and create the new link.

A success message is displayed.

A warning message is displayed if any of the following apply:

- A validation check fails.
- The operation status of one port is Up and the other port is Down.
- The selected ports are not of the same type.
- The Layer 2 technology type is not the same.
- One of the ports is part of another link.

Adding a Link Using the Inventory Window

Step 1 Open the inventory window for the required A Side device.

Step 2 In the navigation pane, navigate to the required port or LAG.

Step 3 Right-click the required port or LAG and choose **Topology > Mark as A Side**.

Step 4 Repeat Step 1 and Step 2 for the Z Side port or LAG.

Step 5 Right-click the required port or LAG and choose **Topology > Mark as Z Side**. A confirmation message is displayed.

Step 6 Click **Yes.**

The ports are connected, and a link is created between the selected ports.

A warning message is displayed if any of the following conditions exist:

- One of the validation checks fails.
- The operation status of one port is Up and the other port is Down.
- The ports selected are not of the same type.
- The Layer 2 technology type is not the same.
- One of the ports is part of another link.

For information about removing a static link, see the *Cisco Prime Network 5.3 Administrator Guide*.

Making Changes to the Device Appearance in the Map

Maps present Prime Network's model of your network devices and connections. This information is constantly updated in a variety of ways to keep the model current. It is important to understand when you are making a change to the Prime Network *model* of a device versus when you are making a change to an *actual device*.

The following table lists actions you can perform from a map. These actions only affect the Prime Network model, not the real network element. Whether you can perform these actions depends on your permissions; see Permissions for Vision Client Maps, page B-2.

To do the following:	Right-click the NE in a map and select:
Change the name of an NE	Apply a business tag to the NE (seeLabelling NEs to Associate Them with Customers (Business Tags), page 4-9)
Add a virtual link between two devices so correlation can proceed through the link but no alarms are generated (for example, if a link goes down)	Right-click the device port or LAG and choose **Topology** (see Adding a Static Link When a Network Link is Missing, page 4-13)
Group the NE with other NEs in the map	Create an aggregation (see Grouping Network Elements into Aggregations, page 4-7)
Change the location of an NE in a map	Drag the NE to the desired location
Change the size of an NE icon	Right-click the NE and choose **Resize**
Change the size of the text that is displayed with the NE icon	Changing Vision Client Default Settings (Sound, Display, Events Age), page 4-15
Do not display an acknowledged badge with NE icon when ticket is acknowledged	
Only display severity status badge at NE icon level (not in NE inventory where event occurred)	

Prime Network provides many context-sensitive commands that you can use to make changes in the network. You can launch these commands by right-clicking an NE and choosing **Commands**. Your permissions determine whether you can run these commands, and the commands that are available depend on the device type, operating system, and if a service or technology is supported and enabled on the device. These commands are documented throughout this guide with the service or technology to which they apply. A complete list of commands, along with the devices that support them, is provided in *Addendum: Additional VNE Support for Cisco Prime Network 5.2*. You can also add support for new commands by downloading and installing Prime Network Device Packages (DPs). For information on DPs, see the discussion about adding new VNE support in the *Cisco Prime Network 5.3 Administrator Guide*. For information on commands that change basic NE properties (for example, SNMP configurations, port and interface properties, an NE's DNS server, and so forth), see Drilling Down into the Properties of a Network Element, page 8-2.

Adding and Removing NEs from Existing Maps

When you add an element to a map, the map is automatically saved in the Prime Network database. You can display all NEs by selecting **Show All** in Step 3, but devices you do not have permission to view are displayed with a lock icon; they are also not returned in search results.

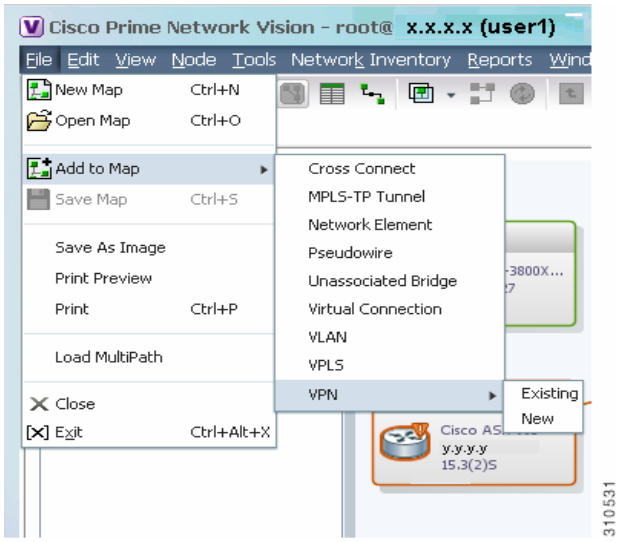
To add an element to a map:

Step 1 Choose **File > Open** and select a map from the map list.

Step 2 Choose **File > Add to Map >** *element*.

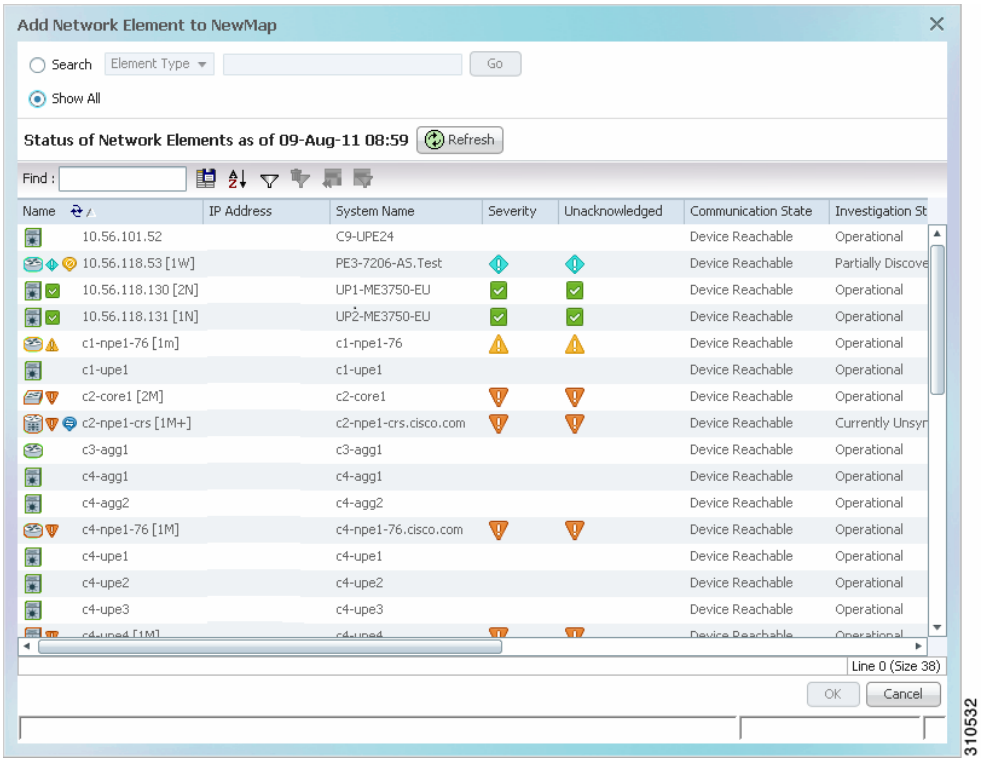
Figure 7-19 shows the type of elements you can add to maps.

Figure 7-19 Available Elements to Add to Maps



Note If you choose to add a new VPN, the Create VPN dialog box is displayed. For information on creating a VPN, see Creating a VPN, page 17-22. In all other instances, the Vision client presents a dialog box similar to Figure 7-20.

Figure 7-20 Add Element Dialog Box



Step 3 Use one of the following tools to locate the NEs you want to add to the map.

- Search for the elements you want to add to the map. For example, you can search Ethernet Services by the system name, NEs element type, pseudowires by their role, and so forth.

  Note If you are working with a large number of NEs, use the search filter. Otherwise, it may take some time for all of the NEs to be listed.

- To view all available elements, choose **Show All**. If you do not have permission to view an NE, it is shown with a lock icon.

The available elements are displayed in the dialog box in table format. The dialog box also displays the date and time at which the list was generated. To update the list, click **Refresh**.

Step 4 Select the elements that you want to add.

Step 5 Click **OK**. If you selected a large number of elements (for example, more than 25 VLANs or VPLS instances), the action may take a while to complete.

The NEs are added to the map and are displayed in the navigation pane and content area. In addition, any associated tickets are displayed in the ticket pane.

Removing Elements from a Map

When you delete an element from a map, it is removed from the map in the database. However, it continues to be managed by Prime Network. Your user account permissions determine whether you can remove items from a map.

To remove a network element from a map, right-click the NE and choose **Remove from Map**.

Grouping NEs Using Aggregations

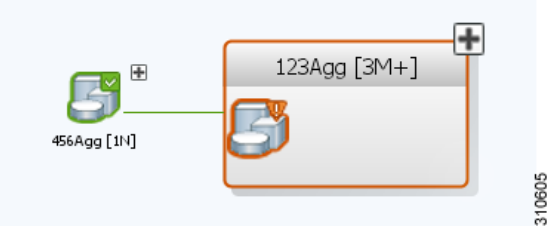
Drilling Down Into NE Groups (Aggregations), page 7-16, explains how to traverse between nested aggregations—that is, aggregations that contain other aggregations. Aggregations can contain network elements, services, other aggregations, and so forth.

Note If you cannot create an aggregation, you either do not have sufficient privileges or the device is not in your scope. See Permissions for Vision Client NE-Related Operations, page B-4.

To aggregate network elements:

Step 1 Select multiple NEs and aggregate them by choosing **Node > Aggregate**.

Step 2 In the Aggregation dialog box, enter a unique name for the aggregation and click **OK**. The aggregation is displayed in the navigation pane and the map pane. Aggregations are displayed as a single entity with the aggregation icon and a plus sign, as in the following two examples:



The aggregation icon changes color according to the alarm severity. For more information about severity colors, see Interpreting NE Icons, Badges, and Colors, page 7-4.

Making Changes to Aggregations

This table shows how to make changes to aggregations:

If you want to...	Do this...
Add an NE to an aggregation (certain restrictions exist; for example, you cannot add an EVC to a VLAN)	1. Double click the thumbnail *frame* so only the aggregation is displayed. 2. Select **File > Add to Map** and select the NE. You can choose NEs that are not in the parent map (the NE will have a dotted grey border around it).
Remove an NE from an aggregation	1. Double click the thumbnail *frame* so only the aggregation is displayed. 2. Right-click the device you want to remove and choose **Remove from Map**. The device is removed from the aggregation but not the parent map.
Ungroup (disaggregate) an aggregation (nested aggregations will be moved up one level)	1. Go to the parent map level. (If you are in a thumbnail, double-click the thumbnail background.) 2. Right-click the aggregation and choose **Disaggregate**.

Closing Maps, Renaming Maps, and Other Map Operations

Note If you cannot perform these tasks, you do not have sufficient privileges.

To perform this operation:	Choose or do the following:
Close a map	**File > Close**
Rename a map	**File >Save as New Map** or 1. Select File > Open. 2. From the Open Map Dialog, select the map and click **Rename Map** in the toolbar.
Save a map's appearance	**File > Save Map**
Save the map as an image	**File > Save as Image**
Print the map	**File > Print**
Display all maps that include a specified NE	Right-click an NE in a map and choose **Open Relevant Maps**
Delete a map from the Vision client and Prime Network database	1. Select File > Open. 2. From the Open Map Dialog, select the map and click **Delete from Map** in the toolbar.

Changing the Vision Client Default Behavior

All users can change their Vision client defaults. The defaults apply only to the client machines—that is, the machine from which you launch the Vision client. You can change:

- What is displayed when you start the Vision client
- Audio alerts and sounds
- NE text (font sizes, whether you can label NEs with business tags)
- Ticket severity information that is displayed with an NE icon
- Age of tickets that are displayed in the Vision client

To change these settings, see Changing Vision Client Default Settings (Sound, Display, Events Age), page 4-15.

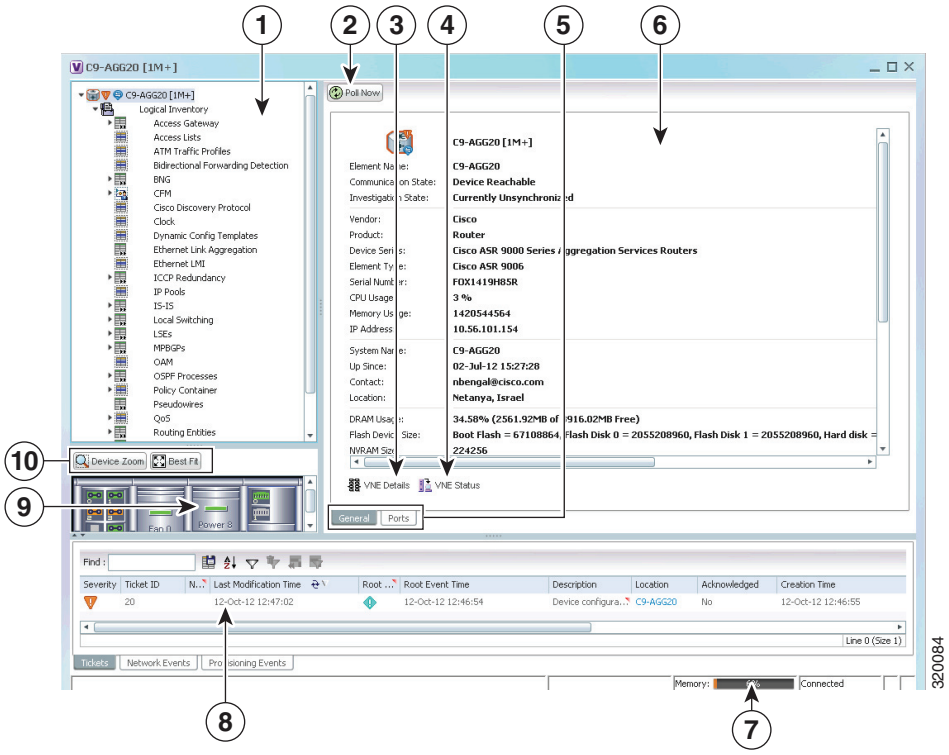
Drilling Down into an NE's Physical and Logical Inventories and Changing Basic NE Properties

The following topics describe how to view a device's physical and logical inventory using the Vision client:

Drilling Down into the Properties of a Network Element

From a map, double-click an NE to open its inventory window. Figure 8-1 provides an example.

Figure 8-1 Inventory Window

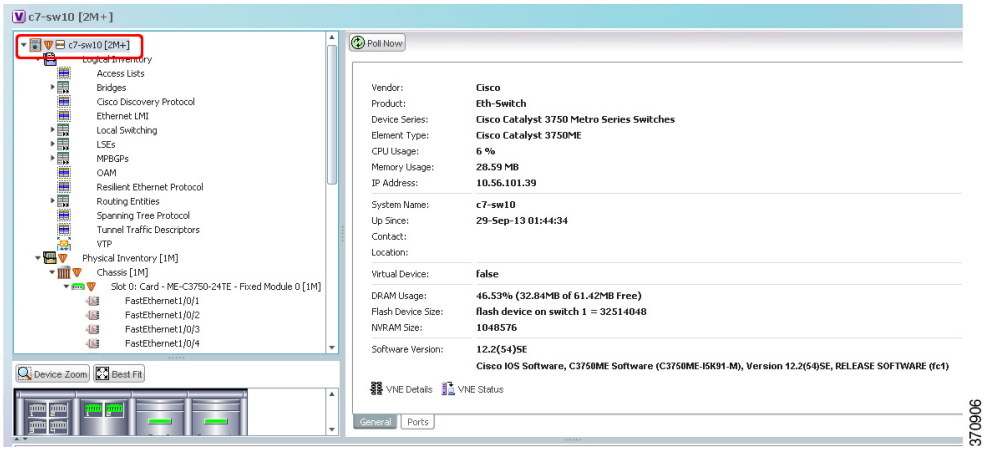


1	Physical and logical inventory—Physical Inventory includes the device components such as chassis, satellite, cards, and subslots. Configuration and status information is continuously updated. Logical inventory includes access lists, ATM traffic profiles, routing entities, and other logical entities.
2	Poll Now button—Initiates a poll of the selected NE.
3	VNE Details button (VNEs are internal components, one VNE per device)—Provides information about whether the VNE is operating correctly, what polling values are set, and so forth.
4	VNE Status button—Lists the protocols the device is using (it can also provide troubleshooting information).
5	Property tabs (General properties and Ports properties in this example)—The Ports tab provides a quick list of all device ports. The tabs displayed depend on what is selected. General tab can also display context-sensitive tabs and buttons.
6	Properties area—Provides inventory details. For a closer view of the Properties panel, see Figure 8-2 on page 8-3. The NE icon may also display: • Colors indicating a ticket and the ticket severity. See Severity Icons and Colors for Events, Tickets, and NEs, page A-15 for an explanation of the colors. • Badges that represent technologies such as a Protected LSP or an STP root. See Network Element Technology-Related Badges, page A-24 for a list of badges.
7	Vision client status bar.

8	Ticket and events pane—Displays tickets associated with the selected NE (from the last 6 hours) and associated Network and Provisioning events. See e Ways You Can View Tickets and Events, page 11-1.
9	Device view—Generic representation of the chassis, slots, modules, subslots and ports. All occupied slots are rendered in the device view pane. Problems are indicated with colors. See Figure 8-3 on page 8-4.
10	Device view tools for zooming and best fit.

Figure 8-2 shows the basic properties window for an NE. To display the basic properties, open the inventory window and select the NE at the very top of the navigation area.

Figure 8-2 NE Basic Properties Window

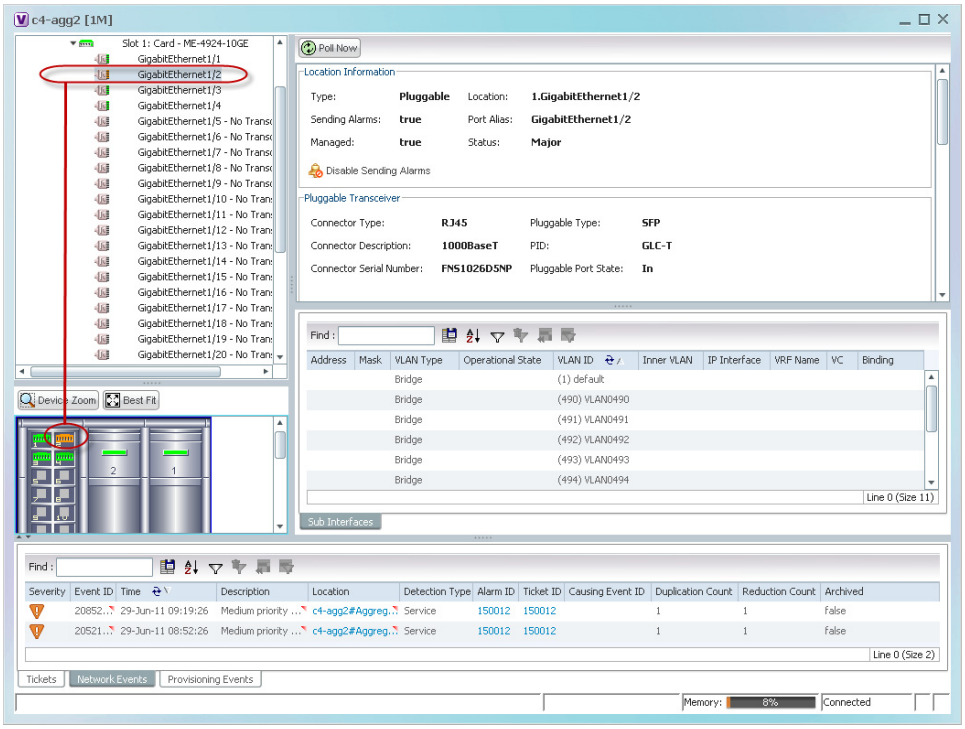


The following table provides information about the fields that are not self-explanatory.

Field	Description
Communication State	Ability of the Prime Network device model to reach the network element and other components in Prime Network.
Investigation State	Level of network element discovery that has been performed or is being performed by the Prime Network device model.
Up Since	Date and time the element was last reset.
Sending Alarms	Whether or not the element is configured for sending alarms (True or False)

Figure 8-3 provides an example of the device view pane for a Cisco device. The circled slot in the device view pane corresponds to the circled slot in the physical inventory navigation pane.

Figure 8-3 Device View Pane



Tip You can display or hide the ticket and events pane by clicking the arrows displayed below the device view panel.

Viewing Single- and Multi-Chassis Devices, Clusters, Satellites and Their Redundancy Settings

To get an NE's chassis details, choose **Physical Inventory > Chassis**. Prime Network displays the chassis serial number and description, along with the equipment in each slot.

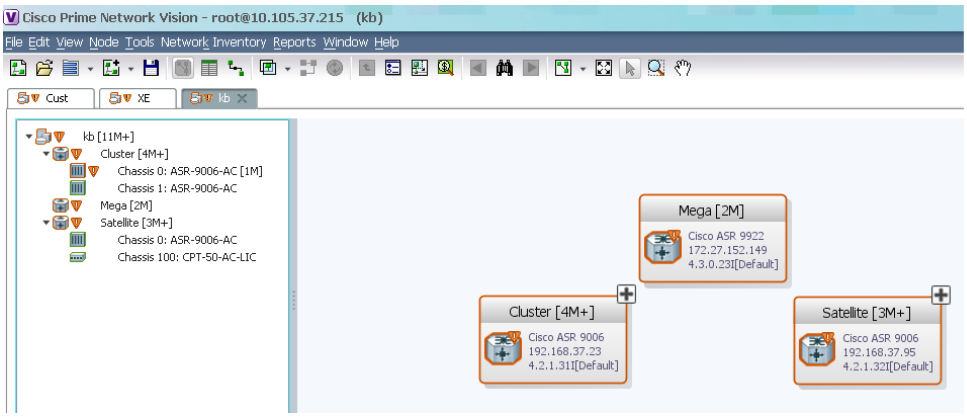
Icon	NE
	Chassis
	Cluster
	Satellite
	Shelf

If any items in the chassis inventory are black, it means the item was physically removed. You can verify this by checking the item status which should display Out. The other properties of the removed item reflect the most recent value that was updated from the device.

Viewing Multi-Chassis Devices

Multi-chassis devices, such Cisco ASR9000 and Cisco UCS devices, are grouped into aggregations and displayed as a single entity with a plus sign as shown in Figure 8-4.

Figure 8-4 Multichassis Devices in Map View



The physical ethernet links used for connecting the multi chassis devices are ICL (Inter Chassis Link) and IRL (Inter Rack Link). For more information on when each of these links are used, see Viewing Cluster Inter-Rack Links (IRLs), page 8-6 and Viewing Satellites and Satellite Inter-Chassis Links (ICLs), page 8-7.

Viewing Redundant (Primary and Secondary) Devices

In the Failover Configuration, two ASA devices are connected to each other. When the primary device becomes unavailable due to failure or down time, then the secondary device takes over the function of the primary device. The ASA device supports the following two failover configurations:

- Active/Active Failover—Also called the group failover, this type of configuration is available only in multiple context mode. In this configuration, both the ASA devices are active and pass traffic. This lets you configure load balancing on your network. When one of the devices becomes unavailable, then its functions are taken over by the other device.

  As mentioned earlier, this configuration has multiple contexts. The security contexts are divided into two failover groups. In other words, each device will have two failover groups.

Note By default, the admin context and any unassigned security contexts are members of failover group 1.

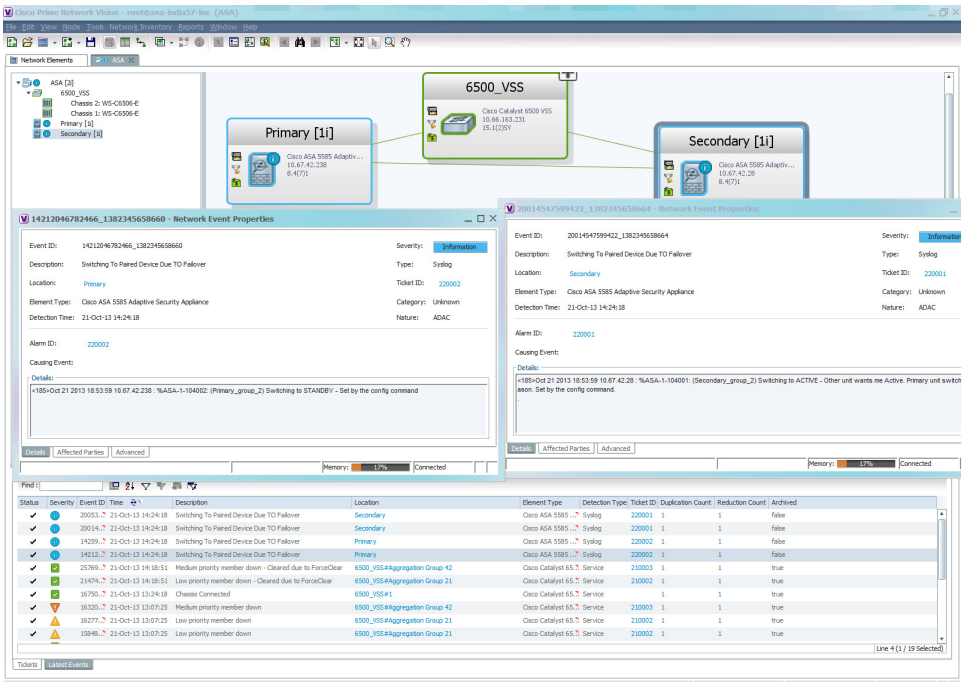
These groups can be in Active, Standby or a combination of Active and Standby modes. If Group 1 of the first ASA device is Active, then Group 1 of the second device must be in Standby mode. If Group 1 of the first ASA device (which is active) becomes unavailable, then Group 1 of the second device (which is in Standby mode) will become active. The same process applies for Group 2 contexts in both the devices.

- Active/Standby Failover—This type of configuration is available either on single or multiple context mode. In this configuration, only one of the units is active while the other one is in standby mode. When the active unit becomes unavailable, then the standby unit becomes active.

When there is a failover, and the secondary device takes over, syslogs are generated. You can view the syslog information in the "Latest Events" tab.

Figure 8-5 depicts the ASA failover scenario, along with the events that are generated after the failover:

Figure 8-5 ASA Failover topology with generated events

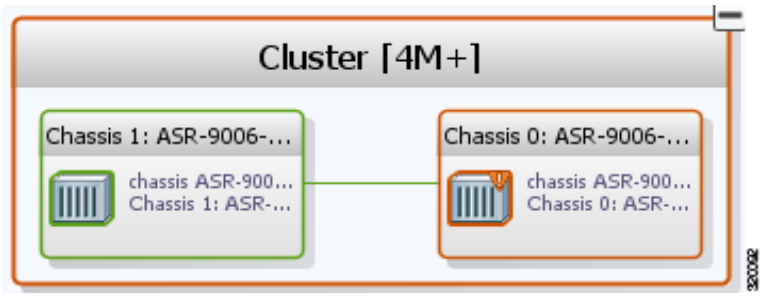


Note These syslogs help Prime Network to identify the devices that are in active and standby mode. When an active device goes into standby mode, and the other device becomes active, Prime Network changes the IP address of these devices. For example, if the primary devices goes into standby mode, the secondary device will take over the IP address of the primary device and starts functioning immediately.

Viewing Cluster Inter-Rack Links (IRLs)

Inter-Rack Links (IRLs) represent connectivity between the cluster chassis as shown in Figure 8-6.

Figure 8-6 Multiple Chassis in a Cluster



To view the cluster IRLs:

Step 1 Double-click the cluster device to open the Inventory window.

Step 2 In the device's Logical Inventory, choose **Cluster IRL.** A list of cluster IRLs is displayed showing the following information:

- A End Point—Device or site that is the source of the link, hyperlinked to the inventory of the device or site.
- Z End Point—Device or site that is the destination of the link, hyperlinked to the relevant entry in the inventory.

Viewing Satellites and Satellite Inter-Chassis Links (ICLs)

The Cisco ASR 9000 Series Router Satellite Network Virtualization (nV) service or the Satellite Switching System enables you to configure a topology in which one or more satellite switches complement one or more Cisco ASR 9000 Series routers, to collectively realize a single virtual switching system. In this system, the satellite switches act under the management control of the routers. The complete configuration and management of the satellite chassis and features are performed through the control plane and management plane of the Cisco ASR 9000 Series Router, which is referred to as the host.

The Satellite nV system supports the dual-homed network architecture, based on which two hosts are connected to a satellite through the Satellite Discovery And Control (SDAC) Protocol. Both these dual-homed hosts act in the active/standby mode for the satellite. The standby host takes control of the satellite only when the active host is down. The two hosts can leverage the Inter-chassis Communication Protocol (ICCP) infrastructure to provide redundant Layer 2 and Layer 3 services for Satellite Ethernet interfaces. The network traffic is switched through the active host. In case of connection loss to the active host due failure such as cut cable and host or client connection interface failure, the standby host becomes the active host and the active host becomes the new standby host. The hosts communicate with each other using ORBIT/ICCP protocols.

The advanced satellite nV system network topologies can be realized based on one of these architecture:

- Hub and Spoke.
- Ring with Dual Home.
- Ring with Layer 2 Fabric.
- Linear and Cascade.

Figure 8-7 shows an example of a satellite ring topology.

Figure 8-7 Satellite Ring Topology

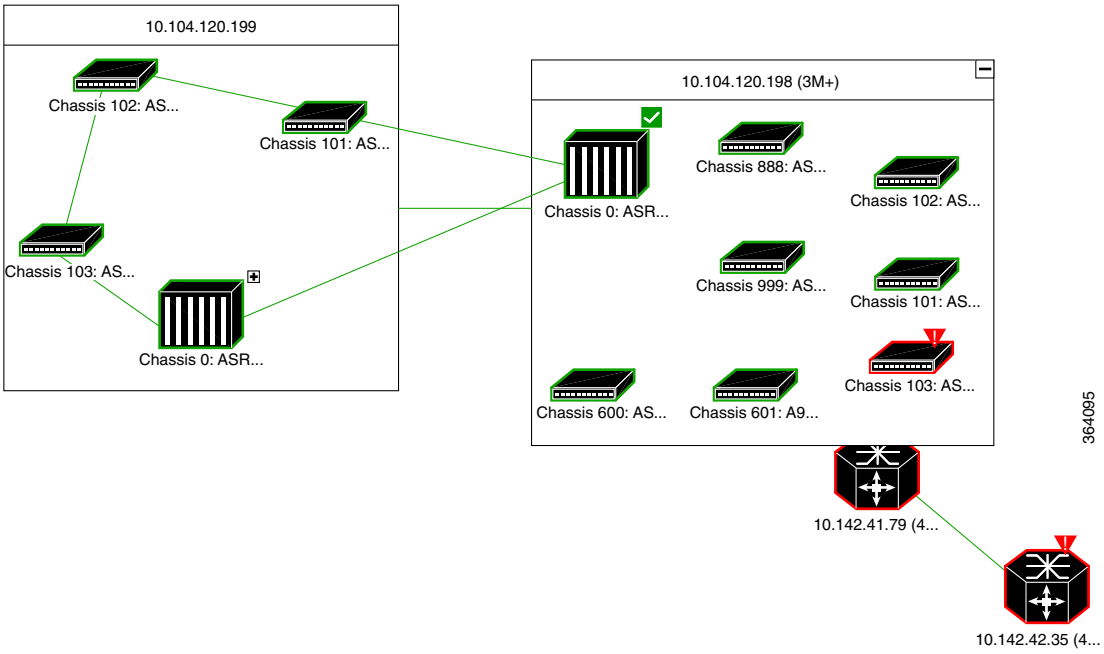


Figure 8-8 shows an example of a hub and spoke topology.

Figure 8-8 Hub and Spoke Topology

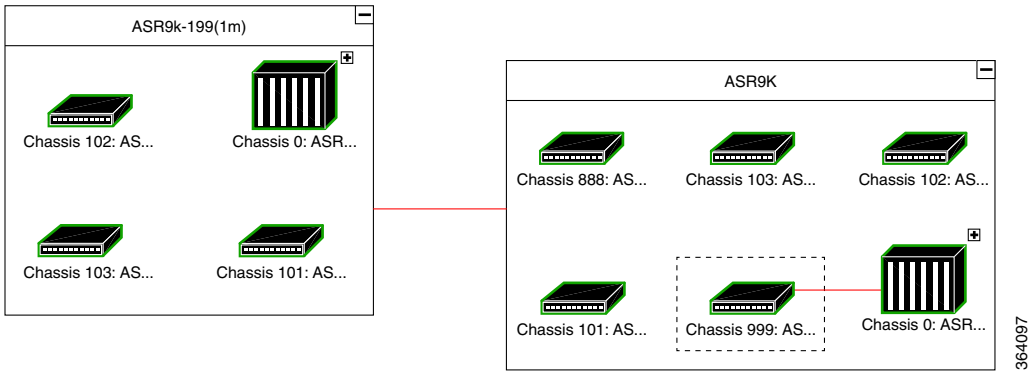
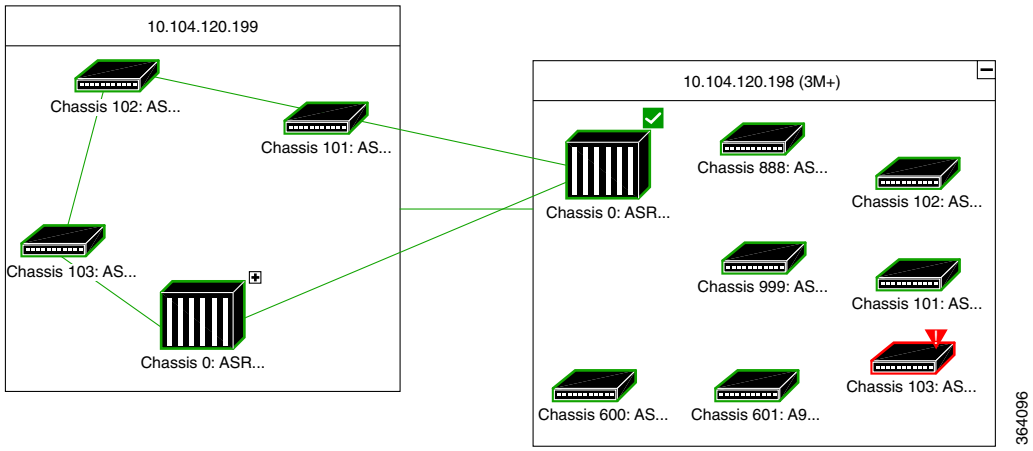


Figure 8-9 shows an example of a ring and cascade topology.

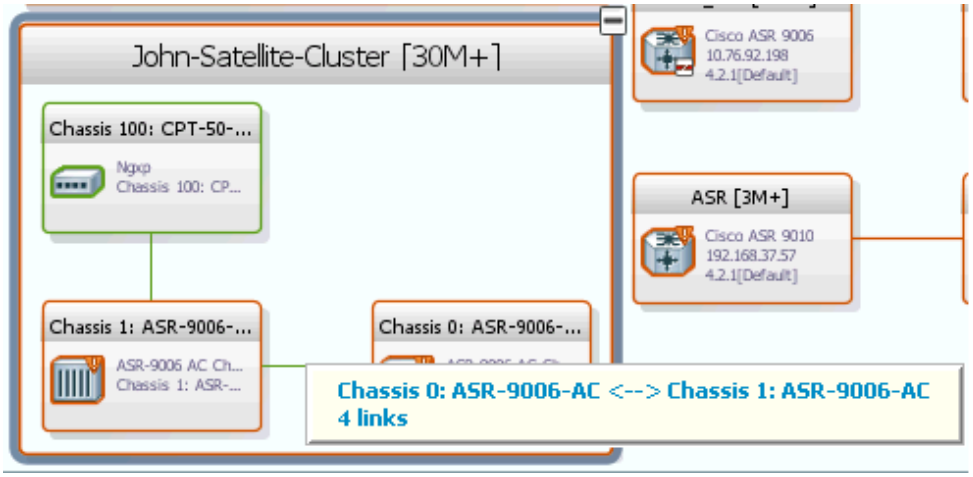
Note Inter-chassis links between the satellites are not supported for ring topologies.

Figure 8-9 Ring and Cascade Topology



Satellites enhance the performance bandwidth of Cisco ASR 9000 NEs. Each satellite is modeled as a chassis in the host Cisco ASR 9000 physical inventory. Satellites are connected to host Cisco ASR 9000 using the physical ethernet links. The physical ethernet links act as the inter-chassis links (ICLs), connecting the satellite to other satellites or chassis in the host. Figure 8-10 provides an example.

Figure 8-10 ICL Connecting a Satellite with a Chassis



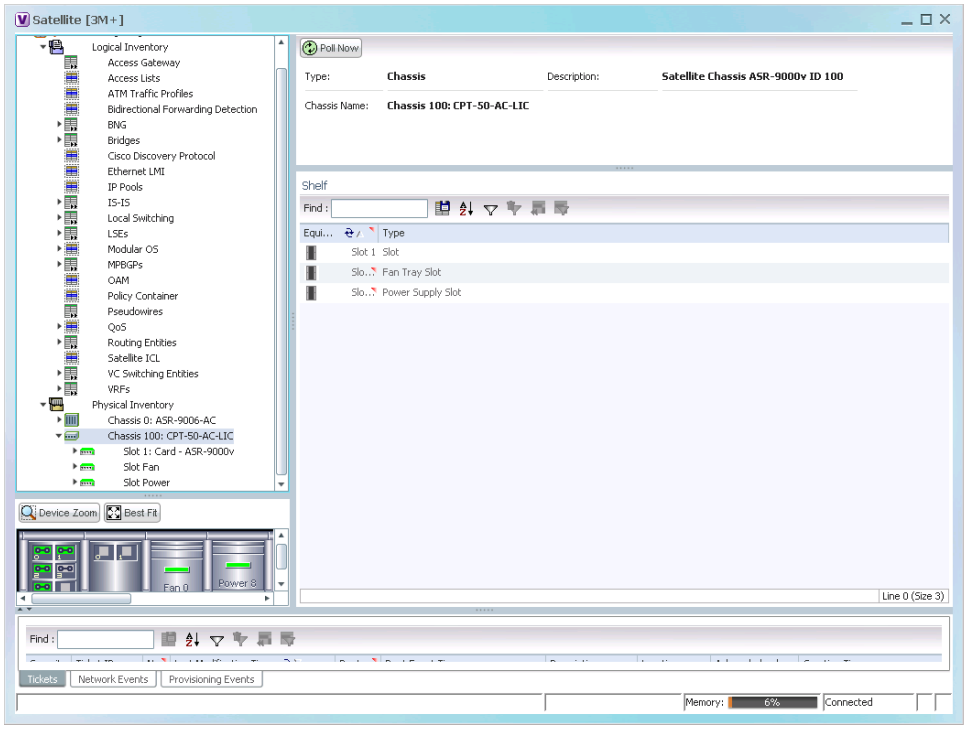
To view the satellite properties and ICLs in physical inventory:

Step 1 In the Vision client, double-click the device in which the satellite is configured.

Step 2 In the **Inventory** window, expand the Physical Inventory node.

Step 3 Click on the particular *Chassis* (the satellite is modeled as a chassis). Figure 8-11 shows an example of the satellite properties.

Figure 8-11 Satellite Properties



To view the satellite details and properties in logical inventory:

Step 1 In the Vision client, double-click the device in which the satellite is configured.

Step 2 In the **Inventory** window, expand the Logical Inventory node.

Step 3 Click *Satellites*. The content pane shows the following information:

Field	Description
Satellite Discovery Protocol	The SDAC Protocol that provides the behavioral, semantic, and syntactic definition of the relationship between a satellite device and its host.
Redundancy Control Protocol	The ICCP protocol.
Associated Redundancy System	A link to the associated redundancy system.

Step 4 Expand the Satellites node. Click on the particular satellite number. The properties of the satellite are displayed in the content pane.

Table 8-1 describes the properties of the satellite.

Table 8-1 Satellite Properties

Field	Description
Satellite ID	The identification number of the satellite.
Satellite Type	The type of the satellite.
Description	The description of the satellite.
IP Address	IP address of the satellite device.
MAC Address	MAC address of the satellite device.
Control Status	Control status of the satellite, whether it is connected or disconnected.
VRF	Virtual Routing and Forwarding (VRF) name, if the pool belongs to a VRF.
Associated Chassis	The chassis associated with the satellite.
Active Host or Standby Host	Displays Active Host if the host is active, else Standby Host is displayed.

Step 5 Click the respective tabs on the content pane to view the details of satellite connections and satellite fabric links.

Table 8-2 describes the details of satellite connections and satellite fabric links.

Table 8-2 Satellite Connections and Satellite Fabric Links Details

Field	Description
Satellite Connections tab	
Interface Name	The name of the interface.
Associated Entity	The associated entity of the interface.
Connection Status	Connection status of the satellite, whether it is connected or disconnected.
Connecting Entity	Shows the type of connection, whether it is to the remote or local host.
Connecting Interface	A link to the connecting entity.
Host Connected Interface	A link to the connected host.
Satellite Fabric Links tab	
Host Interface Name	The name of the host interface.
Associated Host Interface	The interface associated with the host.
Discovery Status	Discovery status of the satellite, whether it is Ready or Not Ready.
Configured Remote Ports	Remote ports that are configured.
Invalid Remote Ports	Remote ports that are invalid.

Viewing ICCP Group Properties

To view the properties of the ICCP Group:

Step 1 Double-click the satellite device to open the **Inventory** window.

Step 2 Choose **Logical Inventory**> **Redundancy Systems**. Click the particular **ICCP Group**. The properties of the ICCP group are displayed on the content pane.

Table 8-3 describes the properties of the ICCP redundancy group.

Table 8-3 ICCP Redundancy Group Properties

Field	Description
ICCP Group	The name of the ICCP Group.
Local System ID	The address of the local system.
Peer System ID	The address of the peer system.
System MAC address	The MAC address of the local system.
Local System Role	The status of the local system, whether it is Active or Standby.
Redundancy Status	The redundancy status of the satellite.
Redundancy Protocol	The ICCP protocol that controls the redundancy groups.
Associated Active System or Associated Standby System	The associated system of the ICCP Group, either Active or Standby.
Application Usage	Application usage can either be mLACP or Satellite ORBIT.
Peer Monitoring Option	Method used to monitor the peer: IP Route-Watch or Bidirectional Forwarding Detection (BFD).

Step 3 Click the respective tabs on the content pane to view the details of control interfaces and access data link aggregations.

Table 8-4 describes the details of control interfaces and access data link aggregations.

Table 8-4 Details of Control Interfaces and Access Data Link Aggregations

Field	Description
Control Interfaces tab	
Name	The name of the control interface.
Associated Entity	The associated entity of the interface.
Status	Status of the interface, whether it is Up or Unknown.

Access Data Link Aggregations tab

Interface Name	The name of the interface.
Associated Entity	A link to Ethernet Link Aggregation.

Satellite ICL alarm support for 9000V Satellite

ICL alarm support is a specific requirement for ASR9000v satellite. It enables identifying the root cause for ICL links and bundle-ether links by generating the Link Down alarms whenever the ICL links go down.

ICL alarm support is applicable for single ICL links and bundle-Ethernet links. In case of bundle, if one of the links goes down, a member/port -down alarm is generated, whereas if all the links in the bundle are down, the ICL alarm is generated.

As part of correlation, ICL alarm Link Down due to admin down/oper down/unreachable needs is created as a separate ticket, and the other alarms like link down syslog, line down syslog and SNMP link down trap are correlated to ICL alarm.

Viewing Cards, Fans, and Power Supplies and Their Redundancy Settings

To view cards, fans, and power supplies, choose **Physical Inventory > Chassis** and click the plus sign to expand the chassis inventory. Prime Network displays any cards, fans, and power supplies that are configured in the chassis slots.

Icon	NE
	Card, Subcard Fan, Power Supply

Fans are listed separately in a fan tray only if they can be separated; if fans cannot be separated, only the fan tray is displayed.

Note Fans and power supplies are only displayed if they are Field Replaceable Units (FRUs).

If any item in a slot is black, it means the item was physically removed. You can verify this by checking the item status which should display Out. The other properties of the removed item reflect the most recent value that was updated from the device.

Redundancy Support

Prime Network provides card redundancy information for Route Switch Processor (RSP) or Route Processor (RP) cards. To find out if redundancy is configured and whether an entity is the active or standby entity:

Step 1 Choose **Physical Inventory > Chassis > Slot**.

Step 2 To find out if redundancy is configured on the NE, check the Redundancy Configured field.

- Working—Redundancy is configured and enabled
- None—Redundancy is not configured
- N/A—Redundancy is not supported

Step 3 To find out if the NE is the active or standby element, check the Redundancy State field.

Note **None** indicates that the card has been physically removed from the slot.

- Standby—The NE is the standby entity
- Active—The NE is not the standby entity
  RP card switchover syslog is supported in CRS and ASR 9K devices. When we remove one RP card from the device, the other card will automatically change to Active state. Even after reinserting the card, the other RP card will still remain in Active state.

Note For example, if there are two cards (RP 1 and RP 2), initially RP 1 is in Active state and RP 2 is Standby. When RP 1 card is removed, RP 2 card is automatically changed to Active state and will remain in Active state even after reinserting the RP 1 card.

Step 4 If you have a Cisco ASR 9000 series and Cisco ASR 903 devices, you can also check the following.

Field	Description
Redundancy Info	Redundancy technology being used; for example Nonstop Routing (NSR), Stateful Switchover (SSO), or Route Processor Redundancy (RPR))
Redundancy Type ()	Stateful (SSO) or Stateless (RPR)

Viewing Port Status and Properties and Checking Port Utilization

To view ports and pluggable transceivers, choose **Physical Inventory > Chassis >** *card* (or subcard) and click the plus sign to expand the card inventory. Prime Network displays any physical ports, logical ports, pluggable transceivers that are configured on the NE. Unmanaged ports are also displayed.

Icon	NE
	Port Logical Port Pluggable Transceiver
	Unmanaged Port

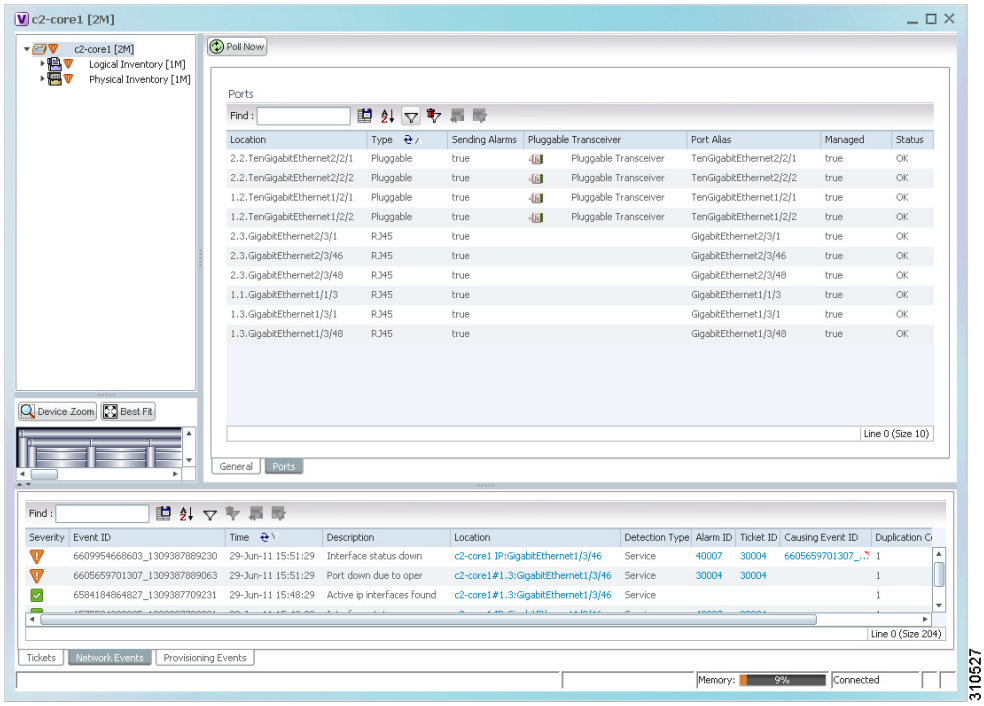
These topics explain how to view the ports on an NE, their status, and their configuration.

- Checking the Status of All Ports on a Device (or Ports on a Card), page 8-15
- Drilling Down Into a Port's Configuration Details (Including Services and Subinterfaces), page 8-17
- Checking a Port's Utilization, page 8-19
- Disabling a Port's Alarms, page 8-20

Checking the Status of All Ports on a Device (or Ports on a Card)

To display all of the ports on a device, open the inventory window. Do not expand the inventory; just select the device as shown in Figure 8-12.

Figure 8-12 Listing All Ports on a Network Element



Prime Network displays the following information about all ports that are configured on the device. If the device has any unmanaged ports, they are also displayed.

Tip To export the port list from the Vision client, click the Export to CSV button in the toolbar.

Field	Description
Location	Location of the port in the device, using the format *slot.module/port*, such as 1.GigabitEthernet1/14.
Type	Port type, such as RJ45 or Pluggable.
Sending Alarms	Whether or not the port is configured for sending alarms: True or False.
Pluggable Transceiver	For the Pluggable port type, indicates that the port can hold a pluggable transceiver.
Port Alias	Name used in the device CLI or EMS for the port.
Managed	Whether or not the port is managed: True or False.
Status	Port status: OK or one of the following: • Major—Port is operationally down • Disabled—Port is administratively down (someone purposely shut the port down) • Out—Port has been physically removed

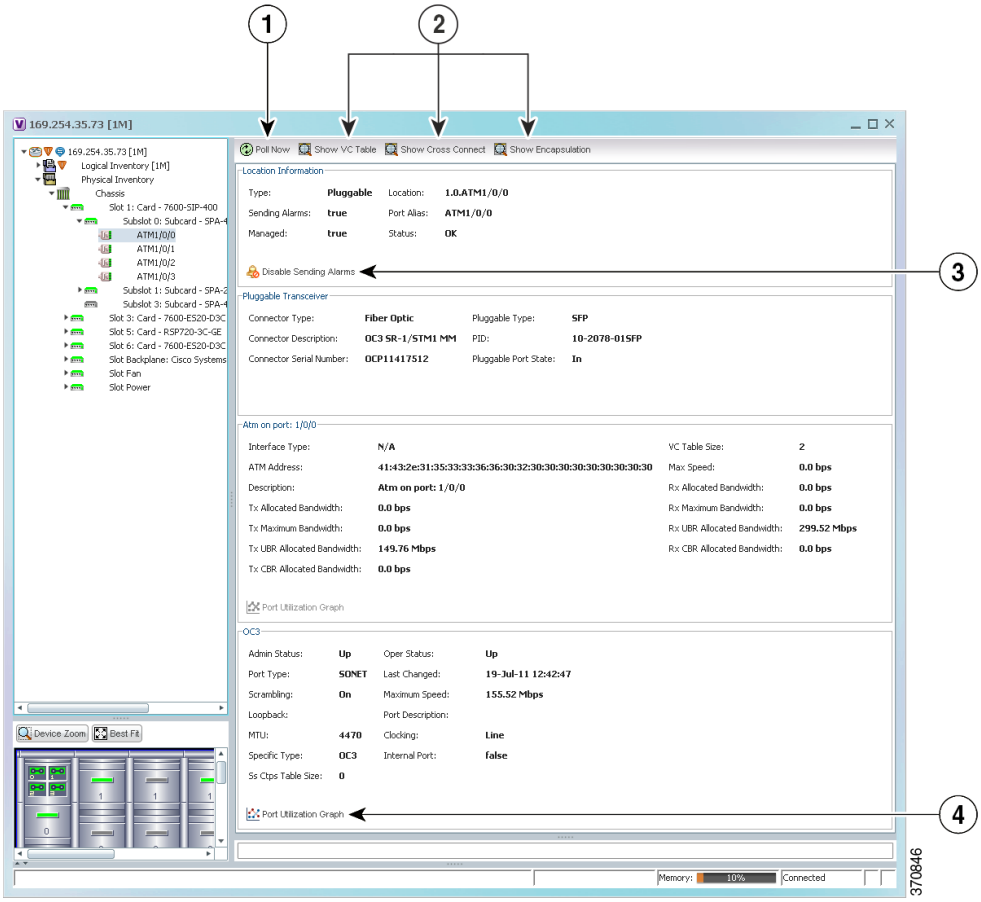
If any ports in the inventory are black, it means the item was physically removed. You can verify this by checking its operational status which should display Out.

To display all of the ports on a specific card's physical inventory, choose the card you are interested in. Prime Network displays the same information as in Figure 8-12, except only for the ports that are configured on the card you selected.

Drilling Down Into a Port's Configuration Details (Including Services and Subinterfaces)

To drill down into a port's inventory, choose **Physical Inventory > Chassis >** *card* **>** *port*. Figure 8-13 shows the physical inventory for a pluggable fiber optic port (managing these types of ports is discussed inViewing Virtual Connection Properties, page 26-5).

Figure 8-13 Viewing the Configuration Details for a Pluggable Fiber Optic Port

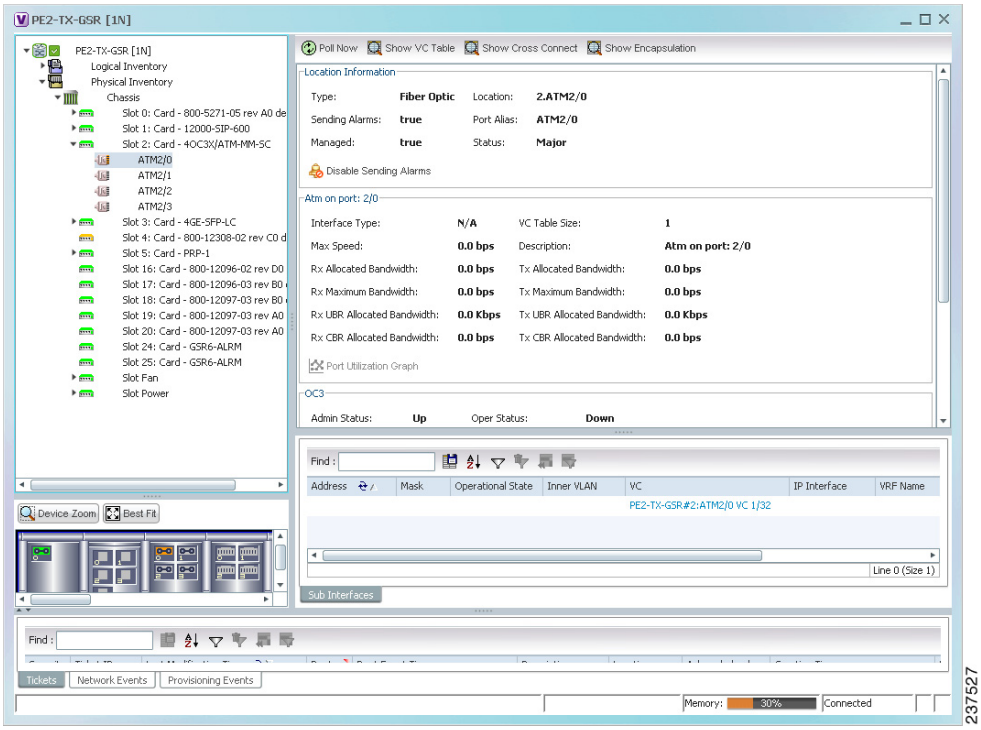


1	Poll Now button—Poll the device and update the information as needed. This choice is available for any type of port.
2	Context-Sensitive Buttons—Action buttons (actual buttons depend on port type). In this fiber optic port example, you can also display virtual circuit (VC) information, cross-connect data for incoming and outgoing ports, and encapsulation data for incoming and outgoing traffic.
3	Disable Sending Alarms button—Turns alarms on or off (for advanced users only). This choice is available for any type of port.
4	Port Utilization Graph button—Displays the selected port traffic statistics: Rx/Tx Rate and Rx/Tx Rate History. This choice is not available for ATM, E1/T1, or ATM IMA interfaces that are included in an IMA group.
—	Show DLCI Table button (not displayed)—Displays data-link connection identifier (DCLI) information for the selected port.

If any ports in the inventory are black, it means the item was physically removed. You can verify this by checking its operational status which should display Out.

Although a subinterface is a logical interface defined in a device, Prime Network displays all of its configuration parameters, as shown in Figure 8-14.

Figure 8-14 Viewing the Configuration Details for a Port with Subinterfaces



The following table lists the subinterface properties that are not self-explanatory. The subinterface configuration determines which properties are displayed. Double-click any properties that are hyperlinks to view additional properties.

Field	Description
VLAN Type	Type of VLAN, such as Bridge or IEEE 802.1Q.
Operational State	Operational state of the subinterface.
VLAN ID	VLAN identifier.
Inner VLAN	CE-VLAN identifier.
IP Interface	IP interface, hyperlinked to the VRF properties in the inventory window.
VRF Name	Name of the VRF.
Is MPLS	Whether this is an MPLS interface: True or False.
VC	Virtual connection (VC) configured on the interface, hyperlinked to the VC Table window. (For more information about VC properties, see Viewing ATM Virtual Connection Cross-Connects, page 26-6.)
Tunnel Edge	Hyperlinked entry to the specific tunnel edge in logical inventory.
Binding	Hyperlinked entry to the specific bridge or pseudowire in logical inventory.

Viewing the Services That Are Configured on a Port

A physical port's configuration details can include services that are provisioned on the port. Information that is displayed includes:

- Physical layer information.
- Layer 2 information, such as ATM and Ethernet.
- Subinterfaces used by a VRF.

For more information on the services, check the logical inventory. See Viewing the Logical Properties of a Device (Traffic, Routing, Information, Tunnels, Data Link Aggregations, Processes), page 8-21.

Checking a Port's Utilization

Prime Network provides a tool that displays a port's current Rx/Tx Rate and historical rate information. These graphs are for physical ports only. Port utilization graphs are not available for ATM, E1/T1, or ATM IMA interfaces that are included in an IMA group. Whether you can run these commands depends on your permissions. See Vision Client Permissions, page B-1.

Step 1 Open the inventory window and select the required port in physical inventory.

Step 2 In the Ethernet CSMA/CD section, click **Port Utilization Graph**. You may have to scroll down the properties area to display this tool.

The following information is displayed in the Port Statistics dialog box:

Rx Rate	Reception rate (percentage)
Rx Rate History	Graphical representation of reception rate history
Tx Rate	Transmission rate (percentage)
Tx Rate History	Graphical representation of transmission rate history

Step 3 Click  to close the Port Statistics dialog box.

Disabling a Port's Alarms

By default, alarms are enabled on all ports. If you expect a port to go down, you can disable alarms on the port so that no alarms are generated or displayed in the ticket and events pane. To disable alarms on ports:

Step 1 Open the inventory window for the required device.

Step 2 To disable alarms on individual ports, right-click the port and choose **Disable Sending Alarms**. The Sending Alarms field displays the value *false*, indicating that the alarm for the required port has been disabled, and the content pane displays the Enable Sending Alarms button.

Step 3 To disable alarms on one or more ports at the same time:

a. In the inventory window, click the **Ports** tab.

b. In the Ports table, select the required ports. You can select multiple ports by using the Ctrl and Shift keys.

c. Right-click one of the selected ports, and choose **Disable Sending Alarms**. In response, the Sending Alarms field displays the value *false* for the selected ports.

To enable alarms, use the previous procedure but choose **Enable Sending Alarms**.

Viewing the Pluggable Optics of Break-Out Mode Capable ports in Physical Inventory

An external physical port could be broken down in to multiple sub ports if it supports the break out functionality. For example, a 100 Giga port can be broken into ten 10-giga ports. In this case, each and every port must be modeled. However, a single pluggable optic must be maintained for each of these ports.

In Prime Network, the ports and the pluggable optics for a NCS6008 device are modeled separately. The pluggable optic as well as the port must be shown separately and at the same level for this device.

To view the pluggable optic details for a NCS device:

Step 1 Right-click the NCS device and choose the **Inventory** option.

Step 2 In the Inventory menu, expand the **Physical Inventory** node.

Step 3 Choose **Chassis** > *Slot* > *port*. In the content pane, view the **Associated Pluggable** field under the **Ethernet CSMA/CD** section.The pluggable transceiver links to the associated slot.

Note You can view the **Associated Pluggable** field only when the pluggable transceiver is available in MIB.

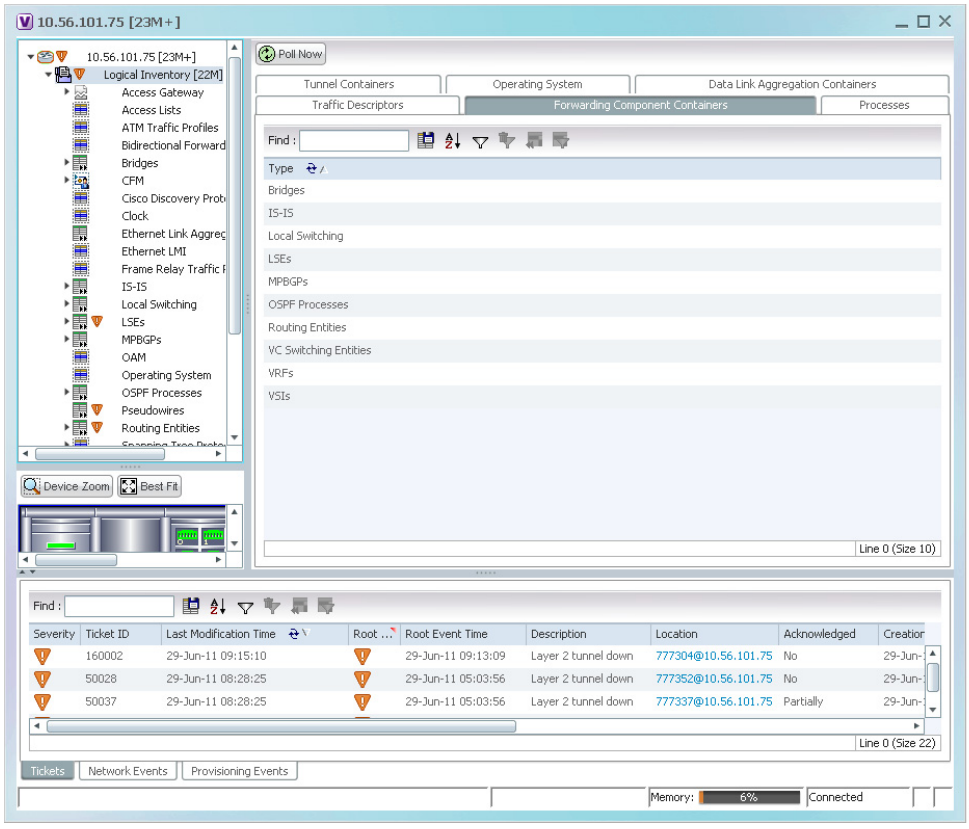
Step 4

Step 5 view the pluggable port in the **Associated Pluggable** field under the **Ethernet CSMA/CD** section.

Viewing the Logical Properties of a Device (Traffic, Routing, Information, Tunnels, Data Link Aggregations, Processes)

The logical inventory lists configuration data, forwarding, and service-related components that affect traffic handling in the element. Figure 8-15 shows an example of the Forwarding Component Containers for a Cisco 7604 router. All of the items listed in the tab are configured on the device. If something is not displayed, that means it has not been configured on the device.

Figure 8-15 Logical Inventory—Forwarding Components for Cisco 7604 Router



These topics describe the information you can obtain when you click the various Logical Inventory tabs.

- Viewing a Device's Traffic Descriptors, page 8-22.
- Viewing a Device's Forwarding Components, Device and VRF Routing Tables, and IP Interfaces, page 8-22.
- Viewing a Device's Tunneling Containers, page 8-23.

- Viewing a Device's Data Link Aggregation Containers, page 8-23.
- Viewing Management Processes that Are Running on a Device, page 8-23.
- Viewing a Device's Operating System Details (and K9 Security), page 8-25.

Viewing a Device's Traffic Descriptors

Traffic descriptors can include access lists, ATM and Frame Relay traffic profiles, OAM, forwarding tables, and so forth. To find out which traffic descriptors are configured on a device:

Step 1 In the Inventory window, choose Logical Inventory.

Step 2 Click the Traffic Descriptors tab. It lists the traffic descriptors that are configured on the NE—for example, ATM and Frame Relay traffic profiles or OAM.

Step 3 Click a traffic descriptor container in the logical inventory for information on that container. For example, if you choose **Logical Inventory > OAM**, you can view the OAM local port and its admin status.

Viewing a Device's Forwarding Components, Device and VRF Routing Tables, and IP Interfaces

To find out which forwarding components are configured on a device:

Step 1 In the Inventory window, choose Logical Inventory.

Step 2 Click the Forwarding Components Container tab. It lists the forwarding components that are configured on the NE—for example, bridges, routing entities, local switching, VRFs, and so forth.

Step 3 Click a forwarding component container in the logical inventory for information on that container. For example, if you choose **Logical Inventory > Routing Entities > Routing Entity**, you can view all interface types configured on the devices, such as Ethernet, GigabitEthernet, loopback, VLAN, and so forth.

- Click the IP Interfaces tab to see the IP address, associated entity, and so forth
- Click the IPv4 (or IPv6) Routing Table tab to see the destination, hops, and so forth

You can also use the following commands to view a device's routing table and the routing table of a selected VRF. The devices that support these commands are listed in the *Addendum: Additional VNE Support for Cisco Prime Network 5.0*. Whether you can run these commands depends on your permissions. See Vision Client Permissions, page B-1.

Command	Navigation	Description
Show > IP Route	**Logical Inventory > Routing Entities > Routing Entity > Commands**	Displays the device routing table.

Command	Navigation	Description
Show > **VRF IP route**	**Logical Inventory** > **VRFs** > *VRF* > **Commands**	Displays the routing table of a selected VRF.
Show > **IP** > **Interface Brief**	*NE* > **Commands**	Lists all IP interfaces on the device.

Viewing a Device's Tunneling Containers

Tunneling containers can include GRE tunnels, pseudowires, traffic engineering tunnels, and so forth.

Step 1 In the Inventory window, choose Logical Inventory.

Step 2 Click the Tunneling Containers tab. It lists the tunneling containers that are configured on the NE—for example, GRE, pseudowire, traffic engineering tunnels, and so forth.

Step 3 Click a tunneling container in the logical inventory for information on that container. For example, if you choose **Logical Inventory > Traffic Engineering Tunnels**, you can view the TE tunnel name, admin and operational status, outgoing label, lockdown status, and so forth.

Viewing a Device's Data Link Aggregation Containers

Use this procedure to view data link aggregation containers such as Ethernet Link Aggregations. ICL and transport are the two types of ethernet link bundles where ICL link type represents the ethernet link bundle between Cisco ASR 9000 device and satellite chassis or between two satellite chassis. Transport link type represents the ethernet link bundle between two Cisco ASR 9000 devices.

Step 1 In the Inventory window, choose **Logical Inventory**.

Step 2 Choose **Logical Inventory > Ethernet Link Aggregation** to view the aggregation type, bandwidth, aggregation control protocol, load balance type (Source and Destination MAC, Source IP, or Destination IP), link type, and so forth.

Viewing Management Processes that Are Running on a Device

Use this procedure to find out which management processes are running on a devices. These processes can include BFD, CFM, CDP, clock, E-LMI, ICCP redundancy, IP SLA responder, LLDP, REP, STP, VTP, and so forth.

Step 1 In the Inventory window, choose Logical Inventory.

Step 2 Click the Processes tab. It lists the management processes that are configured on the NE—for example, BFD, LLDP, clock, E-LMI, and so forth.

Step 3 Click a process container in the logical inventory for information on that container. For example, if you choose **Logical Inventory > Bidirectional Forwarding Detection**, you can view the source and destination IP, the protocols, state, and so forth for a BFD session.

Viewing Technologies and Services Configured on a Device

The inventory window provides detailed information on the different services and technologies configured on a devices. The Vision client may also provide configuration commands that are specific to those technologies and services. See these topics for information on to drill down into a device's inventory to get this information.

To get information about this technology/service on a device:	See:
Carrier Ethernet—CDP, LLDP, STP, REP, HSRP, access gateways, Ethernet Link Aggregation groups, mLACP, provider backbone, EFPs, EVC services, ethernet flow domains VLANs, unassociated bridges, ethernet flow point cross-connects, VPLS and H-VPLS, Pseudowires, Ethernet services, IP SLA, IS-IS, OSPF	Managing Carrier Ethernet Configurations, page 18-1
Carrier Grade NAT—CGNs, VRFs, address pools	Monitoring Carrier Grade NAT Configurations, page 20-1
DWDM—OTU and ODU alarms, FEC info, counter information, performance statistics	Managing DWDM Networks, page 16-1
CFM, E-LMI, L-OAM	Managing Ethernet Networks Using Operations, Administration, and Maintenance Tools, page 19-1
Y.1731 IPSLA—Performance management statistics and probes	Managing IP Service Level Agreement (IP SLA) Configurations, page 22-1
MPLS services—MPLS over IPv6 (6VPE0, MPLS-TP tunnels, VPNs, VRFs, IP interfaces, MPLS-TE, RSVP, BGP, VRRP, Bundle Ethernet	Managing MPLS Networks, page 17-1
IP and MPLS Multicast nodes and protocols, address family (IPv6) profiles, multicast label switching, multicast routing entities	Monitoring IP and MPLS Multicast Configurations, page 23-1
MToP services—SAToP and CESoPSN pseudowire, virtual connections, IMA groups, TDM, channelization, MLPPP and MLPPP links, MPLS pseudowire over GRE, network clock, CEM and virtual CEM, SONET, APS	Managing Mobile Transport Over Pseudowire (MToP) Networks, page 26-1
SBCs—DBEs, SBEs, performance statistics	Managing Session Border Controllers (SBCs), page 24-1
AAA—AAA groups, dynamic authorization profiles, RADIUS and diameter global configurations, charging configurations	Monitoring AAA Configurations, page 15-1

To get information about this technology/service on a device:	See:
IP pool monitoring and configuration	Managing IP Address Pools, page 14-1
BNG—Policy containers and QoS profiles, BBA groups, subscriber access points, DHCP, dynamic configuration and PPP templates	Monitoring BNG Configurations, page 25-1
Mobile technologies—GPRS/UMTS networks (GGSN, GTPU, APNs, GTPP, eGTP, SGSN); LTE networks (SAE-GW, P-GW, S-GW, QCI-QoS mapping, LAC, HSGW, home agent, foreign agent, ePDG, PDSN, LMA); operator polices, APN remaps and profiles; active charging services	Managing Mobile Networks, page 27-1
Data centers—Virtual port channels, Cisco FabricPath, virtualized resources (hypervisors and compute servers, virtual machines, data stores, clusters, resource pools)	Managing Data Center Networks, page 28-1
Cable technologies—Cable ports and interfaces, upstream and downstream configurations, QAM, DEPI, L2TP, MAC domains, narrowband channels	Monitoring Cable Technologies, page 29-1
ADSL2+ and VDSL2—XDSL traffic descriptors, DSL bonding groups, supported transport models, one-to-one and TLS access profiles	Monitoring ADSL2+ and VDSL2 Technologies, page 30-1

Viewing a Device's Operating System Details (and K9 Security)

All devices will display the software version running on the device when you open the NE inventory window and select the NE at the very top of the navigation area (see Figure 8-2 on page 8-3 for an example). Depending on the operating system and device type, you can drill down into more operating system details using one of these methods.

If you need to change the software image on an NE, use the procedures described in Managing Device Software Images, page 9-3.

Note Not all devices will display the same fields; it depends on the device type, operating system, and device configuration.

Open the logical inventory and click the Operating System tab. For groups of devices (such as Nexus data center aggregations), choose **Logical Inventory** > *Nexus management node* > **Operating System**.

Field	Description
Is K9Sec	If the operating system K9 security feature is enabled (true) or disabled (false)
Family	Cisco family, based on the device platform
SDR Mac Addr	(Cisco IOS XR only) Secure Domain Router (SDR) MAC address
Software Version	Operating system software version
Boot Software	System image information
ROM Version	Bootstrap software version

For some Cisco IOS-XR devices, more information will be displayed in the Operating System tab, or by choosing **Logical Inventory > Modular OS**.

Field	Description
Boot Software	System image information
SDR Name	SDR name
SDR Id	SDR identifier
ROM Version	Bootstrap software version
RAM Size	Size (kilobytes) of device processor RAM
OS Packages Table	
Package Info	Package information in the format *device*:package-*version*, such as disk0:hfr-admin-3.9.3.14
Package Description	Description of the package, such as FPD (Field Programmable Device) Package

Composite Name	Name of composite package with date and time, such as:
	`Tues Feb 8 20:37:07.966 UTC`
	`disk0:comp-hfr-mini-3.9.3.14`

Updating the Inventory (Poll Now)

Prime Network polls devices according to settings that configured when the device is added to Prime Network. By default, Prime Network uses its reduced polling mechanism (also called event-based polling) and polls the device when a configuration change syslog is received. In other words, updates are driven by incoming events. Only the affected areas of the NE are polled, and the modeling information is immediately updated.

For example, if you see in the device inventory properties that an NE is in the Currently Unsynchronized investigation state and you suspect an event was dropped, you should perform a manual poll of the device. Or, if you make a manual device configuration change and want to update the Prime Network model, poll the NE that you reconfigured.

Be sure you perform the poll from the right point in the inventory. Follow the below points:

- If one container is populated or dependent on another table (parent table), update the parent table. For example, the GRE tunnels container and the ARP entities container are generated from the IP Interface table. When the IP Interface table is polled, the IP address will be populated and the GRE tunnel and ARP entity properties will be updated accordingly.
- Perform the poll from the most efficient location in the NE. For example, do not poll the entire device if you only made a small change.

When you are ready to perform the poll, select a device in a map, or an NE in a device's physical or logical inventory, and click **Poll Now**.

Changing the NE Host Name

This procedure changes the system name of the network device. After you poll the device, the hostname is updated in the Vision client. Because the NE's information is saved by Prime Network using an ID that cannot be modified, all of the NE's information (such as its ticket history) remains associated with

the NE. Whether you can run this command depends on your permissions. See Permissions for Vision Client NE-Related Operations, page B-4. You can verify whether a device supports this command by checking the information in the *Addendum: Additional VNE Support for Cisco Prime Network 5.0*.

Step 1 Right-click an NE and choose **Commands > Configuration > System >Remove host name**.

Step 2 Click **Execute Now** to remove the device's current host name. The device's hostName value is set to null, and the name is deleted from Prime Network object.

Step 3 Right-click the NE and choose **Commands > Configuration > System >Add host name.**

Step 4 Enter the new host name and click **Execute Now**.

Step 5 Right-click the NE and choose **Poll Now** to update the NE information in the Prime Network inventory.

Changing the SNMP Configuration and Managing SNMP Traps

These commands change these SNMP properties on the real device. If you change the device SNMP configuration, you must also change the settings on the VNE (the model of the device that is maintained by Prime Network). Otherwise, Prime Network will not be able to properly communicate with and model the device. Whether you can run these commands depends on your permissions. See Appendix B, "Permissions Required to Perform Tasks Using the Prime Network Clients". You can verify whether a device supports these commands by checking the information in the *Addendum: Additional VNE Support for Cisco Prime Network 5.3*. From Prime Network 5.1 onwards, to collect the inventory data with the device details, the Vision client, the Command builder, Command manager, and Transaction manager communicates with the devices using SNMPv2 PDUs.

To create a Discovery profile with SNMPV2 credentials, user can create or Run a Discovery Profile, create a VNE, run the job. To change the SNMPV2 version, if required, you need to run the script in PN when the Prime Network is in "Down" status. For more information see the "Using Network Discovery to Add VNEs" section in the *Prime Network 5.3 Administrator Guide*.

Step 1 Right-click a device in the map, or choose the (top-level) device name in the inventory window.

Step 2 Use the following commands to change the device configuration. When you launch the command, click **Preview** to see the actual commands that will be sent to the device.

To do the following:	Right-click device and choose:
Change the SNMP configuration (community settings, read-write access control, view-based access control, group settings, and so forth)	**Commands > Configuration > System > SNMP** > **Add SNMP Configuration** **Commands > Configuration > System > SNMP > Update SNMP Configuration**[1] **Commands > Configuration > System > SNMP** > **Remove SNMP Configuration**
Enable, disable, and remove traps by choosing them from a drop-down list	**Commands > Configuration > System > SNMP** > **Add Traps** **Commands > Configuration > System > SNMP** > **Enable Traps** **Commands > Configuration > System > SNMP** > **Remove Traps**

1. The "Update SNMP configuration" command is not applicable for Cisco UBR10K and RFGW10 cards.

Step 3 To change the SNMP configuration on the device VNE:

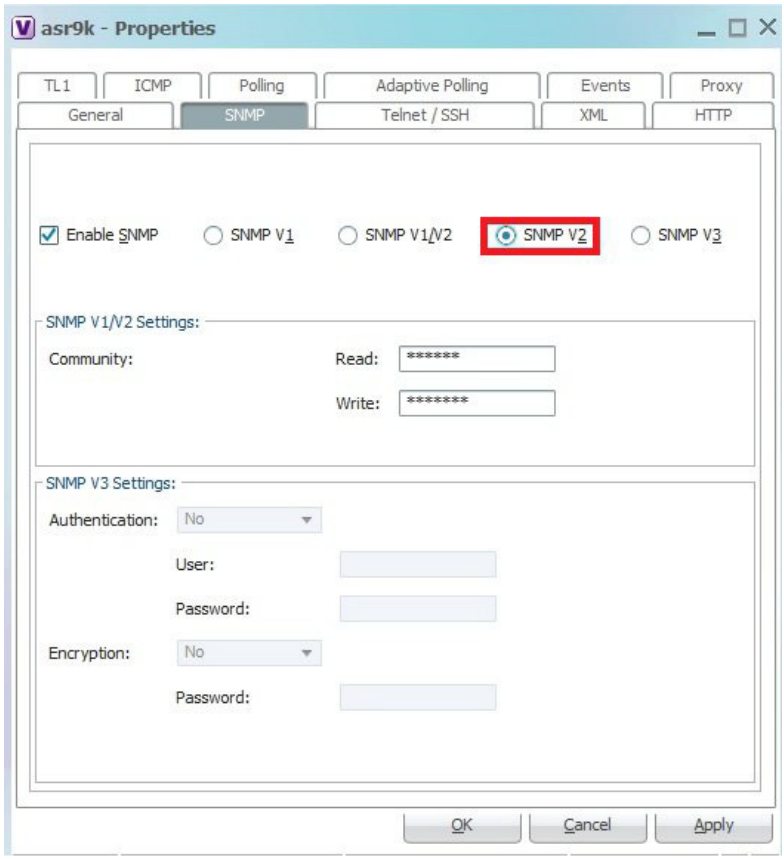
a. Right-click the NE and choose **Properties**.

b. Click **VNE Details**.

c. In the VNE properties window, click the SNMP tab and change the settings so they are consistent with the changes you made in the previous step.

d. Click the **Enable SNMP** radio button.

Note When VNE is configured to use SNMPV1/V2 for discovery, ensure that the device must also be enabled with SNMPV1.



e. Click **OK**.

Step 4 Right-click the NE and choose **VNE Tools > Stop VNE**.

Step 5 When the device icon turns red, right-click the NE and choose **VNE Tools > Start VNE** and Prime Network will poll the device.

Changing Device Port Properties and Disabling Ports

The following commands change the port properties of the real device. Whether you can run these commands depends on your permissions. SeeAppendix B, "Permissions Required to Perform Tasks Using the Prime Network Clients". You can verify whether a device supports these commands by checking the information in the *Addendum: Additional VNE Support for Cisco Prime Network 5.3*.

Step 1 Locate the port in the physical inventory.

Step 2 Change the port configuration using the commands in the following table. When you launch the command, click **Preview** to see the actual commands that will be sent to the device.

To make the following change on a port:	Right-click port in Physical Inventory and choose:
Change port status: Disable (Shutdown) or enable (No Shutdown) For example, shutting down a port prevents a known fault from continuing to generate events	**Commands > Configuration > System > Change Port Status**
Configure the descriptive information that is displayed in Prime Network clients when the port is selected such as customer information or business case details) (You can also label ports using business tags; see Labelling NEs to Associate Them with Customers (Business Tags), page 4-9)	**Commands > Configuration > System >Add Port Description** **Commands > Configuration > System > Remove Port Description** **Commands > Configuration > System > Update Port Description**
Change port characteristics such as bindings, contexts, link aggregations, and so forth	**Commands > Configuration > System > Modify Port**
Assign a port to a VLAN assignment (enter a VLAN between 1-4094); or deassign a port from a VLAN. When assigned, the port can communicate only with or through other devices in that VLAN. When deassigned, you can move a port to a new VLAN. Other VLAN actions are described in Working with VLANs, page 18-62.	**Logical Inventory** > **Routing Entities** > **Routing Entity** > *interface* > **Commands** > **Configuration** > **Assign Port to Vlan** **Logical Inventory** > **Routing Entities** > **Routing Entity** > *interface* > **Commands** > **Configuration** > **DeAssign Port To Vlan**

Step 3 Select the port and click **Poll Now** to synchronize the map information with the new device information.

Note Be sure you perform the poll from the right location in the inventory or your changes may not be reflected correctly in Prime Network. See Updating the Inventory (Poll Now), page 8-26.

Changing Device Interface Properties and Disabling Interfaces

The following commands change the interface properties of the real device. Whether you can run these commands depends on your permissions. See e Appendix B, "Permissions Required to Perform Tasks Using the Prime Network Clients". You can verify whether a device supports these commands by checking the information in the *Addendum: Additional VNE Support for Cisco Prime Network 5.3*.

Step 1 Locate the interface in the logical inventory.

Step 2 Change the interface configuration using the commands in this table. In some cases, a command will affect the interface and its parent port. When you launch the command, click **Preview** to see the actual commands that will be sent to the device.

To make the following change on a port:	Right-click:
Disable or enable an interface and port (for example, disabling faulty interface so it will not continue to generate errors)	**Logical Inventory** > **Routing Entities** > **Routing Entity** > *interface* > **Commands > Configuration > System > Enable Interface** **Logical Inventory** > **Routing Entities** > **Routing Entity** > *interface* > **Commands > Configuration > System > Disable Interface**
Change or remove descriptive information that is displayed in Prime Network clients (for example, customer information or business details) when the interface or port is selected. (You can also label interfaces and ports using business tags; see Labelling NEs to Associate Them with Customers (Business Tags), page 4-9.)	**Logical Inventory** > **Routing Entities** > **Routing Entity** > *interface* > **Commands > Configuration > Update Interface Configuration** **Logical Inventory** > **Routing Entities** > **Routing Entity** > *interface* > **Commands > Configuration > Remove Interface Configuration**
Configure a software-only interface that emulates an interface. If the virtual interface receives traffic, it immediately reroutes it back to the device.	**Logical Inventory** > **Routing Entities** > **Routing Entity** > **Commands** > **Configuration** > **Add Loopback Interface**
Configure descriptive information that is displayed in Prime Network clients (for example, customer information or business details) when the interface or port is selected. (You can also label ports using business tags; see Labelling NEs to Associate Them with Customers (Business Tags), page 4-9.)	**Physical Inventory** > *interface* > **Commands** > **Configuration** > **Add Interface Configuration**

Step 3 Right-click the appropriate logical inventory routing entity and choose **Poll Now** to synchronize the map information with the new device information.

Note Be sure you perform the poll from the right location in the inventory or your changes may not be reflected correctly in Prime Network. See Updating the Inventory (Poll Now), page 8-26.

Changing Server Settings for DNS, NTP, RADIUS, and TACACs

The following commands change the server settings on the real device. Whether you can run this command depends on your permissions. See Appendix B, "Permissions Required to Perform Tasks Using the Prime Network Clients". You can verify whether a device supports these commands by checking the information in the *Addendum: Additional VNE Support for Cisco Prime Network 5.3*.

Configure DNS

Command	Description
DNS > Add DNS Server **DNS > Remove DNS Server**	Assigns the device to a Domain Name System (DNS) server to manage translating the host name to and from the device IP address.

Configure a Device NTP Server

Command	Description
NTP > Add NTP Server **NTP > Remove NTP Server**	Assigns the device to a Network Time Protocol (NTP) server to manage clock synchronization.

Configure RADIUS or TACACS Server on Device

Command	Description
TACACS > Add Tacacs Server **TACACS > Remove Tacacs Server**	Assigns the device to a Terminal Access Controller Access-Control System (TACACS) server to manage authentication (uses TCP or UDP).
TACACS+ > Add Tacacs+ Server **TACACS+ > Remove Tacacs+ Server**	Assigns the device to a TACACS+ server to manage authentication (uses TCP).
RADIUS > Add Radius Server **RADIUS > Remove Radius Server**	Assigns the device to a Remote Authentication Dial In User Service (RADIUS) server to manage centralized authentication, authorization, and accounting (uses UDP).

Suppressing Service Alarms on Virtual Interfaces

In Prime Network Vision, you can suppress or unsuppress virtual interfaces related service alarms by using the Runregtool commands.

You can suppress or unsuppress ipv4/ipv6 virtual interface service alarms on a Device series or VNE levels.

Table 8-5 Suppress or Unsupress Service Alarms on Device Series Level

Suppress Service Alarms on Devices Series	
Service Alarm Name	**Command**
Dual Stack IP removed on Virtual Interface	`runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/<<Device_Series_Name>>/ipcore/software versions/default version/eventmanager/types/Dual stack IP removed on Virtual Interface/default" eventmanager/templates/sub-event/ignore-template`
Dual Stack IP added on Virtual Interface	`runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/<<Device_Series_Name>>/ipcore/software versions/default version/eventmanager/types/Dual stack IP added on Virtual Interface/default" eventmanager/templates/sub-event/ignore-template`
Dual Stack IP removed on Virtual Interface	`runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/<<Device_Series_Name>>/ipcore-evne/software versions/default version/eventmanager/types//Dual stack IP removed on Virtual Interface/default" eventmanager/templates/sub-event/ignore-template`
Dual Stack IP Added on Virtual Interface	`runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/<<Device_Series_Name>>/ipcore-evne/software versions/default version/eventmanager/types/Dual stack IP added on Virtual Interface/default" eventmanager/templates/sub-event/ignore-template`
Unsuppress Service Alarms on Device Series	
Service Alarms Name	**Command**
Dual Stack IP removed on Virtual Interface	`runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/<<Device_Series_Name>>/ipcore/software versions/default version/eventmanager/types/Dual stack IP removed on Virtual Interface/default" eventmanager/templates/sub-event/persistent-template`

Table 8-5 Suppress or Unsupress Service Alarms on Device Series Level

Suppress Service Alarms on Devices Series	
Dual Stack IP Added on Virtual Interface	`runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/<<Device_Series_Name>>/ipcore/software versions/default version/eventmanager/types/Dual stack IP added on Virtual Interface/default" eventmanager/templates/sub-event/persistent-template`
Dual Stack IP removed on Virtual Interface	`runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/<<Device_Series_Name>>/ipcore-evne/software versions/default version/eventmanager/types/Dual stack IP removed on Virtual Interface/default" eventmanager/templates/sub-event/persistent-template`
Dual Stack IP Added on Virtual Interface	`runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/<<Device_Series_Name>>/ipcore-evne/software versions/default version/eventmanager/types/Dual stack IP Changed/Dual stack IP added on Virtual Interface/default" eventmanager/templates/sub-event/persistent-template`

Table 8-6 Suppress or Unsuppress Service Alarms on VNE Level

Suppress Service Alarms	
Service Alarms Name	**Command**
Dual Stack IP Removed on Virtual Interface	`runRegTool.sh 127.0.0.1 set "avm<<AVM_ID>>/agents/da/<<VNE Name>>/eventmanager/types/Dual stack IP removed on Virtual Interface/default" eventmanager/templates/sub-event/ignore-template`
Dual Stack IP Added on Virtual Interface	`runRegTool.sh 127.0.0.1 set "avm<<AVM_ID>>/agents/da/<<VNE Name>>/eventmanager/types/Dual stack IP added on Virtual Interface/default" eventmanager/templates/sub-event/ignore-template`
Unsuppress Service Alarms	
Service Alarms Name	**Command**

Table 8-6 Suppress or Unsuppress Service Alarms on VNE Level

Suppress Service Alarms	
Service Alarms Name	**Command**
Dual Stack IP Removed on Virtual Interface	runRegTool.sh 127.0.0.1 set "avm<<**AVM_ID**>>/agents/da/<<**VNE Name**>>/eventmanager/types/Dual stack IP removed on Virtual Interface/default" eventmanager/templates/sub-event/persistent-template
Dual Stack IP Added on Virtual Interface	runRegTool.sh 127.0.0.1 set "avm<<**AVM_ID**>>/agents/da/<<**VNE Name**>>/eventmanager/types/Dual stack IP added on Virtual Interface/default" eventmanager/templates/sub-event/persistent-template

You can also suppress or unsupress virtual interface IPs of false alarms in Tickets on a Device series or VNE.

Use the following commands to suppress or unsuppress Virtual Interface IPs.

Table 8-7 Suppress or Unsuppress Service Alarms on the Tickets Tab

Suppress	
Service Alarms Name	**Command**
Dual Stack IP Removed on Virtual Interface	runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/<<**Device_Series_Name**>>/ipcore/software versions/default version/eventmanager/applications/event-correlation/application-data/sub-applications/com.sheer.metrocentral.framework.eventapplication.eventcorrelation.SendAlarmMessageUtil/types/Dual stack IP removed on Virtual Interface/is-ticketable" false
Dual Stack IP Added on Virtual Interface	runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/<<**Device_Series_Name**>>/ipcore-evne/software versions/default version/eventmanager/applications/event-correlation/application-data/sub-applications/com.sheer.metrocentral.framework.eventapplication.eventcorrelation.SendAlarmMessageUtil/types/Dual stack IP added on Virtual Interface/is-ticketable" false
Unsuppress	
Service Alarms Name	**Command**

Table 8-7 Suppress or Unsuppress Service Alarms on the Tickets Tab

Suppress	
Service Alarms Name	**Command**
Dual Stack IP Removed on Virtual Interface	runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/<<**Device_Series_Name**>>/ipcore/software versions/default version/eventmanager/applications/event-correlation/application-data/sub-applications/com.sheer.metrocentral.framework.eventapplication.eventcorrelation.SendAlarmMessageUtil/types/Dual stack IP Changed/Dual stack IP removed on Virtual Interface/is-ticketable" true
Dual Stack IP Added on Virtual Interface	runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/**<<Device_Series_Name>>**/ipcore-evne/software versions/default version/eventmanager/applications/event-correlation/application-data/sub-applications/com.sheer.metrocentral.framework.eventapplication.eventcorrelation.SendAlarmMessageUtil/types/Dual stack IP Changed/Dual stack IP added on Virtual Interface/is-ticketable" true

Table 8-8 Suppress or Unsuppress in the Tickets Tab on VNE Level

Suppress	
Service Alarms Name	**Command**
Dual Stack IP Removed on Virtual Interface	runRegTool.sh 127.0.0.1 set "avm<<**AVM_ID**>>/agents/da/<<**VNE Name**>>/eventmanager/applications/event-correlation/application-data/sub-applications/com.sheer.metrocentral.framework.eventapplication.eventcorrelation.SendAlarmMessageUtil/types/Dual stack IP removed on Virtual Interface/is-ticketable" false
Dual Stack IP Added on Virtual Interface	runRegTool.sh 127.0.0.1 set "avm<<**AVM_ID**>>/agents/da/<<**VNE Name**>>/eventmanager/applications/event-correlation/application-data/sub-applications/com.sheer.metrocentral.framework.eventapplication.eventcorrelation.SendAlarmMessageUtil/types/Dual stack IP added on Virtual Interface/is-ticketable" false
Unsupress	
Service Alarms Name	**Command**

Table 8-8 Suppress or Unsuppress in the Tickets Tab on VNE Level

Suppress	
Service Alarms Name	**Command**
Dual Stack IP Removed on Virtual Interface	`runRegTool.sh 127.0.0.1 set "avm<<AVM_ID>>/agents/da/<<VNE Name>>/eventmanager/applications/event-correlation/application-data/sub-applications/com.sheer.metrocentral.framework.eventapplication.eventcorrelation.SendAlarmMessageUtil/types/Dual stack IP removed on Virtual Interface/is-ticketable" true`
Dual Stack IP Added on Virtual Interface	`runRegTool.sh 127.0.0.1 set "avm<<AVM_ID>>/agents/da/<<VNE Name>>/eventmanager/applications/event-correlation/application-data/sub-applications/com.sheer.metrocentral.framework.eventapplication.eventcorrelation.SendAlarmMessageUtil/types/Dual stack IP added on Virtual Interface/is-ticketable" true`

After configuring commands to the device, you can assign the loopback of ipv4 or ipv6 in the Virtual template, change the assignation of loopback of ipv4 or ipv6 in the Virtual template or remove or add the ipv6 or ipv4 address from the loopback.

Changing Assignation of Loopback for both ipv4 and ipv6 in the Virtual Template

To change the assignation of loopback for both ipv4 and ipv6, follow the below steps:

Step 1 Log in to a device. For example, asr1k.

Step 2 Change the assigned Loopback with ipv4 and ipv6.

Step 3 Choose **Logical Inventory** > **Routing Entities** > **Routing Entity**, and then click the **Network Events** Tab in the Prime Network Vision and **Service Alarms** Tab in the Prime Network Event Vision to verify the Service Alarms for Virtual Interfaces.

Step 4 Execute the RunReg tool to block the Virtual Interfaces. For example, you can use RunReg tool command either at the devices series or VNE Level or in the Tickets tab on device series.

Step 5 Repeat steps 1 through 4. The Virtual Interfaces does not show in Prime Network.

Manage Device Configurations and Software Images

Cisco Prime Network Change and Configuration Management (CCM) provides tools for managing the software images and device configuration files used by the devices in your network.

For information on the devices supported by CCM, see the *Cisco Prime Network 5.3 Supported VNEs - Addendum*. For its Supported Protocols see the *Support for Change and Configuration Management in 5.3 tables.*

These topics explain how to use CCM:

Before using CCM, make sure you have completed the setup steps described in Setting Up Configuration Management, page 3-5.

Note CCM is also the launch point for the following Prime Network features which are described in the *Cisco Prime Network 5.3 Customization Guide*:

- Prime Network Transaction Manager, which manages and executes activations on groups of devices.
- Prime Network Command Manager, which provides a repository of all commands available in the system, and can be used to create new commands and command sequences which you can apply to groups of devices.

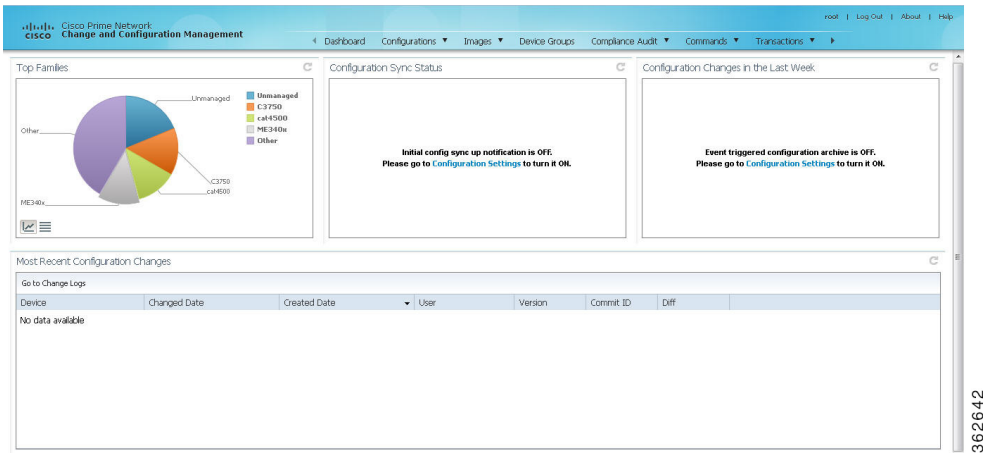
Using the CCM Dashboard

To launch CCM from a web browser, enter the following URL in the address bar:

https://*gateway-IP*:8043/ccmweb/ccm/login.htm

Figure 9-1 shows the CCM Dashboard, which contains four dashlets that display real-time information about the most frequently used software images, any devices with startup and running configurations that are not in sync, and recent device configuration changes.

Figure 9-1 CCM Dashboard



Dashlet	Provides information about:
Top Families	The four largest device families in the network. (Smaller groups can be viewed by toggling to the tabular form.) From here, you can distribute and activate software images to a selected family. In some cases, the actual name of the device family will not be displayed. For example, if c6sup11, s2t54, and s3223 are displayed in this dashlet, you must search Cisco.com to identify the device families for these devices. The c6sup11 device corresponds to the Cisco Catalyst 6500 Series Supervisor Engine 1A / MSFC1 device family, s2t54 device corresponds to the Cisco Catalyst 6500 Series Supervisor Engine 2T device family, and s3223 device corresponds to the Cisco Catalyst 6500 Series Supervisor Engine 32 / MSFC2A device family. **Note** If you have enabled the Right to Left (Hebrew) settings in your browser, you may face resizing issues when you hover the cursor over this dashlet.
Configuration Sync Status	(Cisco IOS) Devices for which the startup and running device configurations are in sync or not in sync. Whenever a Cisco IOS configuration file is retrieved from a device and copied to the archive, CCM compares the latest version of the startup configuration with the latest version of the running configuration file. If there is a mismatch, CCM adds the device to the list of out-of-sync devices. The information is refreshed whenever you click the Dashboard. A “100% Unavailable” message is displayed when there are no Cisco IOS device images or if the initial configuration sync up setting is not enabled (controlled by the “Enable/Disable Initial config sync up on restart” setting on the Configuration Management Settings page).

Dashlet	Provides information about:
Configuration Changes in the Last Week	Number of device configuration changes detected for each day of the current week. This dashlet is empty when configuration change notification is not enabled (controlled by the "Enable/Disable Event-Triggered Config Archive" setting on the Configuration Management Settings page).
Most Recent Configuration Changes	Last five device configuration changes made to devices in the network. This dashlet is empty if configuration change notification is not enabled. It is controlled by the "Enable/Disable Event Triggered Config Archive" setting on the Configuration Management Settings page (see Setting Up Configuration Management, page 3-5). If a device does not support Commit IDs and Diffs, the client displays N/A.

Use the following icons to toggle between different views in the Top Families, Configuration Sync Status, and Configuration Changes in the Last Week dashlets.

Icon	Description
	Displays the details in the form of a pie or bar chart. If you hover your mouse cursor over a section in the pie chart, a tooltip displays the information associated with that section.
	Displays the details in a tabular form.

Managing Device Software Images

The CCM Image Management feature provides tools for performing rapid, reliable software upgrades and automates the steps associated with upgrade planning and monitoring. Device software images are stored in the CCM image repository, to which you can add new images by importing them from Cisco.com, from existing devices, from a local file system, or from an external image repository. The images are stored in binary format in the repository, which is in the Prime Network database. Before an image is distributed, CCM performs an upgrade analysis to ensure that the network element is compatible with the image; after an image is distributed, it takes a minimum of 30 minutes for the image to activate. For Cisco IOS XR devices, you can add individual packages, deactivate packages, test changes before committing them, commit changes, and roll packages back to stored rollback points. CCM saves messages that can be used for debugging in *NETWORKHOME*/XMP_Platform/logs/NEIM.log.

Note Keep these notes in mind when using Image Management:

- Devices must be in the Device Reachable communication state and the Operational investigation state. See Checking the Device State, page 11-19for an explanation of how to check state information.
- CCM does not support special characters for any of the editable fields in the client, including filters.
- Before activating images on multiple devices, install the image on a single device and verify that it operates correctly.

Note If Prime Network is down then debug message is sent to user and no debug message is sent to user when Prime Network is up

The following topics explain how to work with software images and packages:

Adding New Images to the Repository

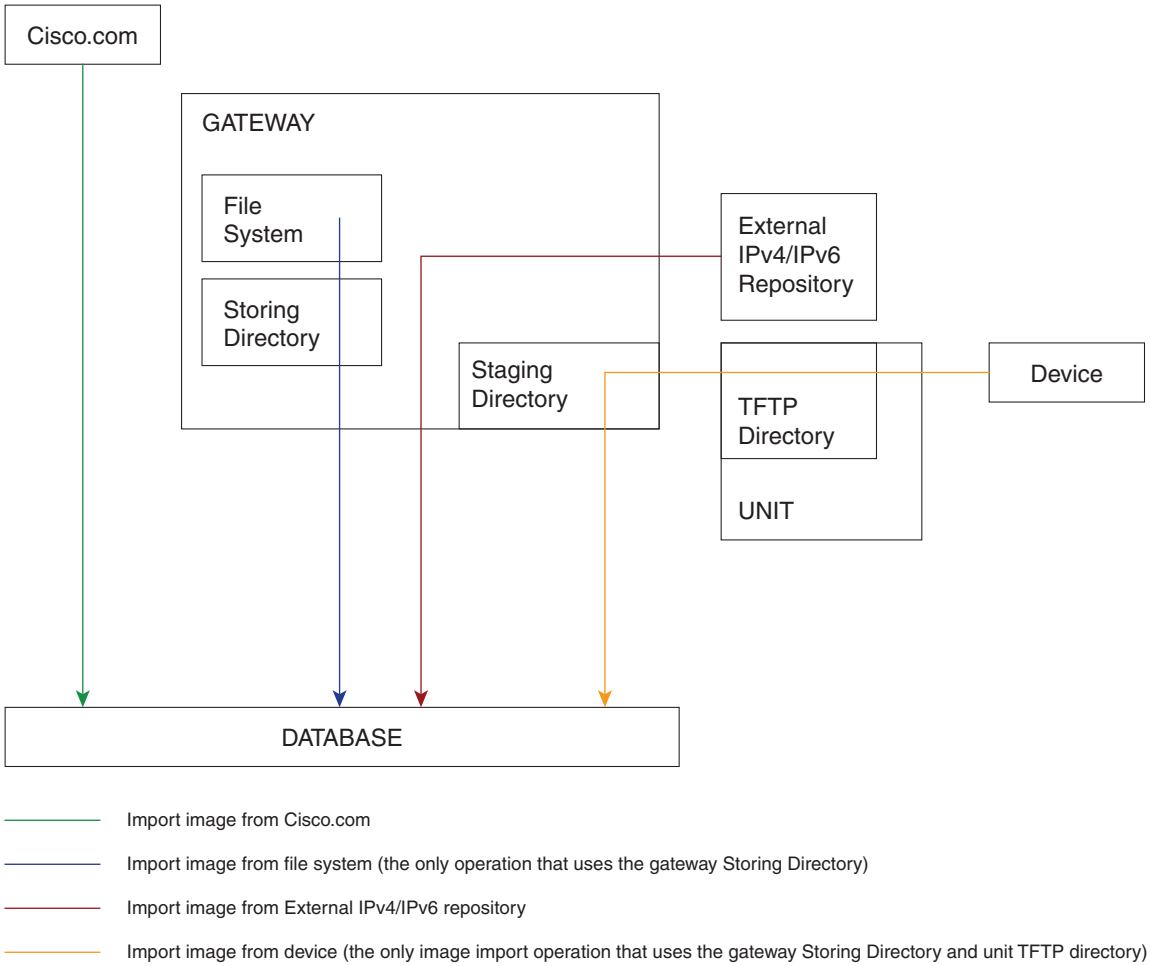
When images are copied to the repository, they are placed in the storing directory specified on the Image Management Settings page. Images are copied from the storing directory into the repository. Before copying an image, CCM verifies whether the new image is different from the existing image in the repository. If they are the same, CCM does not add it to the repository. By default, the storing directory is *NETWORKHOME*/NCCMComponents/NEIM/images.

Note Before importing images, make sure internet connectivity is available to the remote server; otherwise, the imported images will not be populated with RAM, boot ROM, and feature set information.

When you download an image from Cisco.com, CCM creates a job for the download. The job information is saved, along with other job information, in the database.

Figure 9-2 illustrates the process of importing images into the Prime Network database.

Figure 9-2 Import Image Operations



To import images into the CCM image repository:

Step 1 Choose **Images > Repository**.

Step 2 Choose the appropriate method:

To import from:	Choose:	Notes
Cisco.com web site	**from Cisco.com**	Make sure the Cisco.com credentials are set on the Image Management Settings page. You must enter a device type, software version, and feature set.

To import from:	Choose:	Notes
Another IPv4 or IPv6 gateway server	**from External Repository**	CCM will display available images, their size, and whether they already exist in the repository. CCM displays all images or packages (bin, pie, smu, and so on) from the directory specified in the Image Management Settings page, and also from its sub directory in order to support tar files. If you create tar files manually, ensure that you follow the file naming convention as the tar files in the Cisco.com web site so that the correct family name is displayed in the Images Repository page (Images > Repository).
A file system on the local gateway server	**from File System**	

Step 3 Select the images and import them. CCM redirects you to the Jobs page, where you can monitor the status of the import job.

Step 4 Choose **Images > Repository** again to refresh the list of images.

If a field displays NA, the image attributes were not available from the image header. (If pre-existing filters are still in use, you may need to click **Clear Filter**.) We recommend that you manually enter the information to ensure the accuracy of the upgrade analysis.

After an image is successfully imported, CCM removes any images from the unit TFTP directory, the gateway Staging Directory, and the gateway Storing Directory (for import from Cisco.com only). If you import images from a file system, you must manually delete those files from the gateway Storing Directory.

You can also add informational text to the Comments field. To distribute the images, see Distributing Images and Making Sure They Will Work, page 9-15.

Adding an Image from Cisco.com

Note This feature is not supported on any device running StarOS.

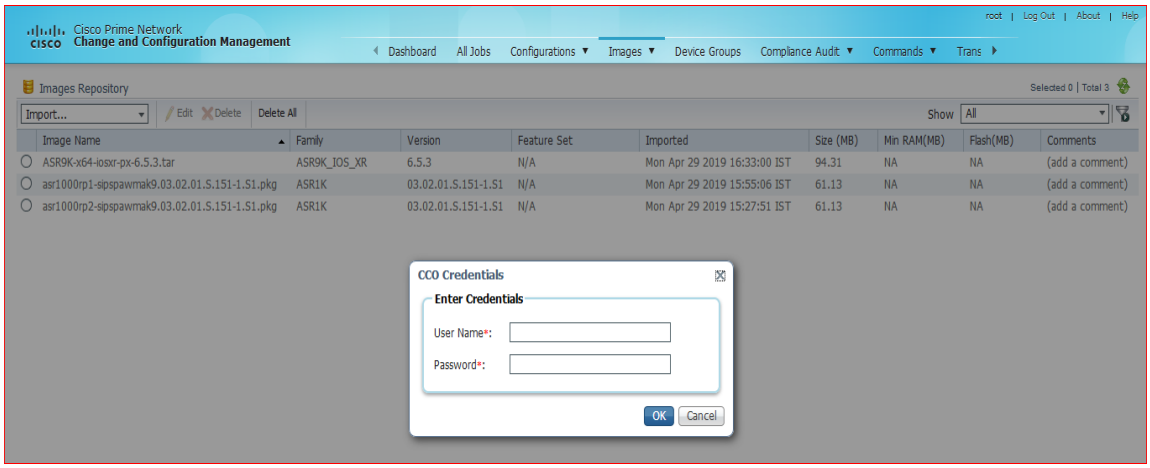
To import an image from Cisco.com into the CCM image repository:

Step 1 Choose **Images** > **Repository**.

Step 2 From the drop down at the left side of the **Images Repository** window, choose **Import...**.

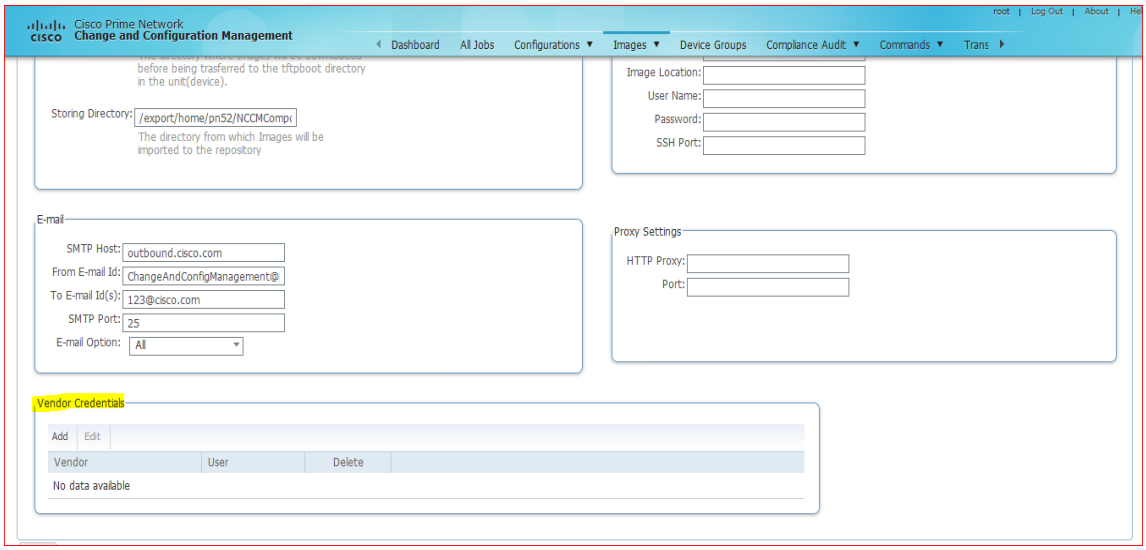
Step 3 From **Import...** box, choose **From Cisco.com** option. The **CCO Credentials** dialog box opens.

Step 4 Enter your credentials and click **OK**.

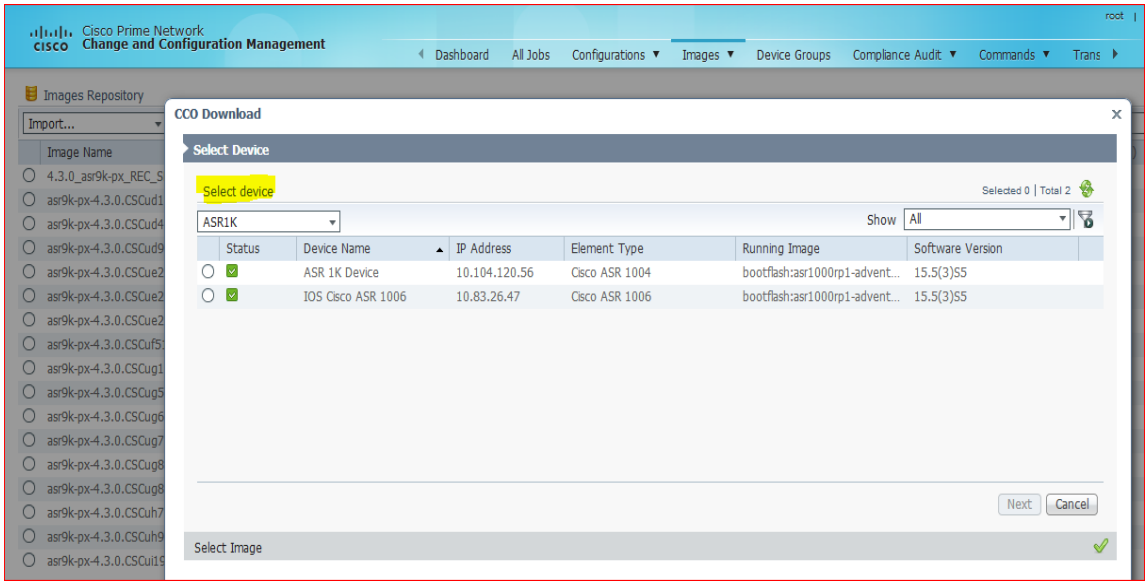


The **CCO Download box** opens upon successful login.

Note **Auto Login feature**: If you have configured user credentials under **Vendor Credentials** panel in **Images** > **Settings** page (as shown in the below image), CCM does not prompt you to enter CCO credentials and takes you directly to the **CCO Download** dialog box.



Step 5 From the **Select Device** panel, choose the required device and click **Next**.



Prime Network checks if the selected device(s) is under Cisco coverage. If the device is not under Cisco coverage, CCM shows "***Device is not under Cisco coverage***" error.

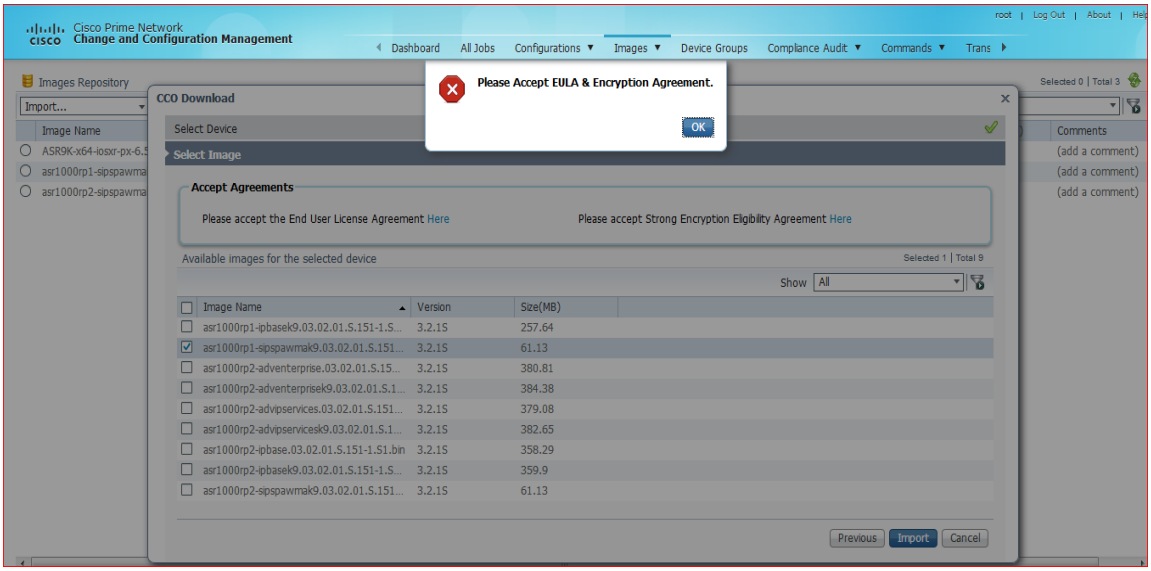
If the selected device(s) is under Cisco coverage, the **CCO Download** box displays the **Select Image** panel.

Step 6 In the **Accept Agreements** panel, the following two options appear:

- Please accept End User License Agreement Here.
- Please accept Encryption Eligibility Agreement Here.

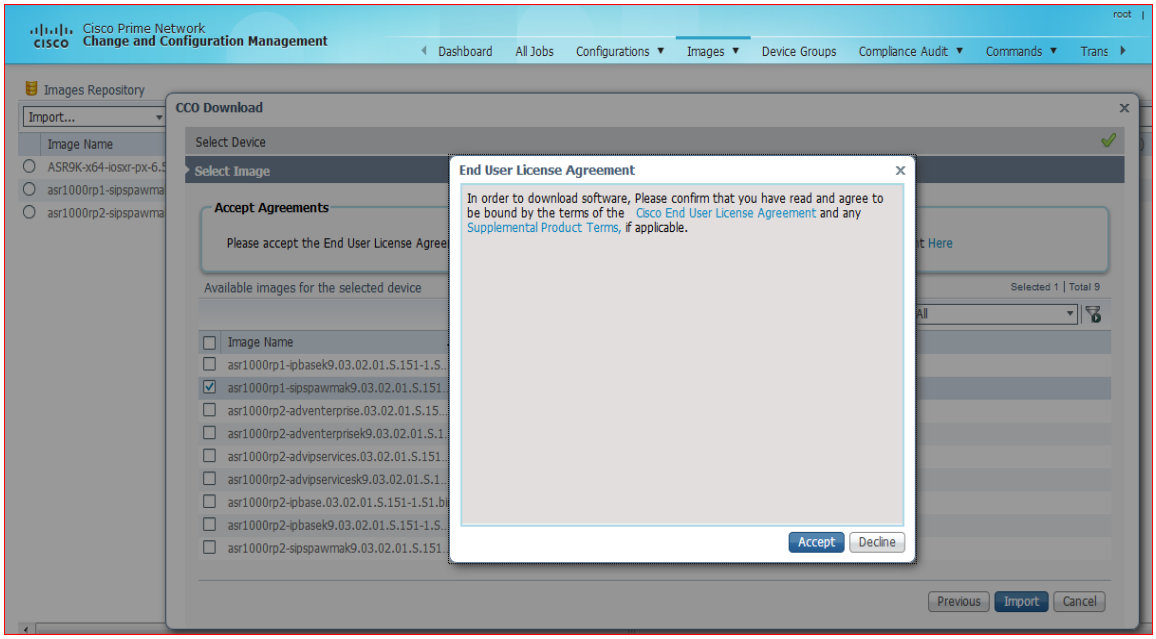
Note The **Accept Agreements** panel is visible only when **EULA (End User License Agreement)** and **Strong Encryption Eligibility Agreement** have not been accepted by the user before. Otherwise, the panel is disabled.

You must accept both the agreements before proceeding to download. Else, the following alert is displayed:



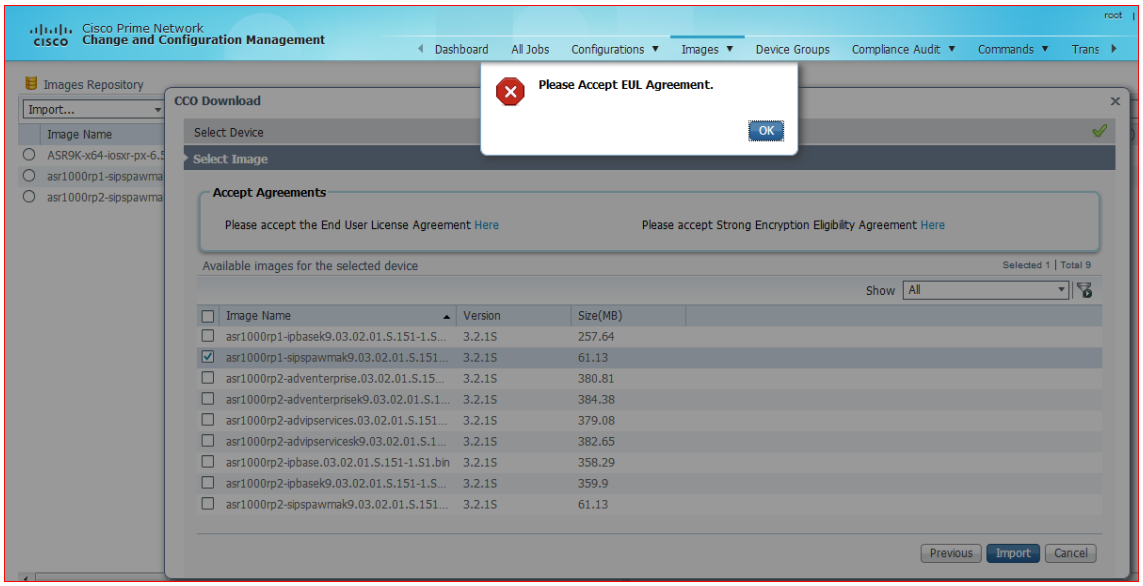
Click **OK** and follow these steps:

a. Click on the corresponding anchor link to view the End User License Agreement. The **End User License Agreement** dialog box opens:



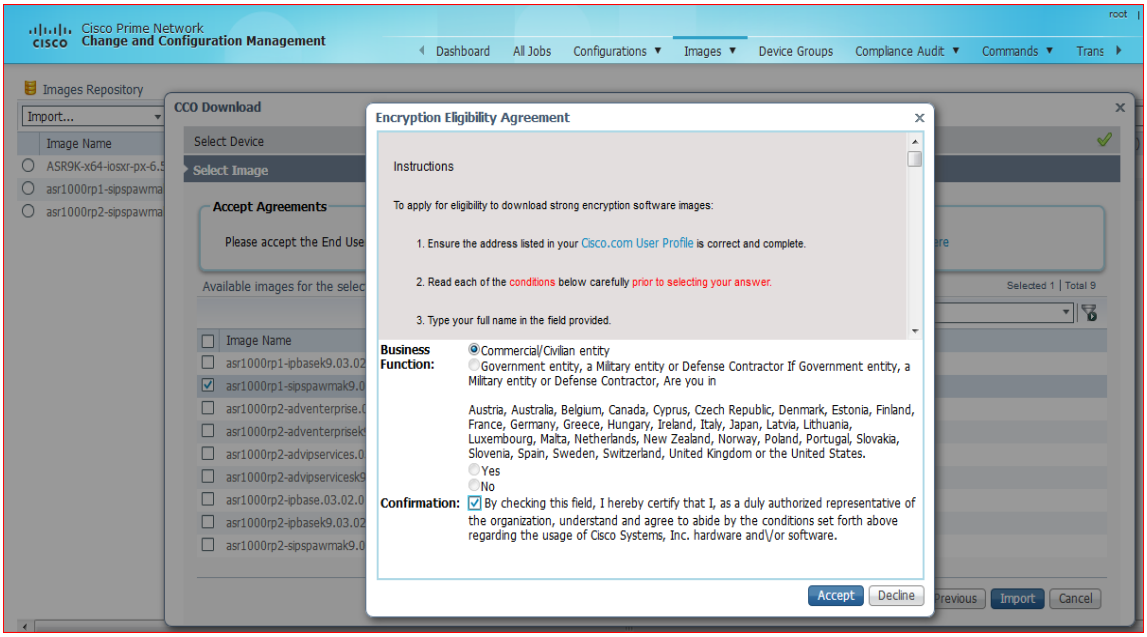
b. Click **Accept**.

You must accept the End User License Agreement before proceeding to the download. Else, the following alert is displayed:



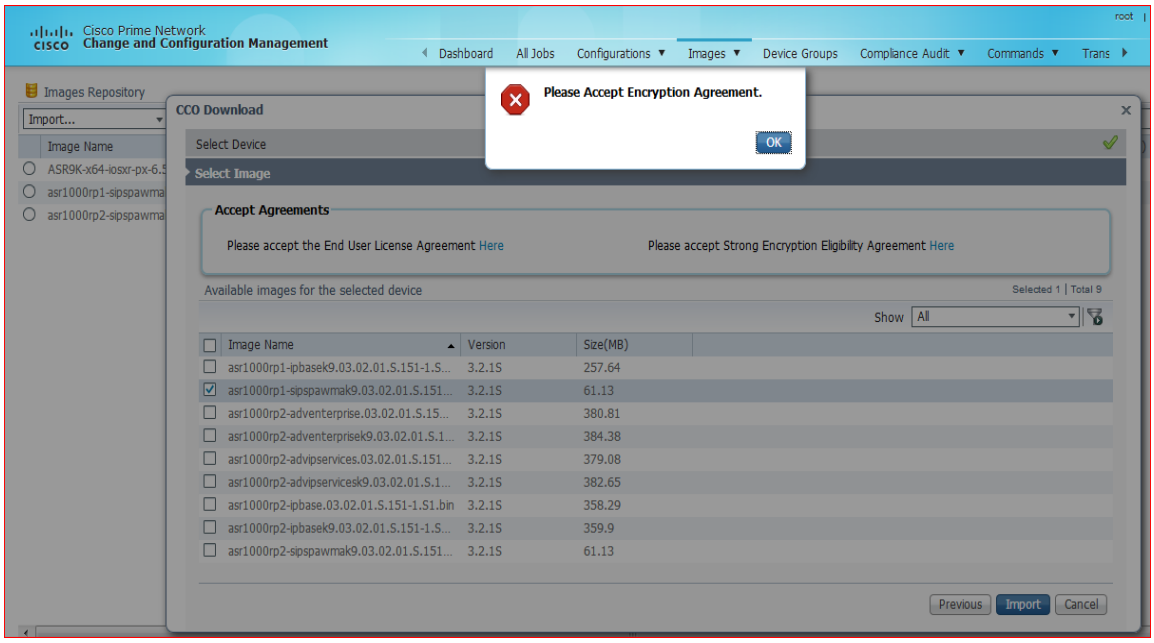
Click **OK** and follow **Steps a** and **b**.

c. Click on the corresponding anchor link to view the Encryption Eligibility Agreement. The **Encryption Eligibility Agreement** dialog box opens:



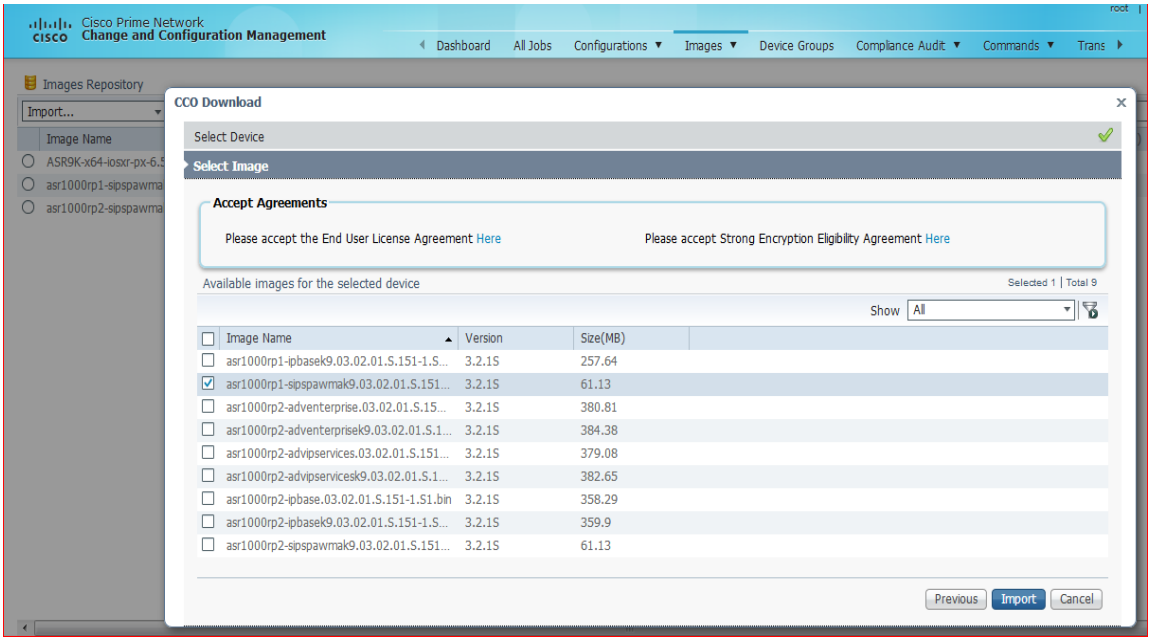
d. Click **Accept**.

You must accept the Encryption Eligibility Agreement before proceeding to the download. Else, the following alert is displayed:



Click **OK** and follow **Steps c** and **d**.

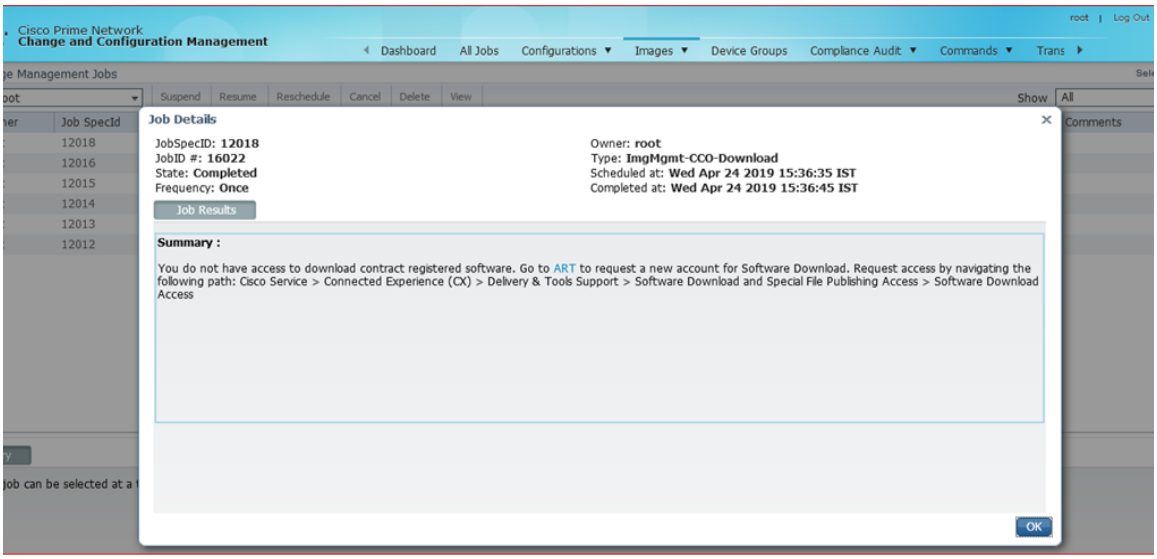
Step 7 From the **Available images for the selected device** panel, choose the image(s) that you want to download.



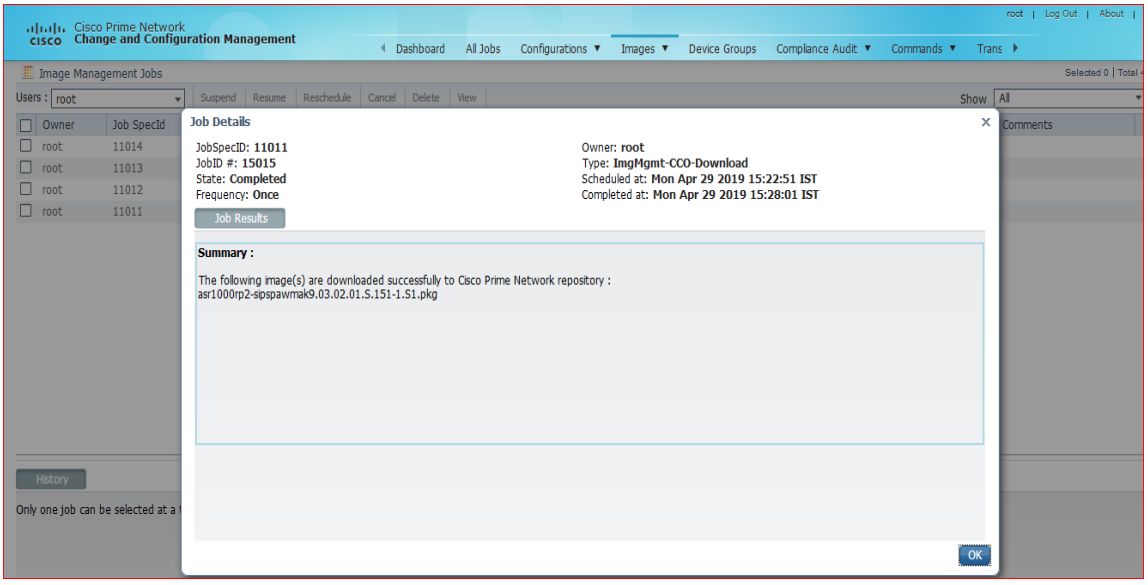
Step 8 Click **Import**. A new job of type **ImgMgmt-CCO-Download** is created.

Note You must have appropriate permissions to import an image from CCO.

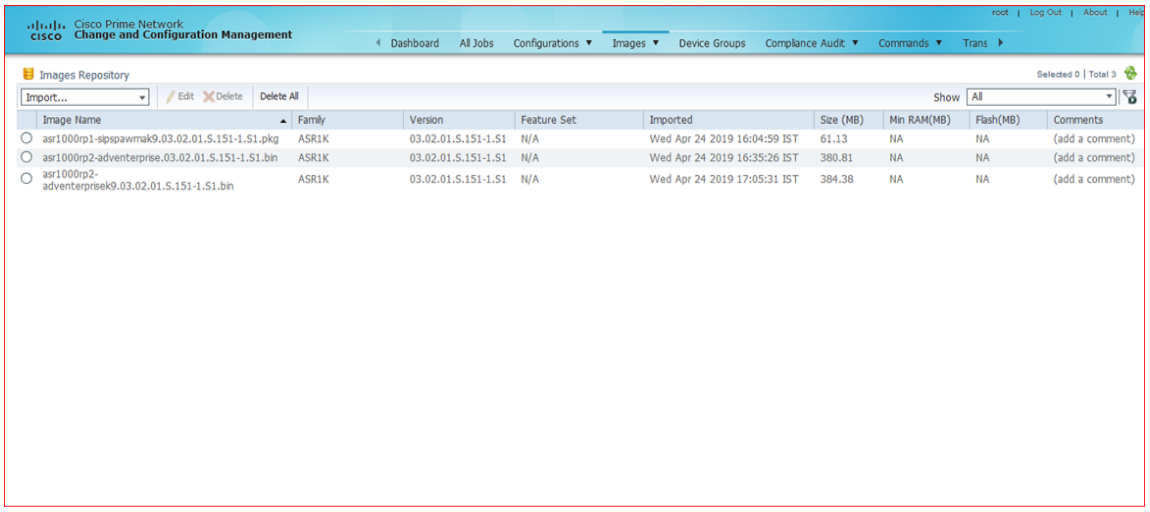
If you don't have permissions to import, the **ImgMgmt-CCO-Download** job fails with the following message:



If you have appropriate permissions, the **ImgMgmt-CCO-Download** job is created successfully:



The downloaded image is available at **Images** > **Repository**:



Creating an Image Baseline for New Devices

Use this method to create an image baseline—that is, directly copy images from existing devices to the image repository. This is useful when you add devices from a new device series or family.

For information on devices that support Image Baseline, see the *Cisco Prime Network 5.3 Supported VNEs - Addendum*.

See Figure 9-2 which illustrates how images are imported from devices into the database.

Note You cannot import tar files from IOS XR devices.

To import images from devices into the CCM image repository:

Step 1 Choose **Images > Repository**.

Step 2 From the Import drop-down list, choose **From Devices**. The Devices dialog box displays information about the device. For long texts in the **Element Type**, **Software Version**, and **Running Image** fields, hover the cursor over the hyperlink to display the entire contents.

Step 3 To import images from devices of a specific group, click **Select Groups**. Click the hyperlinked device group name to view the list of devices that belong to the group. See Setting Up CCM Device Groups, page 3-20 for more information on user-defined device grouping.

Step 4 Select the required device group in the Device Groups page and click **OK**.

The devices that belong to the selected device group are highlighted in the Devices page. You can also import all the devices existing in a group. To do so:

- Select a device group and click **Import from Group**.
- Enter the scheduling information as explained after Step 5 and click **Import from Group**.

Step 5 In the Devices page, click **Import**. A scheduler popup window appears.

Note You might be prompted to enter your device access credentials. This option is enabled if, from the Administration client, **Global Settings > Security Settings > User Account Settings > Execution of Configuration Operations**, you checked the option **Ask for user credentials when running configuration operations**. This is an enhanced security measure to restrict access to devices.

Step 6 Enter the scheduling information. By default, jobs are scheduled to run as soon as possible.

Note The time you specify here to schedule the import job is the gateway time.

Step 7 If you do not want to use the default transfer protocol, select a different protocol:

- TFTP (unsecured)
- SFTP/SCP (secured)
- FTP (unsecured)

For information on the default transfer protocol that each device use, see the *Cisco Prime Network 5.3 Supported VNEs - Addendum* and the *Cisco Prime Network 5.3 Supported Cisco VNEs*. For its Supported Protocols see the *Support for Change and Configuration Management in 5.3 tables.*

Step 8 If you have selected two or more devices, click one of the following to specify the operation mode:

- Parallel Order—Imports images from all devices at the same time.
- Sequential Order—Allows you to specify the order of the devices to import the images from. You can do so by moving the devices up and down in the Device Order box.

Note The Device Order box is only available for sequences containing less than 300 devices. CCM sequences the devices based on the order used when the devices were selected.

Step 9 Enter the e-mail ID(s) to which to send a notification after the import job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.

Note Before you enter the e-mail ID(s), ensure that you have set up the SMTP host and SMTP port in the Image Management Settings page (see Setting Up Image Management, page 3-15). The configured e-mail ID(s) will be displayed by default and can be modified if required.

Step 10 Click **Import**. CCM redirects you to the Jobs page, where you can monitor the status of the import job.

Note If you import all devices from a device group and, after creating the job, there is a change in the group, CCM updates the job accordingly such that all the devices available in the group at the time of the job execution are considered.

Step 11 Choose **Images > Repository** again to refresh the list of images. If any of the image information could not be retrieved, the field will display NA. (If pre-existing filters are still in use, you may need to click **Clear Filter**.) We recommend that you manually enter the information to ensure the accuracy of the upgrade analysis.

Step 12 Delete files from the storing directory (if applicable) to free space for future imports.

After the import, you can also add informational text to the Comments field. Normally at this point you will distribute the images; see Distributing Images and Making Sure They Will Work, page 9-15.

Distributing Images and Making Sure They Will Work

CCM can copy an image to a network element without activating it. This lets you perform these tasks before activating the image:

- Find out if there is insufficient memory, clear the disk space for distributing the image or package
- Do an upgrade analysis to check the suitability of the device for the chosen image

If appropriate, the images can be activated as part of the distribution job, and the following tasks can also be performed:

- Commit Cisco IOS XR (so that changes are saved across device reloads).
- Perform a warm upgrade, where one Cisco IOS image can read in and decompress another Cisco IOS image and transfer control to this new image (thus reducing the downtime of a device during planned software upgrades and downgrades).
- Perform an in-service software upgrade (ISSU) for Cisco ASR 903 devices to update the router software with minimal service interruption. CCM performs a s*ingle command upgrade* that installs a complete set of sub-packages using one command. The device must be configured in SSO redundancy mode. Before you perform an ISSU, you must verify if sufficient memory is available in standby boot flash.

  Note Cisco ASR 903 devices must be booted in sub-package mode only through boot flash and not through any sub-directories of boot flash *before* using CCM to perform an ISSU. For more information, see the *Cisco ASR 903 Series Router Chassis Configuration Guide.*

  In the Activation Scheduler page, check the **Boot in Subpackage mode** radio button to boot the Cisco ASR 903 devices.
- Perform an in-service software upgrade (ISSU) for Cisco 9000 series devices and CRS devices to update the router software with minimal service interruption. The option to perform ISSU is supported only for SMU packages.
- Perform an Image management operations using .iso & .rpm files in NCS6k device. The supported CCM operations are Image Distribution,Package add, Activate, Distribute and Activate and Commit.

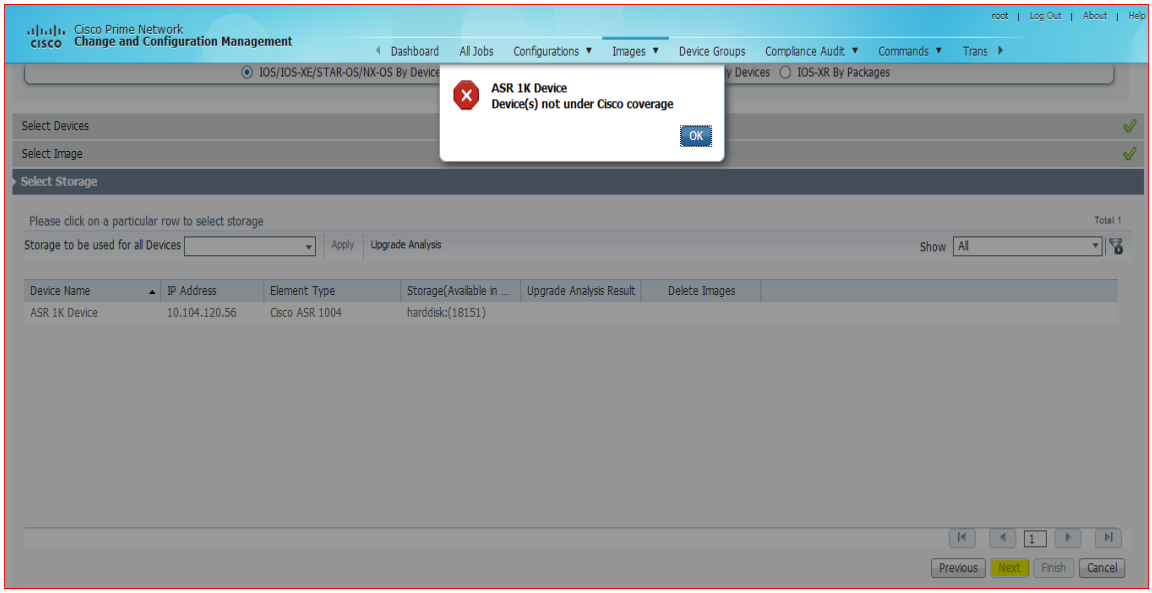
  For information on devices that support ISSU, see the *Cisco Prime Network 5.3 Supported VNEs - Addendum*. For its Supported Protocols see the *Support for Change and Configuration Management in 5.3 tables.*

CCM uses the image staging location and transport protocol (TFTP, by default) specified on the Image Management Settings page. CCM displays the available upgradeable modules and the storage partitions (if any) on the network element for the image distribution, from which you can choose the storage location you want to use.

The final step is to schedule the distribution job to occur either as soon as possible or at a future date (the default is as soon as possible).

Note Distributed devices are validated in real time. To check if a device falls under Cisco coverage, CCM requires your CCO credentials. You must update your CCO credentials in **Vendor Credentials pane** in **Images** > **Settings** page before proceeding to upgrade analysis.

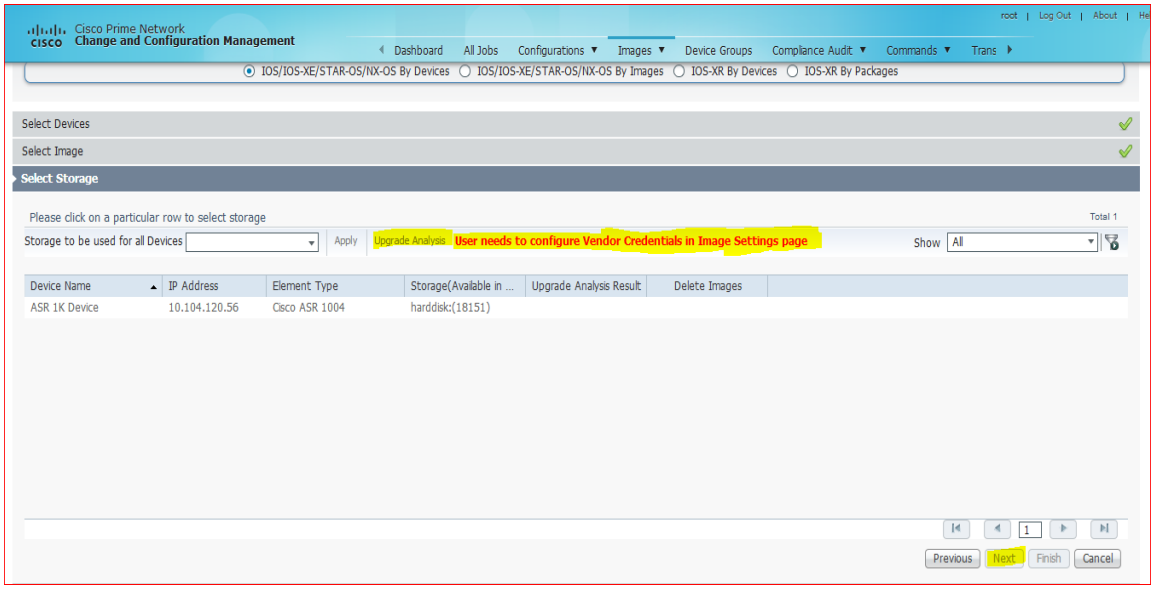
If a selected device is not under Cisco coverage, CCM displays the following error:



In such a case, remove the device.

If the selected device(s) is under Cisco coverage, you are allowed to perform distribution.

Also, if you do not configure your CCO credentials, the **Upgrade Analysis** and **Next** options are disabled in **Select Storage** panel and the following error message is displayed:



If you have configured your CCO credentials in **Vendor Credentials** pane, the **Upgrade Analysis** and **Next** options are enabled for use.

What is Upgrade Analysis?

An upgrade analysis checks the attributes of the selected image, checks certain device features, and generates a separate report for each device. It is required before any image can be distributed. However, even if the upgrade analysis reports errors, CCM will allow you to proceed with the distribution (because an error can be a simple matter of an unpopulated field).

CCM gathers this information from two sources:

- The Image Management repository, which contains information about minimum RAM, minimum Flash, and so on, in the image header.
- The Prime Network inventory, which contains information about the active images on the device, as well as Flash memory, modules, and processor details.

An upgrade analysis verifies that the device contains sufficient RAM or storage, the image is compatible with the device family, and the software version is compatible with the image version running on the device.

Table 9-1 denotes the symbols used on the Distribution page.

Table 9-1 Status Icons

Symbol	Description	
	In Device Status Column	**In Distribution Upgrade Analysis Column or Activation Analysis Results**
	Device is available for upgrade analysis and distribution.	Device passed without warnings.
	Device is not available for upgrade analysis or distribution. Most likely the device is in the Maintenance investigation state or the Unreachable communication state. Click the device hyperlink and open the device properties popup to see details about the device.	Device passed with warnings. Click the icon to get more information.
	n/a	Device did not pass analysis. Click the icon to get more information.

Distribute Images to Devices

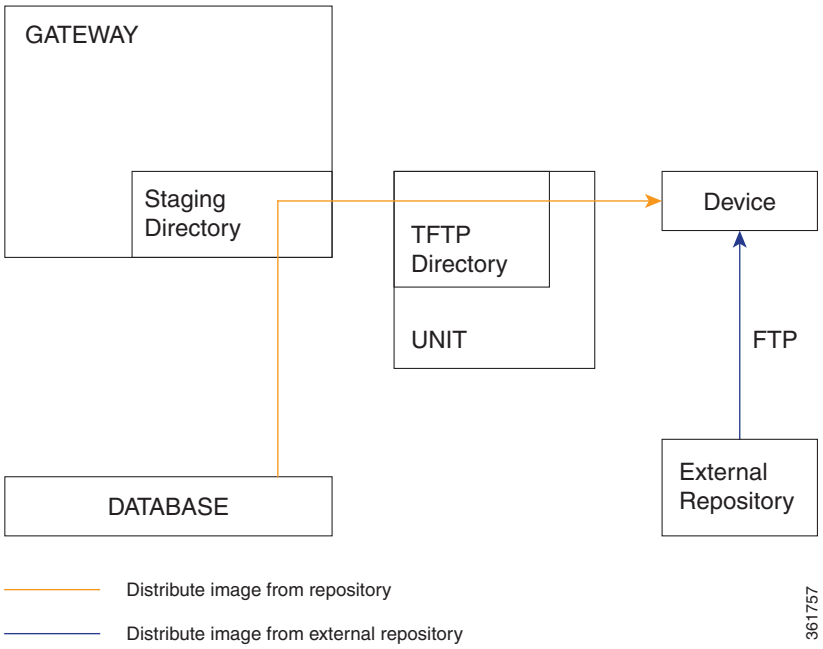
The following procedure explains how to perform an image distribution. You can also use this procedure to perform an upgrade analysis and then exit the procedure before performing the distribution.

Before You Begin

- If you are doing a Cisco IOS XR version upgrade (which upgrades the core package), see Managing Device Software Images, page 9-3 for information about other packages that you should upgrade at the same time.
- Make sure you have the permissions to perform the distribute operation. You will not be allowed to schedule a distribution job, if you do not have permissions.

Figure 9-3 illustrates the process of distributing images to devices.

Figure 9-3 Image Distribution Operations



To distribute images and use upgrade analysis:

Step 1 Choose **Images > Distribute.**

Step 2 Choose the device type (**IOS** or **IOS XR**) and selection method (by image or package, or by device). It is often easier to start with devices due to the sometimes cryptic nature of software image names. In this example we start with devices.

Note CCM does not support tar file operations on IOS devices. Tar file operations are supported only on Cisco Catalyst and IOS XR devices.

a. To choose devices of a specific device group, click **Select Groups** in the table header. Click the hyperlinked device group name to view the list of devices that belong to the group.

b. Select the required device group in the Device Groups page and click **OK**.

c. Choose one or more devices and click **Next**.

Step 3 CCM displays all images or packages, which are valid for the selected devices from the internal image repository (for example, kickstart images for Cisco Nexus 5000 or Cisco Nexus 7000, and boot configs for Cisco ASR 5000). You can also choose **From External Repository** from the drop-down list (in the table header) to display the images or packages from the external image repository.

Note CCM allows image distribution from external repository only through FTP. Make sure you have configured the required credentials for accessing the external image repository in the Image Management Settings page.

If you selected Cisco OLT devices, a list of filenames appear. The image files that do not have filename extensions belong to ONUs and image files that have filename extensions are that of an OLT device. For Cisco OLT devices, after you select the required images, the job scheduling page appears.

If you selected Tar file(s) for IOS XR devices, you cannot select any other non-tar file(s), and vice versa.

If you selected an Nexus devices (except for Nx9K), you can select a corresponding compatible image in the **Select Compatible Image** page, for a selected system image or a kickstart image.

Note Select Compatible Image is only optional. If a compatible image is selected for a System or Kickstart image you can perform both the Distribution and Activation of an image, otherwise you can perform only distribution of an image.

Choose an image and click **Next**.

Step 4 (Applicable only when distributing Cisco ONU images) After you select the required images, you must configure the image properties for a selected ONU image. From the Select ONU Image Properties pane, click **Configure ONU Images.**

When you perform a bulk activation for ONUs, the selected image will be applied to the ONU, the details of which matches with the information that you entered in this window**.**

Enter the following details:

Field	Description
Image Name	The name of the image selected.
ONU Profile ID	From the drop-down list, select an image profile to which this image must be distributed.
Software Version	The software version of ONU as available in the device.
Hardware Version	The hardware version of ONU as available in the device.
Description	A brief description.

Click **Next**. The **Select Storage** panel opens.

Step 5 In the **Select Storage** panel, choose a storage location by device or for all devices. This specifies where on the network element the image or package will be copied when it is distributed.

Step 6 (Not applicable to Cisco OLT devices) Perform an upgrade analysis to check whether the network element has sufficient space for the image or package by clicking **Upgrade Analysis**. After a few moments, CCM displays the results of the analysis in the Upgrade Analysis column. Click the symbol next to the icon to see the Upgrade Analysis report.

Symbol	Description	
	In Device Status Column	**In Distribution Upgrade Analysis Column or Activation Analysis Results**
	Device is available for upgrade analysis and distribution.	Device passed without warnings.
	Device is not available for upgrade analysis or distribution. Most likely the device is in the Maintenance investigation state or the Unreachable communication state. Click the device hyperlink and open the device properties popup to see details about the device.	Device passed with warnings. Click the icon to get more information.
	n/a	Device did not pass analysis. Click the icon to get more information.

If an error is reported, you will see a prompt asking you to confirm whether or not to proceed with the operation.

Step 7 (Not applicable to Cisco OLT devices) If you do not want to distribute any images or packages (for example, if you only wanted to perform a manual upgrade analysis), click **Cancel**. Otherwise, proceed to Step 8.

Step 8 Click **Next** to open the Schedule Distribution page in the wizard, and complete the schedule information.

Note You can proceed with scheduling the distribution only if upgrade analysis is completed for all the devices (spanning across multiple pages) in the Select Storage page.

Field	Description
Schedule Distribution	When the distribution job should run. **Note** The time you specify here to schedule the distribution job is the gateway time.
File Transport Protocol	Overrides the default transfer protocol (as configured on the Image Management Settings page).
Clear Flash	(Optional) In case of insufficient memory, use the **Clear Flash** option (under **Flash Properties**). This deletes any one file (other than the running image) and recovers the disk space occupied by the file. This procedure is repeated until adequate space is available in the selected flash.
E-mail Id(s)	E-mail ID(s) to which to send a notification after the scheduled distribution job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.

Field	Description
Install Add Package(s)	(Optional) Adds packages during distribution for Cisco IOS XR devices. **Note** While adding tar file(s) in the **Select Packages** page of the wizard, you can select the **Install Add Package(s)** and **Schedule Activation** check boxes separately and then schedule the jobs. **Note** If you have selected pie files in the Select Packages page in the wizard, CCM generates a tar file, which will be copied and added to the IOS XR devices.
Schedule Activation	(Optional) Starts an activation job once the images or packages are distributed (immediately or at future time). For multiple devices, we recommend that you perform the activation separately from the distribution. Not applicable to ONU image distribution.
Process	For multi-device jobs, controls the job processes for both distribution and activation. If you chose Sequentially, you can also do the following: • Specify the order in which the operations should be processed, by moving the items up and down in the Reorderable Rows box. • Stop the job if an error is encountered by checking the **Stop if an error occurs** check box. **Note** If the job includes a reload, choose **Sequentially**. Otherwise, routers in the connectivity path of other routers may reload and cause problems.
Commit	Commits the packages after activation for Cisco IOS XR devices.
Warm Upgrade	(For Cisco IOS only) Activates the Warm Upgrade feature to reduce the device downtime during the distribution process.
ISSU	Activates in-service software upgrade (ISSU) to update the router software with minimal service interruption. For information on devices that support ISSU, see the *Cisco Prime Network 5.3 Supported VNEs - Addendum*. For its Supported Protocols see the *Support for Change and Configuration Management in 5.3 tables.*

Step 9 Click **Finished**. You are redirected to the Jobs page, where you can check the status of the distribution job.

Note Distribution fails if a timeout occurs after 30 minutes. You can view the job results for information on why the distribution failed. Remember to delete older images and packages from the staging directory.

File System Clean Up

While performing upgrade analysis, if the available storage space in the device is lesser than the selected image size, then the user can increase the storage space by following the procedure provided below:

Step 1 Click the **Action** link under the **Delete Images** option in the **Select Storage** page. This opens the **Delete Image Table** window with a list of files.

Step 2 Check the check box near each file to select the files to be deleted in the **Delete Image Table** window.

Step 3 Click **Apply**. This deletes the files that are selected, thus increasing the storage space.

Note You can view the increased storage space by clicking the **Upgrade Analysis Result** option in the **Select Storage** page without repeating the upgrade analysis process.The selected files in the **Action** window are actually not deleted when you click the **Apply** button. File deletion in device happens only when you schedule the distribution job.

Activating Cisco IOS Software Images

These topics describe the tasks you can perform from the Activate page:

- Activating Cisco IOS Software Images
- Activating After Performing Boot Priority Modification for Cisco StarOS Devices

When a new Cisco IOS image is activated on a device, it becomes the running image on the disk. Deactivated images remain on the disk to be removed by a user. Older images are automatically deactivated.

Before You Begin

Make sure you have the permissions to perform the activate operation. You will not be allowed to schedule an activation job, if you do not have permissions.

Distributing and activating the images should not be done from standby or alias boot flash. For example, for Cisco Catalyst 6500 Virtual Switching System (VSS), you must use the images from sup-boot disk for activation. Similarly, for Cisco ASR 903 Series Aggregation Services Routers, you must use the images from boot flash for activation.

Activating Cisco IOS Software Images

To activate a Cisco IOS image on a network element:

Step 1 Choose **Images > Activate.**

Step 2 From the Cisco Devices tab, choose **IOS** by activation method (**IOS by Images** or **IOS by Devices**). It is often easier to start with devices due to the sometimes cryptic nature of software image names. In this example we start with devices.

Step 3 CCM displays all managed devices. It also displays the images that are currently running on the devices. You can filter by device name, IP address, element type, running image, or software version.

a. To choose devices of a specific device group, click **Select Groups** in the table header. Click the hyperlinked device group name to view the list of devices that belong to the group.

b. Select the required device group in the Device Groups page and click **OK**.

Note If you selected CPT devices, upon choosing the devices, CCM directs you to the Schedule Activation page directly. You will not be able to choose specific images for CPT devices.

c. Choose one or more devices and click **Next**. CCM displays all images or packages which are valid for the selected devices from the internal image repository (for example, kickstart images for Cisco Nexus 5000 or Cisco Nexus 7000, and boot configs for Cisco ASR 5000). You can also choose **From External Repository** from the drop-down list (in the table header) to display the images or packages from the external image repository.

Step 4 CCM displays all images or packages which are valid for the selected devices from the internal image repository. CCM displays only root level bin files for selection.

Step 5 Choose the image that you want to activate on the devices, and click **Next**.

Step 6 CCM performs an image analysis. Check the Image Analysis page to see if analysis was successful. Click the icon in the Analysis column to get information about why the operation can or cannot proceed.

Symbol	Description	
	In Device Status Column	**In Distribution Upgrade Analysis Column or Activation Analysis Results**
	Device is available for upgrade analysis and distribution.	Device passed without warnings.
	Device is not available for upgrade analysis or distribution. Most likely the device is in the Maintenance investigation state or the Unreachable communication state. Click the device hyperlink and open the device properties popup to see details about the device.	Device passed with warnings. Click the icon to get more information.
	n/a	Device did not pass analysis. Click the icon to get more information.

If it cannot proceed, you will not be permitted to continue. Otherwise, click **Next.**

Step 7 Enter the scheduling information in the **Schedule Activation** page. By default, jobs are scheduled to run as soon as possible.

Note The time you specify here to schedule the activation job is the gateway time.

Step 8 Enter the e-mail ID(s) to which to send a notification after the scheduled activation job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.

Step 9 (For Cisco IOS only) Activate the **Warm Upgrade** option, which allows a Cisco IOS image to read in and decompress another Cisco IOS image and transfer control to this new image (thus reducing the downtime of a device during planned software upgrades and downgrades).

Step 10 Check the **ISSU** option, to update the router software with minimal service interruption.

Step 11 Click one of the following to specify the operation mode, if you have selected two or more devices in the Select Devices page.

- **In Parallel**—Activates all packages for the devices at the same time.
- **Sequentially**—Allows you to define the order of the devices to activate the packages for.

Step 12 Click **Finished to schedule the activation**.

Note For IE2K devices, CCM activation job will fail if the device is configured as “YES” with environment variable "MANUAL_BOOT" (MANUAL_BOOT - decides whether the switch boots up automatically or manually).

Activating After Performing Boot Priority Modification for Cisco StarOS Devices

To modify boot priorities for Cisco StarOS devices and then perform activation:

Step 1 Choose **Images > Activate > IOS** and the activation method (by **Devices**).

Step 2 Choose the Cisco StarOS device family from the table header. CCM displays all managed Cisco StarOS devices. It also displays the images that are currently running on the devices. You can filter by device name, IP address, element type, running image, or software version.

Step 3 Select a Cisco StarOS device, choose the **Perform Edit Boot Priorities** option from the drop-down menu in the table header, and then click **Next**. The Select Boot Config page appears.

Step 4 Click the **Edit Boot Priorities** hyperlink. The Current Boot Priorities table lists the existing boot configuration files with their priorities.

Step 5 Provide the following inputs to set up and fetch the desired boot priorities:

- Number of boot priority entries to be maintained. Value should be in the range of 1-10.
- Boot priority number to start with. Value should be in the range of 1-100. Boot priority starting value should be greater than or equal to the number of boot priorities to be maintained.

Step 6 Click **Go** to generate boot priorities based on the inputs provided. The modified boot priorities are listed in the table below.

Step 7 You can choose to perform one of the following for each row in the table:

- **Edit**—Modify the boot priority value, the image name, and the configuration file, if required. The modified boot priority value should be unique.
- **Delete**—Delete the boot configuration priority.
- **Add Row**—Add boot priorities to the existing list. CCM generates boot priority values based on the inputs provided. Note that only the top ten boot priorities are considered for the device.

Step 8 Click **Save**. A dialog box appears listing the existing and the modified boot priorities for your confirmation.

Step 9 Click **Save** to confirm and apply the boot priority changes.

Step 10 You can then schedule the activation as explained in Activating Cisco IOS Software Images, page 9-22.

Activate OLT Images

Step 1 Choose **Images > Activate.**

Step 2 Select OLT from the drop-down list. Click **Next.**

Only one image is present in the OLT device. Upon performing the activation operation, the OLT image present in the device is activated.

You will be directed to the schedule page.

Activate ONU Images in Bulk

OLT images can be activated using two modes—Manual or Auto. Using the Auto mode, you can activate an image that is marked as the default image. However, using the Auto mode, you can change the image configuration and then activate the image on the selected device.

Step 1 Choose **Images > Activate.**

Step 2 From the Cisco Devices tab, choose **IOS** by activation method (**IOS by Images** or **IOS by Devices**). It is often easier to start with devices due to the sometimes cryptic nature of software image names. In this example we start with devices.

Step 3 Prime Network displays all managed devices. It also displays the images that are currently running on the devices. You can filter by device name, IP address, element type, running image, or software version.

a. To choose devices of a specific device group, click **Select Groups** in the table header. Click the hyperlinked device group name to view the list of devices that belong to the group.

a. Select the required device group in the Device Groups page and click **OK**.

a. Choose one or more devices and click **Next**. Prime Network displays all images or packages which are valid for the selected devices from the internal image repository.

Step 4 Choose the image that you want to activate on the devices. Choose Bulk Upgrade from the drop-down list and then choose the type of mode. Click **Next**. The following combinations are possible:

- Bulk Upgrade and Manual Mode
- Bulk Upgrade and Auto Mode

Bulk Upgrade and Manual Mode

Step 1 From the Selected OLTs for Manual Upgrade pane, click the **Configure ONU Images** hyperlink. This window displays the ONU images that are present in the OLT device.

Using this window, the image properties can be configured. To configure image properties, click the respective cell in the table, and change the value. Click **Save.**

Step 2 Choose an image and click **Manual Upgrade.** Set the slot number, PON number, and ONU ID to which the selected image must be applied. To apply the image on all slots, PONs, or ONUs, select **All**. The image is subsequently applied to all ONUs which have the upgrade mode set to Off in the device.

Step 3 Click **Commit** or **Activate**, as required. Clicking Commit will activate the image when the ONU is restarted. Clicking Activate will active the image immediately. If you choose neither Activate nor Commit, the image will overwrite the existing inactive image. Click **Manual Upgrade**. You are redirected to the original pane.

Step 4 Click **Next**.

You are redirected to the Schedule Activation job page.

Bulk Upgrade and Auto Mode

Step 1 The selected OLTs appear in the Selected OLTs for Auto Upgrade pane. Set the slot and PON to which you want the image to be activated.

- Auto—An ONU profile can have several images, of which only one is default. When you activate the image in Auto mode, only the image which is the default image for the selected ONU profile is applied.
- Planned—The image with which the software version matches with that of the selected ONU is applied.

To configure image properties, click the respective cell in the table, and change the value. Click **Save.**

Step 2 Click **Next**.

You are directed to the Schedule Activation job page.

Activate ONU Image Individually

Step 1 Choose **Images > Activate.**

Step 2 Choose an OLT image and click **Next.**

Step 3 From the Select ONU pane, set the slot, PON, and ONU and click on **Show ONU Image** hyperlink. The Show ONU Images dialog box displays the list of images that can be activated for the selected ONU.

Step 4 From the Show ONU Images dialog box, choose an image. Of the two images that are displayed, you must choose an image that is currently not active.

Step 5 Click **Next**.

You are directed to the Schedule Activation job page.

Activate Nexus OS Image Individually

For Nexus devices you can distribute two images such as System image and Kickstart image. if you want to distribute any image to Nexus device (Except Nx9k), in the **Select image** page, select either of any one of the image and in "Select Compatible image" corresponding compatible image will be shown. This is optional page. This page is applicable only for Nexus device.

Step 1 Choose **Images > Activate.**

Step 2 Choose an Nexus device and click **Next.**

Step 3 From the Select Image pane, set the slot, PON, and ONU and click on **Show ONU Image** hyperlink. The Show ONU Images dialog box displays the list of images that can be activated for the selected ONU.

Step 4 From the Show ONU Images dialog box, choose an image. Of the two images that are displayed, you must choose an image that is currently not active.

Step 5 Click **Next**. You are directed to the Schedule Activation job page.

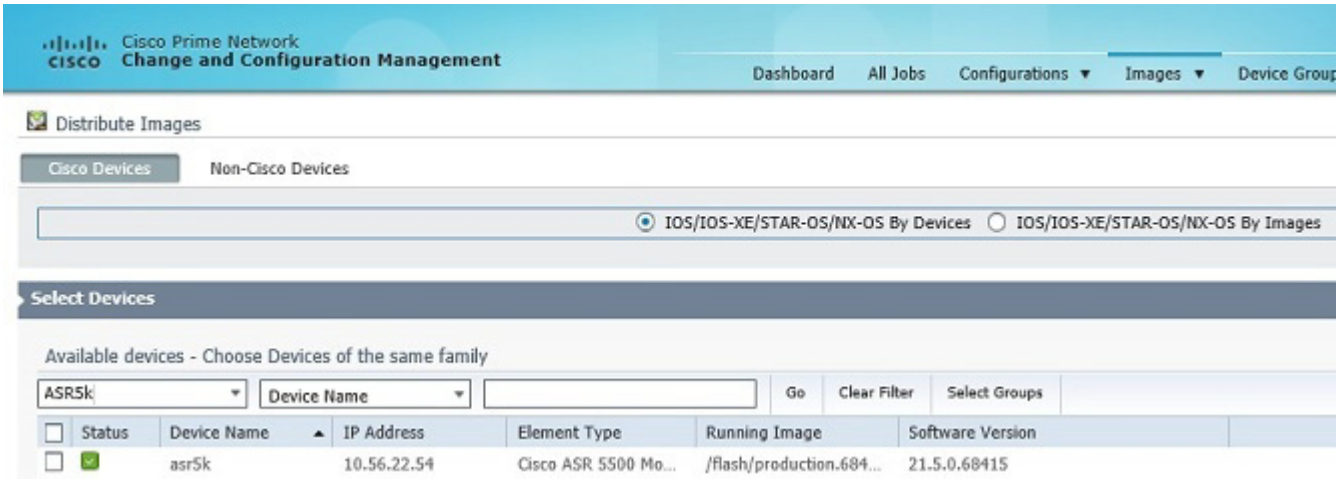
Copy and Distribute BulkStat File for Star OS Devices

You can copy and distribute BulkStat file along with image files for StarOS devices such as ASR5500, or SI or DI devices.

Step 1 Choose **Images > Distribute.**

Step 2 In the Distribute Images window, in the Select Devices area, choose from the **Available Devices** filter fields choose a device and device name of the same family. For example, ASR5k, or SI, or DI.

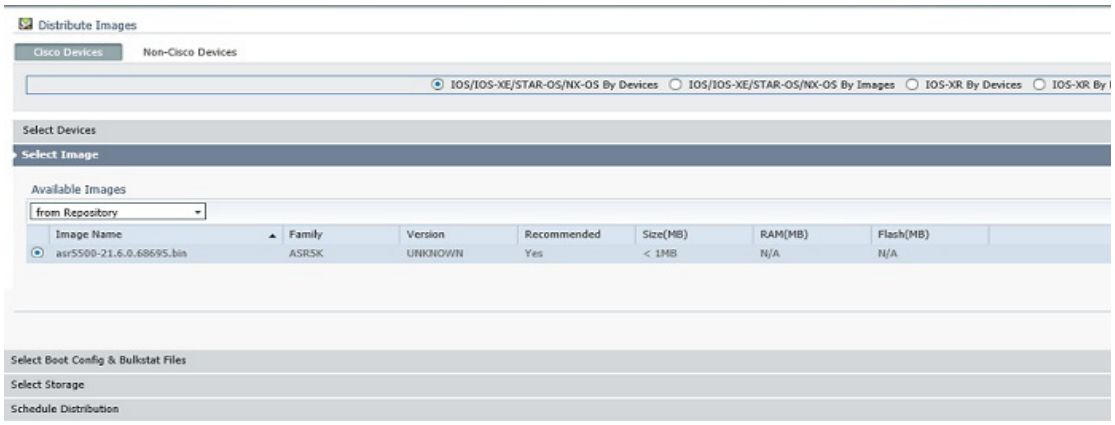
Figure 9-4 Select an ASR 5K or SI or DI Device



Step 3 Click **Next.**

Step 4 In the Select Image area, select an image for distribution to the selected device as shown in Figure 9-5..

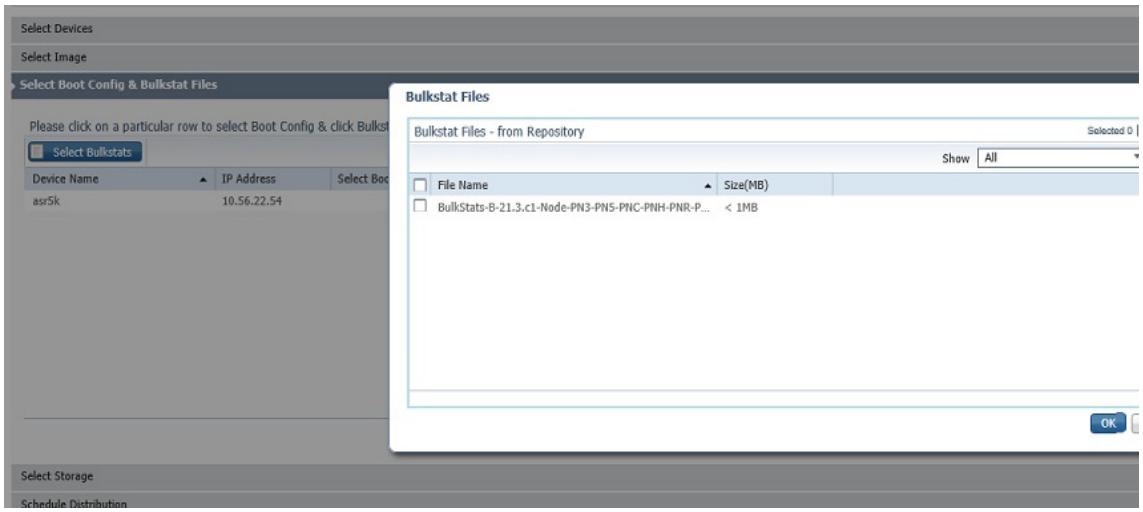
Figure 9-5 Select an Image



Step 5 Click **Next**.

Step 6 In the Select Boot config & Bulkstat files area, If you click the Select **Bulkstats** button, a dialog box appears with available Bulkstat files for upload as shown in Figure 9-6.

Figure 9-6 Select BulkStat files



Step 7 Select a text file or multiple text files along with the image files for distribution to devices.

Step 8 Click **Next**.

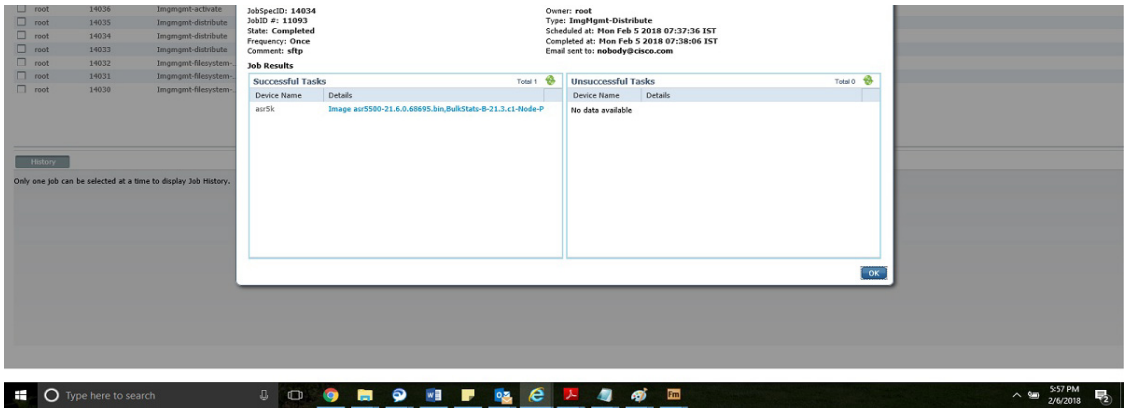
Step 9 In the Select Storage area, from the Storage to be used for all devices list box, choose a storage.

Step 10 Enter the Schedule distribution details, if required.

Step 11 Click **Finish**

Step 12 In the Image Management Jobs page, choose the device name and then click the Success link. The Job Details dialog box appears as shown in Figure 9-7.

Figure 9-7 View Job Details



Step 13 Click **OK** to view the distributed job details for the selected device.

Performing Cisco IOS XR Software Package Operations

Note We recommend that you do *not* commit the package change until the device runs with its configuration for a period of time, until you are sure the change is appropriate. In that way, the change is not yet persisted across device reloads.

These topics explain how to perform package operations:

Notes on Cisco IOS XR Packages

Package management includes the add, activate, deactivate, commit, and rollback operations on Cisco IOS XR devices. Before you perform any of these operations, read the following:

- When doing a version upgrade (which upgrades the core package and involves a router reload) on a Cisco IOS XR device, all of the packages on the router should be upgraded at the same time, as part of the same job. For example, if the c12k-mini, c12k-mgbl, c12k-mpls, c12k-k9sec, and c12k-mcast packages are on the router at version 5.3, when upgrading to version 5.3, all of the packages must be upgraded at the same time to version 5.3.

Note An upgrade pie is required only when you upgrade Cisco IOS XR devices from version 3.x to 4.x. You must deactivate and remove the upgrade pie, if you wish to perform any install operations, including the install commit operation on the devices upgraded from 3.x to 4.x.

- When upgrading the core router package (such as c12k-mini or comp-hfr-mini), the manageability package (such as c12k-mgbl or hfr-mgbl-p) must be upgraded at the same time to ensure that the router remains manageable after the reload.
- Cisco IOS XR routers support the **clear install rollback oldest x** command, that allows you to manage the number of rollback points maintained on the router. Executing this CLI command periodically on the router allows you to limit the number of rollback points. When executing this command, you must ensure that at least one valid rollback point is always maintained to enable CCM to show the package status correctly. We recommend that you maintain about 20 rollback points on the router.
- CCM does not support upgrading a router running Cisco IOS software to Cisco IOS XR software.

For more information, refer to the *System Management Configuration Guide* for the Cisco IOS XR release and device of interest.

Adding Cisco IOS XR Packages

Image Management supports package addition as a separate operation for Cisco IOS XR devices. To complete the package management life cycle, Image Management supports adding a package from a pie file and a tar file, which is already present in the Cisco IOS XR device storage.

Before you begin:

Make sure you have the permissions to perform package addition. You will not be allowed to schedule a package addition job, if you do not have permissions.

To add packages for Cisco IOS XR devices:

Step 1 Choose **Images > Package Add**. The Package Add wizard displays all the Cisco IOS XR devices in the Select Device(s) page.

Step 2 Select a device and click **Next** to open the Select Package(s) page. CCM displays all the packages available for the selected device.

Step 3 Choose the package(s) that you want to add for the selected device and click **Next** to open the Schedule Package Addition page in the wizard.

Step 4 Enter the scheduling information. By default, jobs are scheduled to run as soon as possible.

Note The time you specify here to schedule the package addition job is the gateway time.

Step 5 If you have selected two or more devices in the Select Devices page, click one of the following to specify the operation mode:

- In Parallel Order—Add packages for all devices at the same time.
- In Sequential Order—Allows you to specify the order of the devices to import the packages for.

Step 6 Enter the e-mail ID(s) to which to send a notification after the scheduled package addition job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.

Step 7 Click **Finished**. CCM schedules the job and redirects you to the Jobs page, where you can monitor the status of the job.

Activating, Deactivating, and Deleting Cisco IOS XR Packages

Note For Cisco IOS XR devices, we recommend that you do not commit the package change until the device runs with its configuration for a period of time, until you are sure the change is appropriate. In that way, the change is not yet persisted across device reloads.

Before You Begin

- If you are doing a Cisco IOS XR version upgrade (which upgrades the core package), see Managing Device Software Images, page 9-3 for information about other packages that you should upgrade at the same time.

To activate or deactivate a Cisco IOS XR package, or delete a Cisco IOS XR package from a device:

Step 1 Choose **Images > Activate > IOS-XR** and the activation method (by **Packages** or **Devices**.). It is often easier to start with devices due to the sometimes cryptic nature of software image names. In this example we start with devices.

Step 2 CCM displays all managed devices. (It also displays the packages that are currently running on the devices.) From this page you can also view the running package of the Cisco IOS XR device.

a. To choose devices of a specific device group, click **Select Groups**. In the Device Groups page, you can view the user-defined device groups. Click the hyperlinked device group name to view the list of devices that belong to the group. See Setting Up CCM Device Groups, page 3-20 for more information on user-defined device grouping.

b. Select the required device group in the Device Groups page and click **OK**.

c. Choose one or more devices and click **Next**. CCM displays all packages which are valid for the selected devices. You can filter your results by package name and version.

d. Choose the packages that you want to activate on the devices, and click **Next**.

Step 3 Specify the operations you want to perform. You can perform different operations on different devices or the same operation on all devices (by selecting the desired operation from the **Use the following Operation for all Packages** drop-down list in the table header). When you select a device, CCM will display all of the packages that are installed on the device.

a. Choose a package operation for each package. Cisco IOS XR packages can be removed from a device only if they have been deactivated. If you want to apply the same operation to all packages, choose the operation from the **Use the following Operation for all Packages** drop-down list in the table header, and click **Apply**.

b. (Optional) Check **Test Only** to run a test of the activation (or deactivation) procedure on the device. This will not change the real device configuration. (This is similar to using the Compatibility Check option in the rollback process.)

c. Click **Next**. The Package Analysis page is displayed. Check the Package Analysis page to see if analysis was successful. Click the icon in the Analysis column to get information about why the operation can or cannot proceed (it will be one of the icons listed in Table 9-1 on page 9-17). If it cannot proceed, you will not be permitted to continue. Otherwise, click **Next**.

Step 4 Enter the scheduling information. By default, jobs are scheduled to run as soon as possible.

Note The time you specify here to schedule the activation job is the gateway time.

Step 5 Enter the e-mail ID(s) to which to send a notification after the scheduled activation job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.

Step 6 Check the **ISSU** option, to update the router software with minimal service interruption. For information on devices that support ISSU, see the *Cisco Prime Network 5.3 Supported VNEs - Addendum*. For its Supported Protocols see the *Support for Change and Configuration Management in 5.3 tables.*

Step 7 Check the **Commit** check box to commit the packages after activation.

Note We recommend that you do *not* commit the package change until the device runs with its configuration for a period of time, until you are sure the change is appropriate. In that way, the change is not yet persisted across device reloads.

Step 8 Click one of the following to specify the operation mode, if you have selected two or more devices in the Select Devices page.

- **In Parallel**—Activates packages for all devices at the same time.
- **Sequentially**—Allows you to define the order of the devices to activate the packages for.

Step 9 Click **Finished to schedule the activation**.

Step 10 After the job completes:

- For Test Only jobs, repeat this procedure to activate the packages.
- If you activated or deactivated a Cisco IOS XR package, remember to commit your changes. However, we recommend that you do not commit the package change until the device runs with its configuration for a period of time, until you are sure the change is appropriate. In that way, the change is not yet persisted across device reloads. See Committing Cisco IOS XR Packages Across Device Reloads, page 9-33.

Synchronizing and Upgrading Satellites for Cisco ASR 9000 Devices

CCM provides satellite support for Cisco ASR 9000 devices. Satellites are used to enhance performance bandwidth of Cisco ASR 9000 devices. Each satellite is a Cisco IOS device connected to the Cisco ASR 9000 device. Multiple satellites can be connected to a single Cisco ASR 9000 device and all communications to the satellites happen only through the Cisco ASR 9000 device. Each satellite has its own configuration and software image.

CCM provides the following support for Cisco ASR 9000 device with satellites:

- Synchronization of all satellites together.
- Activation of the satellite pie image on Cisco ASR 9000 device with and without synchronization of satellites. You must run a CLI/XML command to check for compatibility and then push the image to the remote satellite.

Synchronize All Satellites Without Performing an Activation

To synchronize all satellites together without activation:

Step 1 Choose **Images > Activate > IOS-XR** and the activation method (by **Devices**).

Step 2 Choose the Cisco ASR 9000 device family and the **Sync Satellites** option from the **Select Operations** drop-down menu in the table header.

CCM displays all managed Cisco ASR 9000 series devices having satellites. (It also displays the packages that are currently running on the devices.)

Step 3 Click **Next** to schedule the synchronization for all the satellites together. You cannot select a particular satellite for synchronization. The Select Operation function is not applicable for the Sync Satellites option.

Step 4 In the Schedule Activation page, provide the scheduling information for synchronization of all satellites.

Note The time you specify here to schedule the activation job is the gateway time.

Step 5 Check the **Sync Satellite(s)** check box and click **Finished**. The Sync Satellite(s) check box is available only for Cisco ASR 9000 devices having satellites.

Activate Satellite Image on Cisco ASR 9000 Device With or Without Synchronization

To activate a satellite image on the Cisco ASR 9000 device with/without satellite synchronization:

Step 1 Choose **Images > Activate > IOS-XR** and the activation method (by **Devices**).

Step 2 Choose the Cisco ASR 9000 device family and the **Activate and/or Sync Satellites** option from the **Select Operations** drop-down menu in the table header.

Step 3 Perform Step 3 through Step 7 in Activating, Deactivating, and Deleting Cisco IOS XR Packages, page 9-30 topic.

Step 4 Check the **Sync Satellite(s)** check box, if you wish to upgrade and synchronize the satellites. The Sync Satellite(s) check box is available only for Cisco ASR 9000 devices having satellites.

Note Synchronization of satellites is done, only if the operation selected is activation or deactivation. Otherwise, synchronization will not happen even if this check box is selected.

Step 5 Click **Finished to schedule the activation and/or synchronization**.

Committing Cisco IOS XR Packages Across Device Reloads

Committing a Cisco IOS XR package makes the device package configurations persist across device reloads. The commit operation also creates a rollback point on the device. See Rolling Back Cisco IOS XR Packages, page 9-34, for more information on rollback points.

Note We recommend that you do not commit package changes until the device runs with its configuration for a period of time, until you are sure the change is appropriate. In that way, the change is not yet persisted across device reloads.

Before You Begin

- Verify that the package to be committed is operating properly (for example, by doing a **show status** command).
- Make sure you have the permissions to perform the commit operation. You will not be allowed to schedule a commit job, if you do not have permissions.

To commit a package after it has been activated, deactivated, or rolled back:

Step 1 Choose **Images > Commit**.

Step 2 Choose the network elements with the packages you want to commit.

Step 3 Click one of the following (in the table header) to specify the commit mode:

- **Commit in Parallel**—Commits all changes at the same time.
- **Commit Sequentially**—Allows you to define the order in which the changes are committed.

Step 4 Enter the scheduling information.

Note The time you specify here to schedule the commit job is the gateway time.

Step 5 Enter the e-mail ID(s) to which to send a notification e-mail after the scheduled commit job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.

Step 6 Click **Commit**. By default, jobs are scheduled to run as soon as possible.

Rolling Back Cisco IOS XR Packages

Rolling back a Cisco IOS XR package reverts the device packages to a previous installation state—specifically, to a package installation rollback point. If a package has been removed from a device, all rollback points associated with the package are also removed and it is no longer possible to roll back to that point.

Before You Begin

- Read Managing Device Software Images, page 9-3, for information about managing rollback points on Cisco IOS XR devices.
- Make sure you have the permissions to perform the rollback operation. You will not be allowed to schedule a rollback job, if you do not have permissions.

To roll back a Cisco IOS XR package:

Step 1 Choose **Images > Rollback**. CCM displays all Cisco IOS XR devices. You can filter the results by using the **Quick Filter** option.

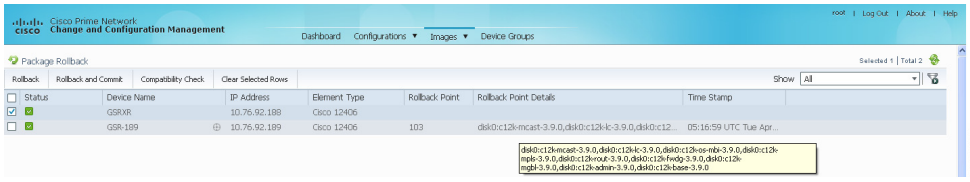
Step 2 Choose the network elements. CCM populates the rollback points for the selected device package.

Step 3 Choose a rollback ID from the Rollback ID drop-down list. The Rollback Point Details field lists the packages that were active when that ID was created.

Step 4 To view all of the packages associated with the rollback point, place the mouse cursor on the Rollback Point Details field; see Figure 9-8 for an example. To view the time stamp associated with the selected rollback, see the value displayed in the Time Stamp field.

Note The date and time stamps are displayed according to the local time zone settings of the client.

Figure 9-8 Packages Rollback Page with Rollback Point Details



Step 5 Click **OK** to close the popup window.

Note If a package has been deleted from the repository, the rollback points of the package are still displayed in CCM. If you choose a rollback point for a deleted package, the rollback will fail. The job results popup provides information explaining why it failed.

Step 6 (Optional) Click **Compatibility Check in the table header** to run a test of the rollback procedure on the device. This will not change the real device configuration. (This is similar to using the Test Only option in the activation process.)

Step 7 Click **Rollback or Rollback and Commit.**

Note We recommend that you do not commit package changes until the device runs with its configuration for a period of time, until you are sure the change is appropriate. In that way, the change is not yet persisted across device reloads. See Committing Cisco IOS XR Packages Across Device Reloads, page 9-33.

Step 8 Enter the scheduling information.

Note The time you specify here to schedule the rollback job is the gateway time.

Step 9 Enter the e-mail ID(s) to which to send a notification after the scheduled rollback job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.

Note Before you enter the e-mail ID(s), ensure that you have set up the SMTP host and SMTP port in the Image Management Settings page (see Setting Up Image Management, page 3-15). The configured e-mail ID(s) will be displayed by default and can be modified if required.

Step 10 Click **Rollback**.

Cleaning Up the Repository

The repository is purged according to the settings described in Setting Up Image Management, page 3-15. When files are removed from the repository, this does not affect files that are installed on the device. However, deleting a package could cause a rollback point to become unexecutable. If a package or version of a package that is associated with a specific rollback point is removed, it will no longer be possible to roll back to that point. See Rolling Back Cisco IOS XR Packages, page 9-34.

To delete images from the CCM image repository:

Step 1 Choose **Images > Repository**.

Step 2 Select the image you want to delete and click the Delete button (with red **X)** in the table header.

Step 3 To collectively delete all images in the repository, click the **Delete All** button in the table header. You will see a prompt asking you to confirm whether or not to proceed with the operation.

Step 4 Click **OK** to confirm and image(s) available in the repository will be deleted.

Managing Device Configurations

The CCM Configuration Management feature enables you to control and track changes that are made to a device configuration. It uses a change management feature to detect ongoing changes to devices in two ways:

- When doing periodic archiving of device configurations. If CCM detects a change in a configuration file, it will get the new version of the file from the device and copy it to the archive.
- When a configuration change notification is received from a device. This is called event-triggered archiving. You can configure CCM to copy a new version of a configuration file to the archive whenever a change is detected, or to queue the changes and then copy the files to the archive according to a schedule.

By default, neither of these methods are enabled. You can configure them from the Configuration Management Settings page (see Setting Up Configuration Management, page 3-5).

Change Logs provide information on the changes made to devices in the network, sorted by their time stamp. The Configuration Management Settings page controls how long these logs are saved. CCM saves messages that can be used for debugging in *NETWORKHOME*/XMP_Platform/logs/ConfigArchive.log.

Note Keep these notes in mind when using Configuration Management:

- Devices must be in the Device Reachable communication state and the Operational investigation state. See Checking the Device State, page 11-19 for an explanation of how to check state information.
- CCM does not support special characters for any of the editable fields in the client, including filters.
- Cisco IOS devices using SNMPv3 must be configured with write permission for the CISCO-CONFIG-COPY-MIB MIB group.

The following topics explain how to work with device configurations:

What is In the Configuration Archive?

Choose **Configurations > Archives** to view the contents of the archive. The configuration archive maintains copies of device configuration files, storing them in the database. Configuration files are stored in readable format, as received from the device. You can edit existing archive files and save for deployment at a later time. The edited archive files are available in the Edited Archive tab. The total number of archives available in the database is also displayed in the header. The configuration, after deployment, can also be restored to the original state. Users can only see devices that are in their device scope. For enhanced security, you might be prompted to enter your device access credentials when you try viewing device details or when you try performing configuration changes on devices. This option is enabled if, from the Administration client, **Global Settings > Security Settings > User Account Settings > Execution of Configuration Operations**, you checked the option **Ask for user credentials when running configuration operations**.

The Archived Configurations page displays the following information about each configuration file.

Table 9-2 Configuration Information Displayed on Archived Configurations Page

Field	Description
Device Name	Name of device. Click the icon next to the device name to open a popup that displays device properties. Additional information is listed depending on the device type: • Current active packages on the device—For Cisco IOS XR devices • Active kickstart images—For Cisco Nexus OS devices • Priority list—For Cisco StarOS devices. The priority list displays various combinations of a configuration file and an image file in priority order for the device.
Version	An internally-used number. A version will not have an associated configuration file under the following circumstances: • The associated configuration file was deleted from the archive. • The associated configuration file has not yet been copied to the archive. (CCM supports queuing change notifications and copying the configuration files to the archive at a later time. See Setting Up Configuration Management, page 3-5.) Click a version number hyperlink to launch the Device Configuration Viewer, from which you can view the contents of a configuration file.
Type	Type of configuration for each device. For information on the devices that support the different configuration type, see the *Cisco Prime Network 5.3 Supported VNEs - Addendum*.
Vendor	Specifies the device vendor: Cisco or non-Cisco device.
Date Changed	Date and time of last change, displayed according to the local time zone settings of the client. For Cisco CPT, Cisco StarOS, and Cisco ME 4600 series OLT devices, this field displays N/A.
Label	User-assigned archive labels.
Running Image	The software image currently running on the device.

Table 9-2 Configuration Information Displayed on Archived Configurations Page (continued)

Field	Description
Context / Module / Priority	For Cisco Nexus OS devices, this field displays the virtual device context (VDC) name. For Cisco 7600 series devices, this field displays the module name. For Cisco StarOS devices, this field displays the boot configuration files with their priorities. For Cisco CPT 200 and Cisco CPT 600 devices, this field displays the operation mode details. For other devices, this field displays N/A. **Note** SNMPv3 and SSHv2 are supported in the CPT 600/200 devices. The support is limited to software version 9.535/9.536.
Comments	User-assigned free text.
Commit Id	(Cisco IOS XR only) ID that identifies the last configuration change on the device (maximum number saved is 100).

Note CCM does not support the view, compare, edit, and, edit and restore operations if the configuration file is in binary format.

Protecting and Labeling Important Configurations in the Archive

Assigning labels to configuration files is a clear, simple way to identify important configurations and convey critical information. You can manage labels by choosing **Labels > Manage**.

- Adding a label adds it to the catalog where it is made available to all users. Add labels by clicking **Add Row**.
- Deleting a label unassigns the label from configurations that are using it. Likewise, if you edit a label, the change is applied to all configurations using the label.
- Unassigning a label does not delete the label from the catalog.
- Labels with the “do not purge” property will not be purged from the archive (the delete action is disabled). When calculating the total number of archives to see if the maximum has been reached and archives should be purged, CCM does not include configurations with this label in the total (see Setting Up Configuration Management, page 3-5).

Editing an Archive Configuration

You can edit an existing device archive file and save the edited file. This edited archived file is stored in the Prime Network database, and the edited file can be deployed at any time. This can be viewed from the **Edited Archive** tab, in the Archive page. Every time you edit and save an existing file, a new version is added in the database, and is also listed in the Edited Archive page.

Note The option to edit existing device archive file and save the edited file is not available for non-Cisco devices.

Edit archive files following the procedure below:

Step 1 From the **Archive** page, choose a configuration file, and click **Edit**.

Step 2 Edit and save the configuration file.

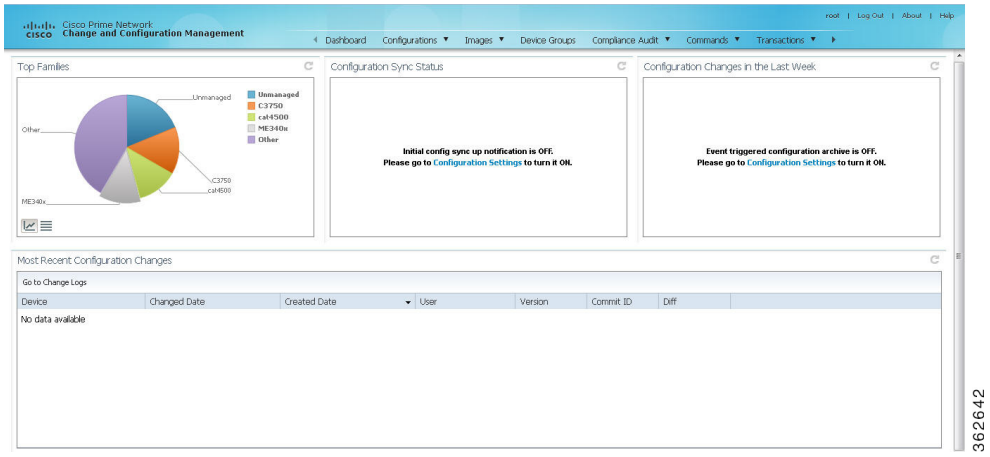
An edited archive version is created. This edited version will belong to the same configuration type as that of the original archive file.

The edited archive files can be restored to the devices.

Finding Out What is Different Between Configurations

CCM allows you to compare two configuration files that are saved in the archive and display them side by side, highlighting configuration differences and allowing you to move between them. CCM excludes a small set of commands by default, such as the NTP clock rate (which constantly changes on a managed network element but is not considered a configuration change). You can change the excluded commands list as described in Setting Up Configuration Management, page 3-5. Additions, deletions, and excluded values are color-coded as shown in the following example.

Figure 9-9 Compare Configurations Dialog Box



You can compare any types of configurations as long as they run on the same operating system. However, you cannot compare a Cisco IOS configuration with Cisco IOS XR configuration.

The following are typical scenarios for using the compare function:

- Compare the latest and next-to-latest configuration to see the most recent change.

- Compare Cisco IOS running and startup configurations to see how they are out of sync.
- Compare the configurations on two different devices to find out how they are different.
- Compare the configurations after eliminating excluded 5.3 from comparison.

Note When you are trying to compare an archive with an active startup, running, or admin configuration, if there is a change in the device configuration, CCM initiates a backup job and creates a latest version of the device configuration file. You can view the latest version of the configuration file in the Archived Configurations page.

To compare configurations:

Step 1 Choose **Configurations > Archives**.

Step 2 Locate the archives you want to compare. You can click the Version hyperlink next to a device to open the Device Configuration Viewer and quickly view the contents of the configuration file.

Step 3 You can choose to do the following:

Device Type or OS	Supported Function
For Cisco IOS XR devices	**Compare > To Active Running** or **Compare > To Active Admin**
Cisco IOS device	**Compare > To Active Startup** or **Compare > To Active Running**
Cisco StarOS device	**Compare > To Active Boot** or **Compare > To Active Running**
All	Compare > Selected Archives

Copying a Configuration File to a Central Server

You can export configurations to an FTP or SFTP server that is specified on the Configuration Management Settings page. They are exported as a .cfg (configuration) file.

Configuration files are saved using the following format:

*deviceName-configurationType-version-configChangeTimestamp***.cfg**

For example, the following file would contain the 18th version of a running configuration for the device named 7200-5, saved on March 27, 2010 at 2:40:30 P.M:

7200-5-RUNNING_CONFIG-18-2010327144030.cfg

Note Export of configuration files of IPv6 devices to servers running Windows OS is not supported.

Before You Begin

Make sure of the following:

- Export location and required credentials, and (for e-mails) SMTP host and port are configured on the Configuration Management Settings page.

- Specified FTP or SFTP server must have sufficient free space to accommodate the exported configurations. Also, the destination subdirectory on the FTP or SFTP server must have the required permissions.

To export configuration files:

Step 1 Choose **Configurations > Archives** and locate the archives you want to export. You can click the Version hyperlink next to a device to open the Device Configuration Viewer and quickly view the contents of the configuration file.

Step 2 Click **Export** and set the desired schedule and enter the e-mail ID(s) to which to send a notification after the scheduled export job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Configuration Management Settings page.

Note The time you specify here to schedule the export job is the gateway time.

Step 3 Click **Export**. The export job is created and you are redirected to the Job Manager page, where you can monitor the status of the job.

Are Running and Startup Configs Mismatched? (Cisco IOS and Cisco Nexus)

Cisco IOS and Cisco Nexus series devices contain a startup and running configuration file. The startup configuration is loaded when a device is restarted. Ongoing changes to the device are applied to the running configuration. As a result, unless the running configuration is saved as the startup configuration, upon a device restart, any changes would be lost. It is therefore important to ensure that the device startup and running configurations are in sync. When CCM synchronizes a file, it overwrites the startup configuration on the device with the configuration that is currently running on the device.

Whenever a configuration file is retrieved from a device and copied to the archive (that is, backed up), CCM compares the latest version of the startup configuration with the latest version of the running configuration file. If there is a mismatch, CCM adds the device to the list of out-of-sync devices.

For Cisco Nexus series devices, CCM backs up the startup and running configurations for all VDCs configured in the device. If there is a mismatch between the startup and running configurations of a VDC, CCM creates an out-of-sync entry for that VDC.

Note The synchronize operation affects only the configurations running on the device. It does not affect any configuration files that are saved in the archive.

The Dashboard maintains a Configuration Sync Status pie chart that shows how many devices have out-of-sync startup and running configuration files. When you click the pie chart (or choose **Configurations > Synchronize**), you are directed to the Out of Sync Devices page, where CCM lists all of the out-of-sync devices in tabular format. The information is refreshed whenever you choose **Configurations > Synchronize**.

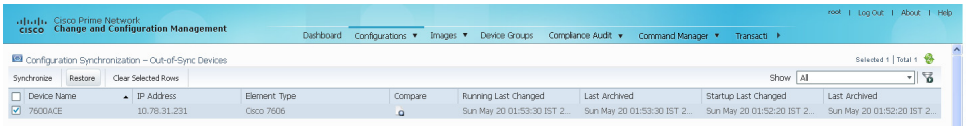
Before You Begin

Make sure the specified FTP or SFTP server must have sufficient free space to accommodate the exported configurations. Also, the destination subdirectory on the FTP or SFTP server must have the required permissions.

To view differences and synchronize configurations:

Step 1 Choose **Configurations > Synchronize**. CCM lists all out-of-sync devices, the date and time when the device configurations were last changed, and when the files were last archived. Figure 9-10 provides an example. The date and time are displayed according to the local time zone settings of the client.

Figure 9-10 Configuration Synchronization - Out of Sync Devices Page



Step 2 Click the **Compare icon** to launch the Compare Configuration window, which provides a side-by-side view of the two configurations and highlights the differences.

Step 3 Choose the network elements you want to synchronize. This directs CCM to overwrite the startup configuration on the device with the configuration that is currently running.

Step 4 Click **Synchronize**. The Schedule Synchronization page opens.

Step 5 Set the desired schedule and enter the e-mail ID(s) to which to send a notification after the scheduled synchronization job is complete. For two or more users, enter a comma-separated list of e-mail IDs. The time you specify here to schedule the synchronization job is the gateway time.

Note You might be prompted to enter your device access credentials. This option is enabled if, from the Administration client, **Global Settings > Security Settings > User Account Settings > Execution of Configuration Operations**, you checked the option **Ask for user credentials when running configuration operations**. This is an enhanced security measure restrict access to devices.

Step 6 Click **Synchronize**. CCM schedules the job and redirects you to the Jobs page, where you can monitor the status of the job.

Copying the Device Files to the Archive (Backups)

Backing up a device configuration entails getting a copy of the configuration file from the device, and copying that file to the configuration archive. As part of the backup procedures, it is compared with the latest archived version of the same type (e.g. running with running, startup with startup). A new version of the file is archived only if the two files are different. If the number of archived versions exceeds the maximum, the oldest archive is purged (according to the values on the Configuration Management Settings page). Configurations marked with a “do not purge” label are not removed from the archive by the auto-purging procedures.

This topic explains how to perform a manual backup. CCM also performs automatic backups according to the specifications on the Global Settings page (see Checking Prime Network Global Settings for CCM Operations, page 3-4). Manual backups do not affect the automatic backups that are controlled from the Global Settings page; they are completely independent of each other.

What Is Backed Up to the Archive

The following table provides the types of configuration files that are backed up to the archive per different types of devices.

Device Type	Configuration File Exported	Condition(s)
Cisco IOS device	Only the latest running configuration	If there is no running version, the latest startup configuration is exported
Cisco IOS XR device	Latest running and startup configuration; includes active packages	Devices must be managed with system user because copy command is not available in command-line interface (CLI) for non-system users
Cisco StarOS devices	Boot configuration file (CCM always overwrites the existing boot configuration in the archive)	If there is no running version, boot configuration is NOT exported
Cisco 7600 device with ACE card	Startup and running configurations of the ACE card	If there is no running version, the latest startup configuration is exported
Cisco Nexus OS device	Startup and running configurations for all VDCs configured in the device.	If there is no running version, the latest startup configuration is exported
Cisco CPT devices	Startup and memory configuration operations.	CCM supports memory configuration operation. Since the memory configuration is in binary format, viewing, comparing, and editing is not possible. **Note** CPT devices are not supported in Compliance Manager.

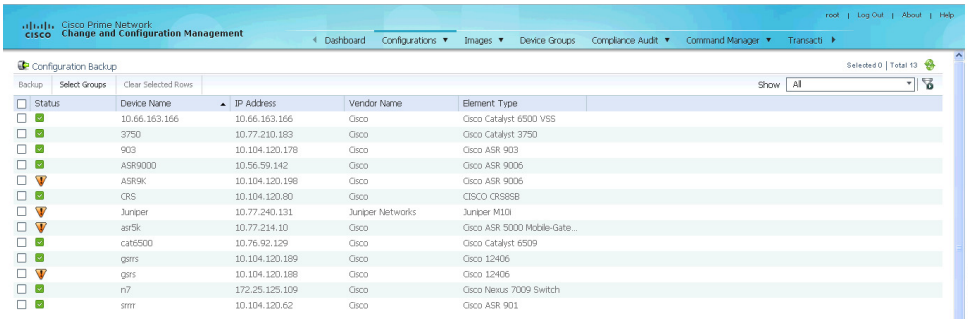
Files are automatically backed up to the archive according to the values on the Configuration Management Settings page. To perform an on-demand backup of configuration files to the archive:

Step 1 Choose **Configurations > Backup**. CCM lists all devices with the following status symbols as shown in Figure 9-11.

Symbol	Description
	Device is available for backup.
	Device is not available for backup. The device is most likely in the Maintenance investigation state or the Unreachable communication state. Click the device hyperlink and open the device properties popup to see details about the device.

Step 2 Choose the devices with files you want to back up.

Figure 9-11 Configuration Backup Page



Step 3 To choose devices from a specific device group, click **Select Groups**. Click the hyperlinked device group name to view the list of devices that belong to the group.

Step 4 Select the required device group in the Device Groups page and click **OK**. The devices that belong to the selected device group are highlighted in the Configuration Backup page. You can also schedule a backup simultaneously for all the devices existing in a group:

- Select a device group and click **Backup Groups**.
- Enter the scheduling information as explained after Step 5 and click **Backup Groups**.

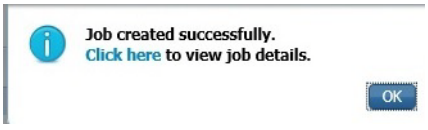
Step 5 In the Configuration Backup page, click **Backup** to configure the backup schedule. By default, the backup is performed as soon as possible. Other schedule choices (once, periodically, weekly, and so forth) are activated when you deselect Start as Soon as Possible. The time you specify here to schedule the backup job is the gateway time.

Note You might be prompted to enter your device access credentials. This option is enabled if, from the Administration client, **Global Settings > Security Settings > User Account Settings > Execution of Configuration Operations**, you checked the option **Ask for user credentials when running configuration operations**. This is an enhanced security measure restrict access to devices.

Step 6 Enter the e-mail ID(s) to which to send a notification after the schedule backup job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Configuration Management Settings page.

Step 7 Click **Backup**. CCM schedules the job and when the job is completed a pop-up appears as shown in Figure 9-12.

Figure 9-12 Job Create Successfully Message



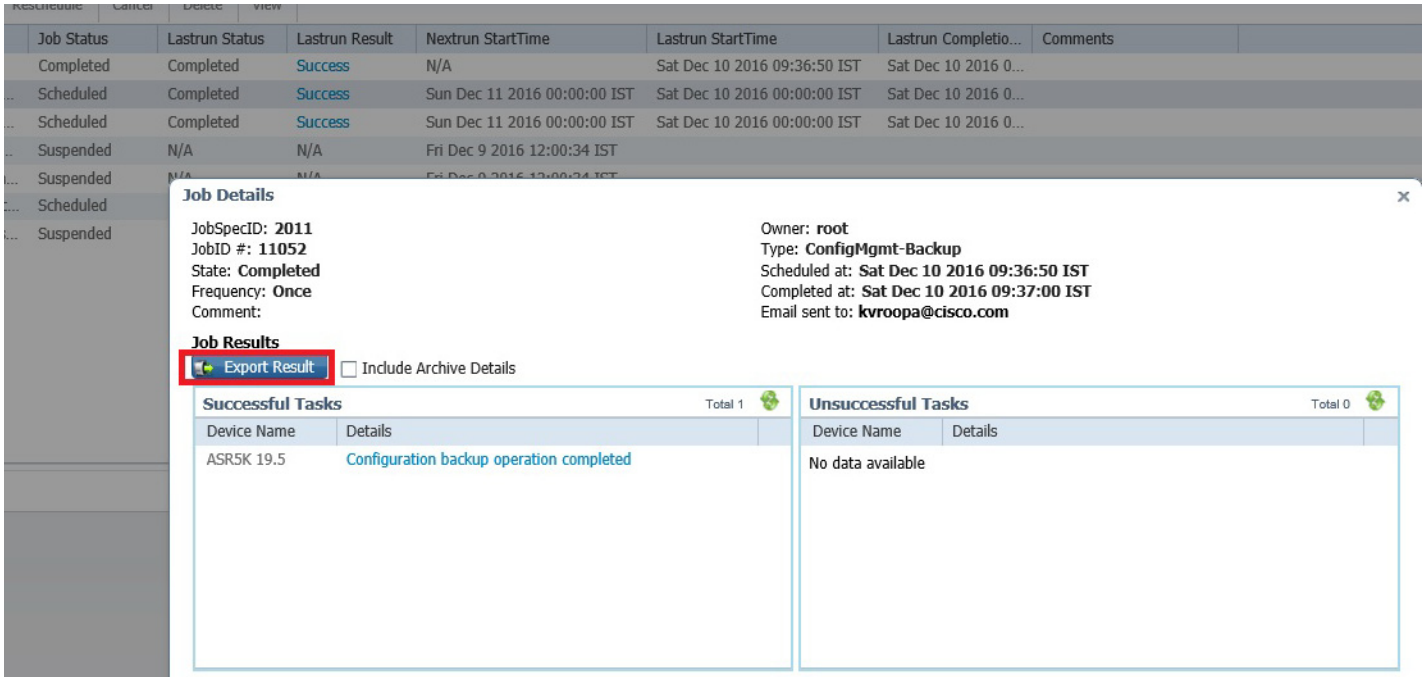
Step 8 Click the hyperlinked **Click here** to open the Configuration Management Jobs page or click **OK** to close and return to the Configuration Backup page.

Note If a backup is scheduled for an entire device group and if there is a change in the group by addition or deletion of devices after job creation, CCM updates the job accordingly such that all the devices available in the group at the time of execution of the job are considered for backup.

Step 9 In the Configuration Management Jobs page, click the hyperlinked **LastRun Result** (Success/Partial Success/Failure) against a particular job in the Jobs table.

To export completed job results in XLS format, click the hyperlinked Success lastrun result. The Job Details page appears as shown in Figure 9-13.

Figure 9-13 Job Details



Note If the **LastRun Results** of a Star-OS device (for example ASR5K) is a Failure, in the **Job Details** window you can view the exact configuration missing file details during the backup operation with either of the 3 supported protocols such as TFTP, FTP, SMTP.

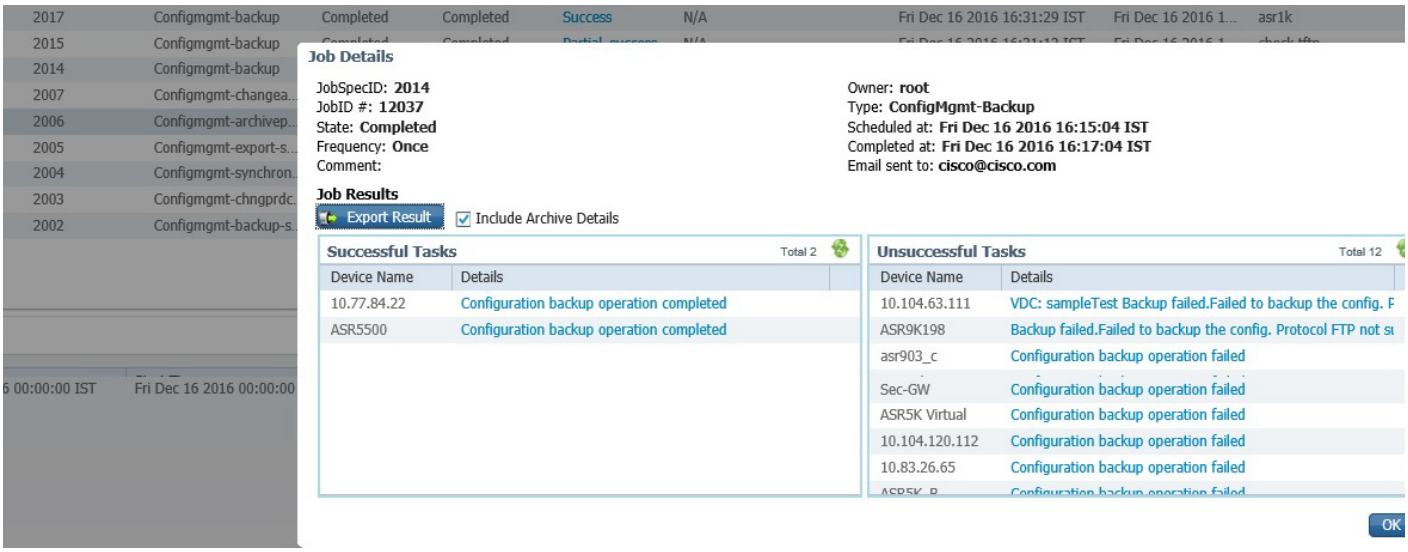
Step 10 Click **Export Result** to export and download the job results in a XLS format.

To view the archived backup job details:

Step 11 In the Job Details page, click the **Include Archive Details** check box, and then click **Export Result**. This allows you to export and download the backup information with the latest archived version in XLS format.

Note If devices do not have previous archive details, IP Address, Device Type, and the Last Archived Details columns in the Exported Result report shows **NA** status.

Figure 9-14 Include Archive Details



Note During the backup operation of Star-OS devices (for example, ASR5K) you can view the exact configuration file missing details. This is applicable with either of the three supported protocols such as TFTP, FTP or SFTP. The message shows the missed priority in devices in th **Job Details** window.

If you clear the **Include Archive Details** check box, the Export Result report will have only the current job details

Step 12 Click **OK** to close and return to the Configuration Management Jobs page.

Fixing a Live Device Configuration (Restore)

CCM performs the configuration restore operation in either *overwrite* or *merge* mode. As part of restore operation, the configuration files are backed up again after the restore procedure is complete.

- Overwrite mode—CCM supports restoring configuration in overwrite mode on all supported devices. CCM overwrites the existing configuration on the device with a configuration file from the archive. After the restore operation is performed, the device configuration is identical to the configuration that was chosen from the archive.
- Merge mode—CCM merges the selected configuration file from the archive with the configuration on the device. New commands in the archived version—that is, commands that are *not* in the device's current configuration—are pushed to the device. After the restore operation, the device configuration file retains its original commands, but it also contains new commands from the archived version.

For information on the devices that support restore operation in overwrite and merge modes, see the *Cisco Prime Network 5.3 Supported VNEs* and the *Cisco Prime Network 5.3 Supported VNEs - Addendum*.

By default, CCM uses the restore mode setting (overwrite or merge) that is specified in the Configuration Management Settings page (see Checking Prime Network Global Settings for CCM Operations, page 3-4. However, you can modify the default mode while scheduling the restore operation. If you have selected the overwrite mode, you can use the **Use Merge on Failure** option to restore the files in merge mode, if overwrite mode fails.

If you select the devices by checking the check box next to Devices (in the table headline), only the first 100 devices in the first page are selected. Click Next to move to the next 100 devices. If you filter the devices based on a parameter, only the filtered details are displayed, and by default, no row is selected. If you selected all the entries in a page, and then deselected one or few options from the selection, and then move to the subsequent pages to select all the devices from the Devices (in the table headline), the selection in the previous page disappears.

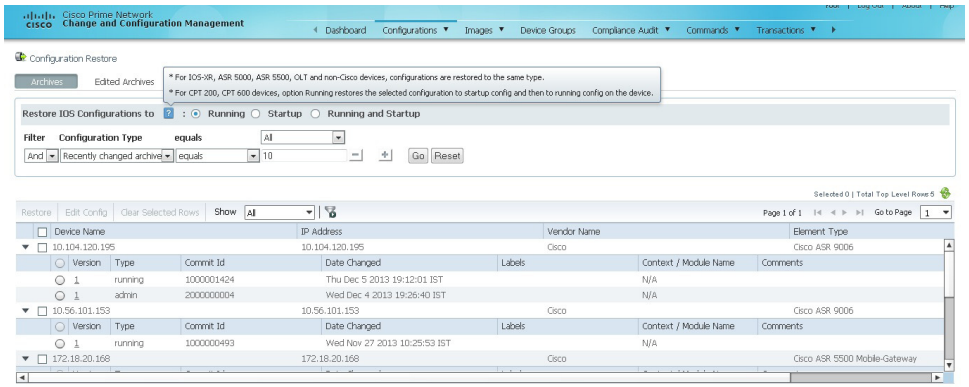
Before You Begin

- Make sure you have installed Flash Player version 10 or higher to view the Configuration Restore page.
- Make sure you have the permissions to perform the restore operation. You will not be allowed to schedule a restore job, if you do not have permissions.

To restore a configuration:

Step 1 Choose **Configurations > Restore**. CCM lists all configuration files in the archive. Figure 9-15 shows an example of a filtered page.

Figure 9-15 Configuration Restore Page



70081

Step 2 (Cisco IOS only) Specify the type of configuration files you want to restore: Running, Startup, or both. If you choose to restore to startup configuration, CCM will first copy the file to running configuration and then to startup configuration.

If you choose to restore to Running and Startup configuration, CCM will first deploy the configuration archive to the running configuration on the device and then CCM will replace the startup configuration on the device with the modified running configuration.

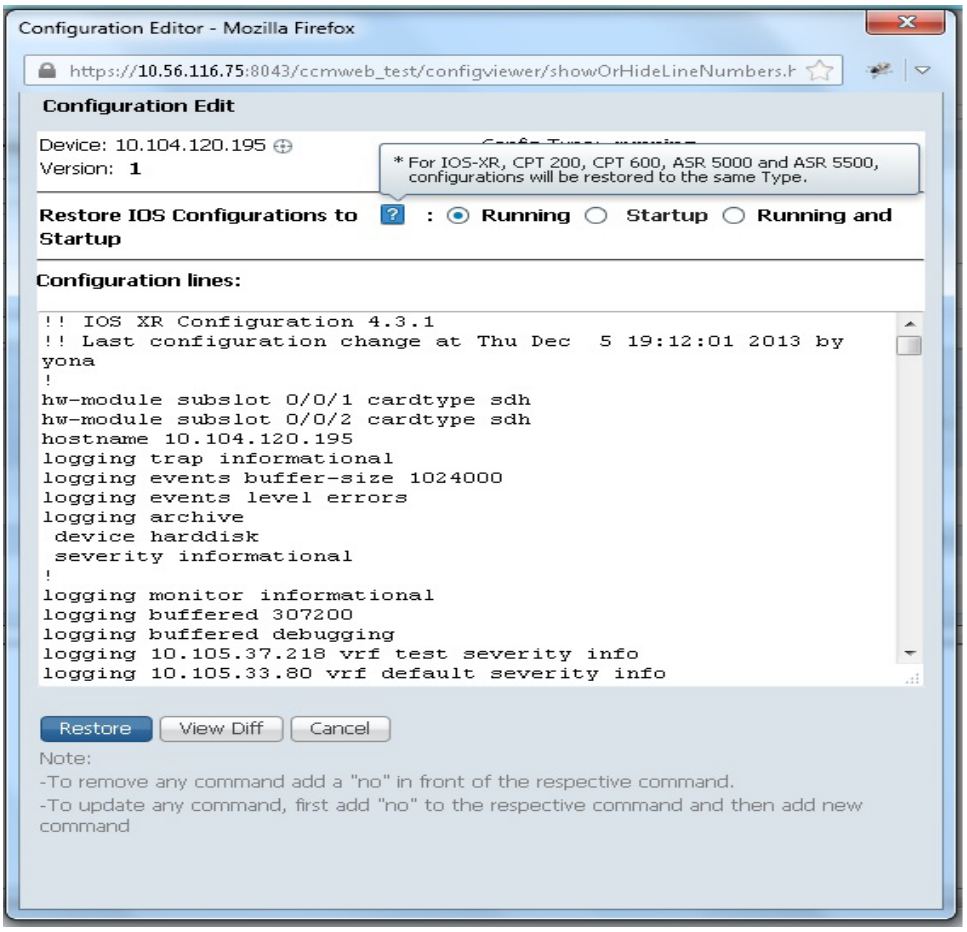
Step 3 Choose the configuration files you want to restore. You can click the arrow mark next to the device name to view the different versions of the configuration file of the device. You can also click the Version hyperlink to view the contents of a file. If the file is a binary file, clicking the version hyperlink does not open the various versions of the configuration file.

If you prefer to restore an edited archive file, open the Edited Archive tab. Select the files and click **Next**. The list of devices that belong to the same device family with respect to the selected edited configuration is displayed. Select the required devices. Skip to Step 5.

Step 4 If you want to edit a file before restoring it, click **Edit Config** (edited files are restored only in merge mode). You can view the details of the selected configuration file in the Configuration Editor page as shown in Figure 9-16.

Note If you selected non-Cisco or OLT (GPON) devices, the **Edit Config** button is disabled.

Figure 9-16 Configuration Edit



Edit the configuration 5.3, as required. Note the following:

- To remove a command, add **no** in front of the command.
- To update a command, add **no** in front of the command and then add the new command.

Step 5 Click **Restore**. The Config Restore Schedule dialog box opens.

Step 6 (Optional) Override the default transport protocol and default restore mode.

Step 7 Enter a comma-separated list of e-mail ID(s) to which to send a notification after the scheduled restore job is complete.

Note You might be prompted to enter your device access credentials. This option is enabled if, from the Administration client, **Global Settings > Security Settings > User Account Settings > Execution of Configuration Operations**, you checked the option **Ask for user credentials when running configuration operations**. This is an enhanced security measure to restrict access to devices.

Step 8 Click **Restore**. CCM schedules the job and redirects you to the Jobs page, where you can monitor the status of the job.

Cleaning Up the Archive

Deleting a file removes it from the archive. You cannot delete an archived file if:

- It is marked "do not purge."
- Deleting it would bring the number of versions below the minimum number of versions that must be retained (as specified on the Configuration Management Settings page).

When a device is removed from CCM, its configuration files are also removed from the archive.

To delete a configuration file from the archive:

Step 1 Choose **Configurations > Archives**.

Step 2 Choose the configuration file you want to delete. You can click the Version hyperlink to verify the contents of the configuration file.

Step 3 To delete a single configuration file, click the delete icon (red **X)** at the end of the row. If the delete icon is disabled, this means the archive is assigned a label that is marked "do not purge." To delete this type of configuration, you must first unassign the label from the configuration.

Step 4 To delete multiple configuration files, select the required files and then click the **Delete** button in the table header.

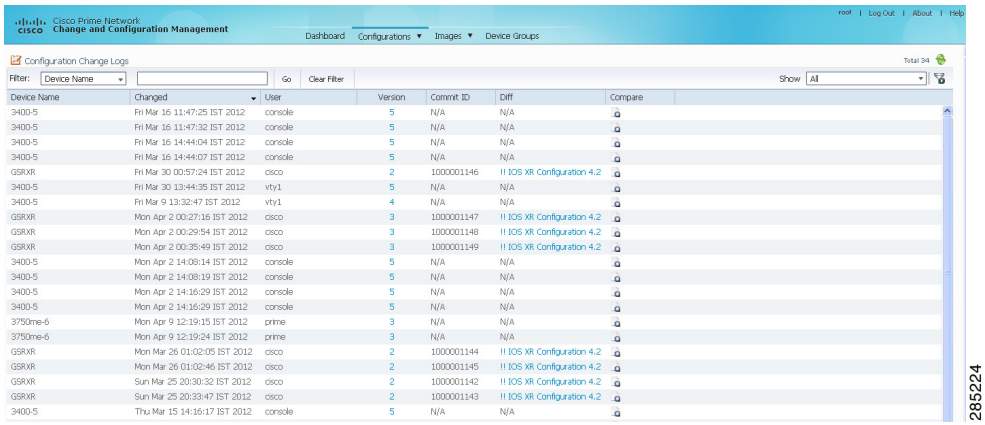
Step 5 Confirm your choice. CCM schedules the job and redirects you to the Jobs page, where you can monitor the status of the job.

Finding Out What Changed on Live Devices

The Change Logs page displays a list of the latest device configuration changes detected by CCM. How CCM responds to these changes depends on the values on the Configuration Management Settings page. By default, CCM does not get new information from the device and copy it to the archive when a change occurs, but you can set it to do so. See Checking Prime Network Global Settings for CCM Operations, page 3-4.

All users can view the change logs, regardless of the user access role or assigned device scopes. To view the latest changes, choose **Configurations > Change Logs**. Figure 9-17 provides an example.

Figure 9-17 Configuration Change Logs



The Configuration Change Logs page displays change information, sorted according to the latest time stamp. (For a description of common fields, see Managing Device Configurations, page 9-36.) The date and time stamps are displayed according to the local time zone settings of the client.

You can view a maximum of 2000 records in the Configuration Change Logs page.

These fields are specific to the Configuration Change Logs page:

Field	Description
Diff	(Cisco IOS XR only) Displays only the commands that were changed. For long text, hover the cursor over the hyperlink to display the entire contents.
Compare	This field is enabled only if two or more versions of the configuration file are available. Click the Compare icon to launch the Compare Configuration window, which displays the associated archive version and the earlier versions of the file. Additions and deletions are color-coded. From here, you can: • Click **Show All 5.3** or **Only Differences** to display the entire file contents or just the differences between the two files. • Click **Previous Diff** or **Next Diff** to jump forward or backward to the previous or next difference between the two files. • Click the arrow buttons or enter the page number to jump forward or backward to view the file contents that are running across pages. • Click Differences Without Excluded 5.3 to eliminate excluded 5.3 from comparison.

Making Sure Devices Conform to Policies Using Compliance Audit

Note Starting in Prime Network 4.1, Compliance Audit replaces the Configuration Audit feature. In Prime Network 5.3, Configuration Audit is deprecated. However, if you enabled the option to retain Configuration Audit during an upgrade procedure from Prime Network 3.11 (or earlier), the feature will still be available from CCM.

Compliance Audit ensures that existing device configurations comply to your deployment's policies. Using Compliance Audit, you can create policies that can contain multiple rules, and policies can be grouped together to create a policy profile which can be run on a set of devices, called audit of devices. There is no limit on the number of policies, profiles, rules, and conditions that you can create using Compliance Audit.

There are 11 system-defined policy groups available in Compliance Audit. Each policy group comprises a set of system-defined policies. You can combine system-defined policies and user-defined policies to create a policy profile. But, you cannot edit, clone, or delete a system-defined policy group or a system-defined policy.

When CCM detects a violation, it can recommend a fix if one is configured by the administrator. Violation details are saved in the database for later reference.

In some scenarios, a fix may be readily available (as configured by the administrator) and can be directly applied, while in some others, the fix has to be carefully scrutinized by the administrator before it is run. Automatic application of some of the fixes can be disabled since it may conflict with other policies and configurations that may be specific to the device and the setup.

These topics explain how to use Compliance Audit:

- Workflow for Creating Policies and Profiles, and Running a Compliance Audit Job, page 9-51
- Creating a Policy, page 9-52
- Creating a Policy Profile, page 9-61
- Choosing the Devices for the Compliance Audit, page 9-69
- Viewing the Results of a Compliance Audit Job and Running Fixes for Violations, page 9-74
- Using Compliance Audit for Device Compliance, page 9-79

Workflow for Creating Policies and Profiles, and Running a Compliance Audit Job

Running an audit job the first time requires you to follow a specific workflow:

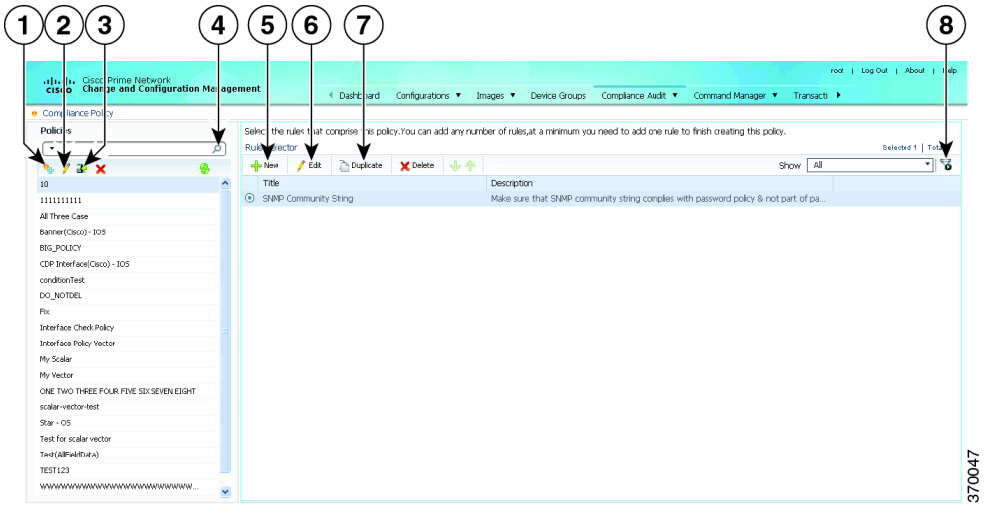
	Description	See:
Step 1	Create a policy containing multiple rules	Creating a Policy, page 9-52
Step 2	Group policies into policy profiles so you can apply them	Creating a Policy Profile, page 9-61

	Description	See:
Step 3	Run the policy against your specified devices	Choosing the Devices for the Compliance Audit, page 9-69
Step 4	View the results and fix any violations	Viewing the Results of a Compliance Audit Job and Running Fixes for Violations, page 9-74

Creating a Policy

Create a policy by choosing **Compliance Audit > Compliance Policies**. The Compliance Policy page (Figure 9-18) appears.

Figure 9-18 Compliance Policy Page



1	Create Compliance Policy icon	**5**	New Rule icon
2	Edit Policy Description icon	**6**	Edit Rule icon
3	Import Policy as XML icon	**7**	Duplicate Rule icon.
4	Search field	**8**	Filter icon
5			

You can either create a new policy or you can import an existing policy by clicking the **Import** icon. You can export existing policies as XML files to your local drive.

Step 1 Click the **Create Compliance Policy** icon and enter the policy details. The policy is listed in the left pane.

Step 2 From the Rule Selector pane, click **New Rule** icon. For more information on creating a new rule, see Creating a Rule.

Manage Advance Filters for a Compliance Audit

After you create a policy profile, you can create advanced filters with multiple filter criterion and save the filter setup as an Advanced Filter option. Whenever a compliance audit job is run, you can select the preset filters for the selected device and perform compliance audit as and when required, modify the filters to add a new device information, element types and so on and save the filter as a different query name. When the system job is run, you can export all configuration data irrespective of the last modification done on the archive.

For more information about Setting up Export device configuration and Periodic export parameters see, the Period Export options section in Table 9-1 and Managing Multilayer Quick Filters for Selected Devices in the Compliance Audit Jobs, page 9-70

Creating a Rule

For a policy to run against devices and generate violations, you must specify rules within the policy and define the conditions and the relevant fixes for violations. Rules are platform-specific. Each policy must contain at least one rule; however, there is no limitation on the number of rules you can define for a policy. You can also duplicate an existing rule and add to a policy. Click **Duplicate** to clone a rule. Follow the procedure below to create a rule and add the rule to a specific policy:

Step 1 From the left navigation pane, select the policy to which you want to add rules.

Step 2 From the work area pane, click **New**.

Step 3 Enter the following details. For sample rules, see Creating Rules—Samples, page 9-59.

Table 9-3 New Rule Fields

Field	Description
Rule Information	
All information entered in this section is free text and does not impact the conditions and the subsequent violations.	
Rule Title	Enter a name for the rule.
Description	Enter a brief description
Impact	Enter a brief note on the impact of the violation that the rule will generate.
Suggested Fix	Enter a brief description of the fix that will help you decide to choose or to not choose the rule against a specific policy. This description appears when you check the rule in the Rule Selector pane.
Platform Selection	
Available Platforms	Check the platforms on which the condition must be run. If you select Cisco Devices, all of Cisco platforms specified in the list are included. The platforms checked in this section impacts the ignore count of an audit job. For example, if you run a rule on all the devices within your scope, including devices not selected in the Available Platforms pane, such devices are not audited and are marked against Ignore count.

Table 9-3 New Rule Fields (continued)

Field	Description
Rule Inputs	
New Input	Click **New** to add inputs for the new rule. The input you create in this pane reflects in the Policy Profile page. You must provide rule inputs for the rule you have selected. For example, you can create an input to be IP Address. Any user who wants to run this rule can enter an IP address specific to the rule and add it to a specific profile. Enter the following details: • Title—Enter a name for the rule input. • Identifier—Click the Generate button to generate an identifier based on the title. The identifier is used in Block Start Expression, Conditions Match Criteria (value field), Action Details Tab - Violation Message, Fix CLI (if action is Raise a Violation, and Violation Message Type is Define Custom Violation Message for the Condition). • Description—Enter a brief description for the rule input. • Scope—Choose the scope of the rule input, whether the input is for execution or fix. • Data Type—Choose a data type from the following options: – Boolean – IP Address – Integer – Interface – Interface Group – IP Mask – String • Input Required—Check the option, as required. The following fields appear based on the option that you choose in the Data Type field: • Is List of Values—Check this check box to add multiple values to be associated with the rule input. A table appears where you can add, edit, and delete values. You can also set a default value. • Accept Multiple Values—Check this check box if you want to provide more than one value at the time of audit. This is applicable only for the execution type rule input. • Min Value—Enter a minimum integer value for the rule input. This is applicable only for the integer data type. • Max Value—Enter a maximum integer value for the rule input. This is applicable only for the integer data type. • Default Value—Enter a default value for the rule input. The format of the value that you enter in this field depends on the data type that you choose in the Data Type field. For example, if you choose Integer as the data type, you can enter an integer value only. • Max Length—Enter the maximum length that is applicable for the rule input. • Val RegExp—Enter a valid regular expression that will be used for execution or fix.
Conditions and Actions	
New Conditions and Actions	Click **New** to create conditions and actions for the new rule.

Table 9-3 New Rule Fields (continued)

Field	Description
New Conditions and Actions—Conditions Details tab	
Condition Scope Details	• Condition Scope—Select the scope of the conditions from one of the below: – Configuration—Checks the complete running configuration. – Device Command Outputs—Checks the output of show commands. – Device Properties—Checks against the device properties and not the running configuration. – Previously Matched Blocks—Runs the conditions against blocks that have been defined in previous conditions. To run the condition with this option, you must have checked Parse as Block option in one of the previous conditions. You cannot select this option for the first condition of a rule. – Function—Checks based on the earlier conditions. Once the Function option is selected, the **Expression** field is enabled, where you can enter mathematical functions such as addition, subtraction, multiplication, and division operations. You need to follow these conditions while using the Function option: • Using Java regular expressions, the value can be extracted and stored in a variable. For example, if you choose the condition as 1, then you need to enter the value as <1.1> in the **Value** field. • Using conditions along with operations, where you can enter the operations to be performed in the **Expression** field. For example, in the **Expression** field, you can enter the value as <1.1> * 1024. • Device Property—Select one of the following device properties: – Device Name – IP Address – OS Name – OS Version **Note** This option is enabled only if you selected Device Properties in the Condition Scope drop-down list. • Show Commands—Select the required show command that is applicable for the platform selected. You can also enter a show command against which the audit must be performed. **Note** This option is enabled only if you selected Device Command Outputs in the Condition Scope drop-down list.
Block Options	
Parse as Blocks	Checking this option enables you to run conditions on specific blocks (as defined in this section) in running configuration files. This option is enabled only if you selected Configuration in the Condition Scope option.
Block Start Expression	This field is mandatory if Parse as Blocks option is enabled. This must be a regular expression. Rule inputs and Grep outputs can be used here.
Block End Expression	This field is optional. By default, blocks end when the top-level or a sub-level command begins. If you prefer to break the block earlier, enter the value as a regular expression.

Table 9-3 New Rule Fields (continued)

Field	Description
Rule Pass Criteria	Check the option, as required. If you select: • All Sub Blocks—The rule is marked a success only if all the blocks fulfill the specified condition. • Any Sub Block—The rule is marked a success even if one of the sub blocks fulfill the condition. • Raise One Violation for Each Failing Instance—If you check this option, the violation count specified in the Job view increases by as many number of violations as the condition encounters in each block.
Condition Match Criteria	
Operator	Choose an option based on the value you will enter in the subsequent fields.
Operator Function	Click Edit. The Select Operator Function page appears. Select a predefined function and enter the function parameters based on the predefined function that you have selected. **Note** This field is available only if you selected the option, Execute a Function from the Operator field.
Value	The value must be a regular expression. Rule inputs and Grep outputs can be used here. This variable can be grepped for use in the subsequent conditions. It follows the convention of condition <number.value number> such as, <2.1> <2.2>... This numerical identifier can be used from the next condition as input parameter for Operator selected in the previous field. If you selected Device Name in the Device Property field, you must enter a valid regular expression that will check the VNE name and not the host name.
Rule Pass Criteria	Check the option, as required. If you select: • All Sub Blocks—The rule is marked a success only if all the blocks fulfill the specified condition. • Any Sub Block—The rule is marked a success even if one of the sub blocks fulfill the condition. • Raise One Violation for Each Failing Instance—If you check this option, the violation count specified in the Job view increases by as many number of violations as the condition encounters in each block.
New Conditions and Actions—Action Details tab (applicable for both Select Match Action and Select Does Not Match Action	
Select Action	Select one of the following actions that Compliance Audit must perform upon detecting a violation: • Continue—If the condition is met or not met, the rule continues to run based on the condition number specified in the field. If a condition number is not specified, the rule skips to the next immediate condition. • Does Not Raise a Violation—Does not raise a violation; stops further execution of rule. • Raise a Violation—Raises a violation and stops further execution of rule.
Condition Number	Specify the condition number to which the rule must continue with in case the condition is met or is not met. You cannot specify a condition number that is lesser than or equal to the current condition number. This field is available only if you selected the option Continue from the Select Action field.
Violation Severity	Specify a severity that Compliance Audit must flag if a violation is detected. This field is available only if you selected the option, Raise a Violation from the Select Action field.

Table 9-3 New Rule Fields (continued)

Field	Description
Violation Message Type	Select one of the following message type: • Default Violation Message—Select this option if you determine a violation as not fixable (or requiring manual intervention). • User defined Violation Message—Select this option to enter a fix or to provide a command script to fix a violation. This field is available only if you selected the option, Raise a Violation from the Select Action field.
Violation Message	**Note** This field is available only if you selected User defined Violation Message in the Violation Message Type field. Enter a violation message that will be displayed in the Job View window. Rule inputs can be used here.

Table 9-3 New Rule Fields (continued)

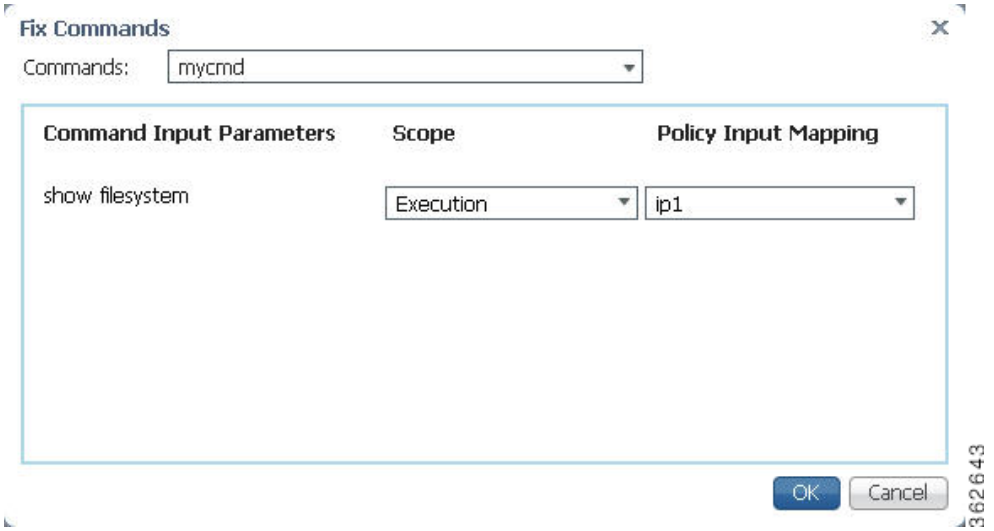
Field	Description
Fix CLI	**Note** This field is available only if you selected User defined Violation Message in the Violation Message Type field. Enter a relevant CLI fix if the device does not meet the condition specified. Do not enter **config t**, **configure**, and its **exit** commands. Rule inputs and Grep outputs can be used here. **Note** The **exit** command is allowed in main and sub-level commands. Following are the formats for the CLI fix that you enter in this field: • For an execution type input, enter <Rule input ID> • For a fix type input, enter ^<Rule input ID>^ • For a grep type output, enter <n.m>, where n is the condition number and m is the output number. If you choose to use the predefined commands that are available in the Command Manager to fix the violation, perform the following tasks: 1. Click **Command**. The Fix Commands window appears. *Figure 9-19 Policy and Command Input Parameter Mapping*  2. From the Commands drop-down list, select a predefined command that you will be executing to fix the compliance violation. The Command Input Parameters that are defined for the selected command are displayed. 3. Select the Scope and Policy Input Mapping for the Command Input Parameter. **Note** The Policy Input Mapping field is used to map the input parameter that is defined when creating the fix command in the Command Manager, with the rule input that is defined when creating a policy rule in the Compliance Manager. The values that you select or enter in the Policy Input Mapping field depends on the scope you select for the Command Input Parameter.

Table 9-3 New Rule Fields (continued)

Field	Description
	Select the scope from the following options: – Default—Select this option to enter the required value in the Policy Input Mapping field. – Execution—Select this option if you want to use the Command Input Parameter for execution purpose during the compliance audit. If the execution rule input is defined in the Compliance Manager, you can select the input in the Policy Input Mapping field. – Fix—Select this option if you want to use the Command Input Parameter for fixing the compliance violation. If the fix rule input is defined in the Compliance Manager, you can select the input in the Policy Input Mapping field. – Grep Output—Select this option if you have a grepped output in the condition. In the Policy Input Mapping field, enter the numerical identifier that follows the convention <condition number.output value number>. For example, if you have a grepped output in the second condition and you want to consider the first output of that condition, enter <2.1>.

After you complete adding rules to the policy, a profile must be created. For more information, see Creating a Policy Profile.

Creating Rules—Samples

This section explains four scenarios in which rules can be created.

Problem This policy checks if at least one of the pre-defined DNS servers are configured on device.

The following condition checks if either **IP name-server** *1.2.3.4* or **IP name-server** *2.3.4.5* is configured on the device, and raises a violation if neither of them are configured.

Solution The following settings have to be made in the appropriate sections.

Field	Value
Condition Scope	Configuration
Operator	Matches the expression
Value	`ip name-server (1.2.3.4|2.3.4.5)$`
Match Action	Do not raise a violation and exit this rule
Does Not Match Action	Raise a violation and exit this rule
Violation Text	DNS Server must be configured as either 1.2.3.4 or 2.3.4.5.

Problem This policy checks if at least two NTP servers are configured on the device for NTP server redundancy.

The following condition checks if the command ntp server appears at least twice.

Solution The following settings have to be made in the appropriate sections.

Field	Value
Condition Scope	Configuration
Operator	Matches the expression

Field	Value
Value	`(ntp server.*\n){2,}`
Match Action	Continue
Does Not Match Action	Raise a violation and exit this rule
Violation Text	At least two NTP servers must be configured.

Problem This policy checks if the device is not configured with any prohibited community strings or community strings that must be avoided for SNMP.

This condition checks if either snmp-server community public or snmp-server community private is configured on the device. If configured, Compliance Audit raises a violation. Note that *<1.1>* in the violation text is replaced with the actual community string configured on the device, at the runtime. In this example, *<1.1>* indicates first captured group in the current condition.

Solution The following settings have to be made in the appropriate sections.

Field	Value
Condition Scope	Configuration
Operator	Matches the expression
Value	snmp-server community (public|private)
Match Action	Raise a violation and exit this rule.
Does Not Match Action	Continue
Violation Text	Community string *<1.1>* configured.

Problem This policy checks if a particular version of the IOS software is installed on a device.

The following condition checks if IOS software version 15.1(1)SY2 is installed on a device.

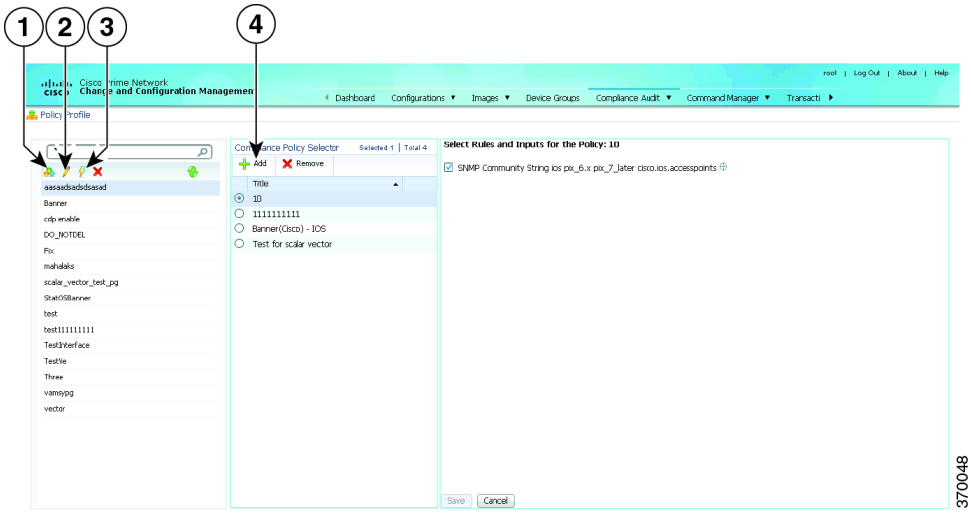
Solution The following settings have to be made in the appropriate sections.

Field	Value
Condition Scope	Device Command Outputs
Show Commands	show version
Operator	contains the string
Value	`15.1(1)SY2`
Match Action	Continue
Does Not Match Action	Raise a Violation
Violation Text	Output of show version must contain the string ‘15.1(1)SY2’.

Creating a Policy Profile

After you have created policies, create a policy profile that will contain a set of policies. Go to **Compliance Audit > Policy Profile**. The Policy Profile page (Figure 9-20) appears.

Figure 9-20 Policy Profile Page



1	Create Policy Profile icon	**3**	Run Compliance Audit icon
2	Edit Policy Profile Description icon	**4**	Add Compliance Policy icon

Follow the procedure below to create a new policy profile:

Step 1 From the left navigation pane, click the **Create Policy Profile** icon. Enter name and description of the policy profile.

Step 2 From the left navigation pane, select the policy profile that you have created. From the Compliance Policy Selector pane, click the **Add Compliance Policy** icon. The list of system-defined policy groups and user-defined policy group appear. See Table 9-4 for the list of policies grouped under each policy group.

Step 3 Choose the required policies.

Step 4 Select the rules and inputs within the selected policies, which you want to audit against. Later, if applicable, enter values for rule inputs. The option to enter rule inputs is available only if you have entered input parameters when you created a new rule. Policy Profiles are created and an audit job can be run.

Table 9-4 Policy Group Details

Policy Group Name	Policies
AAA Services	• AAA • AAA Accounting—Commands • AAA Accounting—Connections • AAA Accounting—Exec • AAA Accounting—Network • AAA Accounting—System • AAA Authentication—Enable • AAA Authentication—Login • AAA Authorization—Commands • AAA Authorization—Configuration • AAA Authorization—Exec • AAA Authorization—Network • Checking at least one of Tacacs+ Radius LDAP authentication should be configured
Audit and Management	• Banners • Console Access • DHCP • Domain Name • Host Name • Logging and Syslog • Terminal Access • User Passwords

Table 9-4 Policy Group Details (continued)

Policy Group Name	Policies
Cisco Security Advisories (PSIRT)	• AAA Command Authorization By-pass - 68840 • ARP Table Overwrite - 13600 • Access Point Memory Exhaustion from ARP Attacks - 68715 • Access Point Web-browser Interface - 70567 • Auth Proxy Buffer Overflow - 66269 • Authentication Proxy Vulnerability - 110478 • BGP Attribute Corruption - 10935 • BGP Logging - 63845 • BGP Long AS path Vulnerability - 110457 • BGP Packet - 53021 • BGP Update Message Vulnerability - 110457 • CEF Data Leak - 20640 • Call Processing Solutions - 63708 • Cisco 10000 Series DoS Vulnerability - 113032 • Cisco IOS Software IGMP Vulnerability - 112027 • Content Services Gateway DOS Vulnerability - 112206 • Content Services Gateway Service policy bypass - 112206 • Crafted Encryption Packet DoS Vulnerability - 110393 • Crafted ICMP Messages DoS for IPSec Tunnels - 64520 • Crafted ICMP Messages DoS for L2TPv2 - 64520 • Crafted ICMP Messages DoS for TCP over IPv4 - 64520 • Crafted ICMP Messages DoS for TCP over IPv6 - 64520 • Crafted IP Option - 81734 • Crafted TCP Packet Denial of Service Vulnerability - 111450 • Crafted UDP Packet Vulnerability - 108558 • Crypto - 91890 • DFS ACL Leakage - 13655 • DHCP - 63312 • DLSw Denial of Service Vulnerabilities - 99758 • DLSw Vulnerability - 77859 • FTP Server - 90782 • Firewall Application Inspection Control Vulnerability - 107716 • H.323 Denial of Service Vulnerability - 111265 • H.323 Protocol DoS Vulnerability - 110396 • H323 DoS Vulnerability - 112021

Table 9-4 Policy Group Details (continued)

Policy Group Name	Policies
Cisco Security Advisories (PSIRT) (contd.)	• HTTP - 13627 • HTTP Auth - 13626 • HTTP Command Injection - 68322 • HTTP GET Vulnerability - 44162 • HTTP Server Query - 13628 • Hard-Coded SNMP Community Names in Cisco Industrial Ethernet 3000 Series Switches Vulnerability- 111895 • IKE Resource Exhaustion Vulnerability - 110559 • IKE Xauth - 64424 • IOS Internet Key Exchange Vulnerability - 20120328 • IOS Software Command Authorization Bypass Vulnerability - 20120328 • IOS Software NAT SIP Memory Starvation Vulnerability - 20120328 • IOS Software RSVP Denial of Service Vulnerability - 20120328 • IOS Software DHCP DoS Vulnerability - 20120926 • IOS Software DHCPv6 DoS Vulnerability - 20120926 • IOS Software Data Link Switching Vulnerability - 112254 • IOS Software ICMPv6 over Multiprotocol Label Switching Vulnerability - 113058 • IOS Software IP Service Level Agreement Vulnerability - 113056 • IOS Software IPS DoS Vulnerability - 20120926 • IOS Software IPS and Zone Based Firewall Memory Leak Vulnerability - 113057 • IOS Software IPS and Zone Based Firewall crafted HTTP packets Vulnerability - 113057 • IOS Software IPv6 DoS Vulnerability - 112252 • IOS Software IPv6 over Multiprotocol Label Switching Vulnerability - 113058 • IOS Software MACE DoS Vulnerability - 20120328 • IOS Software Malformed BGP Vulnerability - 20120926 • IOS Software Memory Leak Associated with Crafted IP Packets Vulnerability - 20120328 • IOS Software Memory Leak in H.323 Inspection Vulnerability - 20120328 • IOS Software Memory Leak in HTTP Inspection Vulnerability - 20120328

Table 9-4 Policy Group Details (continued)

Policy Group Name	Policies
Cisco Security Advisories (PSIRT) (contd.)	• IOS Software Memory Leak in SIP Inspection Vulnerability - 20120328 • IOS Software Multicast Source Discovery Protocol Vulnerability - 20120328 • IOS Software NAT DoS Vulnerability - 20120926 • IOS Software NAT For SIP DoS Vulnerability - 20120926 • IOS Software NAT H.323 Vulnerability - 112253 • IOS Software NAT LDAP Vulnerability - 112253 • IOS Software NAT SIP Vulnerability - 112253 • IOS Software Reverse SSH DoS Vulnerability - 20120328 • IOS Software SIP DoS Vulnerability - 112248 • IOS Software SIP DoS Vulnerability - 20120926 • IOS Software Smart Install DoS Vulnerability - 20120328 • IOS Software Smart Install Vulnerability - 113030 • IOS Software Tunneled Traffic Queue Wedge Vulnerability - 20120926 • IOS Software WAAS DoS Vulnerability - 20120328 • IPS ATOMIC.TCP Signature Vulnerability - 81545 • IPS DoS Vulnerability - 107583 • IPS Fragmented Packet Vulnerability - 81545 • IPSec IKE Malformed Packet - 50430 • IPsec Vulnerability- 111266 • IPv4 - 44020 • IPv6 Crafted Packet - 65783 • IPv6 Routing Header - 72372 • Information Leakage Using IPv6 Routing Header - 97848 • Inter Process Communication (IPC) Vulnerabilty - 107661 • Layer 2 Tunneling Protocol (L2TP) DoS Vulnerability - 107441 • MPLS - 63846 • MPLS Forwarding Infrastructure DoS Vulnerability - 107646 • MPLS VPN May Leak Information Vulnerability - 107578 • Mobile IP and IPv6 Vulnerabilities - 109487 • Multicast Virtual Private Network (MVPN) Data Leak - 100374 • Multiple Crafted IPv6 Packets - 63844 • Multiple DNS Cache Poisoning Attacks-107064 • Multiple Features Crafted TCP Sequence Vulnerability - 109337

Table 9-4 Policy Group Details (continued)

Policy Group Name	Policies
Cisco Security Advisories (PSIRT) (contd.)	• Multiple Features IP Sockets Vulnerability - 109333 • Multiple Multicast Vulnerabilities - 107550 • Multiple SIP DoS Vulnerabilities - 107617 • Multiple SSH Vulnerabilities - 8118 • Multiprotocol Label Switching Packet Vulnerability- 111458 • NAM (Network Analysis Module) Vulnerability - 81863 • NAT - 13659 • NAT Skinny Call Control Protocol Vulnerability - 111268 • NAT Skinny Call Control Protocol Vulnerability - 99866 • NTP - 23445 • NTP Packet Vulnerability - 110447 • Network Address Translation Vulnerability - 112028 • Next Hop Resolution Protocol Vulnerability - 91766 • OSPF Malformed Packet - 61365 • OSPF MPLS VPN Vulnerability - 100526 • Object-Group ACL Bypass Vulnerability - 110398 • OpenSSL Implementation DOS Vulnerability - 45643 • OpenSSL Implementation Vulnerability - 49898 • PPTP - 13640 • Radius - 65328 • Reload After Scanning - 13632 • SAA Packets - 42744 • SGBP Packet - 68793 • SIP - 81825 • SIP DoS Vulnerabilities - 109322 • SIP DoS Vulnerability - 110395 • SIP DoS Vulnerability - 112022 • SNMP Malformed Message Handling - 19294 • SNMP Message Processing - 50980 • SNMP Multiple Community String Vulnerabilities - 13629 • SNMP Read-Write ILMI Community String - 13630 • SNMP Trap Reveals WEP Key - 46468 • SNMP Version 3 Authentication Vulnerability - 107408 • SSH Can Cause a Crash - 24862

Table 9-4 Policy Group Details (continued)

Policy Group Name	Policies
Cisco Security Advisories (PSIRT) (contd.)	• SSH Malformed Packet - 29581 • SSH TACACS+ Authentication - 64439 • SSL - 91888 • SSL Packet Processing Vulnerability - 107631 • SSL VPN Vulnerability - 112029 • Secure Copy Authorization Bypass Vulnerability - 97261 • Secure Copy Privilege Escalation Vulnerability - 109323 • Secure Shell Denial of Service Vulnerabilities - 99725 • Session Initiation Protocol Denial of Service Vulnerability - 111448 • Syslog Crash - 13660 • TCP - 72318 • TCP Conn Reset - 50960 • TCP Denial of Service Vulnerability - 112099 • TCP ISN - 13631 • TCP State Manipulation DoS Vulnerability - 109444 • Telnet DoS - 61671 • Telnet Option - 10939 • Timers Heap Overflow - 68064 • Tunnels DoS Vulnerability - 109482 • Unified Communications Manager Express Vulnerability - 110451 • User Datagram protocol delivery issue - 100638 • Virtual Private Dial-up Network DOS Vulnerability - 97278 • Vulnerabilities Found by PROTOS IPSec Test Suite - 68158 • Vulnerability in IOS Firewall Feature Set - 9360 • WebVPN and SSLVPN Vulnerabilities - 107397 • Zone-Based Policy Firewall Vulnerability - 110410 • cTCP Denial of Service Vulnerability - 109314 • uBR10012 Series Devices SNMP Vulnerability - 107696

Table 9-4 Policy Group Details (continued)

Policy Group Name	Policies
Compliance Policies	• BPDU Filter Disabled on Access Ports • BPDU-Guard Disabled on Access Ports • CDP Enabled on Access Ports • Channel Port in Auto Mode • Loop Guard and Port Fast Enabled on Ports • Non-channel Port in Desirable Mode • Non-trunk Ports in Desirable Mode • Port Fast Enabled on Trunk Port • Port is in Error Disabled State • Trunk Ports in Auto Mode
Global Configuration	• ACLs • CDP • Clock • FTP • NTP Configuration • Traceroute
Network Access Services	• Loopback Interfaces • Remote Commands
Network Protocols	• Check only Secure SNMP enabled • Control Plane Policing • HTTP Server • Hot Standby Router Protocol (HSRP) • ICMP • Miscellaneous Services • Routing and Forwarding • SNMP • SSH Parameters • TCP Parameters
Others	• Device Version Checks • Devices Running outdated OS Versions • Devices with outdated modules • L2 Switch—STIG • L3 Router—STIG • L3 Switch—STIG • Outdated Devices As Per Vendor Specific EOL/EOS Announcements

Table 9-4 Policy Group Details (continued)

Policy Group Name	Policies
Routing Protocols	• BGP • EIGRP • OSPF • RIP
Security	• ACL on Interfaces • Distributed DoS Attacks • Firewall Traffic Rules • Land Attack • Martian Traffic • Null (Black Hole) Routing • Risky Traffic • SMURF Attack • Traffic Rules
Switching	• DHCP Snooping • Dynamic Trunking Protocol • IEEE 802.1x Port-Based Authentication • IEEE 802.3 Flow Control • IP Phone + Host Ports • IP Phone Ports • Management VLAN • Port Security • Spanning Tree Protocol (STP) • Unidirectional Link Detection (UDLD) • Unused Ports • VLAN 1 • VLAN Trunking Protocol (VTP)
Compliance Policies	• All user-defined policies are listed under this policy group.

Choosing the Devices for the Compliance Audit

After you create a policy profile, you must choose the devices or device groups on which the compliance audit must be performed. After you choose the devices or device groups and schedule an audit, a job with the name of the policy profile is created. This name defines the job, and can be scheduled periodically. You can edit the job name.

Step 1 After you have created the profiles, click the **Run Compliance Audit** icon.

Step 2 In the Select Device window, choose one of the following options:

- By Devices—Choose this option to select the device(s) that you want to audit. For more information about how to Manage advance filter options on r for the selected devices, see the Managing Multilayer Quick Filters for Selected Devices in the Compliance Audit Jobs, page 9-70.
- By Groups—Choose this option to select the device group(s) that you want to audit. There must be at least one device added to a device group for the group to be audited. If a device is added to multiple device groups that are selected for auditing, the device will be audited once. For information on how to set up a device group, see the "Setting Up CCM Device Groups" section on page 3-20.

Note The audit will be performed on the devices that are available in the device group at the time of execution.

Step 3 Click **Next**.

Step 4 In the Schedule Audit page, enter the schedule details. In the Choose Configuration option, select one of the following:

- Use Latest Archived Configuration—If you choose this option, the latest Backup Configuration in the archive is used. If the backup configuration is not available, the device is not audited and is marked against non-audited devices.
- Use Current Device Configuration—If you choose this option, Prime Network polls for the latest configuration from the device and then performs the audit. If a Show command is used in the compliance policy, the output of the Show command is taken from the current device configuration.
- Use Send Audit Configuration Report—If you choose this option, a new compliance audit mail job is generated. The compliance audit mail job creates a new audit report and attaches the report as an excel sheet to the email with subject as Config Audit Report for Job ID:<*id*>. The excel sheet contains the details of device name, device IP, timestamp, the profile name, policy name, rule name, rule result, and violation message. You can cancel or delete the compliance audit mail job.
- Use Compare & Send Previous Configuration—If you choose this option, a new compliance audit mail job is generated with a message *Compare & Send Previous Configuration will be performed from next job*. From the next audit job, a new configuration comparison report is generated. If there are any changes between the earlier and the later audit reports, then the fields that have discrepancies appear in red. The configuration comparison report is attached to the email. You can cancel or delete the compliance audit mail job. You can also download the report as an excel sheet, for which you need to choose the devices and click **Compare Previous Config** in the **Audited Devices** window.

Step 5 Click **Audit**. An audit job is scheduled. You can view the status of an audit job from the Jobs page.

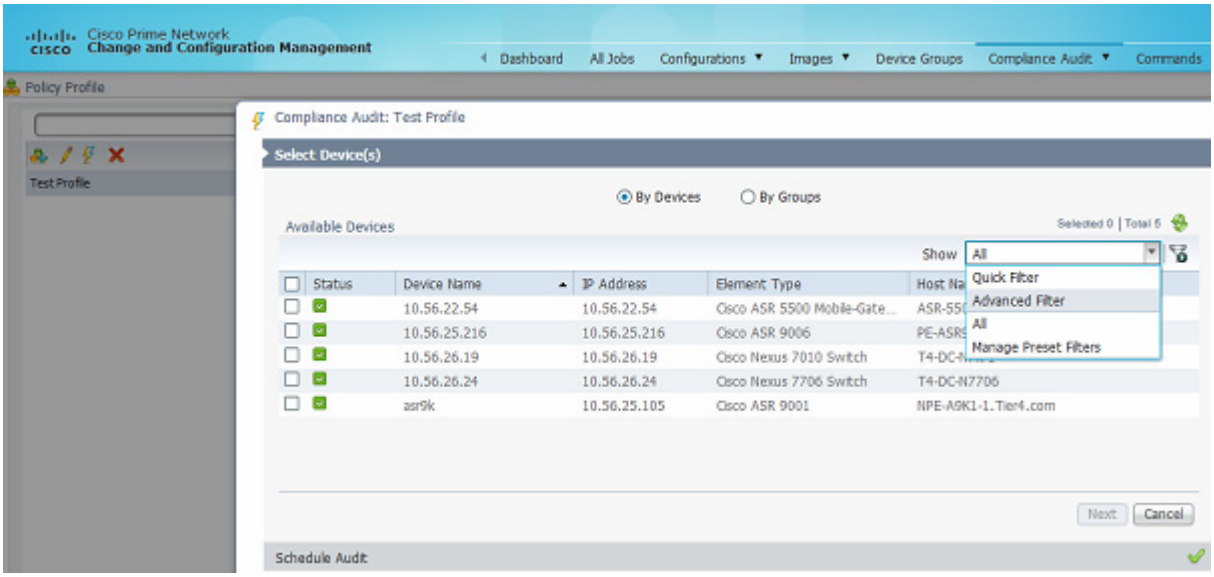
Managing Multilayer Quick Filters for Selected Devices in the Compliance Audit Jobs

After choosing an option in the Select Devices area, use the multilayer advance filters to easily query device items. You can save preset filters for the selected device during a compliance audit, modify the filters to add or remove new device information, element types and so on, and save the filter again as a different name. When the system job is run, you can export all configuration data irrespective of the last modification done on the archive.

To create an Advanced Filter, follow the below steps:

1. In the **Policy Profile** window, choose an profile and the click **Run**. The **Compliance Audit** window appears as shown in the figure 9-17.

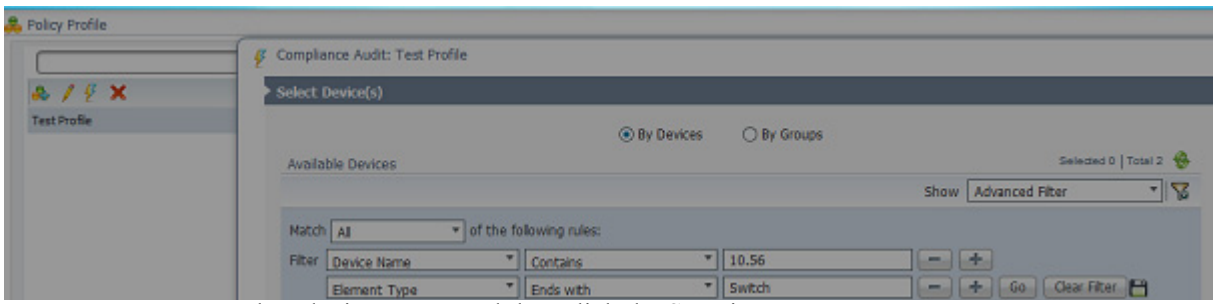
Figure 9-21 Compliance Audit



To Save the already created advanced filters. follow the below steps:

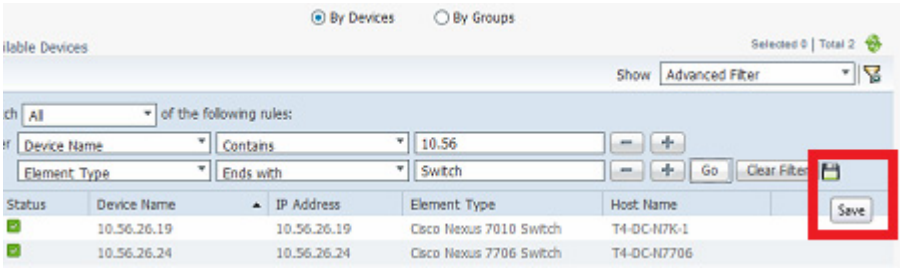
a. From the **Show** drop-down list, choose Advanced Filter. If you want to set the criterion use the Match All of the following rules area. In the **Filter** fields, enter your criteria to view all the device details and then click **Go**.

Figure 9-22 Set Filter Criterion



b. Select device names and then click the **Save** icon.

Figure 9-23 Save Icon

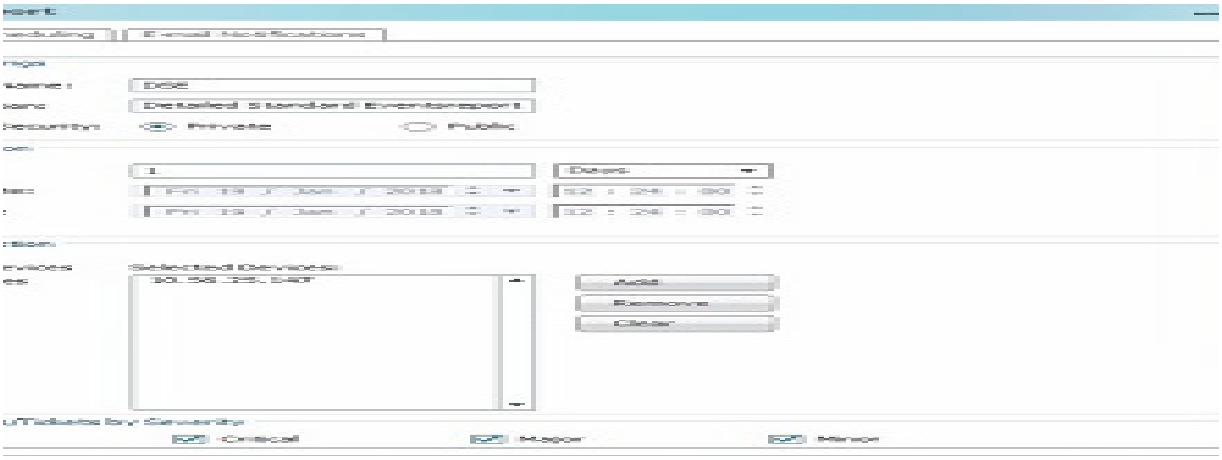


c. In the **Save a Preset filter dialog box, specify a name to the previously selected filter by devices** and then click **Save.**

Figure 9-24 Save a Preset Filter

d. If the filter name already exists, a warning message appears as shown in the Figure 9-25

Figure 9-25 Warning Message

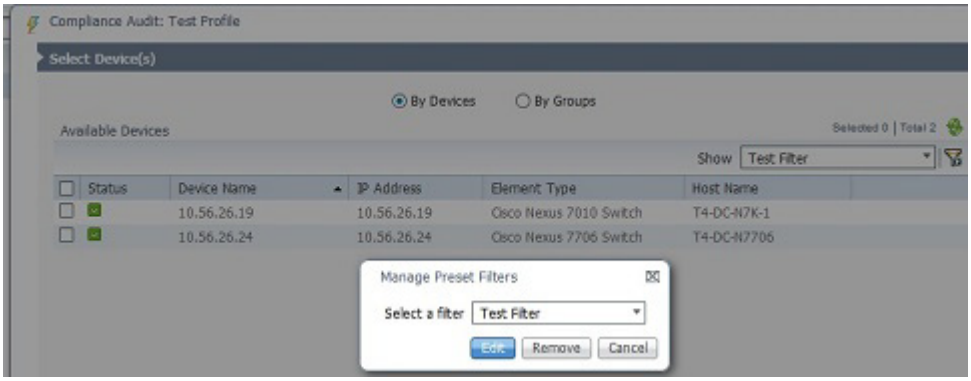


e. Click Yes or No.

To modify, remove, or delete the preset advance filter:

a. In the **Edit Compliance Audit Job** window, from the **Show drop-down list**, choose Manage Preset Filers to edit or remove the previously selected filters. The **Manage a Preset Filter** dialog box appears.

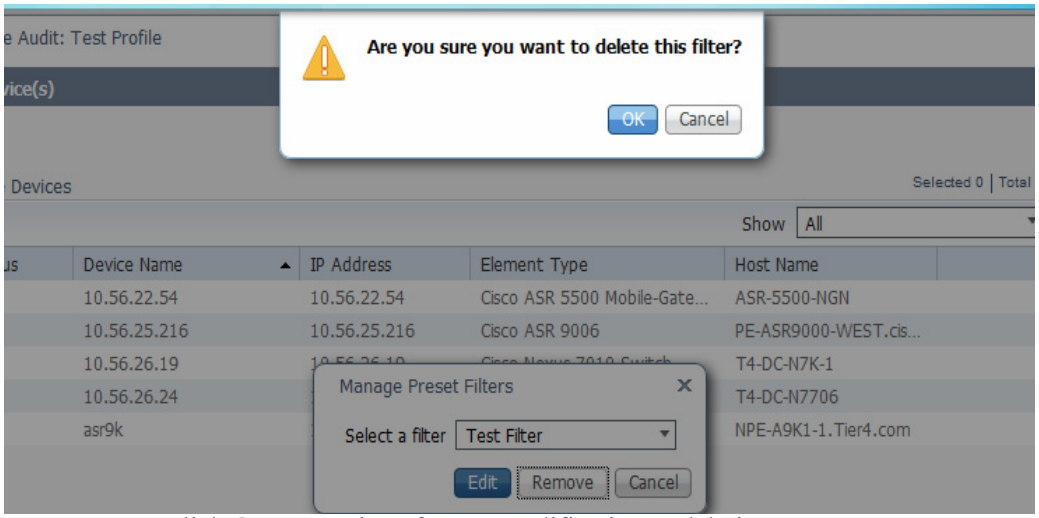
Figure 9-26 Manage Preset Filters



b. From the **Select a filter** drop-down list, choose the relevant filter name to modify or remove the device information.

c. A prompt message for removal or deletion of the advance filter appears your confirmation.

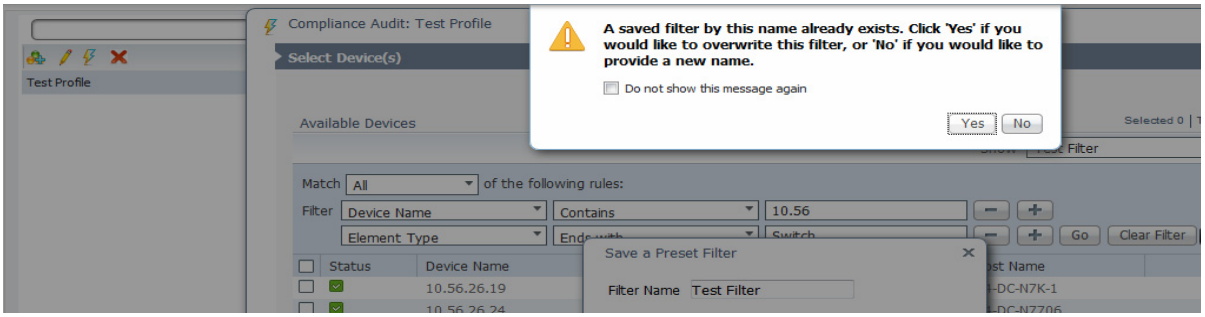
Figure 9-27 A Delete Prompt Message



d. Click **OK** to continue for any modification or deletion.

e. After modification click the **Save** icon to save in a different name. If the filter name already exists, a warning message appears as shown in the figure Figure 9-28.

Figure 9-28 Overwrite the filter



f. Click **Yes** or **No**.

Viewing the Results of a Compliance Audit Job and Running Fixes for Violations

The status of scheduled jobs appears on the Jobs page (**Compliance Audit > Jobs)**. All audits are logged by Prime Network as jobs.

From this page, you can view the violation details and can also apply a fix. To apply a fix for a violation, you can either do a regular fix or use a predefined command that is available in the Command Manager. After a job is created, you can set the following preferences for the job:

- Suspend—Can be applied only on jobs that are scheduled for future. You cannot suspend a job that is running.
- Resume—Can be applied only on jobs that have been suspended.
- Reschedule—Using this option, you can reschedule a job that has been scheduled for a different time. Choose a job, and click **Reschedule**. The Compliance Audit Job Rescheduler window opens. Set your preferences. The following options are available against Choose Configuration option:
  - Use Latest Archived Configuration—If you choose this option, the latest Backup Configuration in the archive is used. If Show command is used in the compliance policy, the output of the Show command is taken from the current device configurations.
  - Use Latest Configuration from Device—If you choose this option, Prime Network polls for the latest configuration from the device and performs the audit.

Note You might be prompted to enter your device access credentials. This option is enabled if, from the Administration client, **Global Settings > Security Settings > User Account Settings > Execution of Configuration Operations**, you checked the option **Ask for user credentials when running configuration operations**. This is an enhanced security measure to restrict access to devices.

- Cancel—Using this option, you can cancel a scheduled job or the job that is in the running state. Once the job is canceled, the job status with Canceled status appears against the **Last Run Status** field. Click the Canceled hyperlink to view the user who has canceled that job.
- View—This option is enabled only for jobs that are in Completed state. Using this option, you can view the details of a job, the associated policies and devices. If you have selected a device group for auditing, click the hyperlinked device group name to display the list of devices included in the device group.
- Edit—Using this option, you can edit a scheduled job. You cannot edit a job that is running. If you have selected **By Groups** in the Select Device page when scheduling an audit, you cannot select **By Devices**, and vice versa, when editing the scheduled job.
- Delete—This option deletes a job that has been scheduled. This deletes the listing from CCM. You cannot delete a job that is running.

All jobs that are completed are listed in the jobs page. The job is flagged a success only if all the devices audited conform to the policies specified in the profile. The result, otherwise, is displayed as Failure. The job is called a partial success if job contains a mix of both audited and non-audited devices, with the compliance status of audited devices being a success.

Export Job Results

You can view the Job status in a XLS format for the completed job from the **All Jobs** tab, or from each module of the CCM. You can view the export option only for the following selected job types from the CCM module.

Table 9-5 CCM Modules and Job Types

Module	Job Types
Configurations	Archives, which includes Backup, Restore, Synchronize and so on
NEIM	Import; from device, Package add, Distribution, Activation, Commit, Rollback
Compliance Audit	Compliance Job
Commands Manager	Commands-manager
Transaction Manager	Transaction-manager

To export and view the job results in XLS format from Change and Configuration:

Step 1 Log in to the Change and Configuration Management client.

Step 2 Click the **All Jobs** tab.

Step 3 Select a row that has a Job type that is mentioned above. Ensure that the **Job Status** is in **Scheduled or Completed** and the **Lastrun Status** is **Success** or **Partial_Success** for a selected job type.

For example, when you click the Lastrunresult of a compliance audit job type, the Compliance Job Audit Details window displays the compliance audit and violation details. For more information about audit violation details, see Job Details and Violations Summary, page 9-75.

Step 4 Click the hyperlinked Lastrunresult displayed against each job to view the details of a specific job.

Step 5 In the **Job Details** window, click **Export Result** to export the job results in a XLS format.

Note Job status details can be exported and downloaded from the other CCM module's Job page.

Step 6 Click **OK** to close a specific Job Details window.

Job Details and Violations Summary

Figure 9-29 displays the information about the available and selected devices, rules that you selected for the compliance audit, compliance state, violation count, instance count, highest severity and ignore count. The information about audited devices from all the devices are displayed separately at the back end.

Figure 9-29 Job Details and Violations Summary

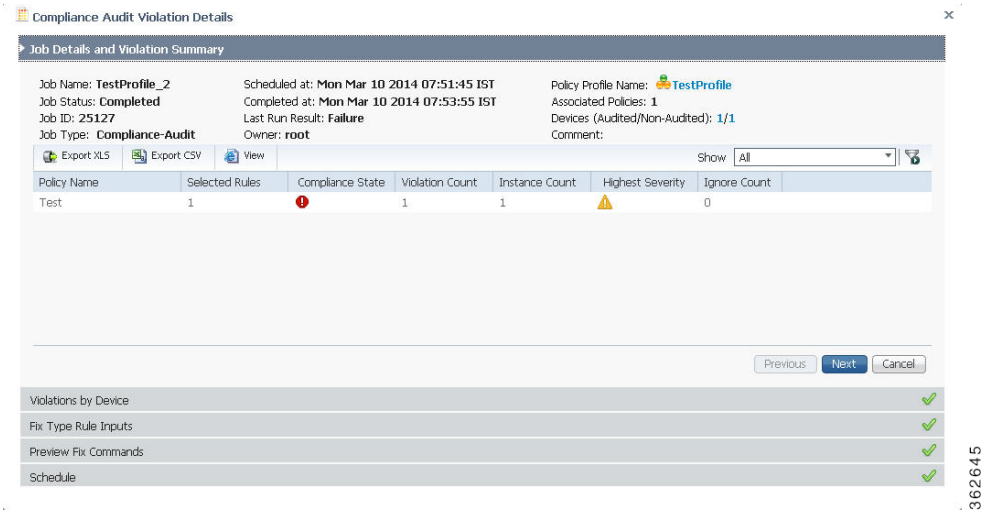


Table 9-6 Job Details and Violations Summary- Fields

Field	Description
Audited/Non-Audited Devices	This displays the number of audited and non-audited devices. For more details on devices, click the hyperlinked count of audited and non-audited devices. The device name and audit status are displayed when you click the hyperlinked count of audited devices. Non-audited devices include the count of the following. • The devices that were within the scope of the user while scheduling the job, but has since changed. At the time job ran, these devices were not within the scope of the user. • The devices that were down or were not reachable when the job ran. • CPT device not in IOS mode. These devices are not audited because they do not contain running configuration, which is required for Compliance Manager. • Third Party Devices. • Device not in sync with Compliance server—that is, the device element type is not available in the Compliance server. • Devices of which backup running configuration cannot be fetched from CCM.
Selected Rules	Number of rules selected in a policy at the time the policy profile was created. This may be subset of the total number of rules defined for the policy.
Compliance State	Displays Pass or Fail. All rules in policy for all devices must confirm for the state to display Pass.
Violation Count	This lists the number of distinct violations (for a particular policy, for the number of devices) that were observed in each job. For example, if a particular policy is violated in 100 devices, the violation count is only 1.
Instance Count	Summation of the violation count for all the device. For example, if a particular policy is violated in 100 devices, the instance count is 100.
Highest Severity	The highest severity of the various rules comprising the policy. The highest (as decided at the time of creating rules) is shown. This overrides the lower severity items.
Ignore Count	This is the count of rules ignored due to devices falling outside the scope of platforms defined against the rule.
Export XLS	Click to export the compliance audit violation details to the XLS file.

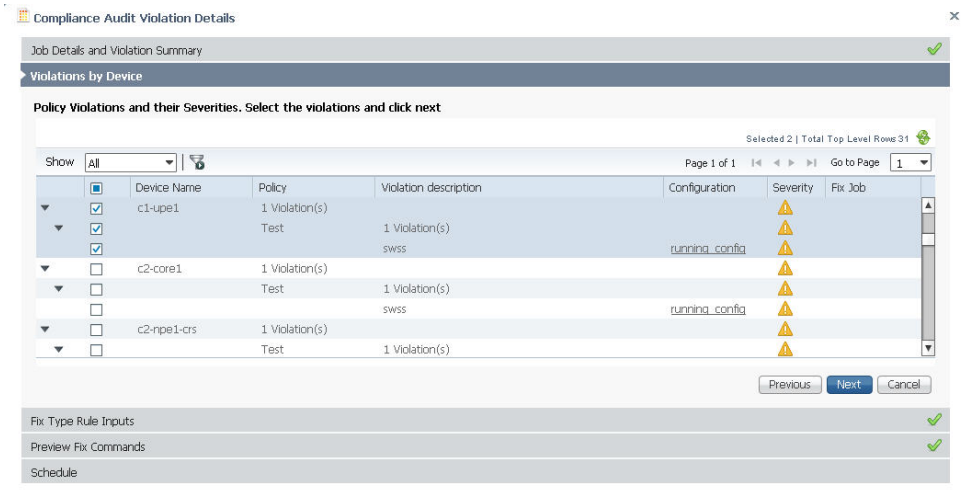
Table 9-6 Job Details and Violations Summary- Fields (continued)

Field	Description
Export CSV	Click to export the compliance audit violation details to the CSV file.
View	Click to view the compliance audit violation details as an HTML page.
Export Audit	Click to export the compliance audit details to the XLS file.

Violations by Device

Figure 9-30 displays the violations at a device level.

Figure 9-30 Violations by Device



Select the devices that require the fix CLI to be applied. The check box for a device will be enabled when:

- a fix CLI is available for the device.
- the violation is not fixed on the device.
- no fix job is running for the violation.

Click the **running config** link under the Configurations column to view the running configurations of the device. If a Show command is used in the compliance policy, the output of the Show command is also displayed.

If a violation has already been fixed or a fix job has been scheduled, the Fix Job column displays the name of the fix job with a hyperlink. Click the hyperlink to view the compliance fix details. The check box for that violation will be disabled.

Click **Next**.

Fix Type Rule Inputs

This window is applicable only if you have a fix type input for the violation. Enter the required rule input to fix the violation. Click **Next**. See Figure 9-31.

Figure 9-31 Fix Type Rule Input

Preview Fix Commands

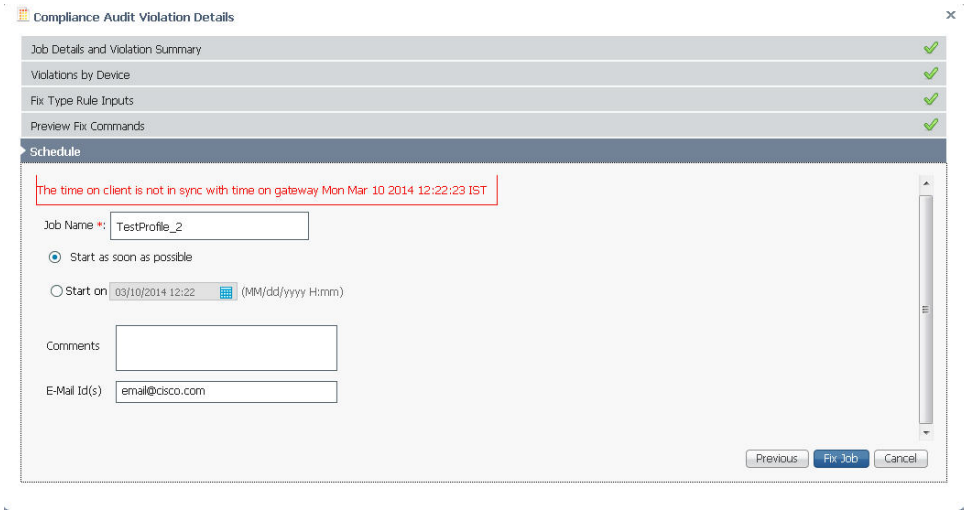
Figure 9-32 displays the preview of the fix CLI that will be applied to the device when you schedule a fix job. If you are using the predefined command that is available in the Command Manager to fix the violation, the command builder script name with a hyperlink is displayed. Click the hyperlink to view the values that will be executed on the device to fix the compliance violation. Click **Next**.

Figure 9-32 Preview Fix Commands

Schedule

Set the scheduling options such as the job name, start time, and email ID. Click **Fix Job** to schedule the job. The details of the fix job can be viewed from **Compliance Audit > Jobs**. The job type is Compliance-Fix. See Figure 9-33.

Figure 9-33 Schedule



You can view the status of a fix job after the job completes. Click the hyperlinked status to view the results of the fix job.

Using Compliance Audit for Device Compliance

Note Starting in Prime Network 4.1, Configuration Audit is being replaced by Compliance Audit. In Prime Network 5.3, Configuration Audit is deprecated. However, if you enabled the option to retain Configuration Audit during an upgrade procedure from Prime Network 3.11 (or earlier), the feature will still available from CCM. For more information on Compliance Audit, see Making Sure Devices Conform to Policies Using Compliance Audit, page 9-51.

These topics describe how to use Compliance Audit:

- Managing Compliance Audit Policies, page 9-81
- Scheduling a Compliance Audit, page 9-82
- Viewing Compliance Audit Jobs and Audit Results, page 9-82

The CCM Compliance Audit feature checks device compliance to ensure they comply to a compliance policy file (the *baseline* or *expected configuration*). Each compliance policy is a set of CLI commands that define a desired baseline or expected configuration. Compliance policies can also be configured using valid, Java-based regular expressions. Table 9-7 provides examples of compliance policy CLIs.

Table 9-7 Configuration Policy CLI Examples

Policy Name	Policy Description	Policy CLI
SamplePolicy1	Sample policy for global configuration auditing	`spanning-tree mode rapid-pvst`
SamplePolicy2	Sample policy for global regex and first sub level cli matching audit	`interface GigabitEthernet(.*)` `  port-type nni`

SamplePolicy3	Sample policy for global regex, first sub level cli matching, and second sub level regex matching	`router (.*)`
		`  address-family ipv4 unicast`
		`  network (.*)`

SamplePolicy4	Sample policy for fixed cli matching	`interface GigabitEthernet3/4` `  address-family ipv4 unicast`

Sample Compliance Policy

The following example shows a policy that performs audit for BGP configuration for a Cisco IOS router:

```
#BGP Compliance Audit
router bgp (.*)
   neighbor (.*) remote-as (.*)
   address-family ipv4
```

If you want an audit check for specific BGP AS or neighbor IP address, the above CLI can be changed accordingly. For example:

```
router bgp 65000
   neighbor (.*) remote-as 65001
    address-family ipv4
```

You can combine multiple different configurations into one policy. For example:

```
#BGP Compliance Audit
router bgp (.*)
   neighbor (.*) remote-as (.*)
   address-family ipv4
# Interface MEP check
interface GigabitEthernet(.*)
   ethernet (.*)
      mep domain UP (.*)
```

Compliance audit can be scheduled against multiple configuration files to obtain an audit report that indicates the existence of configuration sequences stated in the baseline policy and any deviations from the baseline.

You can define a compliance policy, create and save the advance filters and select the devices that need to be audited against the policy, and schedule the audit job to run immediately or at a later point in time. The audit job compares the CLI commands (as part of the configuration policy) against the actual running configuration on the device to identify the discrepancies.

You can view the status of all the scheduled compliance audit jobs in the Job Manager page. The compliance audit results are in the form of a report indicating the discrepancies (missing configuration commands on the device) in red and the matching commands in green.

Managing Compliance Audit Policies

CCM allows you to create, modify, view, and delete configuration policies. Choose **Compliance Audit > Compliance Policies**. The Configuration Policies page provides the list of existing policies. You can search the configuration policies by CLI strings.

Creating a Compliance Policy

To create a compliance policy:

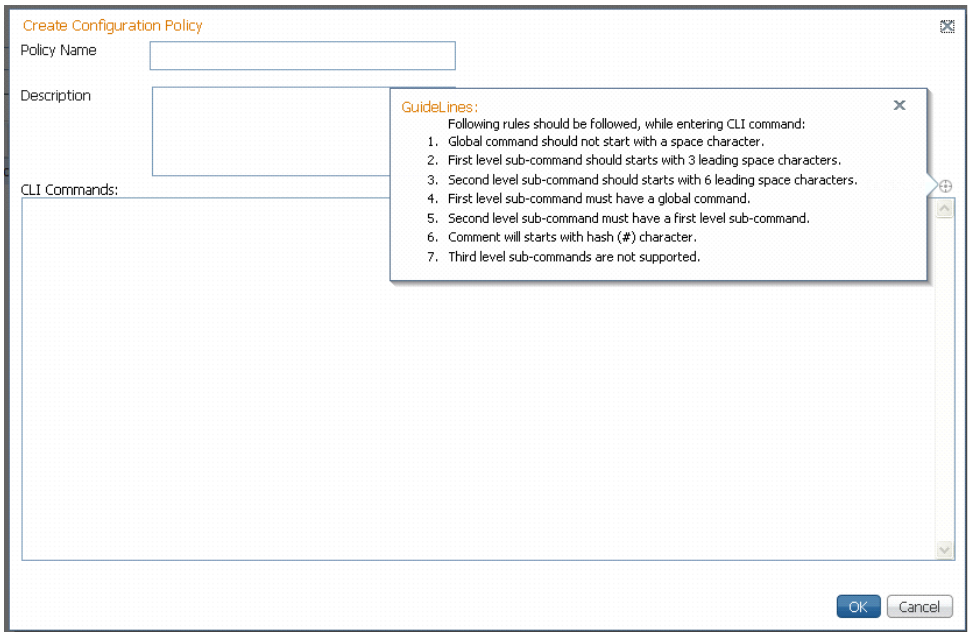
Step 1 In the Configuration Policies page, click the **Create** icon.

Step 2 Provide the policy name and description.

Step 3 Enter the CLI commands to set up a baseline configuration for that policy. This can also be a valid, Java-based regular expression. See Table 9-7 for sample configuration CLIs.

Step 4 Make sure you follow the guide 5.3 while entering the CLI commands. Click **Guide5.3** to view these guide5.3 as shown in Figure 9-34.

Figure 9-34 Create Configuration Policy-Showing Guide5.3



Editing, Viewing, and Deleting Compliance Policy

In the Compliance Policies page, you can also do the following:

- Select a policy and click **Edit** to modify the policy description and CLI commands. You cannot modify the policy name. Keep in mind the policy guide 5.3 while modifying the CLI commands.
- Select a policy and click **View** to view the policy name, description, and CLI commands.
- Select a policy or multiple policies and click **Delete** to delete the configuration policies. You cannot delete a policy if it is part of a scheduled audit job.

Scheduling a Compliance Audit

You can schedule compliance audit jobs to run immediately or at a later point in time.

Note Only a maximum of 10 policies and 500 devices can be used for scheduling an audit job.

To schedule a compliance audit job:

Step 1 Choose **Compliance Audit > Basic Audit**. The Select Configuration Policies page lists the available configuration policies. You can search the configuration policies by using CLI strings.

Step 2 Select the desired configuration policy from the available list and click **Next**.

Step 3 In the Select Devices page, select the devices that must be audited against the selected configuration policy, and then click **Next**.

Step 4 Under the Match the following Rule area, enter the filter details and click the Plus icon to save as a preset filter.

Step 5 Click Go

Step 6 In the Schedule Audit page, provide a job name and the scheduling information for the compliance audit job. You can choose to run the audit job immediately or at a later point in time. A popup with the gateway time is available to assist you in setting up the time for scheduling the audit job.

Step 7 Click **Audit**. You will be redirected to the Compliance Audit Jobs page.

Note Once scheduled, you cannot edit the policies or devices that are part of the scheduled job.

Viewing Compliance Audit Jobs and Audit Results

The Compliance Audit Jobs page (**Compliance Audit > Compliance Audit Jobs**) provides the following details:

- Jobs—This table lists all compliance audit jobs submitted by the login user. The ‘root’ user can view jobs submitted by other users, by selecting the username from the table header.
- History—For a selected job in the Jobs table, this table lists all the instances. You can select only one job at a time to view the history details.

You can select a job and click **View** to view the associated devices and policies, and the schedule for the selected audit job.

You can also use this page to suspend, resume, cancel, delete, or reschedule a job.

To view the compliance audit job details and the audit result:

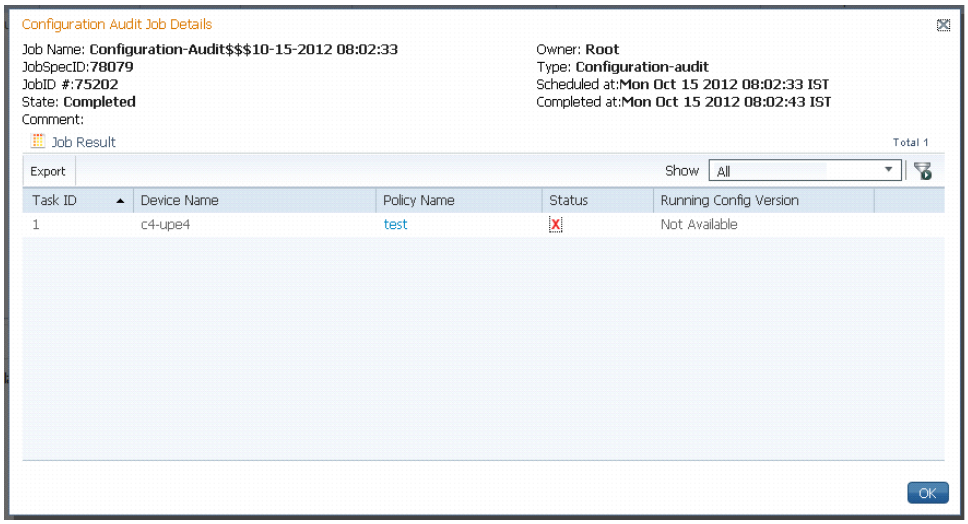
Step 1 Click the hyperlinked **LastRun Result** (Success/Partial Success/Failure) against a particular job in the Jobs table.

The Compliance Audit Job Details dialog box displays the job details and the audit results for a device and policy combination, as shown in Figure 9-35. The Job Results table includes the device audited, policy against which the device was audited, audit status, and the running configuration version used for

the audit. A blue tick mark in the Status column indicates ‘Audit Pass’, and a red X indicates ‘Audit Fail’. Click the hyperlinked policy name to view the configuration policy details, with updates if the policy has been modified.

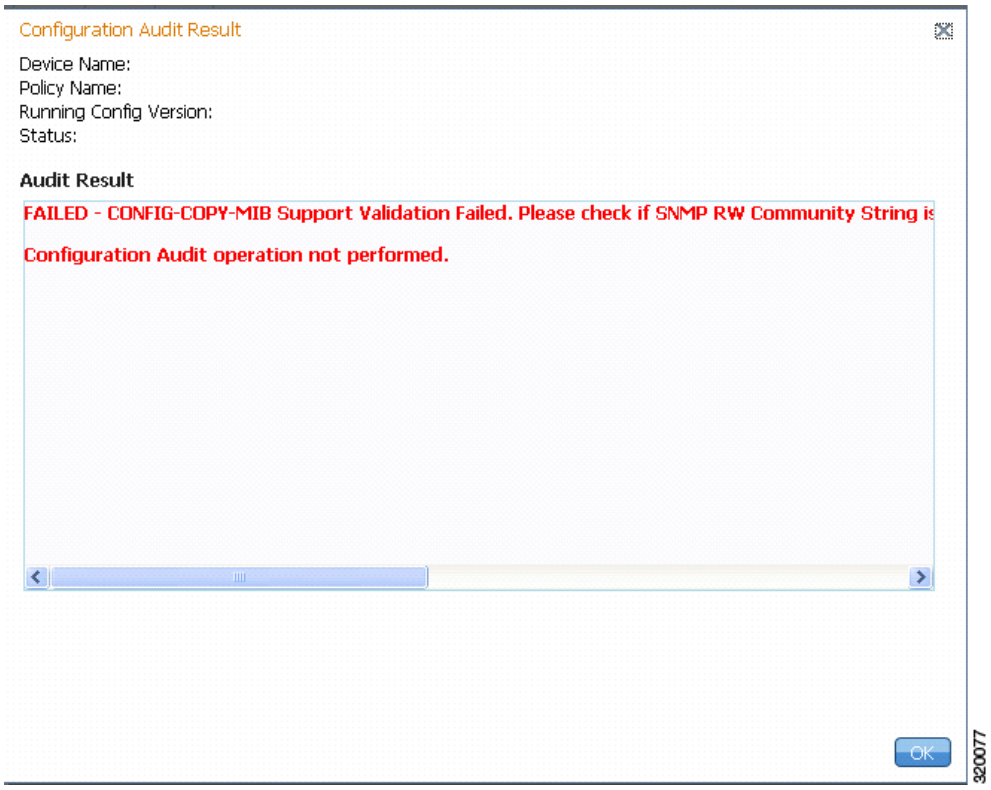
Note For Cisco Nexus devices, the VDC name is also displayed in the Device Name column.

Figure 9-35 Compliance Audit Job Details



Step 2 Click on the hyperlinked **Status** (Pass/Fail icon) in the Job Results table. Or, click the hyperlinked Success or Failure hyperlink in the **Result** field of the History table. The Compliance Audit Result dialog box displays the audit result with matching commands (for ‘Audit Pass’) and discrepancies or missing commands (for ‘Audit Fail’) between the policy and the running configuration on the device. See Figure 9-36 for an example of the Compliance Audit Result dialog box for an ‘Audit Fail’ scenario.

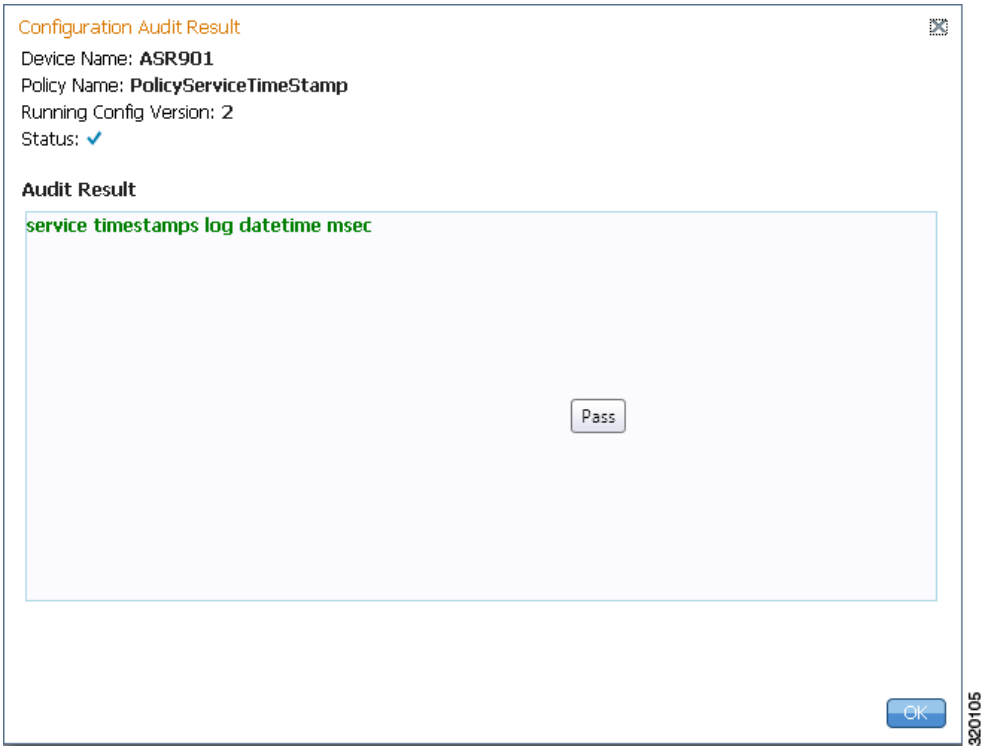
Figure 9-36 Compliance Audit Result - Audit Fail



The matching commands are displayed in green (see Figure 9-37), while the discrepancies are displayed in red (see Figure 9-36). For a failed job, the Audit Result section also displays the reason why the audit was not successful as shown in Figure 9-36. Some reasons for audit failure are:

- Failed to back up running configuration of the device
- Device not reachable
- Unable to download running configuration
- Device not under the scope of the user
- Policy is not available
- Invalid regular expression in the CLI

Figure 9-37 Compliance Audit Result - Audit Pass



Step 3 Click **Export** in the Job Results table to export the audit job results to a .csv file. You can view the job details and audit results in the exported file.

Checking Image Management, Device Management, and Compliance Audit Jobs

When a job is created, Prime Network assigns it a job specification ID and attaches a time stamp, indicating when the job was created. Only the job creator and users with Administrator privileges can change the job settings.

Note Whenever a CCM job is scheduled to run immediately, you will be prompted, either to stay in the same page or to be redirected to the Jobs page.

CCM also facilitates automatic e-mail notification of the status of the CCM jobs upon completion based on the e-mail option you set up in the Image Management Settings page. The notification is sent to a list of e-mail IDs configured either in the settings page or while scheduling the job.

Keep these items in mind when managing jobs:

- All jobs are scheduled based on the gateway time.
- If you choose two or more jobs and click Reschedule, the option defaults to Start as Soon as Possible. To view the original time and then reschedule, choose only one job and click Reschedule.

- Job properties cannot be edited; you must delete the old job and create a new one.
- Jobs are persisted even if the gateway server is restarted.
- Only the job creators and users with Administrator and Configurator privileges can perform the actions provided on the Jobs page (suspend, resume, reschedule, cancel, delete, refresh).
- Configuration and CCM jobs fail under the following conditions:
  - If the device is not under the scope of the user to perform the config or image operation.
  - If the user is not authorized to perform the config or image operation.
- Running jobs cannot be suspended or canceled; you must let them complete.
- System-generated jobs cannot be modified. To change the settings, go to **Settings > Global Settings > Period Export Options**, and modify the options accordingly.
- Cancel stops all future instances of a job. To stop a job and resume it later, use Suspend and Resume
- To view the history of a job, choose a job and view the history from the History tab at the bottom of the page. You cannot view history of multiple jobs at the same time; choose only one job at a time.

Messages that can be used for debugging are saved in *NETWORKHOME*/XMP_Platform/logs/JobManager.log.

See these topics for job examples:

- Viewing the Results of a Compliance Audit Job and Running Fixes for Violations, page 9-74
- Viewing Compliance Audit Jobs and Audit Results, page 9-82

How Prime Network Handles Incoming Events

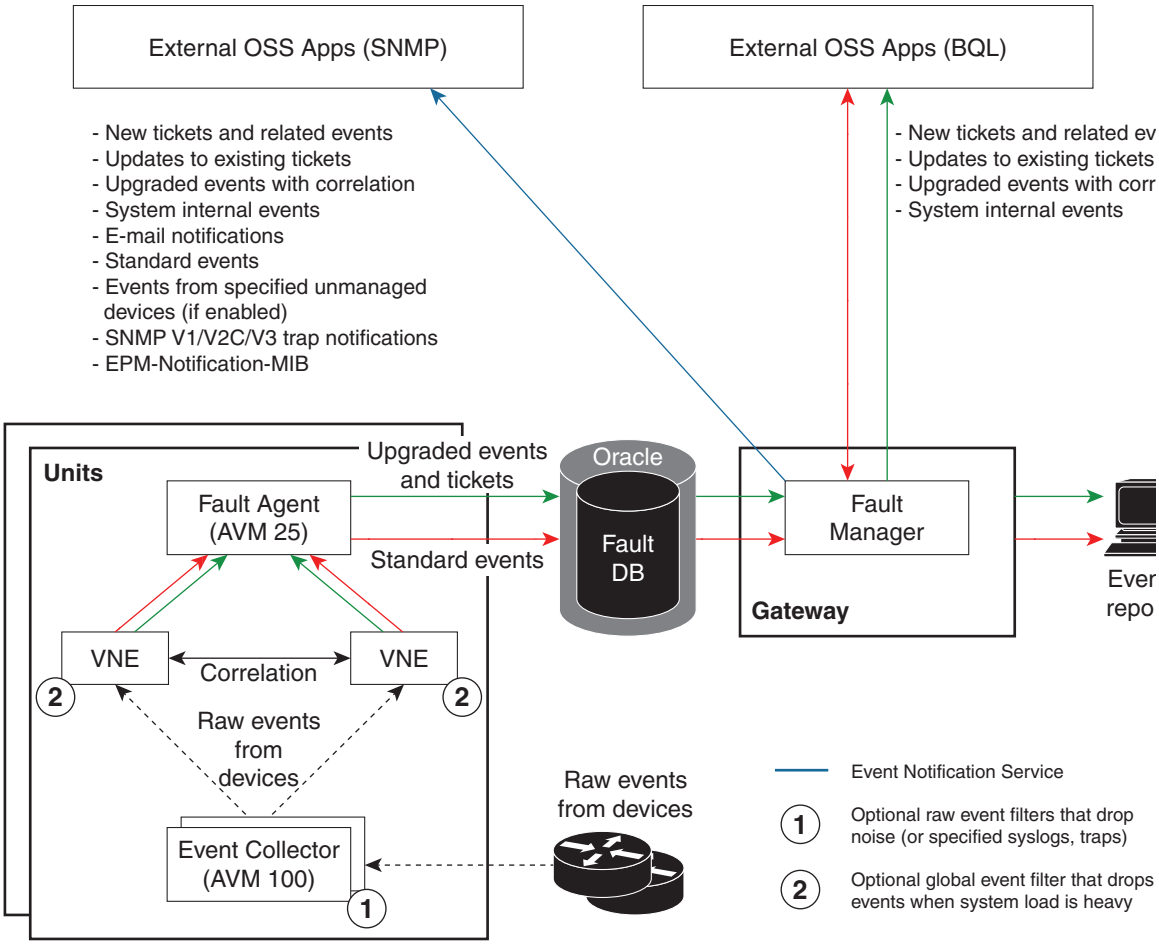
These topics explain how Prime Network handles incoming events and provides information about events and tickets in the GUI clients:

How Events Flow Through Prime Network Components

Figure 10-1 illustrates how Prime Network responds to incoming notifications from devices. The exact flow depends on how Prime Network is configured in your network. The flow is described in detail in How Prime Network Correlates Incoming Events, page 10-4.

Note Figure 10-1 illustrates the *logical* flow of events through Prime Network. The actual network communication is subject to the transport configuration between the gateway server and units.

Figure 10-1 Logical Flow of Incoming Events Received By Prime Network



The main components involved in fault processing are described in the following table.

Component	Located on:	Description
Event Collector (AVM 100)	Gateway or unit(s)[1]	Examines events for basic information and associates and distributes events to corresponding VNEs. If handling events from unmanaged devices is enabled, saves these events to the database; if an Event Notification Service is enabled, forwards these events to the gateway. If a raw event (noise) filter is enabled, drops the events. **Note** User can create AVMs from 101-999 automatically using AUTO-VNE Assignment feature. See Chapter 4 of Cisco Prime Network Administrator Guide
VNEs	Hosting unit	Parses and associates events to specific components in NEs; if the NE is a physical interface, checks if alarms are disabled on the interface. Determines whether events are standard or upgraded (see Standard and Upgraded Events, page 10-4). Attempts to correlate the event, depending on its configuration, and enriches the event with additional information (category, nature). Forwards events to AVM 25. If a global event filter is configured and system load is high, drops any events that match the filter (by default, no filters are implemented; see the *Cisco Prime Network 5.3 Administrator Guide*).
Fault Agent (AVM 25)	All gateways and units	Opens new alarms and tickets, and persists (saves) information in the database. • Uncorrelated events that are ticketable—Opens new alarms and tickets and saves information in database (active partition). • Uncorrelated events that are not ticketable—Saves the information in database as *archived*. • Correlated events—Updates the ticket and saves the information in database. AVM 25 requires a database connection to store information in the Oracle database. If a direct connection is not available, configure Prime Network to forward events to another AVM 25 that has a database connection (called using a *proxy AVM 25*, described in the *Cisco Prime Network 5.3 Administrator Guide*).
Ticket Agent	Oracle database	Associates new events to existing alarms and tickets.
Database	Oracle database	Stores all tickets, alarms, and events which can be viewed from: • Events client—Tickets, Service, Audit, Provisioning, Security, System, Standard, All events • Vision client—Tickets, Network Events, Provisioning Events, Latest Events
Fault Manager	Gateway	If an Event Notification Service is configured, retrieves information for e-mail and trap forwarding and forwards information to external OSS applications.

1. By default, the Event Collector is installed on the gateway. All supported configurations are described in the event monitoring topics in the *Cisco Prime Network 5.3 Administrator Guide*.

For more details about what each component does, see How Prime Network Correlates Incoming Events, page 10-4.

Standard and Upgraded Events

If the VNE cannot extract adequate information about an event, it performs some basic parsing and saves the event in the database. These events are called *standard events*. A standard event is an event that Prime Network cannot match with any of the rules that define events of interest. Standard events are not processed for correlation. They are immediately saved to the database and marked as archived.

Standard events can be viewed from the following clients:

- From the Events client under the **Standard** tab.
- From the Vision client under the **Network Events** tab in a device inventory view. If enabled from the Administration client, standard events are also displayed in the **Latest Events** tab in a map view.

An *upgraded event* is an event that a VNE can match with the rules that determine events of interest. Upgraded events are parsed and if are enabled for correlation, the VNE begins the correlation process. Not all upgraded events are enabled for correlation. For an illustration of how Prime Network handles standard events, see How Prime Network Correlates Incoming Events, page 10-4.

How Prime Network Correlates Incoming Events

Note An event can have many additional correlation and metadata attributes that determine how Prime Network processes the event. Examples are provided in Event Correlation Examples, page C-1.

The correlation process determines the causality for events, event sequences, and tickets. Causality is represented in a ticket's correlation tree, with a root cause event at the top (for an example, see Figure 11-6 on page 11-16). The process begins when Prime Network receives an incoming event.

The Prime Network Event Collector (AVM 100) receives all incoming events—external events like traps and syslogs. The Event Collector performs some basic parsing to associate the event with the appropriate VNE. If handling events from unmanaged devices is enabled, AVM 100 saves these events in the database. If a raw event (noise) filter is enabled, AVM 100 drops the events.

You can configure the Event Notification Service to forward these events to OSSs or e-mail recipients. This is done from the Administration client and is described in *Cisco Prime Network 5.3 Administrator Guide*.

The following figures illustrate how Prime Network handles events that are:

- Enabled for correlation, in Figure 10-2.
- Not enabled for correlation, in Figure 10-3.

Figure 10-2 Event Processing—Events With Correlation Enabled

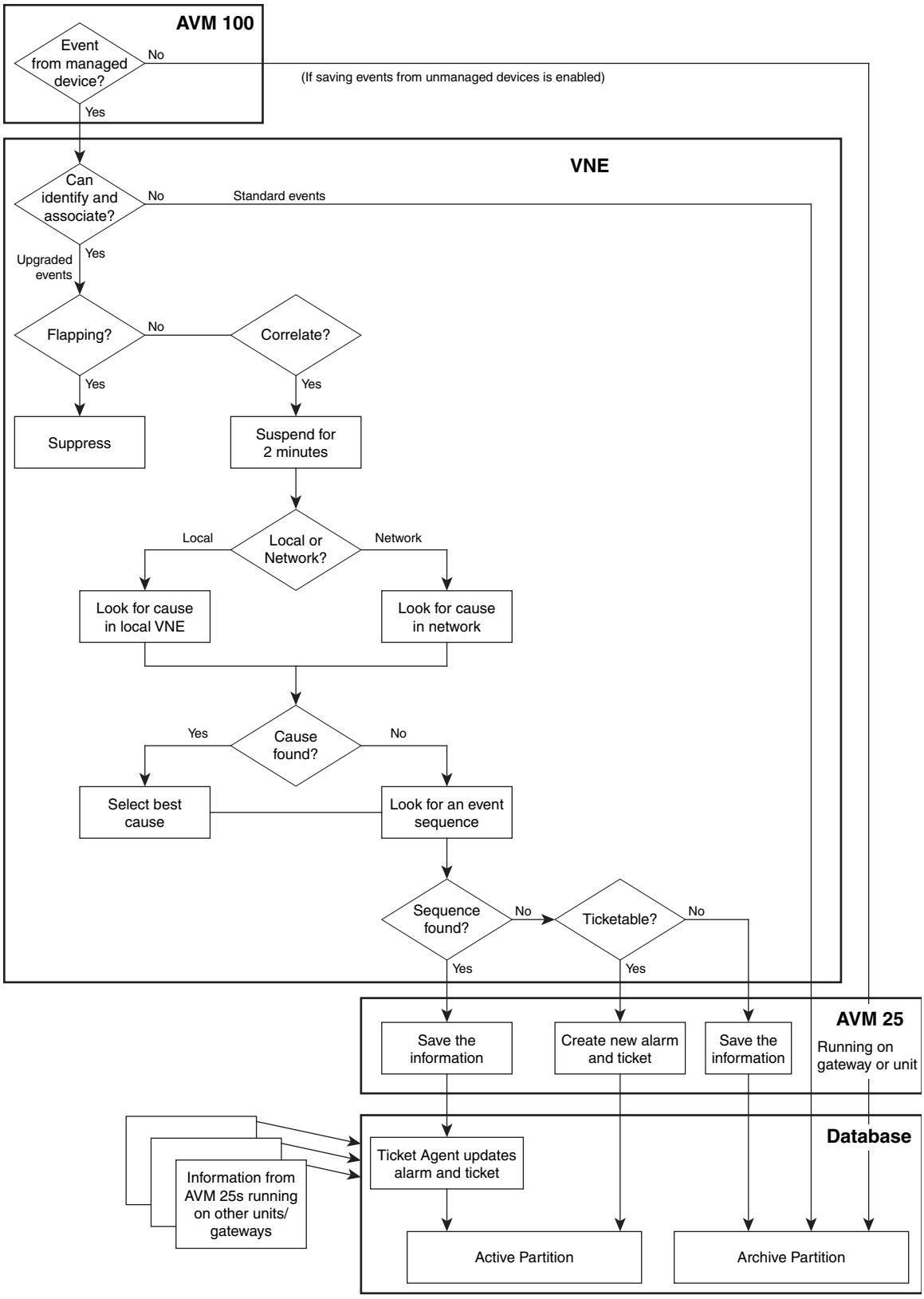
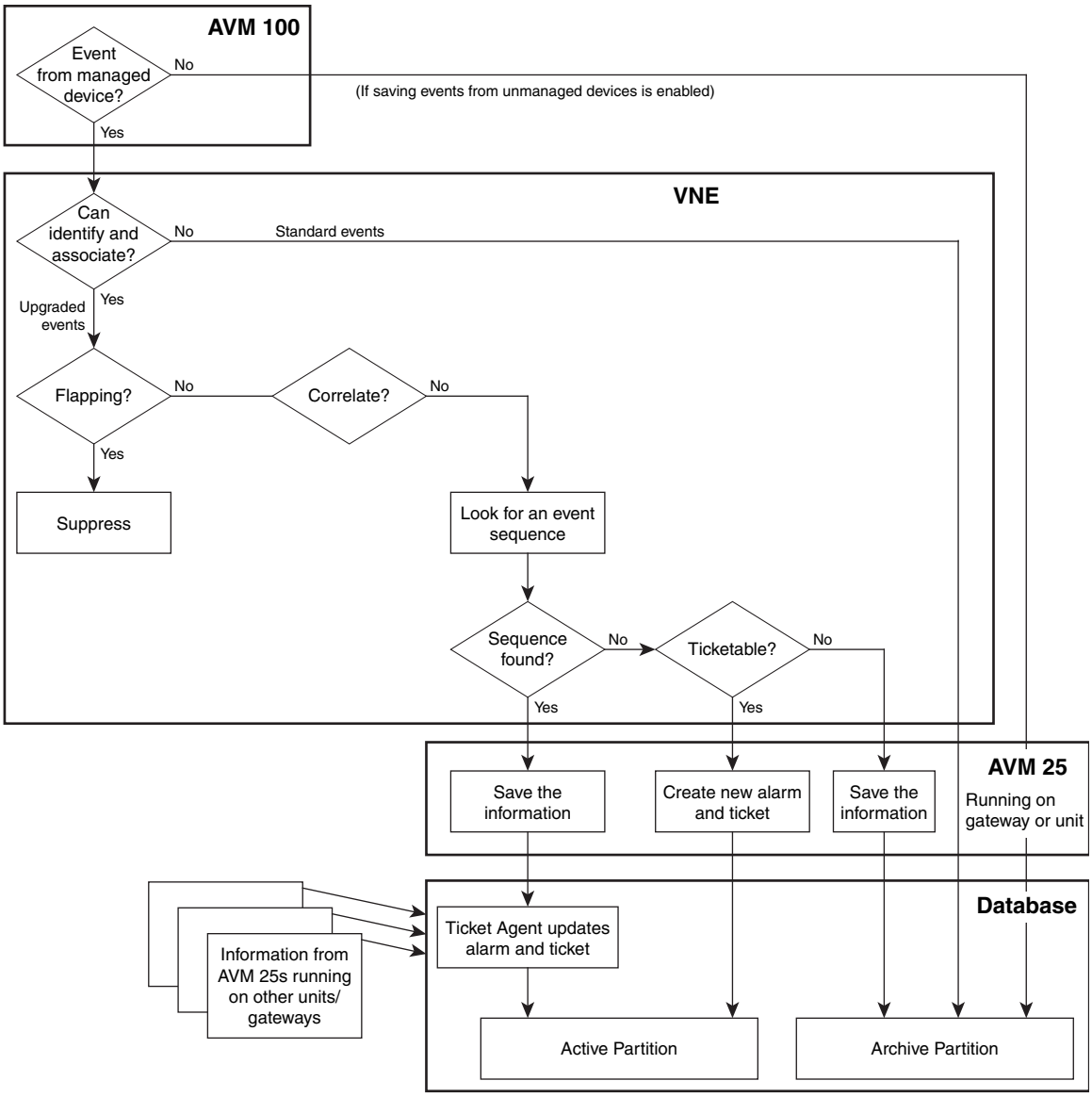


Figure 10-3 Event Processing—Events With No Correlation



Parse the Event To Identify It, Associate It With a Source, And Determine If It Is a Standard or Upgraded Event

The VNE begins the event identification process by extracting and parsing the following information from the raw event:

- Event Functionality Type—Trap, syslog, or Service event
- Event Type and Subtype—Identifier describing the fault, such as Link Down (the subtype provides further information)

- Event description strings—Content of the notification message content and a short description
- Event Severity—Event's importance, derived from the setting for the event's **severity** registry key):
  - Flagging—Indicates a fault: Critical (red), Major (orange), Minor (yellow), or Warning (sky blue)
  - Clearing—Indicates a fault that is resolved: Cleared (green)
  - Informational—Information only (dark blue)

If the VNE cannot extract adequate information, it performs some basic parsing and saves the event in the database. These events are considered *standard events*. No further processing is performed on standard events. They are immediately saved to the database and marked as archived.

If the VNE can extract the information listed above, the event is considered an *upgraded event* and the VNE begins event association (the next step).

Some traps and syslogs may expedite polling, which means that the VNE polls the device for more information without waiting for the device's usual polling cycle. This is the case for traps and syslogs that are likely indicators of a Service event, allowing quicker detection of any problem. (If a VNE is in the maintenance state, it does not expedite events but it will correlate events.)

The VNE continues parsing the event to identify the source location (for example, associating a port down to a device's physical interface).

In rare cases, the event source may not yet be in the VNE model, such as when a new module is installed. Prime Network may not have finished the process of polling the device interfaces and building (populating) the model. A retry mechanism minimizes this occurrence, but if it persists, the association logic falls back to the network element that is the source of the new event.

To check a Trap, Syslog, or Service event's default **severity** setting, see Checking An Event's Registry Settings, page 10-15.

Optimize the Expedite Polling

You can optimize the expedite polling whenever traps and syslogs are received.The optimization can be performed at 2 levels namely VNE level and System level. To enable the optimization polling, use the runRegtool command and then restart VNEs. When optimized-expedite is enabled, Prime Network waits for the specific time (delay time) that is based on the registration delay of the registration that is being expedited or window-length (default value is 20 seconds and configurable), whichever is greater, and then it will expedite.

In the span of delay time, if the same event occurs for multiple times then expedite occurs only once that is after the delay time of the last event received. Table 10-1 describes runRegTool commands for different levels.

Table 10-1 Enable Optimize the Expedite Polling

Level	Command
VNE	`runRegTool.sh -gs localhost set 127.0.0.1 "avm<ID>/agents/da/<VNE-name >/optimized-expedite/enabled " <true/false>`
System	`runRegTool.sh -gs localhost set 127.0.0.1 "site/agentdefaults/da/optim ized-expedite/enabled" <true/false>`

Note 'true' enables the expedite optimization and 'false' disables the expedite optimization.

You can also override the window-length of the time span by using the following runRegTool command and then restart the VNEs:

```
runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"agentdefaults/da/optimized-expedite/window-length" <time-value>
```

Note The time-value should be in milli seconds.

The inventory update for this flapping event or a duplicate event happens after the flapping or duplication stops plus the "delay time".

Examine Event for Flapping

Note Flapping detection is enabled for certain events and disabled for others (the **flapping** registry key is set to true or false). If an event is not configured for flapping, the VNE skips this step. To check a Trap or Syslog event's default **flapping** setting, see Checking An Event's Registry Settings, page 10-15.

After the event is associated with a source location, the VNE examines it to see if it is a flapping event. Flapping is a flood of consecutive event notifications related to the same alarm. It can occur when a fault causes repeated event notifications (for example, a cable with a loosely-fitting connector.)
Prime Network represents the new notifications as a single event with a flapping subtype.

The VNE identifies a sequence of events as flapping if:

- All events are of the same event type and are associated with the same source.
- The event occurs more than 5 times with less than 1 minute between events (default).

If the event is part of a flapping sequence, it is suppressed (not saved in the database or displayed in the clients), and the event's duplication count in the alarm is incremented.

During flapping, the fault management logic generates periodic event notifications with a Flapping Update subtype that also becomes part of the event sequence. After the fault stabilizes and the new event notification frequency returns to normal, the fault management logic terminates the alarms flapping mode by generating a final event notification (either Flapping Stopped Cleared or Flapping Stopped Non-cleared subtype), based on the last received new event notification.

Determine If Event Is Enabled for Correlation

The VNE examines the event to see if it is enabled for correlation—that is, whether Prime Network should attempt to find a root cause for the event. In this example, the event is called Event A:

Event Registry Key	If set to true, Prime Network will:	If set to false, Prime Network will:
correlation	Try to find Event A's root cause.	Not try to find Event A's root cause.
is-correlation-allowed	Allow other events to correlate to (be caused by) Event A.	Not allow other events to correlate to (be caused by) Event A.

An example of an event with a **correlate=false** registry setting is a Link Down Due To Oper Down event, where the event is its own cause. An example of an event with a **is-correlation-allowed=false** registry setting is a syslog that does not cause other events.

The VNE attempts to identify an event sequence (see Identify Event Sequences and Hierarchies, page 10-10). Because clearing events are associated to their predecessor, there is no need to correlate clearing events.

To check Trap, Syslog, or Service event's default **correlation** and **is-correlation allowed** settings, see Checking An Event's Registry Settings, page 10-15

Wait for New Incoming Events

The VNE suspends its correlation process for the event for 2 minutes so other related events can be detected. During this time, the VNE does not perform processing for the new event. (Although this means event updates to the Oracle database and the Vision client are delayed by 2 minutes, the events are immediately displayed in the Vision client **Network Events** tab.)

Check VNE for Correlated Events (Local and Network Correlation) and Identify Root Cause

When the 2-minute suspension period has expired, the VNE begins the process of *local correlation* or *network correlation*. This is controlled by a setting in the registry.

- If an event's **activate-flow** registry key is set to **true**, the VNE performs network (flow) correlation. Examples of events that use network correlation are LSP Down, MPLS TE Tunnel Down, and OSPF Neighbor State Change.
- If an event's **activate-flow** registry key is set to **false**, the VNE performs local (key) correlation.

To check a Trap, Syslog, or Service event's default **activate-flow** setting, see Checking An Event's Registry Settings, page 10-15.

Local (Key) Correlation

In local correlation (key correlation), the event source VNE is examined. In other words, correlation is performed on the local VNE only. Most trap and syslog events use the local correlation process.

The correlation logic examines the local VNE for possible causing events. These potential causing events must fall within the new event's examination time: The 7 minutes *before* the examination process begins, or the 2 minutes *after* the examination process finishes. After this 9 minute period has passed, the new event expires (meaning it cannot be considered a causing event for a new incoming event).

In addition, potential causing events must be configured to allow correlation, and must contain a correlation key that matches one of the new event's correlation keys.

Network (Flow) Correlation

In network correlation (flow correlation), the VNE examines events that occurred on different VNEs to see if they may be the cause of the local problem. Network correlation uses historic snapshots of the VNE model to search both the local and other VNEs for correlated events that meet the following criteria:

- Are configured to allow correlation.
- Arrived within the 7 minutes before the event and up to 2 minutes after the event.
- Exist on VNE components that appear on a flow path traversed according to the forwarding information of the new event.

The correlation is based on a flow that runs across the Prime Network model and topology. Network correlation is most successful if the event holds forwarding information, such as the IP address of a Border Gateway Protocol (BGP) neighbor, or a Frame Relay virtual connection. Network correlation is well suited for the following scenarios:

- The event represents a failure in a connection or service that spans multiple devices. For example, an MPLS traffic engineering (TE) Tunnel Down event tries to correlate to faults on the path that the tunnel traverses.
- Logically, the new event can result from events that occurred in other devices. For example, Prime Network tries to find the root cause for a Device Unreachable event in other devices by performing a flow to the management IP address.

Identifying the Root Cause

If the VNE finds more than one potential causing event, the root cause is determined using event *weight*. The heavier the weight, the more likely it will be chosen as the cause. This is controlled by the **weight** registry key. To check a Trap, Syslog, or Service event's default **weight** setting, see Checking An Event's Registry Settings, page 10-15.

Identify Event Sequences and Hierarchies

Next, the VNE attempts to identify event sequences (alarms). Events that have the same type and the same source are considered part of an event sequence.

VNEs use the predecessor/successor relationship to properly handle incoming duplicates without either discarding them or creating new tickets. When an event arrives, Prime Network searches its stored alarms for a possible predecessor. It identifies possible predecessors and finds the correct predecessor by matching it against the incoming alarm according to the following rules:

- The predecessor and successor both come from the same OID.
- The predecessor and successor are of the same alarm type.
- The predecessor is not archived.

The VNE forwards to AVM 25 the information it has gathered thus far (including uncorrelated events).

Save Information to Database, and Update or Open New Alarm and Ticket

AVM 25 saves all of the information it has received to the database. The actions that Prime Network takes depends on whether Prime Network could find the event's root cause and whether the event is ticketable (**is-ticketable** registry setting);

Root Cause/Ticketable	Prime Network does the following:
Root cause was found (the event was correlated to another event). Does not matter if event is ticketable or not.	AVM 25 saves the information in the database active partition. The database Ticket Agent updates the event and ticket information (severity, last modification time, event counter).
No root cause was found (the event was not correlated to another event), and the event is ticketable.	AVM 25 opens a new alarm and ticket and saves the information in the database active partition.
No root cause was found (the event was not correlated to another event), and the event is not ticketable.	AVM 25 saves the information in the database *archive* partition. This includes events that are enabled for correlation, but no root cause was found.

To check a Trap, Syslog, or Service event's default **is-ticketable** setting, see Checking An Event's Registry Settings, page 10-15.

How Prime Network Calculates and Reports Affected Parties (Impact Analysis)

Prime Network performs impact analysis for some Service events. This means Prime Network automatically calculates any service resources (pairs) that are affected by a ticket, or the specific events in a ticket. These service pairs are called *affected parties* and are listed in the ticket's Affected Parties tab.

Because tickets can be quite complex—for example, a ticket can include both discrete events and events that have been grouped into event sequences (alarms)—Prime Network provides several ways to view affected parties:

- To see the parties affected by a single event, check the *event's* Affected Parties tab.
- To see the parties affected by all of the events in an event sequence (alarm), check the *alarm's* Affected Parties tab.
- To see the parties affected by all event sequences (alarms) in a ticket, check the *ticket's* Affected Parties tab.

These topics explain the information that is displayed in the Affected Parties tab, and how Prime Network calculates the information:

- Impact Analysis and Affected Status: Potential, Real, Recovered, page 10-11
- Accumulating the Affected Parties in an Event Sequence (Alarms), page 10-12
- Accumulating the Affected Parties in the Correlation Tree, page 10-12

Impact Analysis and Affected Status: Potential, Real, Recovered

For each resource pair, the Affected Parties tab will displays an *affected status*, which indicates the degree of certainty that the pair will be impacted. Affected status can be one of the following:

- Potential—The service *might* be affected (for example, rerouting may prevent any problem).
- Real—The service *is* affected.
- Recovered—A service that was potentially affected has recovered. This only indicates that an alternate route was establish (not the service level quality).
- N/A—Not Applicable.

Note If any entries begin with the word *Misconfigured*, it means the flow has stopped unexpectedly between the source and destination points. An unexpected termination point can be a routing entity, bridge, or VC switching entity. Because the link does not terminate as expected, the link is not actually impacted. Check the configuration and status of the affected termination points to make sure there are no errors.

Using the example from How Prime Network Calculates and Reports Affected Parties (Impact Analysis), page 10-11, assume that X and Y are the OIDs of edge points in the network, and a service is running between them. Link (B) Down and BGP Neighbor Loss report on the pair X < > Y as affected:

Link (B) Down reports on X < > Y as *potentially* affected.

BGP Neighbor Loss reports on X < > Y as *real* affected.

The affected severity priorities are:

- Real—Priority 1
- Recovered—Priority 2
- Potential—Priority 3

Card Out reports on X < > Y as real, affected only once.This information is embedded in the ticket along with all of the correlated events. For a list of Service events for which Prime Network performs impact analysis, refer to the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

In some cases (such as the link-down scenario in MPLS networks), Prime Network updates the affected status of the same event sequence over time because it cannot determine the fault's effect on the network until the network has converged. For example, a Link Down alarm creates a series of affected severity updates over time. These updates are added to the previous updates in the system database. In this case, the system provides the following reports:

- The first report of a link down reports on X < > Y as potentially affected.
- Over time, the VNE identifies that this service is real affected or recovered, and generates an updated report.
- The Affected Parties tab of the Ticket Properties dialog box displays the latest severity as real affected.
- The Affected Parties Destination Properties dialog box displays both reported severities.

Accumulating the Affected Parties in an Event Sequence (Alarms)

Event sequences (alarms) can be nested. If two events form part of the same event sequence in a specific alarm, the recurring affected pairs are displayed only once in the Affected Parties tab. If different affected severities are reported for the same pair, the pair is marked with the severity that was reported by the *latest event*, according to the time stamp.

Accumulating the Affected Parties in the Correlation Tree

If two or more event sequences that are part of the same correlation tree report on the same affected pair of edge points but have different affected severities, the affected pairs are displayed only once in the Affected Parties tab. If different affected severities are reported for the same pair, the pair is marked with the *highest severity.*

Clearing, Archiving, and Purging and the Oracle Database

Note The Event Archive is no longer used as of Prime Network 4.1. For more information, see the *Cisco Prime Network 5.3 Administrator Guide*.

The Oracle database contains information about all ticket, standard, and upgraded events. Standard events are events from which a VNE cannot extract adequate information. As a result, the VNE only performs basic parsing and then archives the events in the database. Upgraded event are events that a VNE recognizes, parses, and attempts to correlate to other events (see Standard and Upgraded Events, page 10-4). If Prime Network is configured to handle notifications from unmanaged devices, those events are also stored in the Oracle database.

When a ticket is cleared, that means its root cause and all of its associated events have been cleared, and the problem no longer exists. A cleared ticket is still considered active because new events can still associate to it, which would cause the ticket to be reopened. Finally, if a ticket is unchanged for 1 hour, it is archived. Prime Network will not perform any more actions on it, and the ticket is considered inactive. Archived tickets and events are eventually purged from the database.

Viewing Archived Events in the Vision Client

In general, a limited number of archived events can be viewed from the Vision client— in the device inventory view under the **Network Events** tab, and in a map or list view under the **Latest Events** tab. You can see archived events in these cases:

- An event is associated with a ticket that was recently archived. Cleared, unchanged tickets are archived and removed from the **Tickets** tab after 1 hour. But the Vision client displays events from the past 6 hours, so the ticket's events may still be available.
- An event is a standard event, which means a VNE can only perform basic parsing of the event. Standard events are immediately archived. (Standard events only appear in the **Latest Events** tab if this has been enabled from the Administration client. Because there can be 3 times as many standard events as upgraded events, they are not shown by default to protect system performance.)
- An event is not ticketable and did not correlate to any existing events. These events are also archived.

These topics explain in more depth how ticket and event information is cleared, archived, and purged in Prime Network:

- How Events and Tickets are Cleared and Archived, page 10-13
- How Events and Tickets are Purged from the Oracle Database, page 10-15

How Events and Tickets are Cleared and Archived

When a ticket is cleared, that means its root cause and all of its associated events have cleared. Because a new event could still associate to the ticket (for example, if the root cause recurs), a cleared ticket is still considered active. When a ticket is archived, the ticket and its associated events are moved from an

active database partition to an archive database partition and the ticket is considered inactive. Archived tickets are generally removed from the clients but can be retrieved using the Events client Find in Database tool (see Finding Archived Tickets, Service Events, Syslogs, and Traps, page 12-12).

Clearing Fault Data

When an event, alarm, or ticket is *cleared*, it means it is no longer a problem. For a ticket, this means its root cause and all of its associated events have cleared. When an item is cleared, its severity icon changes to a green check mark, providing a visual indication that the problem has been addressed. (Acknowledging an event is different. Acknowledging indicates that someone is *aware* of the issue. Acknowledging does not change the severity icon; it just changes its Acknowledged value to **True**.) Because a new event could still associate to the ticket (for example, if the root cause recurs), a cleared ticket is still considered *active*.

Tickets can be manually cleared from the Vision client or the Events client by right-clicking the ticket and choosing **Clear**. The ticket description changes to **Cleared due to Force Clear** and all events are marked as acknowledged. The ticket's Audit tab will display the name of the user who cleared the ticket. Once a ticket is cleared, you can manually archive it and remove it from the client display by right-clicking a ticket and choosing **Remove**. To perform both operations at the same time, choose **Clear and Remove**. But keep the following in mind:

- The remove operation cannot be reversed. After you remove a ticket, it can only be viewed from the Events client using the Find in Database tool.
- If any of the ticket's associated events recur, Prime Network will open a *new* ticket instead of reopening the ticket your removed.

Tickets are also auto-cleared by Prime Network. Every 60 seconds, a special mechanism checks to see if uncleared tickets can be cleared. The mechanism looks for the following:

- If the ticket's events are cleared, or
- If the ticket's root cause is cleared, and its other events are configured for auto-clearing (the event's **auto-cleared** registry key is set to true or false). To check a Trap, Syslog, or Service event's default **auto-cleared** setting, see Checking An Event's Registry Settings, page 10-15.

If either of these cases is true and the ticket has not been modified in the last 4 minutes, Prime Network clears the ticket. When an event is auto-cleared, the Vision client displays an event description with **Auto Cleared** in the text—for example, **Auto Cleared - Link Down due to Admin Down**.

Administrators can also customize the following, which are disabled by default (refer to the *Cisco Prime Network 5.3 Administrator Guide*):

- Clear a ticket based on its severity and the number of days since it was last modified. (In this case, the ticket description would say **Cleared due to time expiration**.)
- Adjust when a cleared ticket is locked (no new events can associate to it).

Archiving Fault Data

A ticket is archived if no new events are associated to it for 1 hour (by default). When a ticket or event is *archived, it* means the ticket or event is no longer active. Archived data is moved to an archive partition in the Fault Database. Some data is immediately archived in the Fault Database—standard events, new alarms and upgraded events that are not ticketable, and (if enabled) events from unmanaged devices. (Standard and upgraded events are described in.)

An auto-archiving mechanism runs every 60 seconds and archives tickets if they are unchanged for 1 hour. This protects system performance and stability. Cleared and uncleared tickets may be also archived if their number or size could adversely affect system stability. This table describes the auto-archive criteria:

Auto-Archive Criteria	Ticket is archived if:
Age of ticket	Archive cleared ticket if no new events were associated to it in the past 1 hour.
Size of ticket	Archive a ticket that has more than 150 events associated with one of its alarms. (Prime Network also generates a System event 15 minutes before it archives the ticket.)
	Prime Network found more than 1500 large tickets. (Prime Network also generates a System event as it approaches this number.)
Total of tickets in Oracle database active partition	The total number of tickets exceeds 16,000.

How Events and Tickets are Purged from the Oracle Database

By default, Prime Network purges (deletes) event data from the Oracle database after 14 days—that is, 14 days from the event's creation time. This purge setting is configured in the Administration client. However, events that are associated with uncleared tickets are never purged, regardless of their age.

For more information on managing the Prime Network database, refer to the *Cisco Prime Network 5.3 Administrator Guide*.

Checking An Event's Registry Settings

The following documents list the default registry settings that control how Prime Network processes incoming events. All of these documents are available from Cisco.com:

Document on Cisco.com	Provides registry settings for:
Cisco Prime Network Supported Service Alarms	Notifications that are generated by Prime Network; normally you will find the information you need in this document.
Cisco Prime Network Supported Syslogs	Syslogs received from devices (IOS syslogs, ACE syslogs, Nexus syslogs, ASR syslogs, UCS syslogs, and so forth) and handled by Prime Network.
Cisco Prime Network Supported Traps	SNMPv1, v2, and v3 traps received from devices (ASR traps, IOS, traps, MIB 2 traps, Nexus traps, CPT traps, and so forth) and handled by Prime Network.

Managing Tickets with the Vision Client

Tickets represent attention-worthy fault scenarios that can consist of one event or a complete hierarchy of correlated events that all relate to the same fault. The Vision client provides extensive information on tickets and other network events of interest. These topics explain how to view and manage tickets and network events using the Vision client:

Ways You Can View Tickets and Events

Tickets represent attention-worthy fault scenarios. Specifically, tickets are business objects that are created by Prime Network. A ticket can consist of one event, an event sequence (alarm), or a hierarchy of events and alarms that all correlate to a single root cause. A ticket uses the name of its root cause event—for example, a ticket with a Card Out root cause event would be named a Card Out ticket. When Prime Network receives an event—external events like traps and syslogs, or generated events that Prime Network detects when it polls the network—it verifies whether the new event can be correlated to (caused by) any existing alarms. If it can be correlated to an existing alarm and ticket, the alarm and ticket information is updated. If not, and the event is *ticketable*, Prime Network creates a new ticket. A ticket's severity is equal to the highest-severity event associated with the root cause. A complete explanation of how Prime Network handles incoming events is provided in How Prime Network Correlates Incoming Events, page 10-4.

When you open a map, the tickets that apply to devices in the map are displayed at the bottom of the Vision client window under a Tickets tab. In addition, a Latest Events tab displays the most recent incoming events for devices in the map. For an example of this view, see Viewing Tickets and Latest Events for All Devices in a Map, page 11-3.

When you double-click a device in a map, the Vision client opens the device inventory view, and the view changes to display tickets only for the device. Next to the Tickets tab is a Network Events tab (for device Trap, Syslog, and Service events) and a Provisioning events tab (for changes made to the device).

For an example of this view, see Viewing Tickets and Events for a Specific Device, page 11-4.

To view a ticket, double-click it, and the Vision client provides extensive details about the ticket. A series of tabs provide the ticket history, root cause and events correlated to the root cause, notes attached to the ticket, number of devices affected by the ticket, and more.

The following table provides some basic ways you can view tickets (and events), depending on what you are looking for. You can only view a device's tickets if you have permission to view the device.

For:	To view:	Use this method in the Vision client:
All devices in a map	• Tickets • Syslogs and traps • Service events generated by Prime Network	Open a map or list view in the Vision client and check the tabs at the bottom of the window. See Viewing Tickets and Latest Events for All Devices in a Map, page 11-3.
	The above information filtered according to location, description, last modification time, and many other variables	Open a map in Vision client and, in the tickets table, create a filter. See The following table describes how regular and resynced events detail are displayed in Prime Network:, page 11-6.
A specific device and its components	• Tickets • Incoming traps and syslogs, and Service events generated by Prime Network (Network events) • Changes to the device (Provisioning events)	Double-click a device in Vision client and check the tabs at the bottom of the inventory window. See Viewing Tickets and Events for a Specific Device, page 11-4.

Once a ticket is cleared (its root cause and all of the associated events are cleared), if no new events are associated to it for 1 hour, it is archived, which means it is no longer considered active. Only a subset of archived events can be viewed from the Vision client as described in these topics:

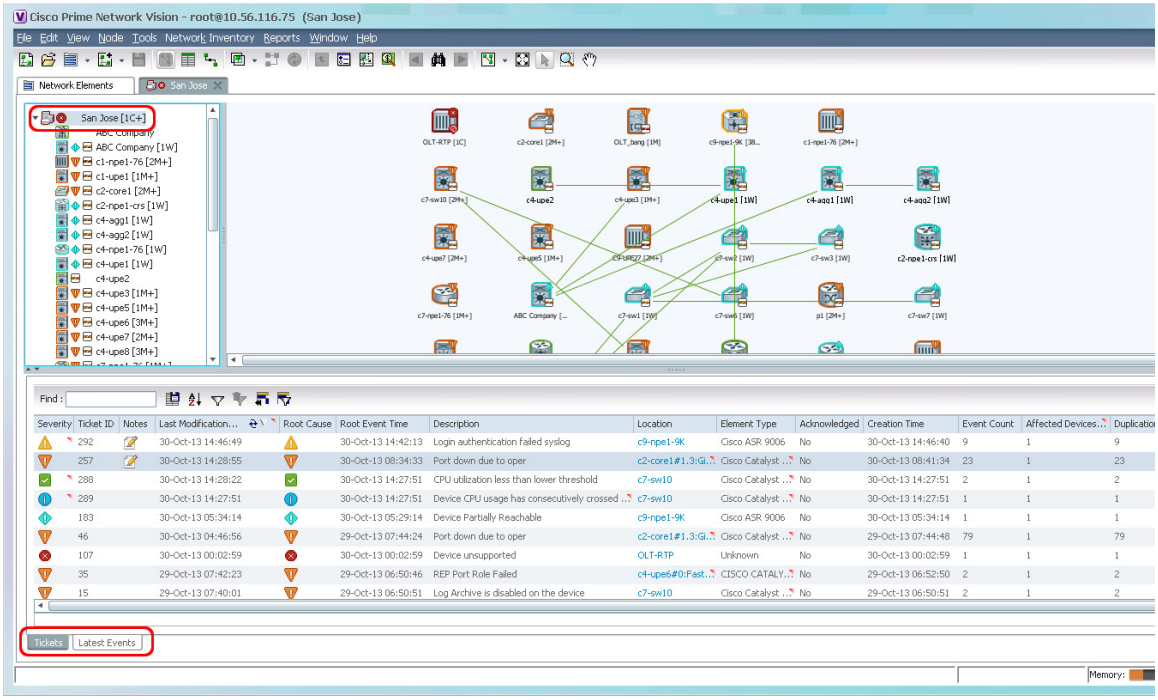
- Viewing Tickets and Latest Events for All Devices in a Map, page 11-3
- Viewing Tickets and Events for a Specific Device, page 11-4

For more information on archiving, see Clearing, Archiving, and Purging and the Oracle Database, page 10-13.

Viewing Tickets and Latest Events for All Devices in a Map

When you open a map, Prime Network displays a view similar to Figure 11-1. Note the Tickets tab and Latest Events tab at the bottom of the window (these tabs are also displayed in the List view).

Figure 11-1 Events Tabs for NEs in a Map



By default, the Vision client displays tickets and events from the past 6 hours. The **Tickets tab** lists the tickets for all devices in the map. You can find specific tickets using the robust ticket filter mechanism; see The following table describes how regular and resynced events detail are displayed in Prime Network:, page 11-6.

Tickets are listed according to their modification time, with the most recently modified ticket listed first. Events are stored in the database in Greenwich Mean Time (GMT) and are converted to match the time zone of the client location. The ticket table provides this information:

Ticket Pane Column	Description
Location	Provides a hyperlink to the entity that triggered the root-cause alarm. If you do not have permission to view the entity, the Vision client will not provide the hyperlink.
Root Event Time	When the *root-cause event* was detected.
Creation Time	When the *ticket* was created.
Open Alarms	Number of alarms that are associated with the ticket *that are not cleared*. For example, 3/4 means three of the ticket's four associated alarms are still not cleared.

Ticket Pane Column	Description
Acknowledged	Whether someone is aware of the ticket. • Yes—Ticket has been acknowledged. The user name of the person who acknowledged it is also listed. • No—The ticket has not been acknowledged, or it was acknowledged then de-acknowledged. • Modified—The ticket was acknowledged, but a new event has been associated to it. Double-click the ticket and check the User Audit tab for a history of who acknowledged/deacknowledge a ticket, and when these actions occurred.
Nature	Indicates whether the event is a type that can or cannot clear itself. • ADAC (Automatically Detected Automatically Cleared)—Clearing is automatically detected and performed by the system (for example, Link Down). • ADMC (Automatically Detected Manually Cleared)—Clearing requires manual intervention (for example, a fatal error).

The **Latest Events tab** displays upgraded events (traps, syslogs, and Service events generated by Prime Network) as they occur. If an event is associated with a ticket, a hyperlink to the ticket properties is provided. If enabled (from the Administration client), the tab may also include standard events, which are events for which Prime Network only performs basic parsing; they are not processed for correlation. The Detection Type column tells you what kind of event it is (trap, syslog, and so forth). For information on those kinds of events, see Viewing Network Events (Service, Trap, and Syslog Events), page 12-13.

Viewing Tickets and Events for a Specific Device

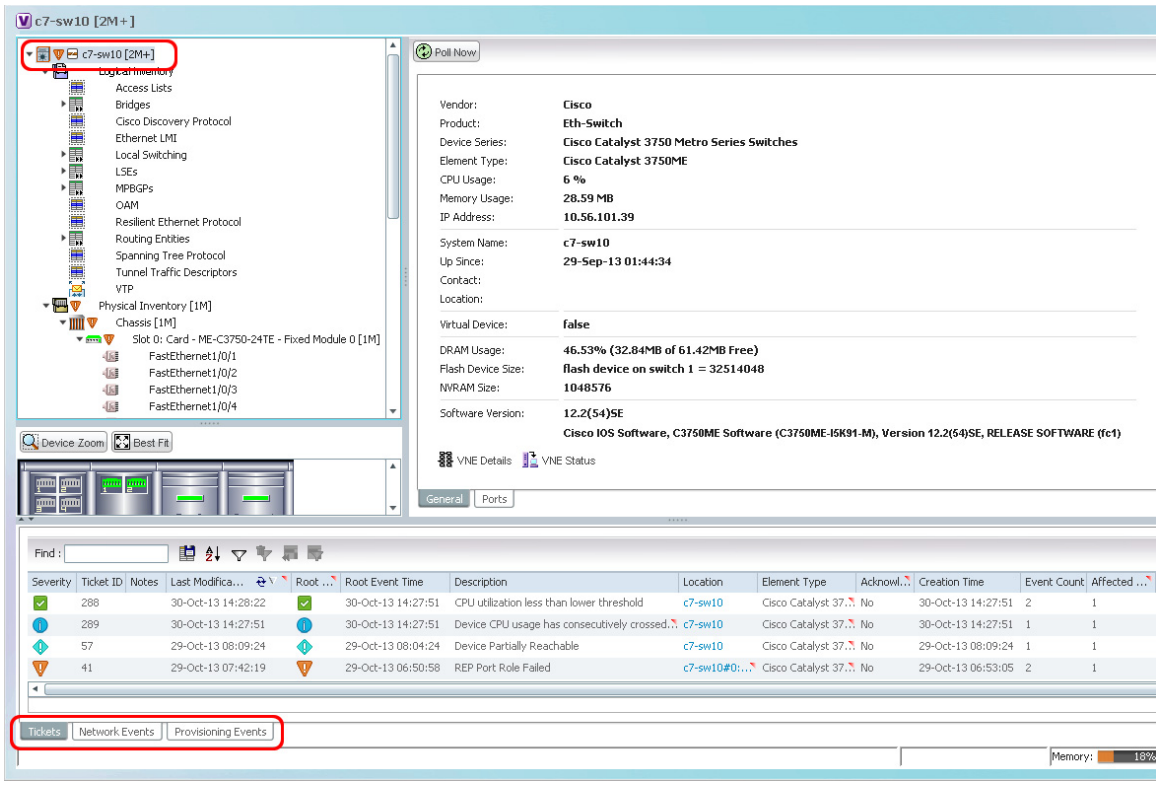
To display the tickets related to a device and its components, double-click a device to open its inventory window, as shown in Figure 11-2. As you expand the inventory, colors and badges indicate any problems.

The tickets listed at the bottom of the window changes as you choose items from the navigation tree. For example, to view all of the device's tickets, select the top-level device entry. If you select Physical Inventory, the Vision client only lists the tickets for any NEs in the physical inventory.

The Vision client also displays a Tickets, Network Events, and Provisioning Events tab at the bottom of the inventory window. Provisioning events reflect any device configuration operations or transactions (activation workflows) that have been executed on the device. The Network Events tab shows all traps, syslogs, and Service events for the device. For information on these other event types, see Viewing All Event Types in Prime Network, page 12-1.

In some cases, if an internal Prime Network component is stopped, or a device Prime Network is managing becomes unreachable, Prime Network will perform a resync when the component starts (or the device becomes reachable). The resync will capture the events that occurred during the down time and will include them in an Informational ticket. This behavior is currently supported for specific devices (for example, the Cisco ASR 5000 series running StarOS). For more information about the correlation and View/Access property for Resync alarm feature see, Viewing Resync Alarm Details in Prime Network, page 11-5

Figure 11-2 Vision Window Showing Device Inventory View and Events Tabs



The **Tickets** tab displays tickets for all devices in the map. To manage tickets, see Viewing Tickets and Events for a Specific Device, page 11-4. To create a ticket filter, see The following table describes how regular and resynced events detail are displayed in Prime Network:, page 11-6.

The **Network Events** tab displays incoming events that are being processed. Prime Network suspends processing for 2 minutes in order to allow correlation with incoming events. When correlation is finished, if an event is associated with a ticket, a hyperlink to the ticket properties is provided. This tab can also include standard events, which are events for which Prime Network only performs basic parsing; they are not processed for correlation. You can identify a standard event by its archive setting, which will be set to true.To create a filter for Network Events, see Permissions for Vision Client NE-Related Operations, page B-4. For information on the traps, syslogs, and other network events displayed in this tab, see Viewing Network Events (Service, Trap, and Syslog Events), page 12-13.

If a ticket is not cleared for Resync Alarms, then you can manually clear the tickets.

The **Provisioning Events** tab displays events related to configuration changes that were made to the device. If you want to create a Provisioning Events filter, see Permissions for Vision Client NE-Related Operations, page B-4. For more information on Provisioning events, see Provisioning Events (Device Configuration Results), page 12-17.

Viewing Resync Alarm Details in Prime Network

When full traps are created in Prime Network, events are processed as normal events. This allows the correlation information for all resynced events to be overwritten, and assigned to the resynced service alarm Ticket ID. The newly created events will have all the event properties similar to the original events rather than the standard event properties. You can view the Ticket ID in the **Traps** tab and the ticket history is displayed as a generic resync single event.

Note On the **Network Events** tab, you can still view details of standard events that are created.

The following table describes how events, traps, tickets details are displayed for Resync alarm tickets:

Table 11-1 Display Behavior

Property	Prior to Prime Network 4.3.1	Prime Network 4.3.1
		Handles both severity and description and shows traps in the regular **V2** tab.
Severity	Displayed as Info	The events will have the severity as defined in Prime Network parsing rules (can be overridden in VCB, and so on).
Type (used in ENS)	Displayed as Standard trap	Displays actual type as defined in Prime Network parsing rules.
Description	Displayed as Trap MIB OID or Translated Name	The trap description as parsed by Prime Network. For example, “Port down”.
Ticket	Displays one Info Resync ticket.	Displays one Info Resync ticket.
Correlation	None	Traps are assigned into the Resync ticket.
View/Access	View or Access Information in the **Standard** tab in the Prime Network Events client	View or access the Resync service alarm ticket information in the **V2 traps** tab in the Prime Network Events client.

The following table describes how regular and resynced events detail are displayed in Prime Network:

Table 11-2 Regular and Resynced Events Processing

Property	Regular Events	Resynced Events
Severity	The processed events specifies the severity as defined in Prime Network parsing rules.	The processed events specifies the same severity as defined in Prime Network parsing rules.
Type (used in ENS)	The type of event as defined in Prime Network parsing rules.	The actual type as defined in Prime Network parsing rules.
Description	The trap description as parsed by Prime Network. Example: Port down.	The trap description as parsed by Prime Network. Example: Port down.
Ticket	Generates ticket based on the incoming Network Event.	Displays Resync ticket with ‘Info’ severity additionally.

Table 11-2 Regular and Resynced Events Processing

Property	Regular Events	Resynced Events
Correlation	Network events like Snmp Link Down/Up and Port Down/Up are assigned to the corresponding service event Port down due to Admin Down.	Traps are assigned to the Resync ticket. **Note** You can view the Ticket Id information in the **Traps** tab. However, in the **History** tab, you can view the ticket history that includes a generic resync single event as before.
View/Access	View or Access information in the V2 traps tab in Prime Network Events client.	View or Access information in the V2 traps tab in Prime Network Events client.

Caution The command output displayed for the events that were lost or for events that were resynced should not be more than 5000 traps. As a result, if the VNE is down for a very long period of time, and the number of events is high, then there is a possibility that the events that were lost during the down time is not resynced and is completely lost.

Finding Tickets Using a Ticket Filter

A shown in Figure 11-3, the Vision client provides a robust filter tool to help you locate tickets using a variety of criteria. The filter locates tickets that meet the filter criteria. This procedure provides an overview of how to create a filter, and then remove it.

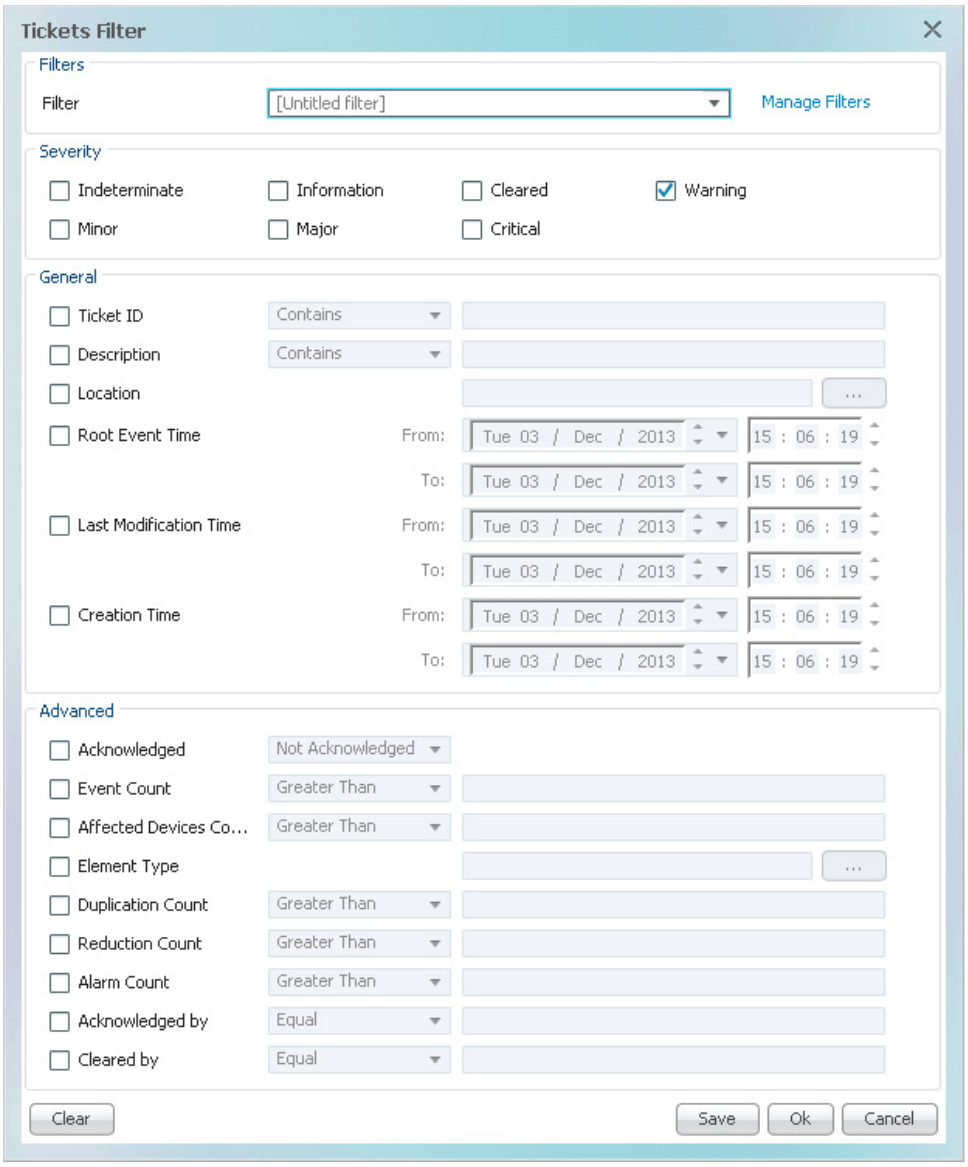
Note The Vision client has global options that can affect filter behavior, such was how many events should be listed in the display. These settings are described in Setting Up Your Events View, page 6-4.

Step 1 Launch the filter:

- To apply the filter against all devices in a map, open the map.
- To apply the filter against a specific device, double-click the device in a map to open its inventory window.

Step 2 Click **Tickets Filter** in the ticket pane toolbar to open the Tickets Filter dialog box.

Figure 11-3 Ticket Filter Dialog Box



Step 3 To create a new filter, make sure that [Untitled filter] is chosen from the Filter drop-down list. (For an example of this list populated with filters, see Creating and Saving Filters for Tickets and Events, page 12-6.)

a. Check the check box for each criterion to use for filtering.

b. As needed, choose the operator for the filter, such as Contains or Does Not Contain.

c. Supply the specific information to apply to the filter, such as the time, a string, or one or more IP addresses.

Step 4 If you want to save the filter so you can choose it from a drop-down list at another time, perform these steps:

Note A filter is saved for later use only if you click **Save**. To simply apply the filter to the current display (without saving the filter), skip this step.

a. Click **Save** and enter a name for the filter in the Save Filter dialog box. (Filters are listed alphabetically in the drop-down list; note that space is limited.)

b. If you want other Vision client users to be able to use your filter, click **Shared**.

c. Click **OK** in the Save Filter dialog box to save the filter for later use.

Step 5 Click **OK** in the Tickets Filter dialog box to apply the filter to the current display.The tickets are displayed in the ticket pane according to the defined criteria, and Filter Enabled is displayed below the tickets table (see Determining Whether a Filter Is On and Turning It Off, page 12-10). Once you apply a ticket filter, it remains applied until you manually clear it.

Note An enabled filter stays enabled as you move between tabs. But if you log out of the client without saving the filter, it is discarded.

Step 6 To remove the ticket filter:

a. Click **Tickets Filter** in the ticket pane toolbar.

b. Click **Clear** and **OK**.

For information on creating a filter for other events, see Creating and Saving Filters for Tickets and Events, page 12-6.

Interpreting the Badges and Colors of an NE

Color-coded icons reflect the severity of an NE's ticket. Because multiple events can be associated with a ticket, ticket severity is determined by the associated event with the highest severity. You can view the severity for all of a ticket's associated events in the ticket itself.

The following table shows the severity indicators.

Icon	Color	Severity	Notes
	Critical	Red	Critical, Major, Minor, and Warning events are considered *flagging events* because they may require attention
	Major	Orange	
	Minor	Yellow	
	Warning	Light Blue	

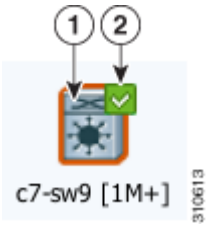
Icon	Color	Severity	Notes
	Cleared, Normal, or OK	Green	
	Information	Medium Blue	
	Indeterminate	Dark Blue	

These examples show how an NE with a Major ticket is displayed.

Value	Navigation Pane	Map	Ticket Pane (Bottom of Vision Window)
Element with ticket of Major severity			Severity Ticket ID 520030

Example 1: Interpreting NE Badges and Colors

Figure 11-4 NE Colors and Badges—Example 1



To find out:	Look at:	Figure 11-4 tells you:	Conclusion:
What is the most serious problem that has not been fixed yet?	(1) Icon *color*—Represents NE's most serious ticket that has *not been cleared* Icon—NE type	The NE has at least one major ticket that has not been cleared. NE is a Cisco MDS device.	This MDS device has a major ticket that has not been cleared yet.
What is the most serious problem that *no one* is aware of?	(2) Badge at top right of NE—Color represents NE's most serious ticket that is *unacknowledged* (no one is aware of it)	The most serious problem that no one is aware of has already been cleared.	The only unacknowledge ticket has already been cleared.

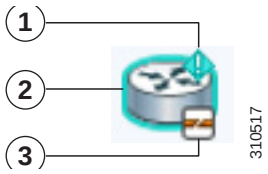
To summarize Figure 11-4:

- The MDS device has a major ticket that has not been cleared. The ticket is still a problem.
- The MDS device has other unacknowledged tickets, but those tickets have been cleared. (This also means the major ticket was already acknowledged.)

There is no more action you need to take.

Example 2: Interpreting NE Badges and Colors

Figure 11-5 NE Colors and Badges—Example 2



To find out:	Look at:	Figure 11-5 tells you:	Conclusion:
Is anyone working on the problem?	(**1**) Badge at top right of NE—Color represents NE's most serious ticket that is *unacknowledged* (no one is aware of it)	NE still has at least one *unacknowledged* ticket.	No one is aware that this Cisco 7600 router has a warning ticket.
Is there a problem now? If yes, how serious is it?	(**2**) Icon *color*—Represents NE's most serious ticket that has *not been cleared* Icon represents NE type	The NE still at least one *warning* ticket that has not been cleared. NE is a Cisco 7600 router.	This Cisco 7600 router has a warning ticket, and it is still a problem.
Is there a device communication problem?	(**3**) Badge at bottom right of NE—Represents device reachability and how fully the NE has been modeled	NE is in the "Device Partially Reachable" communication state.	Prime Network cannot fully communicate with the Cisco 7600 device.

To summarize Figure 11-5:

- The Cisco 7600 router has a warning ticket that has not been cleared.
- The Cisco 7600 router has an unacknowledged warning ticket.
- The Cisco 7600 router is only partially reachable.

This tells you that someone needs to acknowledge the warning ticket and start fixing it (see Letting Others Know You Are Working on the Ticket (Acknowledging a Ticket), page 11-12). It also tells you that the device reachability problem could be the cause of the warning ticket. For information on device reachability and communication states, see Troubleshooting Device Reachability and Performance Issues, page 11-19.

For troubleshooting steps, see Troubleshooting a Ticket, page 11-12.

For a complete list of all icons and badges, see Appendix A, "Icon Reference".

Letting Others Know You Are Working on the Ticket (Acknowledging a Ticket)

When you acknowledge a ticket, it signals to other Vision client users that someone else is working on the problem. The easiest way to check whether a ticket has been acknowledged is from the ticket table (at the bottom of the Vision client window).

If a new event is correlated to an acknowledged ticket, the ticket status changes to Modified and the ticket must be acknowledged again.

To acknowledge a ticket, right-click the ticket and choose **Acknowledge**. The change is indicated in all clients connected to the gateway, and the ticket's User Audit tab is updated to say you acknowledged the ticket.

If you acknowledge a ticket by mistake, you can undo it by right-clicking the ticket and choosing **Deacknowledge**.

Troubleshooting a Ticket

The following table provides a basic workflow for troubleshooting a ticket. Prime Network provides a variety of ways you can get more information about and troubleshoot a ticket. Some of these tools require special permissions; see Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1.

Note Tickets are stored in the database in Greenwich Mean Time (GMT) but are converted to match the time zone of the client location.

Step	Task	Described in:
Step 1	Get any troubleshooting help that is embedded in the ticket and basic information (when the event was detected, its location, and so forth).	Getting a Ticket's Troubleshooting Tips And Basic Information, page 11-13
Step 2	View a chronological listing of all of the events in a ticket.	Checking the History of a Ticket and Its Associated Events, page 11-14
Step 3	Identify which service resources (pairs) are affected by the ticket. (Only populated for events that calculate impact analysis.)	Viewing a Ticket's Affected Parties Tab (Resource Pairs), page 11-15
Step 4	Display a hierarchy of events with the root cause at the top.	Viewing a Ticket's Root Cause and Associated Events (Correlation Information), page 11-16
Step 5	Find out how many devices the ticket affected and view them on a map or in a list view.	Finding Out How Many Devices Are Affected by a Ticket, page 11-17
Step 6	View any ticket notes entered by other users, and find out who changed the ticket (acknowledge, clear, and so forth).	Viewing User-Entered Ticket Notes and Finding Out Who Changed the Ticket, page 11-17

Step	Task	Described in:
Step 7	Check the Prime Network documentation site. It contains event-specific documentation that can be helpful.	Checking the Online Documentation for Ticket Troubleshooting Information, page 11-18
Step 8	Check your deployment for built-in troubleshooting tools. If they are available, you should be able to launch them by right-clicking the NE and choosing **Commands**.	Using Built-in Troubleshooting Scripts and Tools, page 11-18
Step 9	If you have sufficient permissions to use the Events client, search in the database for similar tickets on the same NE.	Finding Archived Tickets, Service Events, Syslogs, and Traps, page 12-12
Step 10	For reachability issues, check the device connectivity information provided in the client. This includes: • Connectivity between the device and Prime Network. • Connectivity between Prime Network components. Also check the VNE investigation state, which represents the extent to which the device and its components were discovered and modeled.	Troubleshooting Device Reachability and Performance Issues, page 11-19
	For performance issues, check device memory and CPU.	Checking Device Memory and CPU Usage, page 11-24

Getting a Ticket's Troubleshooting Tips And Basic Information

A ticket's Details tab provides specific information about the probable cause, action to be taken, and clearing conditions for the ticket. This information is provided in the Details tab's Troubleshooting field.

The Details tab also provides a snapshot of the ticket—where the problem is, when the problem was first detected, when the ticket was created, and how many alarms (event sequences) are associated with the ticket, and so forth.

This table describes some of the fields in the Details tab that may not be self-explanatory.

Details Tab Field	Description
Location	Hyperlink to the entity that triggered the root-cause alarm (the hyperlink is provided only if you have permission to view the location).
Root Event Time	When the *root-cause event* was detected.
Creation Time	When the *ticket* was created.
Open Alarms	Number of uncleared alarms associated with the ticket. For example, 3/4 means three of the ticket's four alarms are still not cleared.

Details Tab Field	Description
Acknowledged	Whether someone is aware of the ticket, with the user name in parentheses. • No—The ticket has not been acknowledged, or it was acknowledged then de-acknowledged (in which case the User Audit tab will provide more details). • Modified—The ticket was acknowledged, but a new event has been associated to it. New events can be associated to a ticket until the ticket is archived. (The optional ticket locking mechanism can also affect whether new event can associate with a ticket; see How Events and Tickets are Purged from the Oracle Database, page 10-15.) Tickets are archived after they have remained clear for 1 hour (even if the ticket locking mechanism is used).
Nature	Whether or not the ticket will automatically clear. • ADAC (Automatically Detected Automatically Cleared)—Clearing is automatically detected and performed by the system (for example, Link Down). • ADMC (Automatically Detected Manually Cleared)—Clearing requires manual intervention (for example, a fatal error).

Checking the History of a Ticket and Its Associated Events

The History in chronological order, every instance of each event associated with a ticket. If the ticket has more than one alarm, you can also drill down to get the alarm details and history by double-clicking the alarm ID. The following table provides a subset of the information provided.

History Tab Field	Description
Detection Type	How the event was detected—Trap, Syslog, or Service event.
Alarm ID	Hyperlink to the alarm the event is associated with. Click the hyperlink to view the alarm details.
Causing Event ID	ID of the event that caused this instance of the alarm. If the same event recurs, it continues to have the same causing event.
Duplication Count	(For flapping) Total number of event duplications in the flapping alarm. (This number is always 1 for regular non-flapping events.) For example, this Link Down Flapping alarm would have a duplication count of 3: link down -> link up -> link down -> link up -> link down -> link up
Reduction Count	(For flapping) Total number of event instances in the flapping alarm. (This number is always 1 for regular non-flapping events.). Using the previous example, the Link Down Flapping alarm would have a reduction count of 6 (with 6 events listed in the History tab).

The Advanced tab provides the ticket's totals for the same information:

Advanced Tab Field	Description
Duplication Count	(For flapping) Sum of the duplication counts for all events and alarms in the ticket. For example, a ticket with the following Link Down Flapping alarms on three different network elements would have a duplication count of 9: NE 1: Link down -> link up -> link down -> link up -> link down -> link up NE 2: Link down -> link up -> link down -> link up -> link down -> link up NE 3: Link down -> link up -> link down -> link up -> link down -> link up
Reduction Count	(For flapping) Sum of the reduction counts for all events and alarms in the ticket. Using the previous example, the ticket would have a reduction count of 18.
Affected Devices	Total number of devices affected by the ticket. To view the devices in a map, see the procedure in Troubleshooting a Ticket, page 11-12.
Alarm Count	Total number of alarms associated with the ticket (includes the root alarm)

For more information about how Prime Network processes flapping events, see How Prime Network Correlates Incoming Events, page 10-4.

Viewing a Ticket's Affected Parties Tab (Resource Pairs)

The Affected Parties tab lists service resources (pairs) that are affected by an event, alarm, or ticket. This information is only populated for events that calculate impact analysis. If it is calculated for the event, the tab lists of all the endpoints that are affected in the Source area and a Destination areas. This includes business tags and IP addresses. If the NE is an IP interface, the subinterface IP address is displayed.

The tab also reports affected *status*, which represents the degree of certainty that the pair will be impacted. Affected Status can be one of the following:

- Potential—The service might be affected (for example, rerouting may prevent any problem).
- Real—The service is affected.
- Recovered—The service has recovered. This state applies only to entries that were marked previously as potentially affected. It indicates only the fact that there is an alternate route to the service, regardless of the service quality level.

If any entries begin with the word *Misconfigured*, it means the flow has stopped unexpectedly between the source and destination points. (An unexpected termination point can be a routing entity, bridge, or VC switching entity.) Because the link does not terminate as expected, the link is not actually impacted. Check the configuration and status of the affected termination points to make sure there are no errors.

As time progresses and more information is accumulated from the network, Prime Network updates the information to indicate which of the potentially affected parties are real or recovered.

For more information on impact analysis, including how Prime Network reports events and alarms that affect the same resource pairs, see How Prime Network Calculates and Reports Affected Parties (Impact Analysis), page 10-11.

Viewing a Ticket's Root Cause and Associated Events (Correlation Information)

The Correlation tab displays the root cause and all of the events it caused presented in a hierarchy with the ticket's root cause at the top. The ticket takes the name of the root cause. If you want to view the historical chronology for the events and alarms in a ticket, click the ticket's History tab.

From here you can also launch windows for individual alarms and events. Each alarm and event will have its own set of tabs: Details, History, Correlation, Affected Parties, and so forth.

Figure 11-6 shows a correlation tree for a Card Down ticket.

Figure 11-6 Correlation Tree for Card Out Ticket

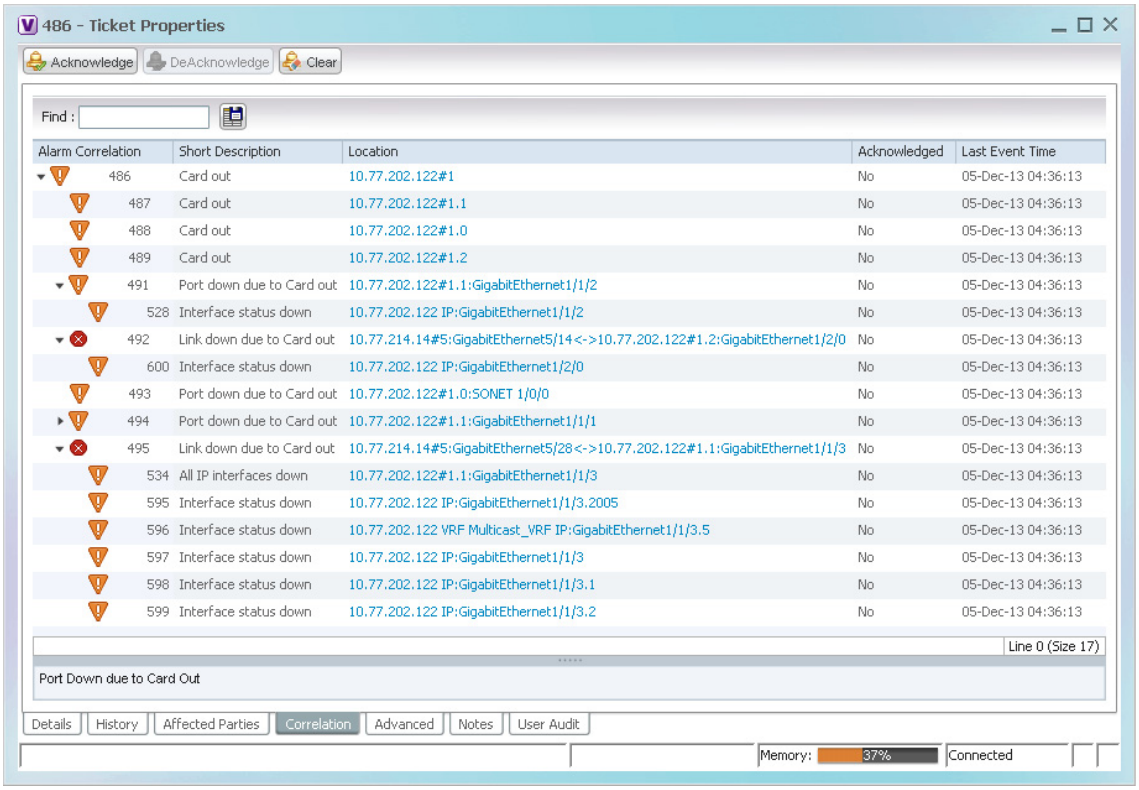
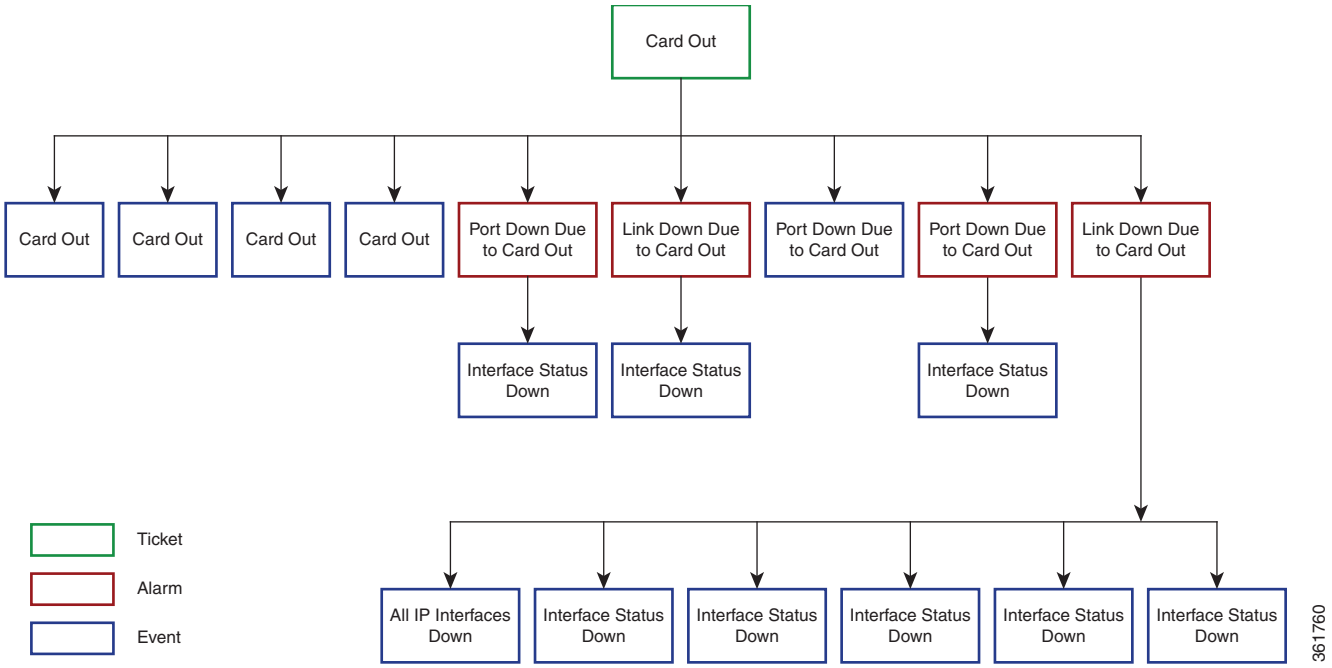


Figure 11-7 illustrates the same correlation tree. The Link Down Due to Card Out alarm is the cause of the Interface Status Down event, and the Card Out alarm is the cause of the Link Down Due to Card Out alarm. The Card Out alarm is also the root cause for all of the events; thus this is a *Card Out ticket*.

Figure 11-7 Alarms and Events in the Card Out Ticket



Finding Out How Many Devices Are Affected by a Ticket

When a fault occurs, Prime Network automatically calculates the affected devices and embeds this information in the ticket in the Advanced tab. If you want to get a quick visual representation of the affected NEs, use the Find Affected Elements feature, which is launched from the tickets table.

Right-click a ticket in the ticket pane and choose **Find Affected Elements**.

- If only one element is affected, it is highlighted in the Vision client map and navigation pane.
- If multiple devices are affected, they are highlighted in a list view.

Viewing User-Entered Ticket Notes and Finding Out Who Changed the Ticket

The Notes tab can contain any free text entered by other users. Once a user has added some notes, the notes cannot be deleted. If used correctly, it can contain helpful information that is not automatically collected by Prime Network.

The User Audit tab lists any users who have acknowledged, deacknowledged, cleared the ticket, or added notes to the ticket, and when the operation was performed. This is a good way to find out who may have already worked with this ticket.

Checking the Online Documentation for Ticket Troubleshooting Information

In addition to checking the Troubleshooting field in the Details tab, you may find additional information as follows:.

- Check the correlation examples in Event Correlation Examples, page C-1. Even if the event you are experiencing is not described, these examples can help you understand how faults are correlated.
- Check the event-specific reference documentation on Cisco.com:

Event Types	Document on Cisco.com
Notifications that are generated by Prime Network; normally you will find the information you need in this document.	*Cisco Prime Network Supported Service Alarms*
Syslogs received from devices (IOS syslogs, ACE syslogs, Nexus syslogs, ASR syslogs, UCS syslogs, and so forth) and handled by Prime Network.	*Cisco Prime Network Supported Syslogs*
SNMPv1, v2, and v3 traps received from devices (ASR traps, IOS, traps, MIB 2 traps, Nexus traps, CPT traps, and so forth) and handled by Prime Network.	*Cisco Prime Network Supported Traps*
Client login and user activities related to manage the system and the environment (user accounts, device scopes, logging in and out, password issues, unit changes. Events concerning Prime Network components; for example, reachability events, database-related events, system overload prevention steps, and so forth.	*Cisco Prime Network Supported Security and System Events*

Using Built-in Troubleshooting Scripts and Tools

The NE may have some built-in troubleshooting scripts that can be launched by right-clicking the NE and choosing **Commands**. Helpful scripts and commands may be available from that menu. These commands are documented throughout this guide under the technology or topology they apply to. For information on which devices and device software support the commands, see the *Addendum: Additional VNE Support for Cisco Prime Network 5.3*.

For example, to check device reachability, you can use the NE right-click Tools menu to run a ping or Telnet. These tools contact the device from the client machine.The devices that support the following commands are listed in the *Addendum: Additional VNE Support for Cisco Prime Network 5.3*. Whether you can run these commands depends on your permissions. See Permissions for Vision Client NE-Related Operations, page B-4.

If you are using Windows 7, you must enable the windows telnet client before you can use the Prime Network telnet option. The telnet communicates with the device using the telnet window from the client station.

To enable the windows telnet client:

Step 1 From the **Start** menu, choose **Control Panel** > **Turn Windows features on or off**.

The **Turn Windows features on or off** dialog box appears.

Step 2 Check the **Telnet Client** check box.

Step 3 Click **OK**.

The devices that support the following commands are listed in the *Addendum: Additional VNE Support for Cisco Prime Network 5.3*. Whether you can run these commands depends on your permissions. See Permissions for Vision Client NE-Related Operations, page B-4.

Command	Navigation	Description
OAM > **Trace Route from Device**	*NE* > **Commands**	Performs a traceroute to a destination address, showing how many hops were required and how long each hop takes.
OAM > **Ping** > **Destination From Device**		Pings a specified IP address to see if the IP address is accessible.
OAM > **Traceroute VRF**[1]	**Logical Inventory** > **VRFs** > *VRF* > **Commands**	Performs a traceroute from selected VRF to a destination address, showing how many hops were required and how long each hop takes.
OAM > **Ping VRF**[1]		Pings a specified VRF to see if the VRF is accessible.

1. Not applicable for Cisco UBR10K and RFGW10 cards.

Troubleshooting Device Reachability and Performance Issues

These topics provide some guidance for responding to problems with reachability and performance:

- Checking the Device State, page 11-19
- Checking Device Memory and CPU Usage, page 11-24

Checking the Device State

These topics explain how to troubleshoot reachability issues and identifying the source of a communication problem:

- Checking the VNE Management State Badge, page 11-19
- Checking the VNE Status to See If It Is an Internal Prime Network Problem, page 11-21
- Checking the Communication Between the VNE and the Device, page 11-23

Checking the VNE Management State Badge

Tickets can result from device connectivity issues, or if Prime Network cannot fully discovery a device for various reasons. These kinds of problems are signaled by a badge at the bottom right of the device icon. For example, a router that is partially reachable by the Vision client is displayed as illustrated in Figure 11-8.

Figure 11-8 Element with Device Partially Reachable Badge

This badge represents the *VNE management state.* In the Prime Network model, each device is represented by one *Virtual Network Element* (VNE) that contains a complete model of the device. VNEs are created by system administrators using the Administration client. After a VNE is created and started, Prime Network investigates the network element and automatically builds a live model of it including its physical and logical inventory, configuration, and status. As different VNEs build their model, a complete model of the network is created.

This VNE managements state badge represents:

- VNE communication state, which represents the status of connectivity between the device and Prime Network.

VNE investigation state, which represents the extent to which the device and its components were discovered. Table 11-3 lists the VNE communication states and their icons. The table describes the default behavior. (Administrators can change the settings that determine when a device is considered partially or fully unreachable; refer to the *Cisco Prime Network 5.3 Administrator Guide*.) In most cases, rectifying these problems will require the support of your system administrator.

Table 11-3 VNE Communication States

Badge	State Name	Description
	Device Unreachable	The connection between the VNE and the device is down because all of the protocols are down (though the device might be sending traps or syslogs).
	Device Partially Reachable	The VNE is not fully reachable because at least one protocol is not operational.
	VNE/Agent Unreachable	The VNE is not responding to the gateway. This can happen if a Prime Network component is overutilized, connections between Prime Network components were lost, or the VNE is not responding in a timely fashion. (A VNE in this state does not mean the device is down; it might still be processing network traffic.)
None	Connecting	The VNE is starting and the initial connection has not yet been made to the device. This is a momentary state.
None	Device Reachable	All element protocols are enabled and connected.
None	Tracking Disabled	The reachability detection process is not enabled for any of the protocols used by the VNE. The VNE will not perform reachability tests nor will Prime Network generate reachability-related events. (In some cases this is desirable; for example, tracking for Cloud VNEs should be disabled because Cloud VNEs represent unmanaged network segments.)
None	Agent Not Loaded	The VNE is not responding because it was stopped, or it was just created.

Table 11-4 lists the VNE investigation states, which describe the degree to which Prime Network could discover and model the device.

Table 11-4 VNE Investigation States

Badge	State Name	Description
	Unsupported	The device type is either not supported by Prime Network or is misconfigured.
	Partially Discovered	The VNE model is inconsistent with the device because a required device command failed, even after repeated retries. A common cause of this state is that the device contains an unsupported module.
	Currently Unsynchronized	The VNE model is inconsistent with the device; however, this is often recoverable, or may indicated a small inconsistency (such as a minor inventory component not being properly modeled). It could also be due to a more serious issue, such as an inability to reach a configured protocol on the device. Because this state can be due to a variety of reasons, check the VNE Status Details window for more information (see Checking the Communication Between the VNE and the Device, page 11-23).
	Discovering	The VNE is building the model of the device (the device type was found and is supported by Cisco Prime Network). A VNE remains in this state until all device commands are successfully executed at least once, or until there is a discovery timeout.
	Maintenance	VNE polling was suspended because it was manually moved to this state by an Administration client user. The VNE remains in this state until it is manually restarted. A VNE in the maintenance state has the following characteristics: • Does not poll the device or process traps and syslogs. • Maintains the status of any existing links. • Responds to VNE reachability requests. • Passively participates in correlation flow issues (but is not an initiator). The VNE is moved to the Stopped state if there are changes in other Prime Network components (for example, Prime Network is restarted).
	Shutting Down	The VNE has been stopped or deleted by the user, and the VNE is terminating its connection to the device.
None	Operational	The VNE has a stable model of the device. Modeling may not be fully complete, but there is enough information to monitor the device and make its data available to other applications, such as transactions (activation workflows). A VNE remains in this state unless it is stopped or moved to the maintenance state, or there are device errors.
None	Stopped	The VNE process has terminated (it will immediately move to Defined Not Started).
None	Initializing	The VNE is managed and support of its device type is being validated.
None	Defined Not Started	A new VNE was created (and is starting); or an existing VNE was stopped. A VNE remains in this state until it is started (or restarted).

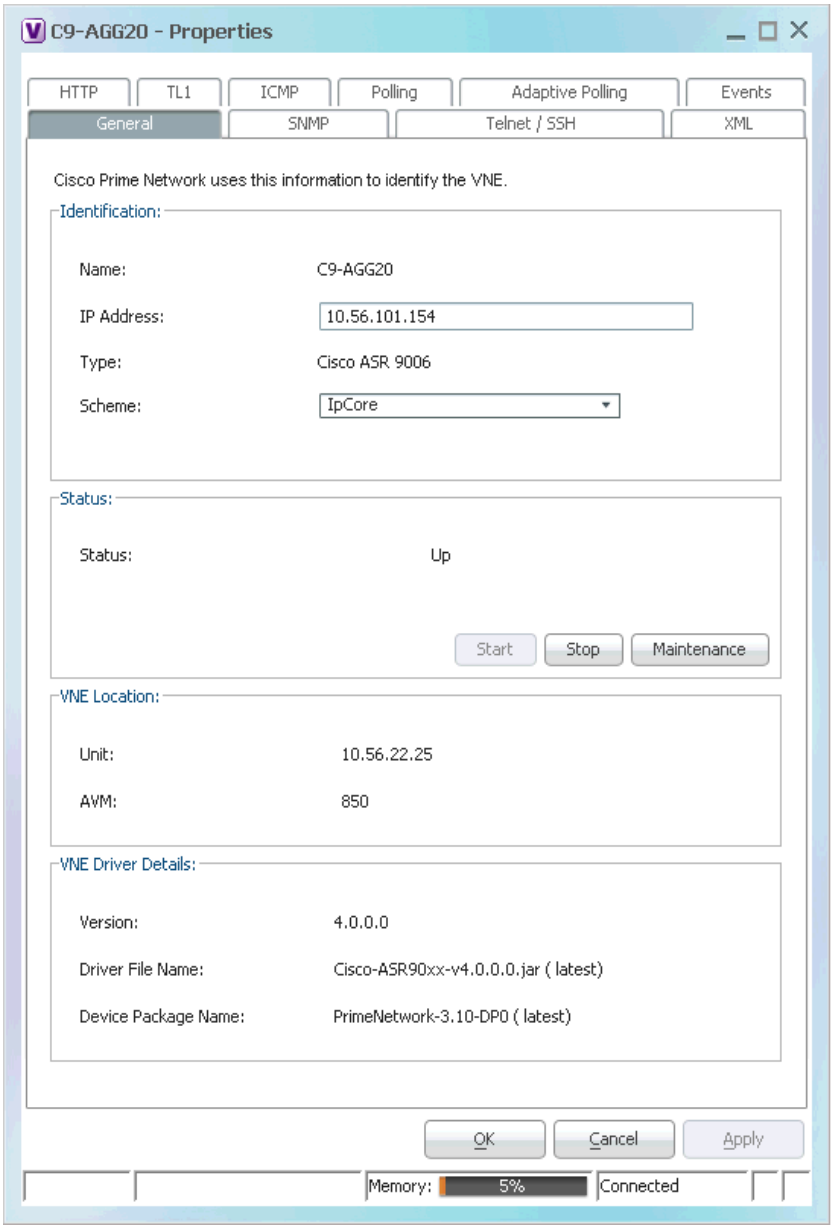
Checking the VNE Status to See If It Is an Internal Prime Network Problem

To check the status of the device's VNE, open the inventory window and click **VNE Status** in the properties pane. Figure 11-9 provides an example of a VNE properties window. This VNE is modeling a Cisco 3620 router.

Note VNE status is not the same as device status. A device may be fully reachable and operating even though a VNE status is Down, Unreachable, or Disconnected.

If the VNE status is down, the device may still be fully operational. This indicates a problem in Prime Network, not the device.

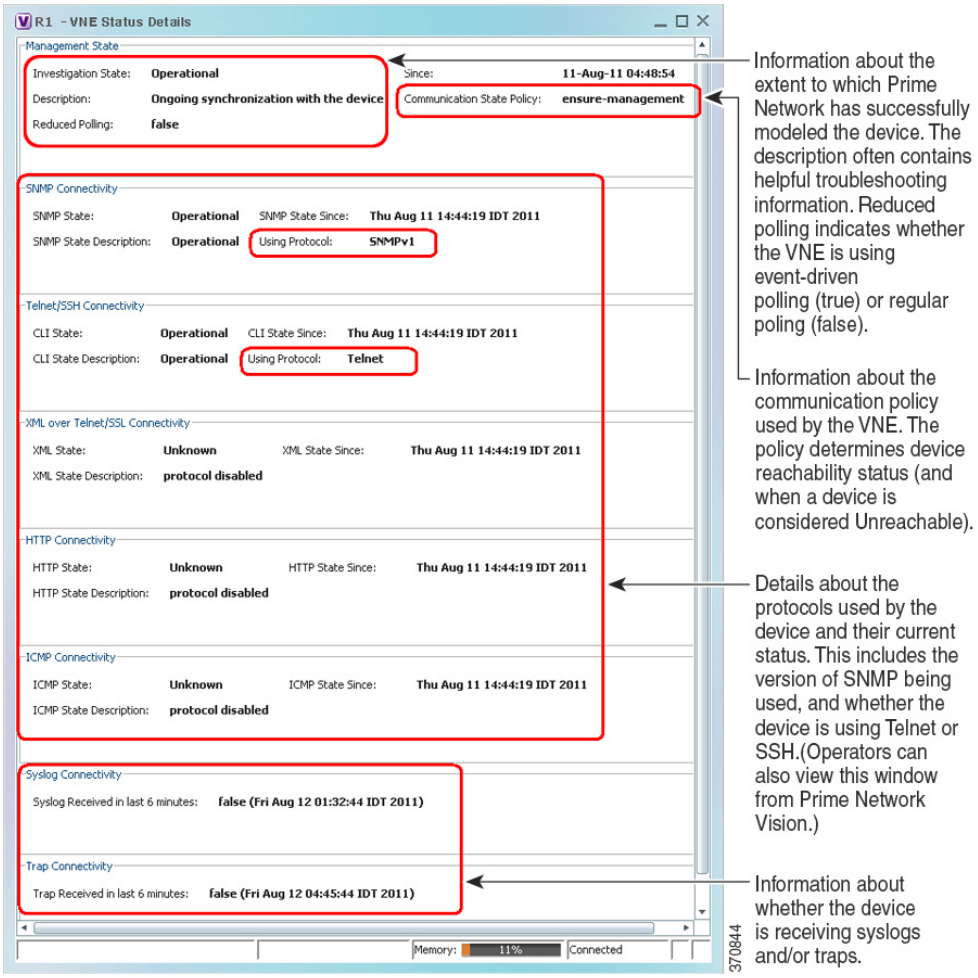
Figure 11-9 VNE Properties Window



Checking the Communication Between the VNE and the Device

To check the status of the communication between the device and the VNE that is modeling it, open the inventory window and click **VNE Details** in the properties pane. Figure 11-10 provides an example of a VNE Status Details window.

Figure 11-10 VNE Status Details Window



The VNE Status Details window provides this information about the VNE:

- Its management connectivity state, which has to do with how the VNE was configured
- The protocols the VNE is using to communicate with the device and the status of each
- Whether the device is generating syslogs or traps

In the Management State area, if the Reduced Polling field is true, this means updates are driven by incoming events. If the Investigation State is Currently Unsynchronized, perform a manual device poll by clicking **Poll Now** in the inventory window.

For more information on this topic, see the *Cisco Prime Network 5.3 Administrator Guide*.

Using Ping, Telnet, and Trace Route

To check device reachability, you can use the NE right-click Tools menu to run a ping or Telnet. These tools contact the device from the client machine. The devices that support these commands are listed in the *Addendum: Additional VNE Support for Cisco Prime Network 5.3*. Whether you can run these commands depends on your permissions. See Permissions for Vision Client NE-Related Operations, page B-4.

Note If you are using Windows 7, you must enable the windows telnet client before you can use the Prime Network telnet option. See Using Built-in Troubleshooting Scripts and Tools, page 11-18.

Command	Navigation	Description
OAM > Trace Route from Device	*NE* > **Commands**	Performs a traceroute to a destination address, showing how many hops were required and how long each hop takes.
OAM > Ping > Destination From Device		Pings a specified IP address to see if the IP address is accessible.
OAM > Traceroute VRF[1]	**Logical Inventory > VRFs >** *VRF* **> Commands**	Performs a traceroute from selected VRF to a destination address, showing how many hops were required and how long each hop takes.
OAM > Ping VRF[1]		Pings a specified VRF to see if the VRF is accessible.

1. Not applicable for Cisco UBR10K and RFGW10 cards.

Checking Device Memory and CPU Usage

The Vision client provides a tool that displays memory and CPU usage information for a device or network element, including its history. To open the CPU usage graph:

Step 1 Right-click a network element in the navigation tree and choose **Tools > CPU Usage**.

The CPU Usage dialog box displays the following information:

- CPU Usage—The CPU usage rate as a percentage.
- CPU Usage History—The CPU usage rate history is graphically displayed.
- Memory Usage—The memory usage rate as a percentage.
- Memory Usage History—The memory usage rate history is graphically displayed.

Step 2 If desired, click **Save to CSV File** to export the displayed data.

Step 3 Click the upper right corner to close the CPU Usage dialog box.

Prime Network also provides a web-based Monitoring tool for administrators that tracks how the gateway, units, and individual AVMs are operating—Java heap, dropped messages, CPU usage, and so forth. This information is provided in graphical form and you can use it to locate and diagnose problems. This tool is described in the *Cisco Prime Network 5.3 Administrator Guide*.

Letting Others Know What is Being Done to Fix a Ticket

Update the ticket notes to advise others of any actions you performed towards fixing the ticket. When you add a note, a note icon appears next to the ticket so that other users can see that a note is available. If a ticket affects several devices, you must have sufficient permissions on the device that contains the ticket's root alarm.

Note You cannot remove notes once you have added them to a ticket.

When you update a ticket's notes, earlier content is moved to the Previous Notes section (with the name of the user who added the note and the time it was added). If the user is an external user (for example, a Netcool user), the username will be displayed in the following format:

`Added by prime-networkUserName (as externalUserName)`

Letting Others Know the Problem Was Fixed (Clearing a Ticket)

Tickets can be cleared manually or automatically, as described in the following topics. Once a ticket is cleared, it remains active for 1 hour (default). If any incoming events are correlated to the ticket during this time, the ticket is reopened. If no incoming events are correlated to it, the ticket is removed from the display and archived. (The optional ticket locking mechanism can also affect whether new events can be associated with a ticket; see How Events and Tickets are Purged from the Oracle Database, page 10-15.) Once a ticket is archived, it is considered to be inactive. Archived tickets cannot be reopened; if an event recurs, a new ticket is opened

For more details about these actions, see Clearing, Archiving, and Purging and the Oracle Database, page 10-13.

Manually Clearing Tickets

You can manually clear a ticket by right-clicking it and choosing **Clear**. The ticket description changes to **Cleared due to Force Clear** and all events are marked as acknowledged. The ticket's User Audit tab will display the name of the user who cleared the ticket. Whether you can manually clear a ticket depends on your permissions; see Permissions for Business Tags and Business Elements (Vision and Events Clients), page B-10.

Note Do not choose **Clear and *Remove*** unless you are sure you want to archive the ticket. The remove operation cannot be reversed.

By default, cleared tickets are removed from the display (and archived) if no new events have associated to the tickets for 1 hour. This archive setting is not overriden by the ticket locking mechanism (which, if enabled, specifies at how many minutes a cleared ticket will be *locked*, meaning no new events can associate to it—for example, 20 minutes). Choosing **Clear and Remove** does override the 60-minute auto-archive setting. If you remove the ticket and one of its events recur, Prime Network will open a new ticket. See Removing a Ticket from the Vision Client Display (Archiving a Ticket), page 11-26.

Automatically Clearing Tickets

Every 60 seconds, a clearing mechanism checks all tickets to see if the ticket's root cause is cleared. If the root cause and all of the ticket's associated events are cleared, the mechanism clears (and acknowledges) the entire ticket.

Situations can occur in which a ticket's root cause is cleared, but one of the ticket's associated events is not cleared—for example, because of a missed syslog or a device reachability problem. For this reason, events have an **auto-cleared** registry setting. (The registry contains configuration settings for Prime Network components and features.) If the uncleared event's auto-cleared setting is true, the mechanism clears the event. Then the entire ticket can be cleared.

Prime Network has an additional ticket auto-clear mechanism, but it is disabled by default. It clears tickets depending on their severity. This mechanism is controlled from the Administration client and is described in the *Cisco Prime Network 5.3 Administrator Guide*.

Removing a Ticket from the Vision Client Display (Archiving a Ticket)

When a cleared ticket is removed from the Vision client, it is archived and is no longer considered active. Archiving means the ticket and all of its associated events are moved from an active partition to an archive partition in the database. Once a ticket is archived, if any of the archived ticket's associated events recur, a *new* ticket is opened. Archived tickets are never reopened. Details about the Prime Network archiving and purging mechanism are provided in Clearing, Archiving, and Purging and the Oracle Database, page 10-13.

Automatically Archiving Tickets

By default, cleared tickets are automatically removed from the Vision client when they have remained clear (no new events have associated to them) for 1 hour. Prime Network has an auto-archiving mechanism that runs every 60 seconds and archives any tickets that meet any of the following criteria.

Auto-Archive Based On:	Ticket is archived if:
Age of ticket	No new events were associated to the cleared ticket in the past 1 hour. **Note** Manually removing a ticket overrides this setting and archives the ticket immediately. However, the ticket locking mechanism does *not* override this setting. The locking mechanism specifies the interval at which new events can no longer associate to a cleared ticket (for example, if the ticket has been cleared for 20 minutes) The locking mechanism is disabled by default. See How Events and Tickets are Purged from the Oracle Database, page 10-15.
Size of ticket	The ticket has more than 150 events associated with one of its alarms. (Prime Network also generates a System event 15 minutes before it archives the ticket.)
	Prime Network found more than 1500 large tickets. (Prime Network also generates a System event as it approaches this number.)
Total of tickets in Oracle database active partition	The total number of tickets exceeds 16,000.

Manually Removing Tickets

Note Do not choose **Remove** unless you are sure you want to archive the ticket. The remove operation cannot be reversed.

You can manually remove cleared tickets from the display by right-clicking a ticket and choosing **Remove**. This removes the ticket and all of its associated events, and archives them. This operation overrides the 60-minute auto-archive setting described in the previous topic.

Remember that if you remove a ticket:

- The remove operation cannot be reversed.
- If any of the ticket's associated events recur, Prime Network will open a *new* ticket instead of updating the ticket your removed.

Whether you can manually remove a ticket depends on your permissions; see Permissions for Business Tags and Business Elements (Vision and Events Clients), page B-10.

Changing the Vision Client Behavior

All users can change their Vision client defaults. The defaults apply only to the client machines—that is, the machine from which you launch the Vision client. You can change the following ticket-related behavior:

- Enabling audio alerts and sounds
- Adjusting the ticket severity information that is displayed with an NE icon
- Controlling the age of tickets that are displayed in the Vision client

To change these settings, see Changing Vision Client Default Settings (Sound, Display, Events Age), page 4-15.

If Prime Network is being used with Prime Central, it is possible to disable ticket management operations from the Vision client. When these operations are disallowed, users can only manage the ticket lifecycle through BQL or the external OSS. For more information, see the discussion about setting up event monitoring in the *Cisco Prime Network 5.3 Administrator Guide*.

Viewing All Event Types in Prime Network

An event is a distinct incident that occurs at a specific point in time. Some events can indicate an error, failure, or exceptional condition in the network. How Prime Network responds to fault events is described in How Prime Network Correlates Incoming Events, page 10-4. Prime Network also provides extensive details about other events it receives—device configuration changes, activations, and changes in Prime Network components. Advanced users can use the Events client to view all event types—Traps, Syslogs, Tickets, Service events, Provisioning and Audit events, and System and Security events.

These topics explain how to view all of the event types in Prime Network:

Who Can Launch the Events Client

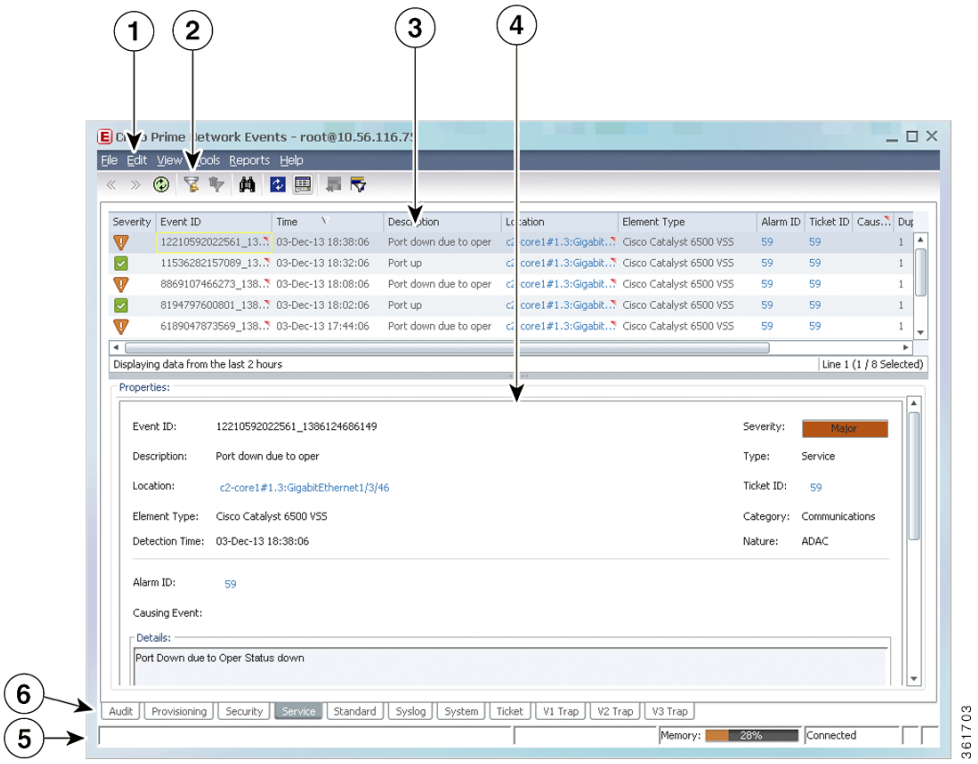
By default, only users with Administrator privileges can use the Events client. Users with lesser privileges can log into the Events client only if the required privileges have been reset from the Administration client. For more information, see the description of the Registry Controller in the *Cisco Prime Network 5.3 Administrator Guide*.

Events are sorted by date, with the newest item displayed first. *Tickets* are listed according to their modification time, with the most recently modified ticket listed first. Events are stored in the database in Greenwich Mean Time (GMT) but are converted to match the time zone of the client location.

By default, the Events client displays events from the past 2 hours. This is controlled from the Events client Options dialog. To protect performance, do not change the display time frame to more than 2 hours. For information on this and other client options, see Setting Up Your Events View, page 6-4.

Figure 12-1 provides an overview of the Events client window.

Figure 12-1 Events Client Window



1	Main menu—Create filters, export data, client options, online help, icon reference, and so forth.	**4**	Events details pane—Shows the selected ticket details at the bottom of the Vision client window (**View > Details**).
2	Toolbar—Tools for finding events in the database, creating and saving customized filters, and navigating through tables with multiple pages.	**5**	Status bar (shows commands sent to gateway, memory used by client, and gateway connection status)
3	Table panel—Lists events according to tab selected.	**6**	Event categories, one per tab

Ways You Can View Events

Events are displayed according to event categories, which are represented by tabs in the Events client. By default, the Events client displays events that occurred in the last 2 hours (or up to 50 events per table).

The following table provides some examples of the ways you can use the Events client.

To view:	Do this in the Events client:
Traps and syslogs received from devices, which Prime Network attempts to correlate (upgraded events)	Choose the Syslogs, V1 Trap, V2 Trap, and V3 Trap tabs.
Archived tickets and events that are no longer displayed in the clients	Use the **Find in Database** tool (specify a data range for best performance).
Events by the devices on which they occurred	Choose the event type tab, then create a filter that uses the Location, Severity, Description, or other criteria to fine-tune your search.
All events by the devices on which they occurred	Choose **File > Open All Tab** to display the All tab, then create a filter that uses the Location criteria.
Tickets by: • When the ticket's root cause was detected. • When the ticket was modified • When the ticket were created	Choose the **Tickets** tab, then create a filter that uses: • Root Event Time criteria • Modification Time criteria • Creation Time criteria
Tickets by how many alarms they contain	Choose the **Tickets** tab, then create a filter that uses the Alarm Count criteria.
Tickets that were cleared or acknowledged by specific users	Choose the **Tickets** tab, then create a filter that uses the Acknowledged By and Cleared By criteria.
Tickets that have or have not been acknowledged	Choose the **Tickets** tab, then create a filter that uses the Acknowledged criteria.
Network events by: • How many events are still a problem (uncleared). • How many times the event has occurred (Many criteria choices are supported.)	Choose the events tab, then create a filter that uses: • Duplication Count criteria • Reduction Count criteria
Tickets by how many devices they affect	Choose the Tickets tab, then create a filter that uses the Affected Devices Count criteria.
Traps and syslogs for which Prime Network can only perform basic parsing (they are not processed for correlation)	Choose the Standard tab.
CCM configuration commands executed on gateway	Choose the Audit tab.
Configurations performed on devices	Choose the Provisioning tab.
Prime Network client login and user activities	Choose the Security tab.
Events that occurred on Prime Network components	Choose the System tab.

Event Types and Categories

Each event tab displays basic information, including severity, event ID, time, and description. In addition, most event tabs show the Location parameter, which indicates the entity that triggered the event, with a hyperlink to the entity's properties. The following table describes the event categories in the Events client.

You can also open the optional All tab that displays a flat list of all events and tickets by choosing **File > Open All Tab**).

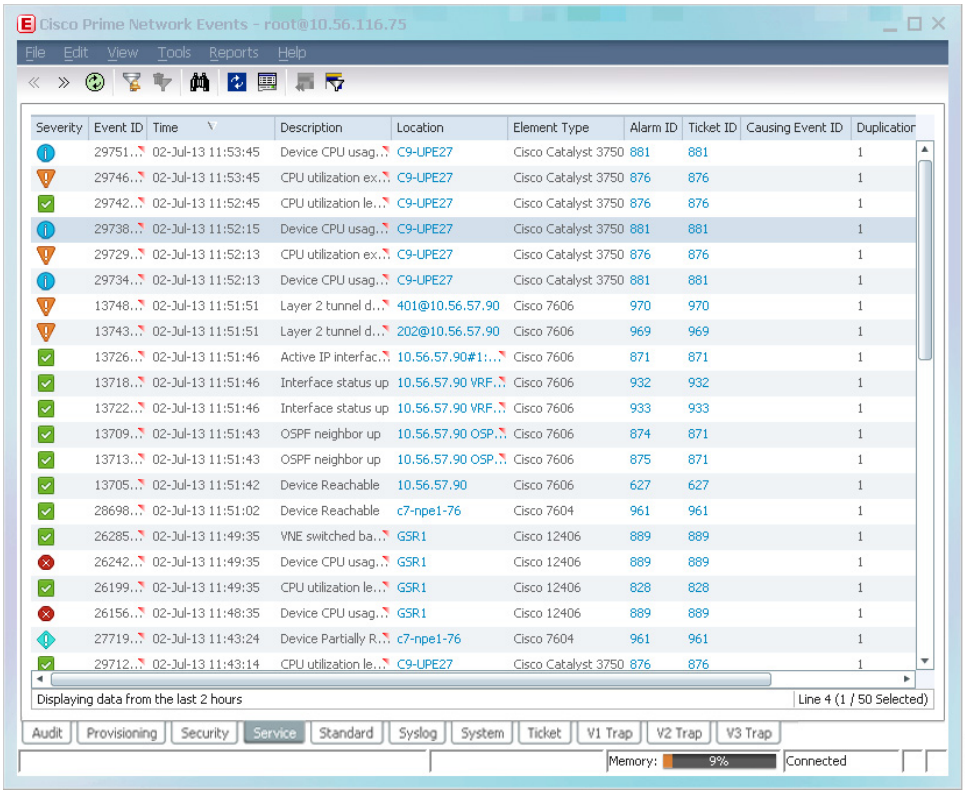
Table 12-1 Event Categories in Events client

General Event Category	Events Client Tab	Contains events related to:	For more information:
Tickets	Ticket	An attention-worthy root cause alarm handled by Prime Network.	Viewing Tickets, page 12-17
Network Events	Service	Events that are generated by Prime Network.	Viewing Network Events (Service, Trap, and Syslog Events), page 12-13
	Syslog	Syslogs received from devices (IOS syslogs, ACE syslogs, Nexus syslogs, ASR syslogs, UCS syslogs, and so forth) and handled by Prime Network. These syslogs are parsed and Prime Network attempts to correlate them.	
	V1 Trap	SNMPv1, v2, and v3 traps received from devices (ASR traps, IOS, traps, MIB 2 traps, Nexus traps, CPT traps, and so forth). These traps are parsed and Prime Network attempts to correlate them.	
	V2 Trap		
	V3 Trap		
	Standard	Traps and syslogs that Prime Network cannot match with any of the rules that define events of interest; they are not processed for correlation.	Viewing Tickets, page 12-17
Non-Network Events	Audit	Configuration commands that are executed on the Prime Network gateway (NE right-click commands, CCM and Compliance Audit operations, and so forth).	Viewing Non-Network Events (Audit, Provisioning, System and Security Events), page 12-17
	Provisioning	Configuration and provisioning activities, including CCM, Command Manager, and Transaction Manager.	
	Security	Client login and user activities related to manage the system and the environment (user accounts, device scopes, logging in and out, password issues, unit changes.	
	System	Prime Network and its components (for example, reachability events, database-related events, system overload prevention steps, and so forth.	

Interpreting Event Severity Indicators

Prime Network clients use the same indicators and colors to signal events and tickets in the network. The following example shows a Service events table in the Events client. The colors and badges in the Severity column indicate the seriousness of the event.

Figure 12-2 Events Client with Event Severity Indicators



The following table shows the event severity indicators. The same colors and indicators are used for all event types—System, Audit, Tickets, Syslogs, and so forth.

Icon	Color	Severity	Notes
	Critical	Red	Critical, Major, Minor, and Warning events are considered *flagging events* because they may require attention
	Major	Orange	
	Minor	Yellow	
	Warning	Light Blue	
	Cleared, Normal, or OK	Green	
	Information	Medium Blue	
	Indeterminate	Dark Blue	

Creating and Saving Filters for Tickets and Events

These topics explain how to create and manage filters:

- Creating a New Filter and Saving It, page 12-7
- Determining Whether a Filter Is On and Turning It Off, page 12-10
- Modifying Saved Filters and Managing the Filter List, page 12-12

Both the Events client and Vision client provide a robust framework for creating filters that can be applied against ticket and event data. Filters are applied to the current display (the defaults are 6 hours for the Vision client and 2 hours for the Events client), but you can specify a different date range using the filter settings.

Filters apply *only to their event category*. In other words, if you create a filter for Service events, it cannot be used for Ticket events. In addition, filters apply *only to their client*. Filters created in the Vision client cannot be used in the Events client, and vice versa.

When you apply a filter to a display and then navigate to another part of the client, the filter remains enabled when you return to the original display (by default). Unless you save a filter, it is discarded when you log out of the client.

You can also save your filters for later use and, if desired, make them public so that other client users can apply them. If a filter is not shared, only the creator can use it. Shared filters can be accessed by all client users, regardless of their user privileges, but can only be edited or deleted by the filter creator, or users that have the same (or higher) user privileges as the filter creator. If users with lesser privileges want to create a similar filter, then can save a copy of the filter under a different name.

Note The Events client global options that can affect filter behavior, such whether filtered content should be saved when you move between tabs. These settings are described in Setting Up Your Events View, page 6-4.

These topics explain how to create new and change existing filters:

- Creating a New Filter and Saving It, page 12-7
- Modifying Saved Filters and Managing the Filter List, page 12-12

Creating a New Filter and Saving It

Use this procedure to create filters in the Vision client and Events client.

Before You Begin

When you consider a filter name, remember that filters are listed alphabetically. Space is limited, so use concise names.

Step 1 Make sure you are working from the desired filter category. The filters you can create and the devices you can choose depend on your user account permissions.)

Client	To find:	On:	...Start from:
Vision client	Tickets	All or specified devices	Tickets tab from map
		Only a specific device	Tickets tab from inventory window
	Upgraded trap events, Syslog events, and Service events (upgraded events are events Prime Network recognizes and attempts to correlate)	All or a group of devices	Latest Events tab from map
		Only a specific device	Network Events tab from inventory window
	Device configuration changes	For a specific device	Provisioning tab from inventory window

Client	To find:	On:	...Start from:
Events client	Events related to the Prime Network system	N/A	System tab
	Events related to Prime Network security		Security tab
	Active and archived events that are generated by Prime Network	All or specified devices	Service tab
	All syslogs and traps handled by Prime Network	All or specified devices	Syslog tab Traps tabs
	Trap events and Syslog events that Prime Network cannot match with any of the rules that define events of interest (no further processing is performed)	All or specified devices	Standard tab
	Device configuration changes on managed devices	All or specified devices	Provisioning tab
	Users that executed device configuration changes on managed devices	All devices	Audit tab

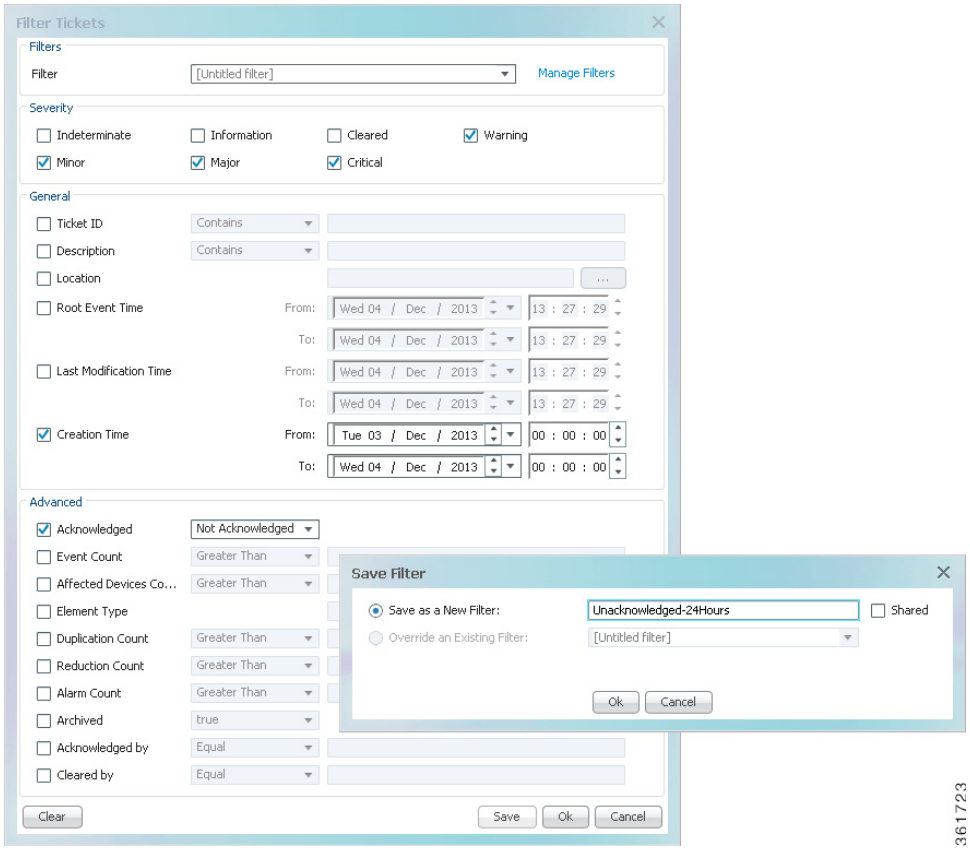
Step 2 Open the filter dialog.

	Launch by:	
Filter Name and Description	**Choosing**	**Clicking**
Filter—Finds events in the display that match the filter criteria. Events client only: You can also find archived network events.	**Edit > Filter**	
Find in Database—Finds events in the database that match the criteria. You can also find archived events. **Note** This choice is only available on the Events client. Specify a date range for best performance.	**Edit > Find**	

Step 3 Configure your filter. Links to topics that describe the filter options are provided after this procedure.

In this example, a ticket filter is created to find unacknowledged Critical, Major, Minor, and Warning tickets created in a 24-hour period. This particular filter is launched from the Events client (the Vision client does not support the Archive criteria for tickets).

Figure 12-3 Ticket Filter Example



Step 4 Click **Save** and do the following in the Save Filter dialog box:

a. Enter a name (for example, **Unacknowledged-24hours**).

b. Check **Share** to make the filter available to other users *of the same client* (filters created in the Vision client cannot be used from the Events client). If you share a filter, users with the same or higher privileges will be permitted to edit your filter.

c. Click **OK** to close the Save Filter dialog box.

d. In the Filter or Find dialog box, click **OK** to apply your filter to the current display. The filter name is displayed under the table; for example, **Filter Enabled: Unacknowledged-24hours**.

If you move to another tab in the client, the filter is still enabled when you return to the Tickets tab. (You can change this and other filter behaviors by choosing **Tools > Options**. See Setting Up Your Events View, page 6-4.)

Step 5 To clear a filter, choose **Edit > Clear Filter** (or click).

When log out and log back into the client, your filter will be available from the Filter drop-down list, as shown in the following figure.

Figure 12-4 Filter Drop-Down List

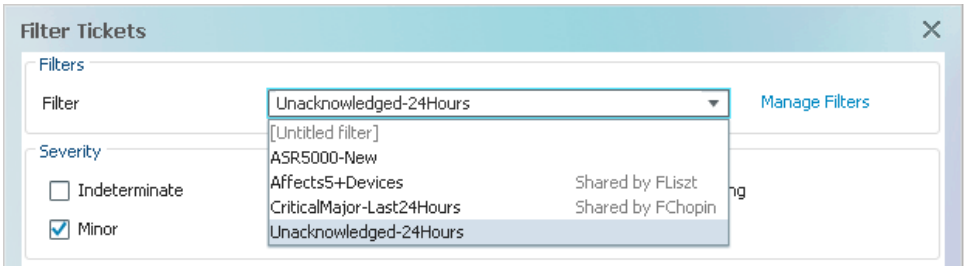


Figure 12-4 shows the new filter along with these pre-existing filters:

- ASR500-new (created by the current user, JSBach).
- Affects5+Devices, a shared filter created by user FLiszt.
- CriticalMajor-Last24Hours, a shared filter created by FChopin.

Any filters created by other users but *not* shared are not displayed. Only the filter creators can see those filters.

For information on the different filter criteria you can use, see:

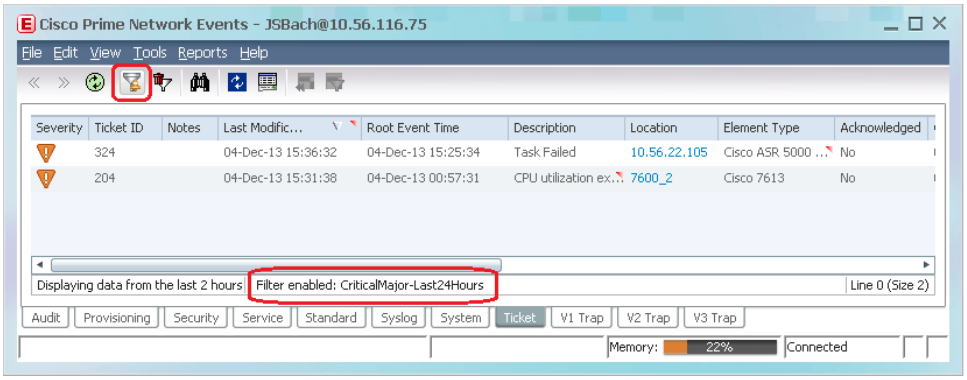
- Viewing Network Events (Service, Trap, and Syslog Events), page 12-13
- Viewing Tickets, page 12-17
- Viewing Non-Network Events (Audit, Provisioning, System and Security Events), page 12-17
- Viewing Standard Traps and Syslogs Not Recognized by Prime Network, page 12-19

Determining Whether a Filter Is On and Turning It Off

If the  icon appears above a table, a filter is enabled. To turn the filter off, click the icon or choose **Edit > Clear Filter** or **Edit > Clear Find**.

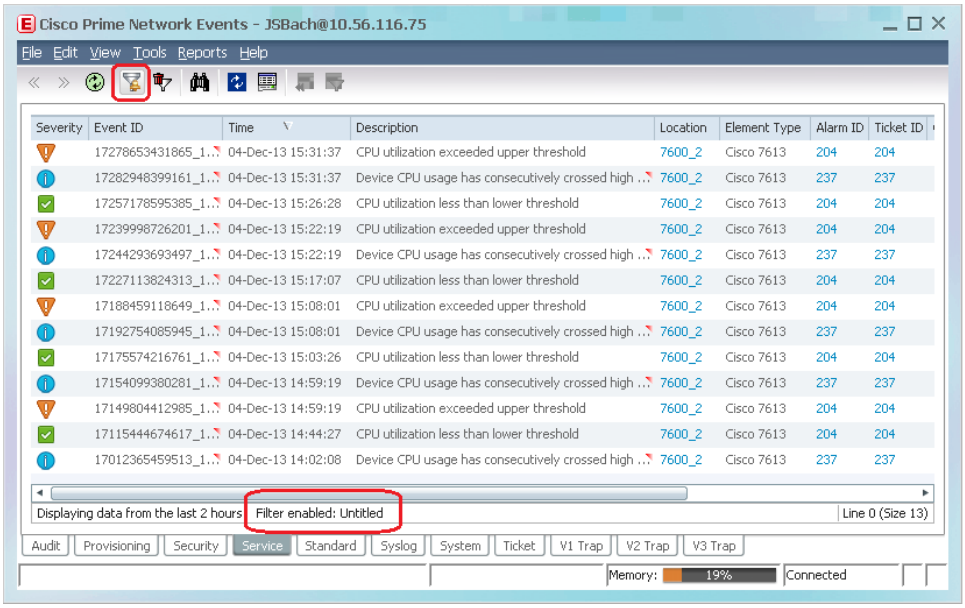
If a basic filter is applied, the client displays **Filter Enabled** at the bottom of the events table. If the display is using a saved filter, the filter name is also displayed, as in Figure 12-7. In this example, a user has applied a saved filter named **Unacknowledged-24Hours** to the display.

Figure 12-5 Basic Filter—Saved Filter Applied to Display



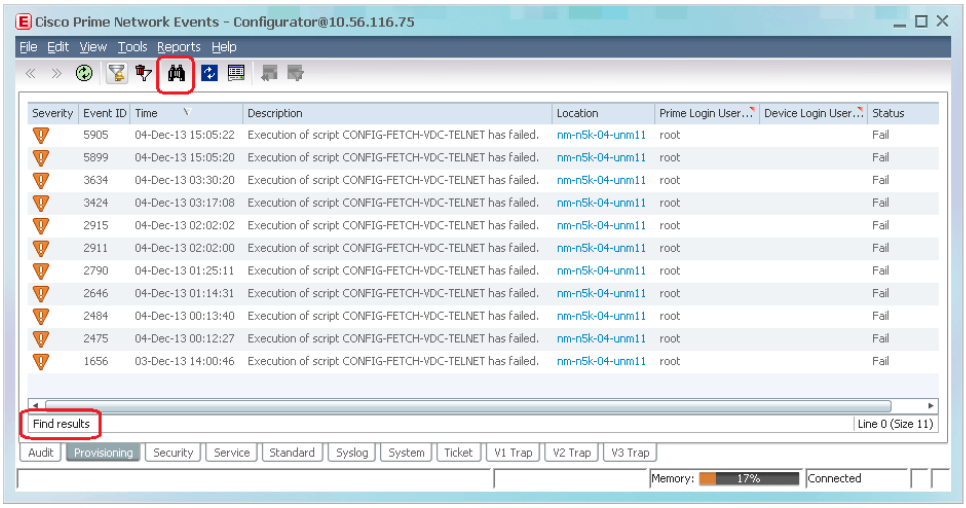
If the display is using a basic filter that was not saved, the client displays **Filter Enabled: Untitled**, as illustrated in Figure 12-6.

Figure 12-6 Basic Filter—(Unsaved) Filter Applied to Display



If a Find in Database filter is applied to an Events client display, the client displays **Find Results** at the bottom of the events table as illustrated in Figure 12-7.

Figure 12-7 Find in Database—Filter Applied (Events Client Only)



To disable any type of filter, do the following:

Filter Type	Disable by:	
	Choosing	Clicking
Basic filter	**Edit > Clear Filter**	
Find in Database filter (Events client only)	**Edit > Clear Find**	

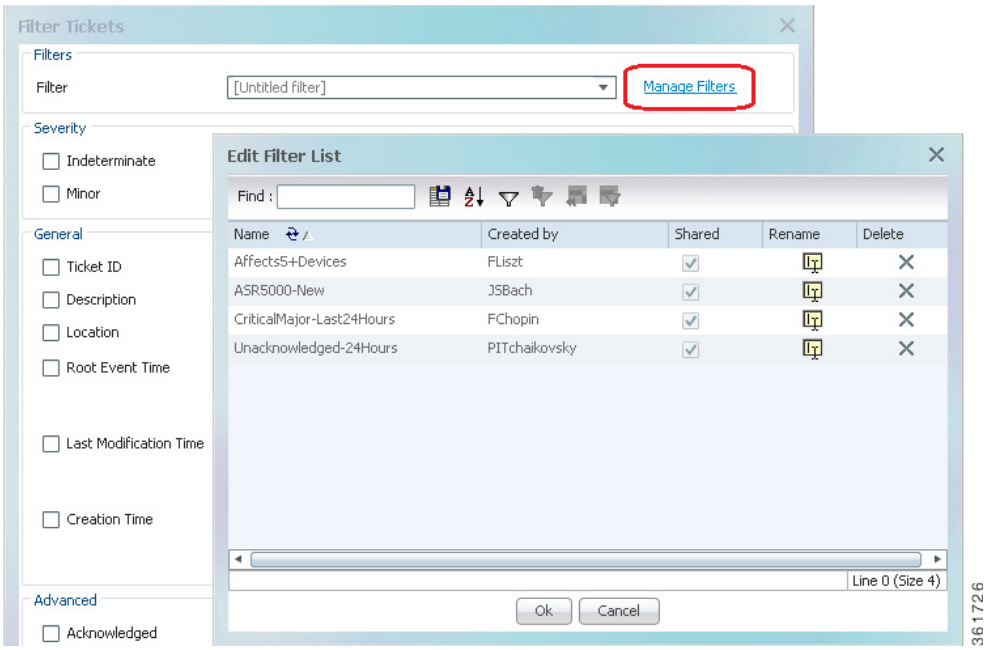
To clear the Find in Database filter, click the Find in Database filter icon in the toolbar and choose **Clear**.

Modifying Saved Filters and Managing the Filter List

To manage existing filters, open a filter dialog and click **Manage Filters**. In addition to filters created by the user, the Edit Filter List dialog provides an alphabetical lists of all shared filters. You can only rename or delete a filter you are the filter creator or if you have the same or higher permissions as the filter creator. If a filter is shared, the name of the filter creator is also displayed.

In this example, the current user has lesser permissions than the filter creators, so the user can employ the filters, but cannot edit or delete the filters. However, the user could create a similar filter by saving it under another name.

Figure 12-8 Managing Saved Filters



Finding Archived Tickets, Service Events, Syslogs, and Traps

The Prime Network database contains active and archive partitions. When a ticket or event is archived, it is moved to the archive database partition and is considered inactive, which means Prime Network will not perform any more actions on the ticket or event. In most cases, once a ticket is archived, you need to use a filter to view it and its associated events. Tickets are normally archived if they have been clear for 1 hour (no new events have been associated to the ticket). Cleared tickets can be archived sooner using the remove operation. For detail about the Prime Network clearing and archiving mechanism, see Clearing, Archiving, and Purging and the Oracle Database, page 10-13.

Some archived events are displayed in the clients, but only if those events fall within the GUI client's display parameters (by default, the last 2 hours for the Events client and the last 6 hours for the Vision client).

- Standard events—Standard events are events for which Prime Network only performs basic parsing; they are not processed for correlation. Standard events are archived as soon as they are received but are displayed in the **Standard** tab in the Events client, and in the **Network Events** tab in the Vision client map (or list view). If enabled, standard events are also shown in the **Latest Events** tab in the Vision client NE inventory window.
- Events associated with recently archived tickets—Tickets are normally archived after being cleared for 1 hour, but the Vision client reflects events from the past 6 hours. For this reason, some archived events may appear in the **Network Events** tab in the Vision client map or list view, and in **Latest Events** tab in the Vision client NE inventory window.
- Events that were not correlated to other events—These events are archived and displayed in the **Latest Events** tab in the Vision client NE inventory window.

Archived events that fall outside of the Events client and Vision client display parameters can only be viewed from the Events client using a filter. To find an archived ticket or network events, use the standard filters and set the Archive setting to **true**. See these topics for more information:

- Creating and Saving Filters for Tickets and Events, page 12-6 for a description of how to create filters using these tools
- Viewing Network Events (Service, Trap, and Syslog Events), page 12-13
- Viewing Tickets, page 12-17
- Viewing Non-Network Events (Audit, Provisioning, System and Security Events), page 12-17
- Viewing Tickets, page 12-17

Viewing Network Events (Service, Trap, and Syslog Events)

You can view all active and archived Service, Trap, and Syslog events using Events client filters. All network events provide the following information (other information is also supplied but those fields are self-explanatory). You can use this and other criteria for event filters as described in Creating and Saving Filters for Tickets and Events, page 12-6.

Table 12-2 Common Information Provided for Service, Trap, Syslog, and Ticket Events

Tab	Description
Details tab	• Detection Type—How the event was detected: V1 Trap, V2 Trap, V3 Trap, Syslogs, or Service event. • Alarm ID and Ticket ID—Identifier for alarms and ticket that the event is associated with (if applicable). • Causing Event—Event that caused the network event (if applicable) • Category—Fault category, one of the following: Communications, Quality of Service, Processing error, Environmental, Equipment, or Undetermined. • Nature—Whether the event will automatically clear: – ADAC (Automatically Detected Automatically Cleared)—Clearing is automatically detected and performed by the system (for example, Link Down). – ADMC (Automatically Detected Manually Cleared)—Clearing requires manual intervention (for example, a fatal error).
Affected Parties	Service resources (pairs) that are affected by the event. It lists of all the endpoints that are affected. See Viewing a Ticket's Affected Parties Tab (Resource Pairs), page 11-15. (This tab is only provided for events that calculate impact analysis. It has no relation to the Affected Devices count.)
Advanced	• Duplication Count—(For flapping) Total number of event duplications in the flapping alarm. (This number is always 1 for regular non-flapping events.) For example, this Link Down Flapping alarm would have a duplication count of 3: link down -> link up -> link down -> link up -> link down -> link up For tickets, this number is the sum of the duplication counts for all events and alarms in the ticket. • Reduction Count—(For flapping) Total number of event instances in the flapping alarm. (This number is always 1 for regular non-flapping events.). Using the previous example, the Link Down Flapping alarm would have a reduction count of 6 (with 6 events listed in the History tab). For tickets, this number is the sum of the reduction counts for all events and alarms in the ticket. • Alarm Count—Total number of alarms associated with the ticket. • Affected Devices—Total number of NEs affected by the ticket. (You can view the devices in a Vision client map)

For information on the other fields that are displayed, see:

- Service Events, page 12-14
- Syslogs and Traps, page 12-15

Service Events

Service events are generated by the Prime Network system in response to changes in the network. In response to these events, Prime Network will generate Service events, such as BGP Neighbor Loss, MPLS TP Tunnel Down, Link Down, Adaptive Polling (for high CPU issues), and so forth.

If you are looking for specific Service events, use the Events filters. You can search for events based on location (devices), a string included (or not included) in the description, and other common filter criteria (severity, description, and so forth). Once you create the filter, you can search for recent events or all events that are stored in the Oracle database. To create a filter, see Creating and Saving Filters for Tickets and Events, page 12-6. To find archived Service events, see Finding Archived Tickets, Service Events, Syslogs, and Traps, page 12-12.

Refer to these documents for extensive explanations about supported Service events, descriptions, whether they are ticketable, whether they auto-clear, and so forth, *Cisco Prime Network 5.3 Supported Service Alarms*.

Syslogs and Traps

When a device generates a syslog or trap, Prime Network attempts to match it to a predefined set of rules to determine if it is of interest to Prime Network. If it is of interest, Prime Network generates a syslog or a trap event. If not, it is saved to the database. These are other ways to view traps:

- Syslogs and traps handled by Prime Network but not processed for correlation—Click the **Standard** tab. (See Viewing Standard Traps and Syslogs Not Recognized by Prime Network, page 12-19).
- Archived syslogs and traps—Create a filter and set the **Archive** field to **true**.

In Prime Network, all syslogs and traps are configured to clear automatically, except:

- Syslogs and traps that are ticketable.
- A few important syslogs and traps that do not have a corresponding Service event. For example, a device that suddenly loses power does not send a Down event. Instead, it sends a cold start trap when it subsequently recovers. This trap is not cleared automatically because no corresponding Down event exists. If the cold start trap is automatically cleared, the device-recovery notification will be lost.

When you double-click a trap event, the Events client displays the Details, Affected Parties, and Advanced Tabs. These details provide the same information that is provided for tickets (see Getting a Ticket's Troubleshooting Tips And Basic Information, page 11-13).

Trap events also display a **Trap** tab with the following information (depending on the trap version):

	Field	Description
V1, V2, and V3 Traps	Version	SNMP version: version 1, version 2c, or version-3.
	Community String	Community that the device sends in the Protocol Data Unit (PDU).
	Error Status	Error status: No Error, Too Big, No Such Name, Bad Value, Read Only, and General Error.

	Field	Description
V1 and V2 Traps	**Values Table**	
	Translated OID	String representation of the OID. For example, 1.3.6 is translated into iso.org.dod where: • 1 represents iso. • 3 represents org. • 6 represents dod.
	Translated Value	String representation of the OID value. For example, 1.3 is translated to iso(1).org.10, or a specific value, such as “down” or “4 days, 20 hours, 32 minutes, 11 seconds.”
	OID	OID that is not translated. It is a dot notation representation of the OID, such as 1.3.6.1.4.1.9.
	Value	Value that is not translated.
V3 Traps	**Values Table**	
	Trap Type OID	Trap object identifier.
	Translated Enterprise	Translation of the OID using the MIB. For example, an enterprise OID of .1.3.6.1.2.1.88.2 is displayed in this column as .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
	Enterprise	Enterprise OID for the trap, representing the company or organization that is associated with the trap.

Note If a SNMP agent is enabled in a VM, then all the traps that are generated from the VM should be associated to **IManagedElement** node of the VNE.

If you are looking for specific traps, create a trap filter as described in Creating and Saving Filters for Tickets and Events, page 12-6.

Note For IPv6, we need to configure device to send events on specific ports (1514,1162 and 1161). For example, to configure on device: **snmp-server host 10.105.39.217 version 2c public udp-port 1162**

Refer to these documents for extensive explanations about supported traps and syslogs, including their descriptions, whether they are ticketable, whether they auto-clear, whether they are considered flapping events, and so forth:

- *Cisco Prime Network Supported Syslogs*
- *Cisco Prime Network Supported Traps*

Viewing Tickets

The Events and Vision client display the same ticket information, and the same operations can be performed from both clients. However, if you want to view archived tickets, use the Events client filters. See Viewing Non-Network Events (Audit, Provisioning, System and Security Events), page 12-17. To view Resync service alarm ticket information, see the topic Viewing Resync Alarm Details in Prime Network, page 11-5

Refer to Managing Tickets with the Vision Client, page 11-1 for complete information on how to find and manage tickets.

Viewing Non-Network Events (Audit, Provisioning, System and Security Events)

Audit Events (Executed Commands)

Audit events provide information about configuration commands that are executed on the Prime Network gateway. This can include NE right-click commands, CCM and Compliance Audit operations, and so forth. For example, if a CCM user activated an IOS-XR image, the Events client would display an event **Activation was executed by *user* on the device *device* for the image *image***.

The Provisioning tab provides the results of the command. You would find an associated Provisioning event that would list the results (**Execution of script !NEIMActivateIOSXRPackage** *status*) along with the exact commands sent to and received from the device.

Audit events also provide the following information, which you can also use as criteria for an Audit event filter:

Field	Description
Command Name	Audit-specific command name, such as CCM_Config_Restore for a CCM restore operation
Command Signature	Arguments used to create the command (often left blank).
Command Parameters	Command parameters issued with the command, such as CONFIG-DEPLOY for the CCM restore operation
Originating IP	IP address of the client that issued the command (127.0.0.1 is the gateway)

When you double-click the event, Prime Network displays the commands that were sent from Prime Network to the device.

If you are looking for specific Audit events, use the Events filters. You can search for events based on the originating IP address, strings included (or not included) in the command name, signature, or parameters, and other common filter criteria (severity, description, and so forth). Once you create the filter, you can search for recent events or all events that are stored in the Oracle database. To create a filter, see Creating and Saving Filters for Tickets and Events, page 12-6.

Provisioning Events (Device Configuration Results)

Provisioning events display the results of device configuration operations. For example, if a Vision client user right-clicks an NE and chooses **Commands > Show > Users (Telnet sessions)**, the Provisioning tab creates a new event called E**xecution of script !Device_ShowUser_xr succeeded**. The

event includes the device the command was executed on and the status of the command (Configuring, Success, Fail). It also includes this information, which you can use as criteria for a Provisioning event filter:

Field	Description
Prime Login Username	Username of the user that executed the command.
Device Login Username	Username that was used to access the device. It can be either of the following: • **From VNE Login**—Username specified when the device was added to Prime Network • *username*—*username* entered when the user ran the command and was prompted for their credentials.

Provisioning events display the results of operations performed by other Prime Network features such as Change and Configuration Management, Command Manager, and Transaction Manager. When you double-click the event, Prime Network displays the results returned from the device and the operation status.

If you are looking for specific Provisioning events, use the Events filters. You can search for events based on location (devices), the Prime or device username, the status (success, fail, configuring, unknown), and other common filter criteria (severity, description, and so forth). Once you create the filter, you can search for recent events or all events that are stored in the Oracle database. To create a filter, see Creating and Saving Filters for Tickets and Events, page 12-6.

Prime Network Security Events

Security events are related to user authentication, session management, and information about who is making system changes (disabling and enabling AVMs, adding new VNEs to the system, and so forth). An example is **User *user* authenticated successfully**. If you double-click the event, you can find out which client the user logged into.

If you are looking for specific Security events, use the Events filters. You can search for events based on a string that is included (or not included) in the username, the IP address where the event was triggered, and other common filter criteria (severity, description, and so forth). Once you create the filter, you can search for recent events or all events that are stored in the Oracle database. To create a filter, see Creating and Saving Filters for Tickets and Events, page 12-6.

For information on how to respond to specific Security events (including their probable cause), refer to *Cisco Prime Network Supported System and Security Events*.

Prime Network System Events

System events represent the everyday working of Prime Network and its components. Examples are:

- State or reachability changes in Prime Network components
- Database events (ticket archiving, disk space, dropped events, synchronization issues)
- Unit protection (standby unit) events

Most System events occur on AVM 11 (the gateway). If an event occurs on device, a hyperlink to the device is provided in the event details. For information on how to respond to specific System events (including their probable cause), refer to *Cisco Prime Network Supported System and Security Events*.

If you are looking for specific System events, use the Events filters. You can search for events based on a string that is included (or not included) in the description, specific devices, and other common filter criteria (severity, time, and so forth). Once you create the filter, you can search for recent events or all events that are stored in the Oracle database. To create a filter, see Creating and Saving Filters for Tickets and Events, page 12-6.

Viewing Standard Traps and Syslogs Not Recognized by Prime Network

Standard events are events that Prime Network could not match with any of the rules that define events of interest. Prime Network does a best effort at extracting information from these syslogs and traps, but does not process them for correlation. Standard events are saved to the database and can be viewed in the Standard tab. You can also create an event filter for Standard syslog and trap events using the same criteria for events displayed in the Syslogs tab and the V1 Trap, V2 Trap, and V3 Trap tabs. See Viewing Network Events (Service, Trap, and Syslog Events), page 12-13 for more information.

Standard events also appear in the Vision client:

- In the **Latest Events** tab in a map view (if enabled from the Administration client)
- In the **Network Events** tab in a device inventory view

Changing How Often Event Information is Refreshed

By default, the Events client displays event information from the last 2 hours (up to 50 records per table). Data is refreshed when you log into the Events client, and when you move between the Events tabs. To refresh the data in a table you are viewing, click **Refresh Now**. You can also enable the auto-refresh mechanism which will update the data every 60 seconds. The manual and auto refresh buttons are shown below.

Button	Name	Function
	Refresh Now	Manually refreshes the events list (same as choosing **View > Refresh**).
	Auto Refresh	Enables auto refresh of events tables (every 60 seconds). Filters remain intact. **Note** By default, tabular data is not refreshed on an ongoing basis.

The following table shows the default settings for data display and refresh, and how you can adjust them.

To control:	Default Setting	To change setting:
Updating data when you log into Events client	Enabled	Switch to Find in Database mode (see Creating a New Filter and Saving It, page 12-7)
Updating events data whenever you move between Events tabs (“Find” mode)	Enabled	Choose **Tools > Options**
Updating the displayed data: • On an ongoing basis, and	Disabled	Click **Auto Refresh**

To control:	Default Setting	To change setting:
• At a specific interval	60 seconds	Choose **Tools > Options**
How much data to display in the events tables (age and number of records per page)	2 hours 50 records	Choose **Tools > Options** **Note** Increasing the interval beyond 2 hours can adversely affect the display performance.

Exporting Events Data

When you export data, it is saved as a CSV file. Prime Network will export all of the data listed in the table, up to the number of records specified in the Events client Options dialog. You can check the setting by choosing **Tools > Options** from the main menu.

To export an Events table to a CSV file:

Step 1 Choose **File > Export**.

Step 2 Browse to the directory where you want to save the file and enter a name for the file.

Step 3 Click **Save**. The displayed records are saved in a CSV file.

Changing the Events Client Defaults

Events client users can change their default settings. This includes:

- Saving filters and using them by default when you open Events
- How many records to display in the Events client
- How many records can be exported at one time
- How often data should be refreshed
- The age of data to display
- Enabling manual event retrieval (so that events are not retrieved immediately when you first log in or when you switch between tabs)

To change these settings, see Setting Up Your Events View, page 6-4.

Finding Available Network Paths Using PathTracer

Cisco PathTracer uses Prime Network's inner logic to show available paths between two network elements. It creates a virtual path, without modifying any real network elements, and shows all devices and components the path flows through, including performance data.

The following topics describe Cisco PathTracer and how to use it:

Cisco PathTracer

Cisco PathTracer enables you to launch end-to-end route traces and view related performance information for Layer 1, Layer 2, and Layer 3 traffic. Upon receiving a path's start and endpoint, Cisco PathTracer visually traces the route through the network. For example, in an ATM network environment, Cisco PathTracer identifies all information regarding the connection of a subscriber to a provider, including all ATM PVCs, ATM switching tables, ATM class of service (CoS) definitions, IP-related information, and so on.

You can also use Cisco PathTracer to:

- Trace paths using IPv4, IPv6, or both IPv4 and IPv6 addresses for the source and destination.
- Trace a hypothetical Ethernet frame from a VLAN interface to a specified MAC address.
- Trace a hypothetical Ethernet frame from an Ethernet interface to a specified MAC address within a specific VLAN identifier.

In MPLS and Carrier Ethernet environments, Cisco PathTracer can trace paths across:

- Carrier Supporting Carrier (CSC) configurations—A path trace along a CSC flow follows the path from the customer CE through the customer carrier VPN, across the customer backbone carrier VPN, back to the customer carrier VPN, and to the destination CE.
- VLANs—A path trace across VLANs follows the path based on the forwarding table, which means that the trace follows ports in the Forwarding STP state.
- Q-in-Q—A path trace across Q-in-Q creates a single path trace (if the MAC address is learned) or a multiple-path (multipath) trace if the MAC address is not in the forwarding table. If the VLAN bridge has not learned a given MAC address, the bridge floods the Ethernet frame to the confines of a given VLAN or switching entity and across those ports that allow the given VLAN identifier. A MAC/VLAN path trace can be conducted from a customer edge (CE) VLAN interface across a service provider (SP) VLAN; that is, across Q-in-Q configurations with the CE-VLAN identifier as the inner VLAN identifier and Cisco PathTracer detecting the outer SP-VLAN identifier that encapsulates the CE-VLAN.
- Pseudowires (also known as EoMPLS)—A MAC/VLAN path trace can be conducted from a VLAN interface across a VLAN attachment to a pseudowire.
- VLAN-VPLS-VLAN configurations—A multiple-point MAC/VLAN path trace can be conducted on CE-VLANs across a service provider VPLS transport from a VLAN interface that attaches to the VPLS.

In addition, Cisco PathTracer can trace a path:

- If the destination MAC address is not reachable—If Cisco PathTracer cannot complete a MAC/VLAN path trace to a specified destination MAC address across an MPLS core, VPLS, or H-VPLS, then Cisco PathTracer displays the portion of the path that Cisco PathTracer can trace toward the destination MAC address.
- That contains a simulated Ethernet frame—Cisco PathTracer can trace a simulated Ethernet frame from a VLAN port, across a VLAN (VLAN-based flow domain fragment), VPLS (VPLS-based flow domain fragment), and VLAN, for an end-to-end MAC address trace.

Prime Network derives the various paths on the network from its up-to-date knowledge of the network. After a user selects a source and destination, Cisco PathTracer finds and retrieves the path of a specified service, and displays the path in the Cisco PathTracer window. The retrieved information contains network elements in the path, including all properties at Layer 1, Layer 2, and Layer 3, plus alarm information, counters, and more, all of which is available via Cisco PathTracer.

Launching Path Tracer

Cisco PathTracer can be launched from a bridge, switching entity, Ethernet interface, Ethernet flow point, VLAN interface, ATM VC, DLCI, or IP interface entry point. Ethernet flow points can be starting points whether they are associated with an interface, bridge, or LAG.

The virtual route is found according to the cross connect table of each ATM switch or Frame Relay device. The IP routing and path-finding process is enabled according to the VRF tables of each router, and the Ethernet-simulated path is found according to the various Layer 2 forwarding tables, such as bridges or VSIs.

To view a specific path, you must specify an initial point and a destination, such as an IP or MAC address. If you specify VC or DLCI information, which ends in a router, Cisco PathTracer finds the next hop according to the destination IP address. If you do not specify a destination IP or MAC address, Cisco PathTracer uses the default gateway in the router. Any business tags that are associated with the physical or logical entities are also displayed.

Note A path can also be launched if a business tag attached to an endpoint that can be used as the starting point.

Path Traces and Blocked Ports

The following conditions apply for blocked ports:

- You can launch a path trace from a blocked port. This action is equivalent to launching a path trace from a bridge.
- You can specify a blocked port as a destination.
- If Cisco PathTracer encounters a blocked port in its path to the destination, the path trace stops. Path traces do not traverse blocked ports.

Table 13-1 identifies the available path trace launching points and their locations within the Vision client. Cisco PathTracer is available in each location as a right-click menu option.

Supported Launch Points for Cisco PathTracer

Cisco PathTracer is launched by using right-click menu options. Table 13-1 identifies the launching points for the different types of elements.

Table 13-1 Cisco PathTracer Right-Click Menu Options

Element	Location
Affected Parties	• Inventory window • Ticket Properties window (Affected Parties tab)
Bridge	Inventory window
Business tag	The path can be found using a business tag, which is attached to the VPI/VCI, or using an IP interface by entering its key. The path can then be opened from the Find Business Tag dialog box.
Ethernet flow point	• Map view or navigation pane • Inventory window
IP interface	• Inventory window • Affected entry
Layer 2 MPLS tunnel	Inventory window
MPLS-TE tunnel	Inventory window
MPLS-TP tunnel endpoint	• Map view or navigation pane • Inventory window
Port	Inventory window
Pseudowire endpoint	• Map view or navigation pane • Inventory window
Site	Map view
Switching entity	Map view

Table 13-1 Cisco PathTracer Right-Click Menu Options (continued)

Element	Location
Virtual connection	Inventory window: • Cross Connect window • VC Table window
VLAN	• Navigation pane • Map view

Starting a Path Trace

To start a path trace:

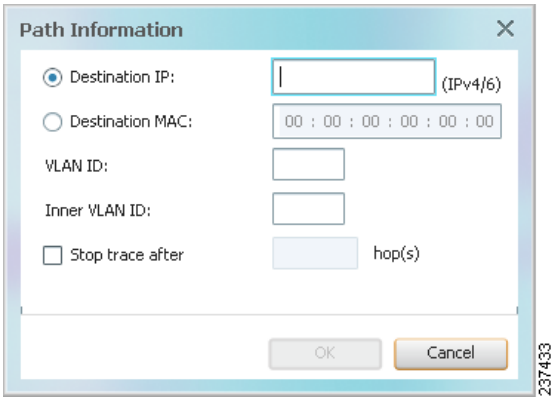
Step 1 Start the path trace in one of the following ways:

Note If you select an IP interface as the launch point, the right-click menu displays IPv4 and IPv6 options. These options are enabled or dimmed, depending on whether the IP interface has an IPv4 address, an IPv6 address, or both IPv4 and IPv6 addresses. For an example, see Figure 13-3.

Launch Point	Steps
VLAN (from map view)	1. Double-click a VLAN to view its entities. 2. Right-click the required item and choose **PathTracer > From Here to Destination** or **PathTracer > Start Here**.
VPN (from map view)	1. Double-click the VPN to view its entities. 2. Right-click the site and choose **PathTracer > From Here to Destination** or **PathTracer > Start Here**.
Ethernet Flow Point (from map view)	1. Choose **Network Inventory > Ethernet Flow Domains**. 2. In the Ethernet Flow Domain List Properties window, double-click the required domain. 3. In the Ethernet Flow Domain Properties window, right-click the required element and choose **PathTracer > From Here to Destination** or **PathTracer > Start Here**.
NE physical or logical inventory	1. Right-click one of the following: – IP interface – MPLS-TP tunnel endpoint – Port – Pseudowire endpoint – VLAN bridge 2. Choose **PathTracer > From Here to Destination** or **PathTracer > Start Here**.

Step 2 If you choose **PathTracer > From Here to Destination**, complete the Path Information dialog box (Figure 13-1).

Figure 13-1 Path Information Dialog Box



a. In the Path Information dialog box, enter the required information. The contents depend on your launch point.

Field	Description
Destination IP	Specify an IPv4 or IPv6 address.
Destination MAC	MAC address
VLAN ID	Enter the VLAN identifier (For example, VLAN id 1-4094).
Inner VLAN ID	Inner VLAN identifier
Stop trace after	Check this check box to enter a maximum of hops that Cisco PathTracer makes in its attempt to reach the destination

b. Click **OK**.

Step 3 If you choose **Start Here**, navigate to the destination interface, port, or bridge, right-click it, and choose **End Here**. The Cisco PathTracer window is displayed showing the path or paths that were found.

Step 4 To view additional details regarding the path traces, select one or more paths in the paths pane.

Step 5 In the toolbar, click **Cisco PathTracer**.

- If you select one or more paths in the paths pane, each selected path is displayed in its own window with the Layer 1, Layer 2, Layer 3, and Business Tag tabs.
- If you select nothing in the Paths pane, each path found is displayed in its own window with the Layer 1, Layer 2, Layer 3, and Business Tag tabs.

For more information about the end-to-end path and networking layer details, see Saving and Opening Cisco PathTracer Map Files, page 13-17.

Examples of Launching Cisco PathTracer

The following topics provide examples for launching Cisco PathTracer from different locations in the Vision client:

- Using an Ethernet Flow Point, page 13-6
- Using an IP Interface, page 13-7
- Using a VLAN Bridge, page 13-8
- Using an Ethernet Port, page 13-9
- Using a Pseudowire, page 13-10
- Using an MPLS-TP Tunnel Endpoint, page 13-11

Using an Ethernet Flow Point

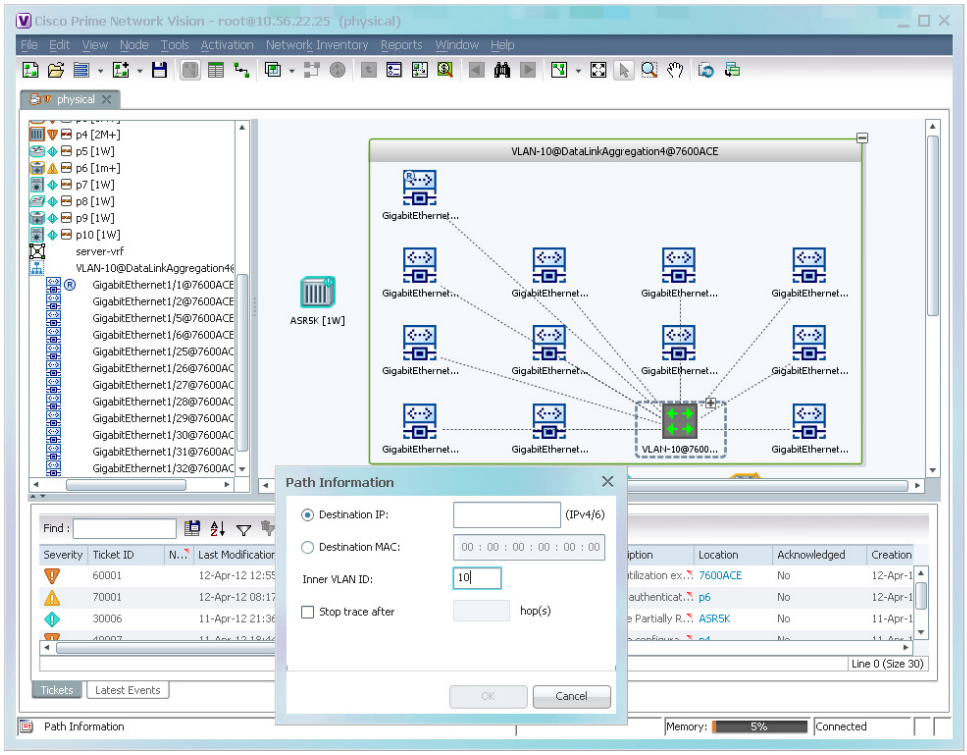
A network VLAN is required for you to start a path trace using an Ethernet flow point.

To launch a path trace from an Ethernet flow point:

Step 1 In the Vision client navigation pane or map pane, expand the required network VLAN.

Step 2 In the VLAN, right-click the required Ethernet flow point and choose **PathTracer > From Here to Destination**. The Path Information dialog box is displayed as shown in Figure 13-2.

Figure 13-2 Ethernet Flow Point Path Trace Launch Point



Step 3 Specify the destination.

Step 4 To limit the number of hops for the path trace, check the *Stop trace after* check box, and enter the maximum number of hops for the path trace.

Step 5 Click **OK**. The Cisco PathTracer window is displayed with the resulting path trace.

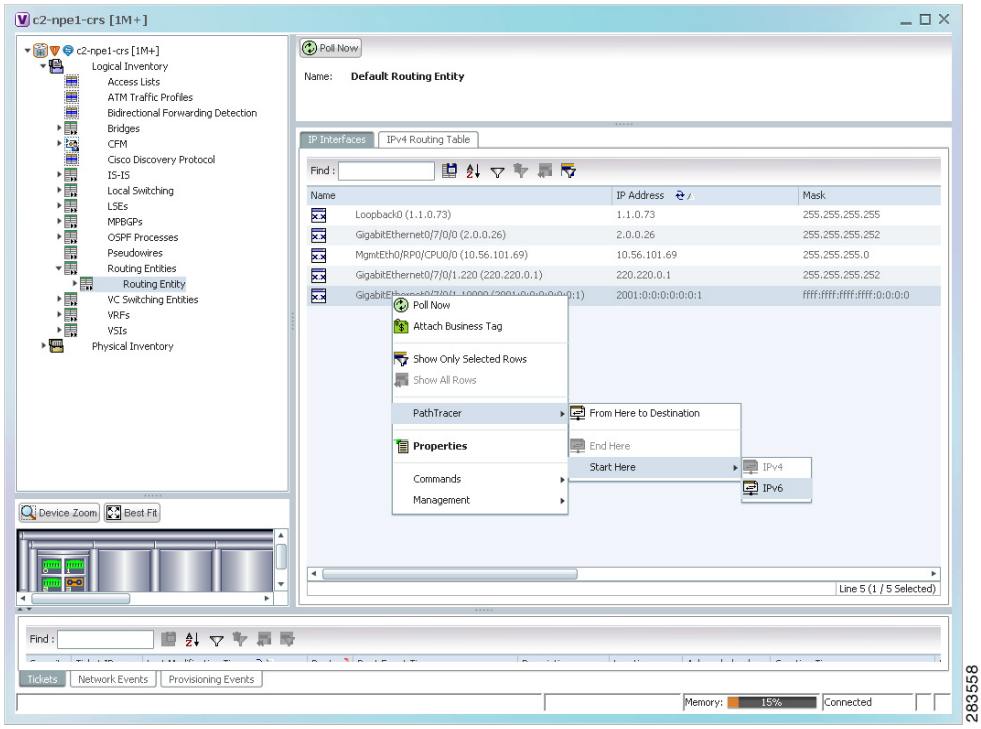
Using an IP Interface

Both IPv4 and IPv6 addresses are supported as valid path trace sources and destinations as illustrated in the following procedure.

Step 1 In logical inventory, right-click the required IP interface (**Logical Inventory > Routing Entities > Routing Entity >** *ip-interface*).

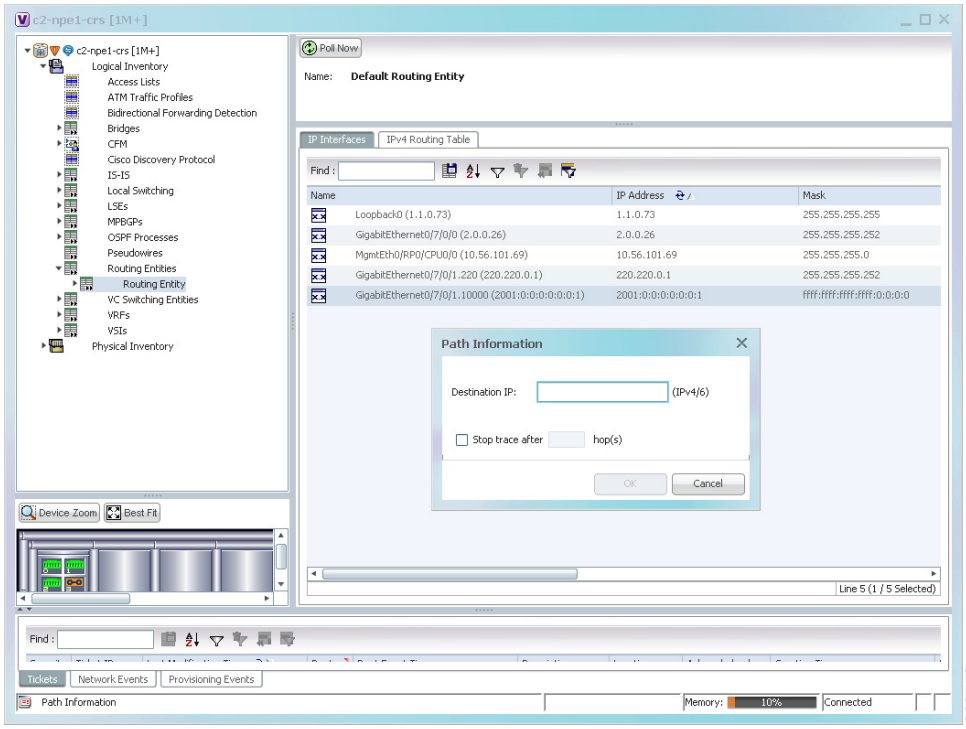
The right-click menu displays IPv4 and IPv6 options. These options are enabled or dimmed, depending on whether the IP interface has an IPv4 address, an IPv6 address, or both IPv4 and IPv6 addresses. See Figure 13-3.

Figure 13-3 IP Interface Path Trace Launch Point - Right-Click Menu



Step 2 Choose **PathTracer > From Here to Destination**. The Path Information dialog box is displayed as shown in Figure 13-4.

Figure 13-4 IP Interface Path Trace Launch Point - Path Information Dialog Box



Step 3 In the Destination IP field, enter the IPv4 or IPv6 address.

Step 4 To limit the number of hops for the path trace, check the *Stop trace after* check box, and enter the maximum number of hops for the path trace.

Step 5 Click **OK**.

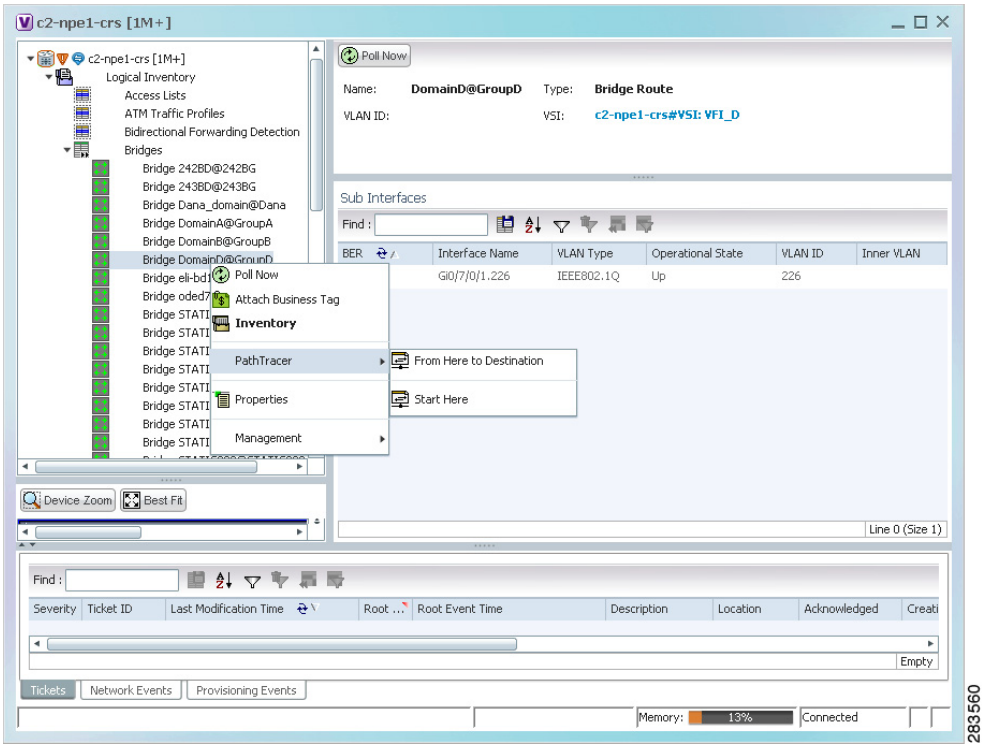
Using a VLAN Bridge

You can launch path traces from VLAN bridges. Additionally, MAC addresses in the VLAN bridge forwarding table can be path trace destinations.

Step 1 In logical inventory, right-click the required bridge (**Logical Inventory > Bridges >** *bridge*) and choose one of the following options as shown in Figure 13-5:

- **PathTracer > From Here to Destination**
- **PathTracer > Start Here**

Figure 13-5 VLAN Bridge Path Trace Launch Point



Step 2 If you choose **From Here to Destination** in Step 1, the Path Information dialog box is displayed. Specify the required destination.

Step 3 If you choose **Start Here**, navigate to the destination, right-click it, and choose **End Here**. Destination options include:

- IP interface—**Logical Inventory > Routing Entities > Routing Entity >** *IP-interface*
- Bridge—**Logical Inventory > Bridges >** *bridge*
- MAC address—**Logical Inventory > Bridges >** *bridge* **> Bridge Table >** *MAC-address*
- Ethernet port—**Physical Inventory >** *chassis* **>** *slot* **>** *port*

When a destination is selected, the system extracts the relevant IP address from this point and uses it as the destination.

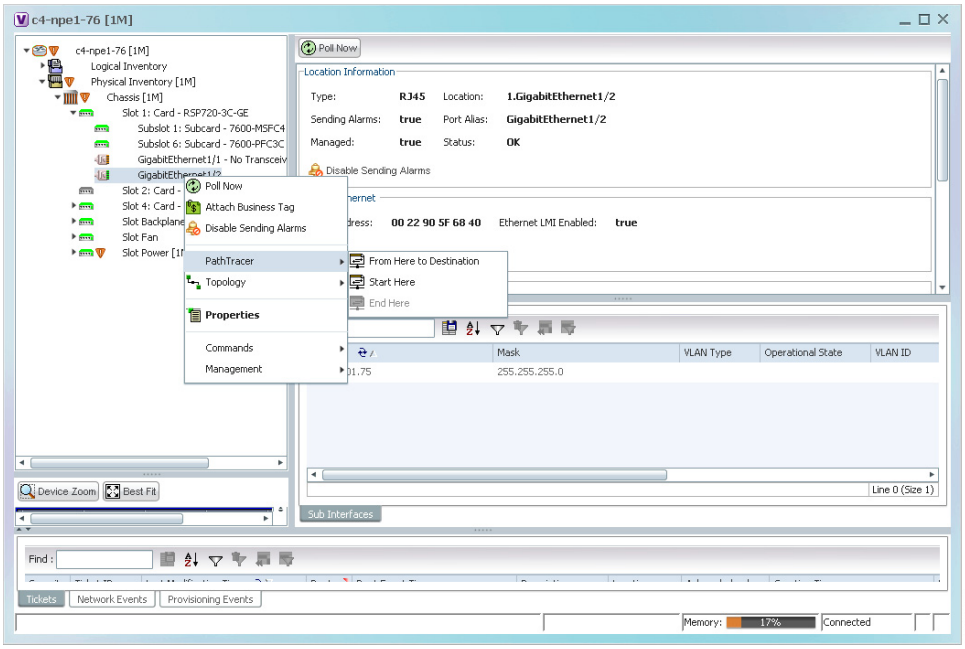
Using an Ethernet Port

To launch a path trace from an Ethernet port:

Step 1 In physical inventory, right-click the required port (**Physical Inventory > Chassis >** *slot* **>** *subslot* **>** *port*) and choose one of the following options as shown in Figure 13-6:

- **PathTracer > From Here to Destination**
- **PathTracer > Start Here**

Figure 13-6 Ethernet Port Path Trace Launch Point



Step 2 Depending on your choice in Step 1, specify the required destination information or select the path trace endpoint.

The Cisco PathTracer window appears, displaying the resulting path trace.

Using a Pseudowire

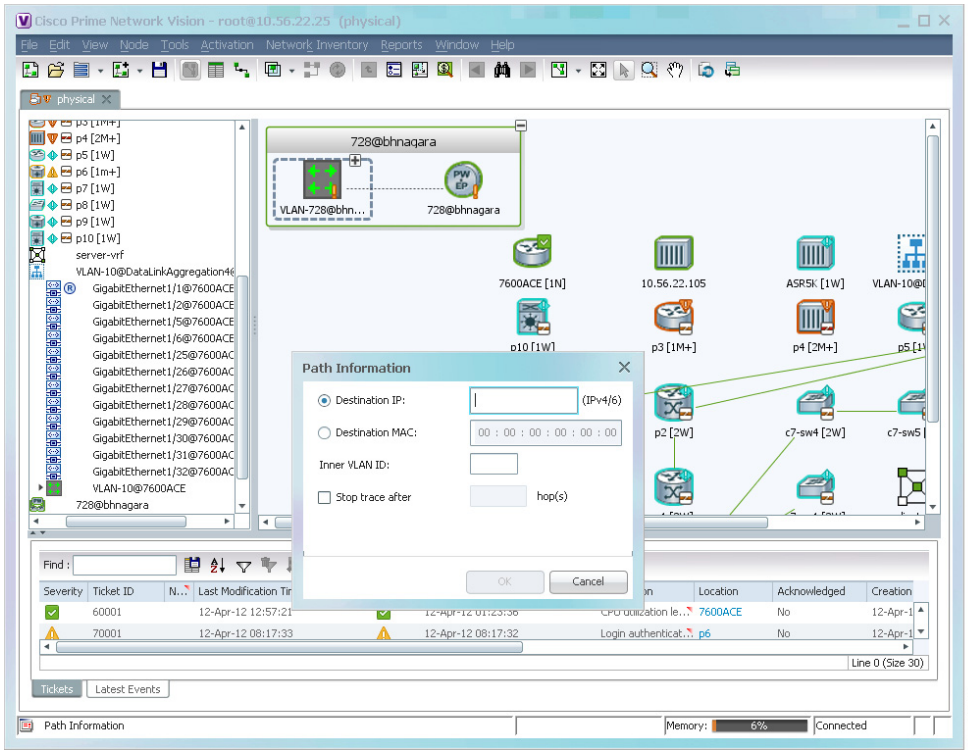
To launch a path trace from a network pseudowire endpoint:

Step 1 In the navigation pane or map pane, expand the required network pseudowire.

Step 2 Right-click the required pseudowire endpoint and choose **PathTracer > From Here to Destination**.

The Path Information dialog box is displayed as shown in Figure 13-7.

Figure 13-7 Path Information Dialog Box for a Network Pseudowire



Step 3 Specify the destination.

Step 4 To limit the number of hops for the path trace, check the *Stop trace after* check box, and enter the maximum number of hops for the path trace.

The Cisco PathTracer window appears, displaying the resulting path trace.

Using an MPLS-TP Tunnel Endpoint

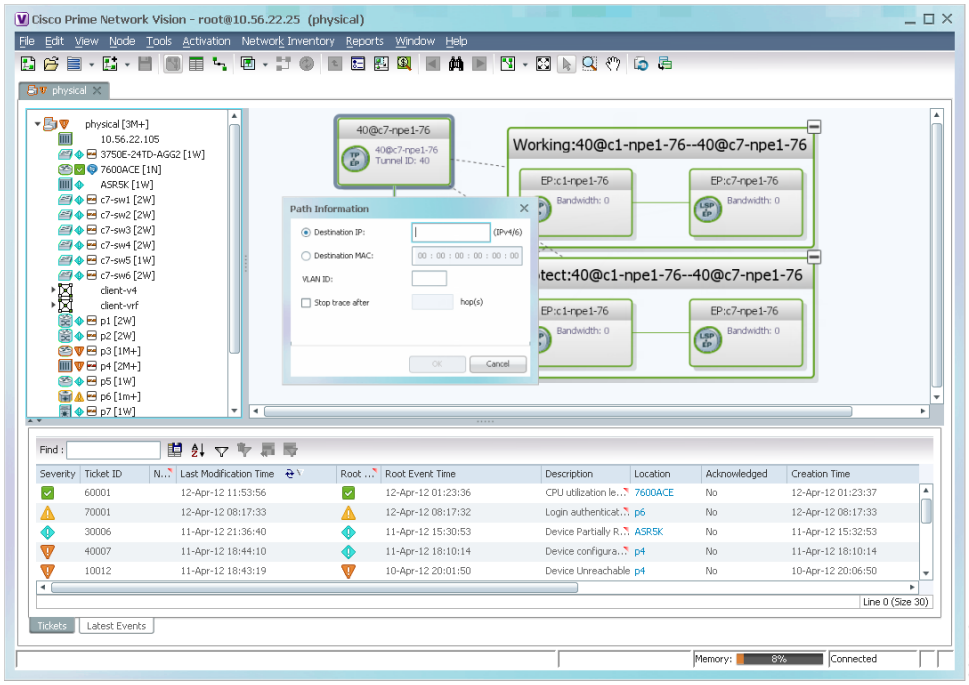
To launch a path trace from an MPLS-TP tunnel endpoint:

Step 1 In the navigation pane or map pane, expand the required MPLS-TP tunnel.

Step 2 Right-click the required MPLS-TP tunnel endpoint and choose **PathTracer > From Here to Destination**.

The Path Information dialog box is displayed as shown in Figure 13-8.

Figure 13-8 MPLS-TP Tunnel Endpoint Path Trace Launch



Step 3 Specify the destination.

Step 4 To limit the number of hops for the path trace, check the *Stop trace after* check box, and enter the maximum number of hops for the path trace.

The Cisco PathTracer window appears, displaying the resulting path trace.

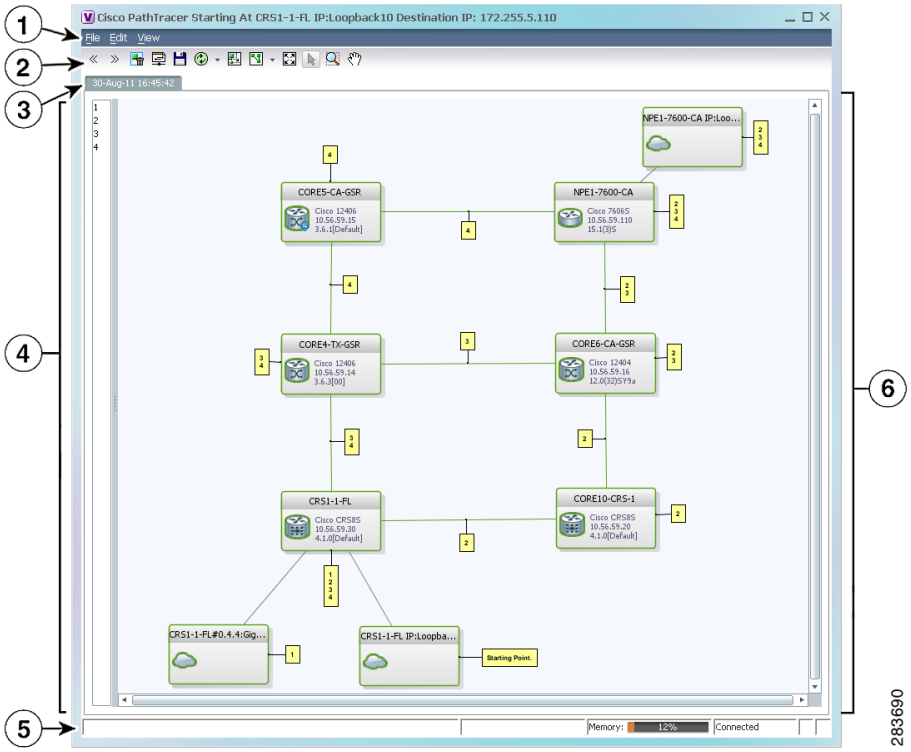
Viewing Path Traces

The Cisco PathTracer window displays all discovered paths for the specified source and destination of the path trace, including the devices and physical links. Form the window you can:

- View multiple paths for a selected source and destination either sequentially or simultaneously.
- View individual paths with networking layer details.
- Save a map with multiple paths to a file.
- Run Cisco PathTracer again, using the same trace or with a different limit number of hops.

Figure 13-9 shows an example of the Cisco PathTracer window with a multiple-path trace.

Figure 13-9 Cisco PathTracer Window - Multiple-Path Trace



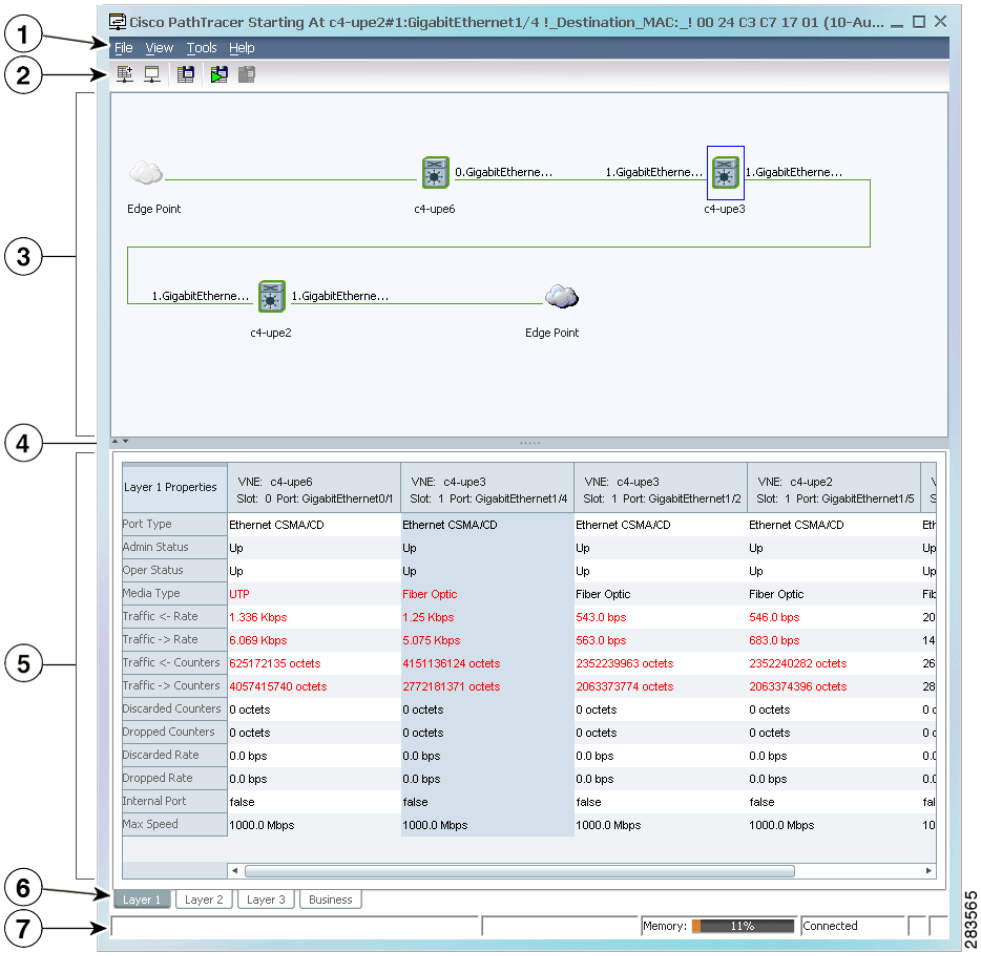
	Window Area	Description
1	Menu bar	—
2	Toolbar	Cisco PathTracer Toolbar, page 13-16
3	Trace tab	Displays the discovered path with a tab that displays the date and time when Prime Network started the path tracing process (snapshot time). New runs are represented in new tabs. To use a saved path in the same window, the source and destination must be the same.
4	Paths pan	Lists all the paths discovered in the path trace (one path for each source and destination pair, identified by a number). If you launch a path trace with a specific hop count, the paths pane displays First *n* Hops where *n* is the number of hops specified. You can choose different paths in the path pane or by using the toolbar icons. Click **Clear Path Selection** to de-select a path.
5	Status bar	—
6	Path trace pane	Displays the devices, links, and topological paths in path trace. All links and nodes are labeled with their relevant path numbers. The starting point is labeled with a Starting Point callout. All other edge points are displayed as clouds. The same coloring conventions that are used for links in the Prime Network content pane are used to display links in the Cisco PathTracer path trace pane. (See Links, page A-11.)

Click **PathTracer** from the toolbar to display the following information:

- Each NE's relevant parameters for each interface on all layers along the path; for each layer, an indication of a mismatch between the parameters of the interfaces on both sides of a link; and traffic statistics along the path.
- Status and traffic information for all links along the path.
- View In and Out port properties.

If you select multiple paths, a separate window is opened for each path. Figure 13-10 shows an example of the Cisco PathTracer details window.

Figure 13-10 Cisco PathTracer Details Window



1	Menu bar	—
2	Toolbar	—
3	Path trace pane	Displays information related to the selected tab (for example, Layer 2). If you choose an element or link in the path trace pane, the related parameters are highlighted in the details pane. By default, the path trace pane includes: • Edge points • Elements included in the path trace, including badges • Links included in the path trace Hovering your mouse over an element displays a tooltip that contains the element name, device type, and IP address. Hovering your mouse over the link to the right or left of the element displays the associated incoming or outgoing interface for that element and link.
4	Hide/display path trace pane	—
5	Details pane	Selecting a device or link in the path trace pane automatically highlights the related parameters in the details pane. Displays information about device or link selected in Path trace pane, such as Layer and Business tabs, supported parameters of the selected element in a table, with the ingress and egress ports along the top and the parameters on the left. Colors indicate any inconsistencies between the two connected ports. The information parameters are arranged as follows: • Layer *n* tabs—Provide information about each network element, including ingress and egress port information. The information is either plain data that is extracted from the element or calculated data, such as rates or statistics. This information is displayed in the Layer 1, Layer 2, and Layer 3 tabs, as follows: – Layer 1—Displays the Layer 1 information in the selected path and the link parameters, device name, subslot, slot, and port details. – Layer 2—Displays the Layer 2 information in the selected path and the link and connection parameters. For each device, the name and MAC address are displayed, as well as the VPI/VCI in an ATM link or the DLCI in a Frame Relay link. (This tab is active by default.). – Layer 3—Displays the Layer 3 information in the selected path and the link parameters and devicenames. Fields are only displayed if they are populated. For example, if none of the interfaces is configured for MTU, the MTU row is not displayed in the table. • Business tab—Provides the name and key of business tags that are attached to the network entities displayed, including ports, devices (physical entities), VCIs, VPIs, DLCIs, contexts (logical entities), or MPLS.
6	Layer and Business tabs	—
7	Status bar	—

Cisco PathTracer Toolbar

Table 13-2 describes the options available in the Cisco PathTracer toolbar.

Table 13-2 Cisco PathTracer Toolbar Options

Button	Function
	Displays the previous path in the path trace pane.
	Displays the next path in the path trace pane.
	Clears the path selection made in the path trace pane.
	Opens the Cisco PathTracer details window. A map is displayed for the selected path, including network element details, links, and property information. For more information, see Saving and Opening Cisco PathTracer Map Files, page 13-17.
	Saves the current multiple-path trace to an XML file on your local system. For more information, see Saving and Opening Cisco PathTracer Map Files, page 13-17.
	Offers the following options for running Cisco PathTracer again for the same source and destination: • Change Hop Count—Enables you to enter a new hop count. • Repeat Last Trace—Runs the previous trace with the same settings. • Run Full Path Trace—Runs the previous trace without a hop count limit. The new path trace map is displayed in the path trace pane. A new tab with the up-to-date (or refreshed) path map is created for each run, with each tab representing a run and the tab label indicating the snapshot time.
	Opens a window displaying a high level view of the path trace currently displayed in the path trace pane.
	Specifies how the elements are arranged in the path trace pane: circular, hierarchical, orthogonal, or symmetric.
	Fits the entire path trace in the path trace pane.
	Activates the normal selection mode. The button toggles when selected or deselected.
	Activates the zoom selection mode, which enables you to select a specific area in the path to zoom in on by clicking and dragging. The button toggles when selected or deselected.
	Activates the pan mode, which enables you to move around in the path trace by clicking and dragging. The button toggles when selected or deselected.

Saving and Opening Cisco PathTracer Map Files

Prime Network enables you to export multiple-path trace maps that are displayed in the Cisco PathTracer window to an XML file. You can view the data later to assess whether anything has changed.

Saving Cisco PathTracer Map Files

To save Cisco PathTracer map files:

Step 1 Open the Cisco PathTracer window as described in Launching Path Tracer, page 13-2.

Step 2 Click **Save MultiPath** in the toolbar.

Step 3 In the Save dialog box, navigate to the directory where you want to save the file and enter a name for the map file.

Step 4 Click **Save**. The map file is saved in the selected directory.

Opening Cisco PathTracer Map Files

Prime Network enables you to open saved XML-formatted path-tracing maps.

The following conditions apply when working with multiple-path trace files:

- When you load a multiple-path trace file, Prime Network queries the file (not the network), and loads the persisted information.
- If you load a multiple-path trace file that does not contain the same start and end points, the map is automatically opened in a new Cisco PathTracer window.

To open Cisco PathTracer map files:

Step 1 In the Vision client, choose **File > Load MultiPath** from the main menu. The Open dialog box is displayed.

Step 2 Navigate to the directory of the saved file and select the file.

Step 3 Click **Open**. The previously saved map is displayed in the Cisco PathTracer window.

Saving Cisco PathTracer Counter Values

Prime Network enables you to export, over a period of time, the counter values of the path displayed in the Cisco PathTracer window to a CSV file. The data can then be viewed later, as required.

Note This topic applies to the Cisco PathTracer details window only.

To save Cisco PathTracer counter values that are generated over a period of time:

Step 1 Open the Cisco PathTracer details window as described in Launching Path Tracer, page 13-2.

Step 2 Click **Start Saving to File** in the toolbar.

Step 3 In the Export Table to File dialog box, navigate to the directory where you want to save the Cisco PathTracer counter values.

Step 4 In the File name field, enter a name for the file in which to save the counter values.

Step 5 Click **Save**. Cisco PathTracer starts saving the counter values to the specified file.

Step 6 To stop exporting counter values to the file, click **Stop Saving to File** in the toolbar.

Cisco PathTracer stops exporting the counter values to the file.

Rerunning a Path and Comparing Results

If you save a path to a file (see Saving and Opening Cisco PathTracer Map Files, page 13-17), you can use the file to rerun the same path automatically with the same source and destination. You can also compare the saved path to a newly run path to determine if the path has changed or to assess a problem.

To rerun a saved path:

Step 1 Load the required map file as described in Saving and Opening Cisco PathTracer Map Files, page 13-17. The Cisco PathTracer window is displayed with the previously saved map file.

Step 2 Click **Run Again** in the toolbar.

The path trace runs automatically using the same source and destination as the loaded map file, and a new tab is displayed in the Cisco PathTracer window with the updated map. The tab displays the date and time when the path was rerun.

Step 3 Compare the previous map to the updated one by switching between the tabs in the Cisco PathTracer window.

Note

- If you load a Cisco PathTracer map file that does not contain the same source and destination information as the map that is currently displayed in the window, the map is automatically opened in a new Cisco PathTracer window.
- If you load a Cisco PathTracer map file that contains the same source and destination information as a map that is currently displayed in the window, the map is loaded in a new tab in the same window.

Viewing Q-in-Q Path Information

The Q-in-Q (IEEE 802.1) tagging technology (also known as Dot1q tunneling) allows the nesting of another VLAN tag in a packet, in addition to an existing one. Either VLAN tag is considered an 802.1Q header.

Cisco PathTracer uses the VLAN tags of the Ethernet header and the port configuration to trace the path from one interface to another over the network. Among other things, you can:

- View a Layer 2 path across a LAN domain with all the VLAN tag information.
- For each network element, view the relevant parameters for each interface on all layers along the path.

Q-in-Q and Dot1q information is displayed in the Cisco PathTracer window when a path is traced over Ethernet ports with Dot1q and a Q-in-Q configuration.

As described in Launching Path Tracer, page 13-2, to view a specific path, you must specify an initial start point, such as an IP interface, and then an endpoint, such as a destination IP address.

To trace a Q-in-Q path, you start the path from any:

- Router or switch that is part of the Ethernet domain with Dot1q and Q-in-Q configurations.
- IP destination that can be reached from that point of the network.

After you select the endpoint, the Cisco PathTracer window is displayed. From this window, you can open the Cisco PathTracer details window, with the appropriate Q-in-Q information displayed in the Layer 2 tab.

The Layer 2 tab can display the following information specific to Q-in-Q and VLAN port configurations:

- VLAN Mode—The work mode for the interface: Unknown, Access, Trunk, or Dot1Q Tunnel. Trunk mode also refers to multiple tagging.
- Native VLAN ID—The VLAN identifier that is used to tag untagged traffic received on a trunked interface:
  - If VLAN tagging is enabled, the default native VLAN identifier is 1.
  - If VLAN tagging is disabled, the native VLAN identifier is 0 (zero) or “no VLAN ID.”
- CE VLAN ID—The customer edge device VLAN identifier.
- SP VLAN ID—The service provider VLAN identifier.

Viewing L2TP Path Information

Cisco PathTracer uses VC ID encapsulation information to trace the path from one tunnel interface to another over the network. The Cisco PathTracer tool enables you to:

- View a path for the defined Layer 2 Tunneling Protocol (L2TP) session across the network.
- For each network element, view the relevant parameters for each interface on all layers along the path.

The Layer 3 tab displays the peer name for L2TP tunnels.

Table 13-3 describes the information that is displayed in the Layer 2 tab for L2TP tunnels.

Table 13-3 Layer 2 Tab Information for L2TP Tunnels

Field	Description
Encapsulation Type	Encapsulation type, such as Point-to-Point Protocol over ATM (PPPoA).
Binding Information	Name of the subscriber.
Binding Status	Binding status: bound or unbound.
Tunnel Session Count	Number of current sessions.

Table 13-3 Layer 2 Tab Information for L2TP Tunnels (continued)

Field	Description
Tunnel Remote ID	Remote tunnel identifier.
Tunnel ID	Local tunnel identifier.
Tunnel Name	Name of the subscriber and the tunnel identifier.
Session ID	Session identifier.
Traffic > L2TPSession Counters	Number of ingress traffic packets passing through the L2TP tunnel.
Traffic < L2TPSessionCounters	Number of egress traffic packets passing through the L2TP tunnel.
Tunnel Ctl Errors	Number of control errors.
Tunnel State	Tunnel state: unknown, idle, connecting, established, or disconnecting.
Session Type	Session type: unknown, LAC, or LNS.
Peer Name	Peer name.
Tunnel Remote IP	Remote IP address of the tunnel.
Last Error Code	Value of the last error code that caused the tunnel disconnection.
Session State	Session state: unknown, idle, connecting, established, or disconnecting.
Remote Session ID	Remote session identifier.

Using Cisco PathTracer in MPLS Networks

You can open and view Cisco PathTracer information between service endpoints, such as an IP interface that is attached to the VRF over an MPLS network. The LSP in the MPLS network is found according to the cross-connect table of each router.

Note An LSP can be traced and displayed by Cisco PathTracer as part of an end-to-end tracing of a service; for example, when viewing a path between one CE device and another. Cisco PathTracer traces the path that goes over circuits or VLANs in the access networks. It also traces the LSPs between the VRFs going through all intermediate devices such as CE devices, aggregation switches, PE routers, and core routers.

To view a specific path, you must specify an initial starting point, such as an IP interface; specifying a destination IP address is optional. If the traced path (for example, a VC or VLAN) ends in a router, Cisco PathTracer finds the next hop according to the destination IP address. If you select an endpoint, Cisco PathTracer extracts the relevant IP address from this point and uses it as the destination.

The following topics provide more information on using Cisco PathTracer in MPLS networks:

- Cisco PathTracer MPLS Start and Endpoints, page 13-21
- Using Cisco PathTracer for CSC Configurations, page 13-22
- Using Cisco PathTracer for Layer 3 VPNs, page 13-22
- Using Cisco PathTracer for Layer 2 VPNs, page 13-23
- Using Cisco PathTracer for MPLS TE Tunnels, page 13-24

Cisco PathTracer MPLS Start and Endpoints

You can open Cisco PathTracer by right-clicking a starting point and entering the required destination IP address. Table 13-4 lists the Cisco PathTracer starting points.

Table 13-4 Cisco PathTracer MPLS Starting Points

Element	Location	Start Options
IP interface	• Inventory window • Affected entity (enabled only if the affected entity has an IP interface)	• From Here to Destination • Start Here
MPLS-TP tunnel endpoint	• Navigation or map pane • Inventory window	• From Here to Destination • Start Here
Site	Service view map	• From Here to Destination • To Subnet Destination • Start Here
Business tag attached to the VPI/VCI or IP interface	The path can be found using a business tag, which is attached to the VPI/VCI or IP interface by entering its key. It can then be opened from the Find Business Tag window.	From Here to Destination
Layer 2 MPLS Tunnel	Inventory window	From Here to Destination

If you choose the Start Here option, Table 13-5 lists the endpoints that can be selected as path destinations.

Table 13-5 Cisco PathTracer MPLS Endpoints

Element	Location	End Options
IP interface	• Inventory window • Affected entity (enabled only if the affected entity has an IP interface)	End Here
MPLS-TP tunnel endpoint	Inventory window	End Here
Site	Service view map	End Here

The Cisco PathTracer window is displayed. From this window you can open the Cisco PathTracer details window with the VPN information displayed in the Layer 2 and Layer 3 tabs.

Note If multiple paths are selected in the paths pane, or if nothing is selected in the paths pane, all available paths are opened automatically, and each is displayed in a separate Cisco PathTracer window.

Using Cisco PathTracer for CSC Configurations

Cisco PathTracer traces a CSC flow from the customer CE through the customer carrier VPN, across the customer backbone carrier VPN, back to the customer carrier VPN, and to the destination CE.

To launch a path trace for a CSC configuration:

Step 1 In a map, double-click the required CE device.

Step 2 In the **Inventory** window, choose **Logical Inventory > Routing Entities > Routing Entity**.

Step 3 In the IP Interfaces table, right-click the required interface and choose **PathTracer > Start Here >** *IPvn* where *IPvn* represents IPv4 or IPv6.

Step 4 Navigate to the destination CE device and double-click it.

Step 5 In the **Inventory** window, choose **Logical Inventory > Routing Entities > Routing Entity**.

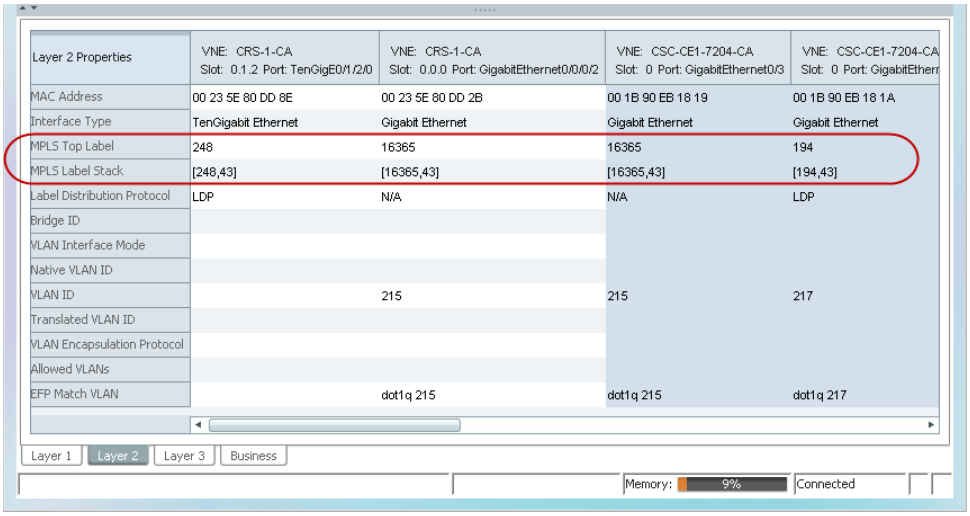
Step 6 In the IP Interfaces table, right-click the required interface and choose **PathTracer > End Here**.

The path trace is displayed in the Cisco PathTracer window.

Step 7 To view the detailed pane, click Cisco PathTracer in the toolbar.

The Layer 2 tab displays a single outer label and two inner labels for each interface, reflecting the CSC configuration. (See Figure 13-11.)

Figure 13-11 CSC Configuration Path Trace



Using Cisco PathTracer for Layer 3 VPNs

Cisco PathTracer uses VRF routing and label switching information to trace the path from one VRF interface to another. If you choose a launch point and destination from the right-click menu, you can open the Cisco PathTracer for Layer 3 VPNs. The Cisco PathTracer window shows the VPN topology map. From this window, you can open the Cisco PathTracer details window with the appropriate VPN information displayed in the Layer 2 and Layer 3 tabs.

For Layer 3 path information, Prime Network uses VRF routing and label switching information to trace the path from one VRF interface to another. Layer 3 path trace information is displayed in the Cisco PathTracer window when the path goes over connections and ends in VRFs.

If a VRF table includes more than one path toward a destination, Cisco PathTracer shows all paths.

To view Layer 3 path information, choose the **Layer 3** tab and choose **Show All** from the View menu. The path information is displayed in the active tab.

The table displays the Layer 3 VPN information on the device that has a VRF. The following Layer 3 properties displayed in the Layer 3 tab relate specifically to VPNs:

- Name—The name of the site. For example, ATM4/0.100(10.0.0.1) is a combination of the interface name and IP address used to reach the site. Each site belongs to a particular VPN, so the address must be unique within the VPN.
- IP Address—The IP address of the interface.
- Mask—The mask of the specific network.
- State—The state of the interface (up or down).
- VRF Name—The name of the VRF.

Cisco PathTracer does not display or trace EXP bits for Layer 3 VPNs that use policy-based tunnel selection (PBTS).

Using Cisco PathTracer for Layer 2 VPNs

Cisco PathTracer uses VC ID and label switching information to trace the path from one tunnel interface to another over the MPLS network.

Cisco PathTracer also covers end-to-end Layer 2 VPN service paths from one CE router to another. The path goes over circuits (such as a VC) or VLANs in access networks and over LSP between the Layer 2 tunnel edge.

The Cisco PathTracer window shows the VPN topology map for the relevant devices and links. From this window, you can open the Cisco PathTracer details window with the appropriate VPN information displayed in the Layer 2 and Layer 3 tabs.

For Layer 2 path information, Cisco PathTracer uses VC ID, AGI, SAII, TAII, and label switching information to trace the path from one tunnel interface to another. Layer 2 path trace information is displayed in the Cisco PathTracer window when the path goes over pseudowire tunnels.

To view Layer 2 path information, choose the **Layer 2** tab and then **View > Show All**. The path information is displayed in the active tab.

Table 13-6 describes the Layer 2 properties that can be displayed in the Layer 2 tab specifically for VPNs.

Table 13-6 Cisco PathTracer Layer 2 Properties for VPNs

Field	Description
Top Label	Details of the outer MPLS label.
Label Stack	Details of the inner MPLS label.
MAC Address	MAC address.
Tunnel ID	Tunnel identifier. The identifier and the router IP address of the two tunnel edges identify the pseudowire tunnel.

Table 13-6 Cisco PathTracer Layer 2 Properties for VPNs (continued)

Field	Description
Tunnel Type	Tunnel type: • 0—Unknown • 1—PWE3 • 2—TE
Tunnel Status	Operational state of the tunnel: Up or Down.
Tunnel Local VC Label	MPLS label that is used by the router to identify or access the tunnel. It is inserted in the MPLS label stack by the local router.
Tunnel Peer VC Label	MPLS label that is used by the router to identify or access the tunnel. It is inserted in the MPLS label stack by the peer router.
Tunnel Local Router IP	IP address of the tunnel edge, which is used as the MPLS router identifier.
Tunnel Peer Router IP	IP address of the peer tunnel edge, which is used as the MPLS router identifier.
Distribution Protocol Type	Protocol used by MPLS to build the tunnel, such as LDP or TDP.
Peer OID	Tunnel identifier and device name.

Using Cisco PathTracer for MPLS TE Tunnels

Cisco PathTracer uses label switching information to trace the end-to-end path of a TE tunnel path from one PE router to another.

Using MPLS TE technology, Cisco PathTracer enables you to:

- View a path or list of devices.
- View the following information for each network element:
  - The relevant parameters for each interface on all layers along the path.
  - The path for the defined MPLS TE-LSP across the network.

The Cisco PathTracer window is displayed showing the MPLS TE tunnel topology map. From this window, you can open the Cisco PathTracer details window with the appropriate MPLS TE tunnel information displayed in the Layer 2 tab.

Note Cisco PathTracer does not display or trace EXP bits for Layer 3 VPNs that use PBTS.

Layer 2 and Layer 3 path trace information is displayed in the Cisco PathTracer details window when a path is traced over MPLS TE tunnels. To view Layer 2 path information, choose the **Layer 2** tab and then **View > Show All**. The path information is displayed in the active tab.

Table 13-7 describes the Layer 2 properties that can be displayed in the Layer 2 tab specifically for MPLS TE tunnels.

Table 13-7 Cisco PathTracer Layer 2 Properties for MPLS TE Tunnels

Field	Description
MPLS TE Properties	MPLS TE data set in an MPLS interface, primarily bandwidth allocation levels and signaling protocol.
Tunnel Oper Status	Operational status of the tunnel: Up or Down. If this value is Up, the Tunnel Admin Status must also be Up. See Tunnel Admin Status properties for additional information.
Tunnel Bandwidth Kbps	Configured bandwidth (in Kb/s) for the tunnel.
Tunnel Description	Description of the tunnel.
Tunnel Name	Interface name.
Tunnel Admin Status	Administrative status of the tunnel (Up or Down) with the following caveats: • If the Tunnel Oper Status value is Up, the Tunnel Admin Status value must also be Up. • If the Tunnel Admin Status value is Down, the Tunnel Oper Status value must also be Down.
Tunnel Lockdown	Whether or not the tunnel can be rerouted: • Enabled—The tunnel cannot be rerouted. • Disabled—The tunnel can be rerouted.
Tunnel LSP ID	LSP identifier.
Tunnel Auto Route	Whether or not destinations behind the tunnel are routed through the tunnel: Enabled or disabled.
Tunnel Hold Priority	Tunnel priority after path setup.
Tunnel Setup Priority	Tunnel priority upon path setup.
Tunnel Path Option	Tunnel path option: • Dynamic—The tunnel is routed along the ordinary routing decisions after taking into account the tunnel constraints such as attributes, priority, and bandwidth. • Explicit—The route is explicitly mapped with the included and excluded links.
Tunnel Out Label	TE tunnel MPLS label distinguishing the LSP selection in the adjacent device.
Tunnel Affinity	Tunnel's preferential bits for specific links.
Tunnel Destination Address	IP address of the device in which the tunnel ends.
Tunnel Peak Rate Kbps	Peak flow specification (in Kb/s) for this tunnel.
Tunnel Out Interface	Interface through which the tunnel exits the device.
Tunnel Burst Kbps	Burst flow specification (in Kb/s) for this tunnel.

Table 13-7 Cisco PathTracer Layer 2 Properties for MPLS TE Tunnels (continued)

Field	Description
Tunnel Average Rate Kbps	Tunnel average rate in Kb/s.
Tunnel Affinity Mask	Tunnel affinity bits that should be compared to the link attribute bits.

Managing IP Address Pools

An IP pool is a sequential range of IP addresses within a certain network. You can have multiple pool configurations. Each pool can have a priority and can be assigned to a group.

IP addresses can be assigned dynamically from a single pool or from a group of pools. The Least Recently Used (LRU) method is used to assign IP addresses. In each pool, the addresses are placed in a queue. At the time of assigning, the address at the head of the queue is assigned, and when released is placed at the end of the queue.

When a group of pools have the same priority, an algorithm is used to determine a probability for each pool based on the number of available addresses. A pool is selected based on the probability determined. This method allocates addresses evenly from the group of pools.

IP pool supports both IPv4 and IPv6 addresses. With the IP Pool feature, Prime Network provides the flexibility of assigning IP addresses dynamically for services running on a network element. A service running on a network element can refer to an appropriate IP pool and an IP address gets assigned to the service from the IP pool.

These topics describe how to use the Vision client to view and manage IP pools. If you cannot perform an operation that is described in these topics, you may not have sufficient permissions; see Appendix B, "Permissions Required to Perform Tasks Using the Prime Network Clients".

Viewing the IP Pool Properties

To view the IP pool properties for a device:

Step 1 In the Vision client, right-click the required device, and choose **Inventory**.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **IP Pools**. A list of IP pools are displayed in the content pane.

Table 14-1 describes the fields that are displayed in the content pane.

Table 14-1 IP Pool Properties

Field Name	Description
Table Types	Displays the type of table, which is **IP Pools**.
IP Pools	

Table 14-1 IP Pool Properties

Field Name	Description
Name	Name of the IP pool.
IP Pool Entries	Indicates whether entries exist for this pool.

Step 3 Right-click the IP pool name and choose **Properties**. The IP Pool Properties dialog box is displayed as shown in Figure 14-1.

Figure 14-1 IP Pool Properties

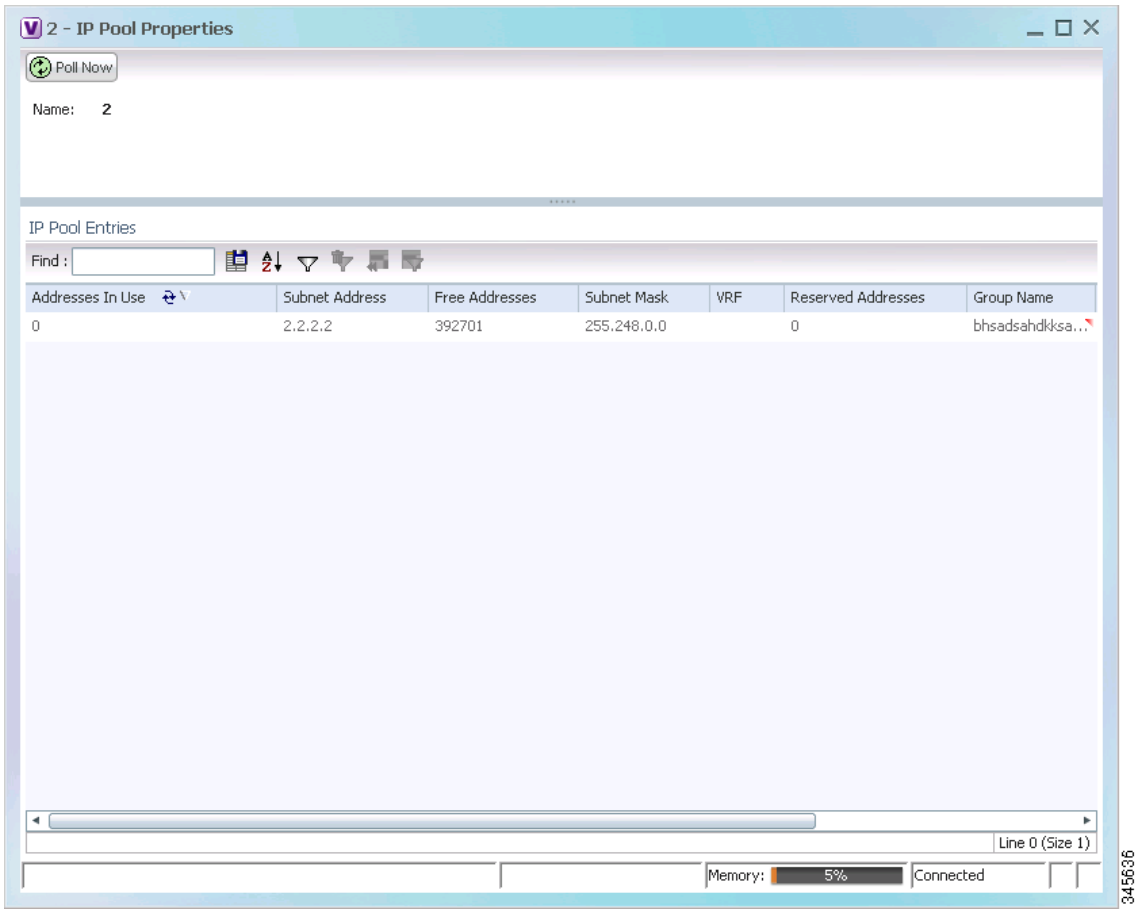


Table 14-2 describes the fields that are displayed in the IP Pool Properties dialog box.

Table 14-2 IP Pool Properties

Field Name	Description
Name	Name of the IP pool.
IP Pool Entries	
Addresses In Use	Number of IP addresses assigned from the pool.
Start Address/Subnet Address	Could be one of the following: • Starting IP address in the pool, if the pool is configured with a range. • Subnet address, if the pool is configured with a subnet mask.
Free Addresses	Number of free addresses available in the pool.
End Address/Subnet Mask	Could be one of the following: • Ending IP address in the pool, if the pool is configured with a range. • Subnet mask, if the pool is configured with a subnet mask.
VRF	Virtual Routing and Forwarding (VRF) name, if the pool belongs to a VRF.
Reserved Addresses	Number of reserved addresses in the pool.
Group Name	Name of the group to which the pool belongs.
Pool Status	Status of the pool.
Pool Type	Type of the pool, which could be Public, Private, Static, Resource, or NAT.
Pool Priority	Priority of the pool, which is used when multiple pools are available.

Modifying and Deleting IP Pools

The following commands can be launched from the inventory by right-clicking on an IP pool name and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see Appendix B, "Permissions Required to Perform Tasks Using the Prime Network Clients"). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Navigation	Description
Delete IP Pool	*Right-click on IP Pool name* > **Commands** > **Configuration**	Use this command to delete an IP Pool
Modify IP Pool		Use this command to modify IP Pool details.

Monitoring AAA Configurations

AAA refers to Authentication, Authorization, and Accounting, which is a security architecture for distributed systems that determines the access given to users for specific services and the amount of resources they have used.

- Authentication—This method identifies users, including their login and password, challenge and response, messaging support, and encryption. Authentication is the way to identify a subscriber before providing access to the network and network services.
- Authorization—This method provides access control, including authorization for a subscriber or domain profile. AAA authorization sends a set of attributes to the service describing the services that the user can access. These attributes determine the user's actual capabilities and restrictions.
- Accounting—This method collects and sends subscriber usage and access information used for billing, auditing, and reporting. For example, user identities, start and stop times, performed actions, number of packets, and number of bytes. Accounting enables an operator to analyze the services that the users access as well as the amount of network resources they consume. Accounting records comprise accounting Attribute Value Pairs (AVPs) and are stored on the accounting server. This accounting information can then be analyzed for network management, client billing, and/or auditing.

These topics describe how to use the Vision client to view and manage AAA configurations. If you cannot perform an operation that is described in these topics, you may not have sufficient permissions; see Permissions for Managing AAA, page B-21.

Supported AAA Network Protocols

AAA supports the following protocols:

- Diameter—This is a networking protocol that provides centralized AAA management for devices to connect and use a network service, and an alternative to RADIUS. Diameter Applications can extend the base protocol, by adding new commands and/or attributes.
- Remote Authentication Dial In User Service (RADIUS)—This is a networking protocol that provides centralized AAA management for devices to connect and use a network service. RADIUS is a client/server protocol that runs in the application layer, using UDP as transport. The Remote

Access Server (RAS), the Virtual Private Network (VPN) server, the network switch with port-based authentication, and the Network Access Server (NAS), are all gateways that control access to the network, and all have a RADIUS client component that communicates with the RADIUS server.

- Terminal Access Controller Access Control System (TACACS) is an authentication program used on Unix and Linux based systems, along with certain network routers. TACACS allows a remote access server to communicate with an authentication server to determine whether or not a user has the proper rights to access a network or database. TACACS forwards username and password information to a centralized security server.
- TACACS+ is a networking protocol that provides centralized AAA management for devices to connect and use a network service. Derived from TACACS, TACACS+ provides for separate and modular AAA facilities and uses TCP as transport.

Viewing AAA Configurations

This topic contains the following sections:

For information on the devices that support AAA, refer to *Cisco Prime Network 5.0 Supported VNEs*.

Viewing AAA Group Profile

To view the AAA group profile:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **AAA**. The AAA attribute details are displayed in the content pane. (The attributes that are displayed depend on the device type.)

Table 15-1 describes the fields that are displayed in the content pane.

Table 15-1 AAA Attributes

Field Name	Description
Type	Customization applied to the attribute.
Key	Unique format name applied to the attribute.
Value	Formatting applied to the attribute.

Step 3 In the **Inventory** window, choose **AAA group** node under the AAA node. In the Content pane you can view the AAA method in the **Group Type** field. The group Type displayed are None, TACACS+, RADIUS, or DIAMETER for the existing device types.

Step 4 Under the **AAA group** node, select and expand the required group and choose the **Radius Configuration** option. The group details are displayed in the content pane.

Table 15-2 describes the fields that are displayed in the Radius Configuration dialog box.

Table 15-2 Radius Configuration Details

Field Name	Description
Load Balancing Method	The load balancing method.
Ignore Preferred Server	Indicates if a transaction associated with a single AAA session should attempt to use the same server or not.
Dead Time	The deadtime for the profile.

Viewing a Dynamic Authorization Profile

To view the dynamic authorization profile:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **AAA** > **Dynamic Authorization**. The authorization details are displayed in the content pane. You can click on the tabs to view more details. (The attributes that are displayed depend on the device type.)

Table 15-3 describes the fields that are displayed in the Dynamic authorization content pane.

Table 15-3 Dynamic Authorization Details

Field Name	Description
Protocol	The name of the protocol.
Server Listen Port	The port number that receives service requests.
Ignore Server Key	Indicates whether the server key must be ignored. Values are: • true • false
CoA Clients Tab	
IP Address	The IP address of the Change of Authorization (CoA) client.
VRF	The associated VRF to which the CoA client belongs. Click the hyperlink to view the relevant node under the VRF node.

Viewing a Dynamic Dictionary

To view the dynamic dictionary:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **local** > **AAA** > AAA **Dynamic Dictionaries** > *Context*. The dynamic dictionary VID details are displayed in the content pane.

Table 15-4 describes the fields that are displayed in the Dynamic dictionary content pane.

Table 15-4 Dynamic Dictionary Details

Field Name	Description
Dynamic Dictionary Name	The name of the configured diameter dynamic dictionary.
Base Static Dictionary	The static dictionary number and name from which the dynamic dictionary is derived.
AAA Dynamic Dictionary VID Entries	
Vid	The vendor ID.

Viewing a Radius Global Configuration Details

To view the radius global configuration details:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **AAA** > **Radius Global Configuration**. The authorization details are displayed in the content pane. (The attributes that are displayed depend on the device type.)

Table 15-5 describes the fields that are displayed in the Radius global configuration content pane.

Table 15-5 Radius Global Configuration Details

Field Name	Description
Load Balancing Method	The load balancing method using which the next host is selected. The server with the least transactions outstanding is generally picked as the next host.
Ignored Preferred Server	Indicates if a transaction associated with a single AAA session should attempt to use the same server or not.
Request Timeout	The request timeout value for the device.
Dead Time	The amount of time (in minutes) after which the dead RADIUS server will be treated as active.
Retransmit	Indicates whether retransmission of data is allowed.
Retransmit Count	The retransmission count.
Dead Criteria Time	The time interval after which the device is considered unavailable.
Dead Criteria Retransmit Count	The retransmission count after the dead criteria time.
Accounting Servers/ Authentication Servers	
Server IP	The IP address of the server.
Server Port	The server port.
Preference	The preferred server.
Operational State	The current operational state of the interface.
Administrative Status	The administrative status of the interface.
Retain Administrative Status After Reboot	Indicates whether the administrative status must be retained after the system reboots.
Keepalive Representative Group	The keepalive representative group.
Request Timeout	The request timeout value for the device.
Retransmit Count	The retransmission count.

Viewing TACACS+ Global Configuration Details

To view the TACACS+ global configuration details:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **AAA** > **TACACS+ Global Configuration**. The configuration details are displayed in the content pane. (The attributes that are displayed depend on the device type.)

Table 15-6 describes the fields that are displayed in the TACACS+ global configuration content pane.

Table 15-6 TACACS+ Global Configuration Details

Field Name	Description
Source Interface	Specifies that the IP address of this specified interface is used for all outgoing TACACS+ packets.
VRF	The VRF for the specified source interface configuration.
Timeout	Specifies the time to wait for the TACACS+ server to reply in seconds.
IPv4 DSCP	Specifies the IPv4 Differentiated Services Code Point (DSCP) to be used in the outgoing IP headers.
IPv6 DSCP	Specifies the IPv6 Differentiated Services Code Point (DSCP) to be used in the outgoing IP headers.
Administration	Specifies if the handling of administrative messages by the TACACS+ daemon is enabled.
Allow Unknown Attribute	Specifies if unknown TACACS+ attributes are ignored instead of trying to parse them.
Packet Max Size	Specifies the maximum size of TACACS+ packets.
DNS Alias Lookup	Specifies if IP Domain Name System (DNS) alias lookup is enabled for TACACS+ servers.
Cache Expiry Time	Specifies the length of time, in hours, for a cache database profile entry to expire.
Cache Expiry Rule	Specifies how the expired cached database profile entries in this TACACS+ server group are to be used: • Enforce—Indicates not to use expired entries. • Failover—Indicates to use an expired entry if all other methods fail.
Cache Authentication Profile Name	The name of the cache authentication profile used in this TACACS+ server group.
Cache Authorization Profile Name	The name of the cache authentication profile used in this TACACS+ server group.
Directed Request	Specifies if only the username (and not the entire string) is sent to an AAA TACACS+ server.
Directed Request <Restricted>	Specifies that queries are restricted to directed request servers only.
Directed Request <No-Truncate>	Specifies '@hostname' is not truncated from the username.
Domain Stripping	
Right-to-Left	Specifies that the stripping configuration at the first delimiter found when parsing the full username from right to left will be applied.
Prefix Delimiter	Specifies that the prefix stripping is enabled and the specified character(s) are to be recognized as a prefix delimiter(s).
Suffix Delimiter	Specifies the character(s) that are to be recognized as a suffix delimiter.
Strip Suffix	Specifies the suffix to strip from the username.
VRF	Specifies the VRF that the domain stripping configuration is applicable to.

Viewing TACACS+ Servers Configuration Details

To view the TACACS+ Servers configuration details:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **AAA** > **TACACS+ Servers**. The configuration details for each TACACS+ server are displayed in the content pane. (The attributes that are displayed depend on the device type.)

Table 15-7 describes the fields that are displayed in the TACACS+ Servers configuration content pane.

Table 15-7 TACACS+ Servers Configuration Details

Field Name	Description
Server Address	The IP address or host name of the TACACS+ server.
Port	The TCP port used to communicate with the TACACS+ server.
Server Name	The name of the TACACS+ server.
Status	Specifies the operational state of the interface with the TACACS+ server.
Visibility	Specifies whether a TACACS+ server is public or private within the scope of an AAA group server.
Timeout	Specifies the time to wait for the TACACS+ server to reply in seconds.
Single Connection	Specifies whether all requests to a TACACS+ server are multiplexed over a single TCP connection to server (for CiscoSecure).
Send NAT Address	Specifies whether a client's post NAT address is sent to the TACACS+ server.

Viewing AAA Group Configuration Details

For certain devices, the Vision client allows you to view the following configurations for an AAA group:

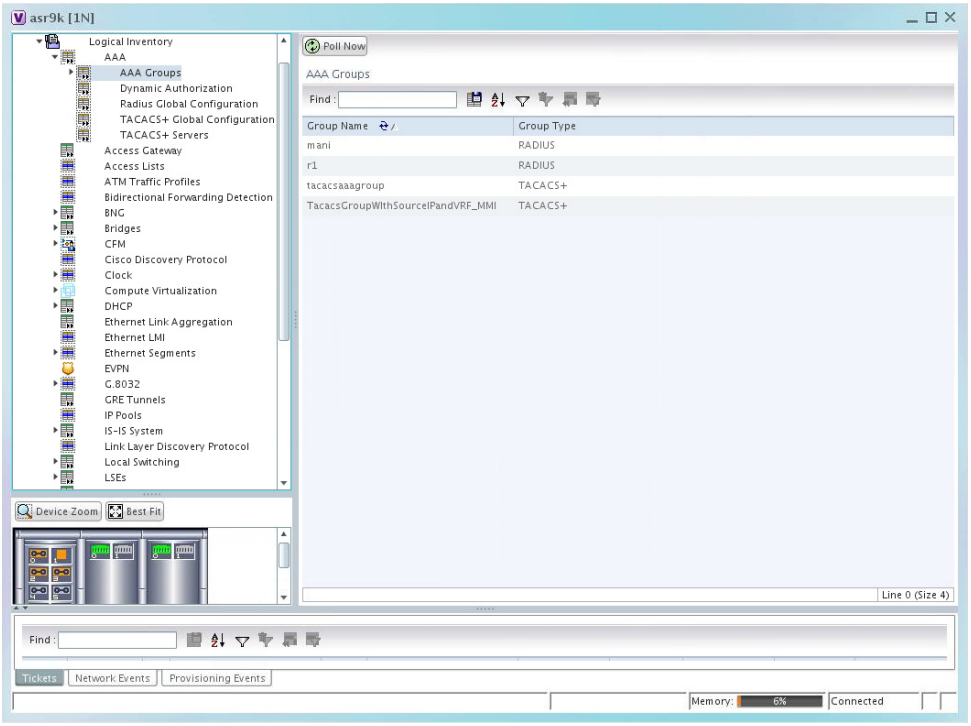
- Diameter Configuration
  - Accounting Configuration
  - Authentication Configuration
- Radius Configuration
  - Accounting Configuration
  - Accounting Keepalive and Detect Dead Server Configuration
  - Authentication Configuration
  - Authentication Keepalive and Detect Dead Server Configuration
  - Charging Configuration

  - Charging Triggers
- TACACS+ Configuration

(Refer to *Cisco Prime Network 5.0 Supported VNEs* for more information.)

The Vision client displays the AAA configuration details under the AAA container as shown in Figure 15-1. You can view the individual AAA group details by choosing **Logical Inventory** > *Context* > **AAA** > **AAA Groups**.

Figure 15-1 AAA Groups in Logical Inventory



Viewing Diameter Configuration Details for an AAA Group

To view the diameter configuration details for a AAA group:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Groups**.

You can view the AAA groups on the content pane.

Step 3 Choose **Diameter Configuration** under a specific AAA group node. The diameter configurations made for accounting servers and authentication servers are displayed in the respective tabs on the content pane. Click on the tabs to view more details.

Table 15-8 describes the diameter configuration details for accounting and authentication servers.

Table 15-8 Diameter Configuration

Field Name	Description
Accounting Servers/Authentication Servers	
Server Host	Host name of the diameter authentication/accounting server.
Priority	Relative priority of the diameter authentication/accounting server.
Number of Instances in Up State	Number of instances between the diameter authentication/accounting server and the AAA manager that are in UP status.
Number of Instances in Down State	Number of instances between the diameter authentication/accounting server and the AAA manager that are in DOWN status.

Step 4 In the **Inventory** window, choose **Accounting Configuration** or **Authentication Configuration** under the **Diameter Configuration** node. The configuration details are displayed on the content pane.

Table 15-9 describes the accounting/authentication diameter configuration details.

Table 15-9 Accounting/Authentication Diameter Configuration

Field Name	Description
Dictionary	Diameter dictionary used for accounting/authentication.
Endpoint Name	Diameter endpoint used for accounting/authentication.
Maximum Transmissions	Maximum number of transmission attempts for diameter accounting/authentication.
Maximum Retries	Number of retry attempts for diameter accounting/authentication requests.
Request Timeout	Diameter accounting/authentication request timeout period.
Redirect Host AVP	Indicates whether to use: • one returned AVP • the first returned AVP as the primary host and the second returned AVP as the secondary host. This field is applicable only for Authentication configuration.
Upgrade -dict-avps	Sets the release version to 3GPP Rel.8 for upgrading diameter accounting dictionary in the current AAA group.

Table 15-9 Accounting/Authentication Diameter Configuration

Field Name	Description
HD-mode	Sends records to the Diameter server. If all Diameter servers are down or unreachable, then periodically retries the diameter service.
HD-Policy	Associates a specific HD storage policy with a AAA group.
Supported Features	Disables the CLI command and does not send supported features AVP.
Active Start Trigger	Enables an R-P event when an active start trigger is received from the PCF and there is a parameter change.
Active Stop Trigger	Enables an R-P event when an active stop trigger is received from the PCF.
AirlinkUsage Counter Rollover	The AirlinkUsage RADIUS accounting policy for R-P.
Stop Start Trigger	Indicates that a stop or start RADIUS accounting pair is sent to the RADIUS server at the time of R-P event occurrence.
Active Handoff Trigger	Enables a single R-P event when an active PCF-to-PCF handoff occurs.
Trigger Policy	Designates to use a custom RADIUS accounting policy for R-P. You can specify parameters to form custom accounting policy. By default, all optional parameters are disabled
Handoff Policy	Specifies the behavior of generating accounting STOP when handoff occurs.
MIP HA Policy	The RADIUS accounting policy for Mobile IP HA calls.
TOD Values	
TOD Minutes/Hours	A time of day at which an R-P event should occur. **Note** Up to four time of day events are displayed,

Viewing Radius Configuration Details for an AAA Group

To view the radius configuration details for an AAA group:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration**. The configurations made for accounting, authentication, charging, and charging accounting servers are displayed in the respective tabs on the content pane. Click on the tabs to view more details.

Table 15-10 describes the radius configuration details for accounting, authentication, charging, and charging accounting servers.

Table 15-10 Radius Configuration

Field Name	Description
Dictionary	The radius dictionary.
Strip Domain	Indicates whether the domain must be stripped from the user name prior to authentication or accounting.
Authenticator Validation	Indicates whether the MD5 authentication of the user is enabled or disabled.
Allow Server Down Authentication	Indicates whether subscriber sessions are allowed when RADIUS authentication is unavailable.
Allow Server Down Accounting	Indicates whether subscriber sessions are allowed when RADIUS accounting is unavailable.
Accounting Servers/Authentication Servers/Charging Servers/Charging Accounting Servers	
Server Name	IP address of the RADIUS server.
Server Port	Port used to communicate with the RADIUS server.
Preference	Preference of the RADIUS server.
Operational State	Status of the RADIUS server.
Administrative Status	Administrative status of the RADIUS server.
Retain Administrative Status after Reboot	Indicates whether the administrative status must be retained when the system reboots.
Keepalive Representative Group	Name of the Keepalive representative group.

Viewing Radius Client Configuration Details for an AAA Group

To view the radius configuration details for an AAA group:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Groups** > *AAA Group* > **Default** > **AAA Radius Client Configuration**. The configurations made for accounting, authentication, charging, and charging accounting servers are displayed in the respective tabs on the content pane. Click on the tabs to view more details.

Table 15-11 describes the radius client configuration details for accounting, authentication, charging, and charging accounting servers.

Table 15-11 Radius Client Configuration

Field Name	Description
Radius Client Status	The status of the RADIUS client: Up or Down.
Active NAS IP Address	The NAS IP address configured to the client that is currently active.
Configured Primary NAS IP Address	The NAS IP address configured as the primary IP address to the RADIUS client.
Primary IP Address Interface State	The status of the interface to which the primary NAS IP address is configured: Up or down.
Configured Backup NAS IP Address	The NAS IP address configured as the secondary or backup IP address to the RADIUS client.
Secondary IP Address Interface State	The status of the interface to which the secondary or backup NAS IP address is configured: Up or down.

Viewing Radius Accounting Configuration Details for an AAA Group

To view the radius accounting configuration details for an AAA group:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Accounting Configuration**. The accounting configuration details are displayed in the content pane.

Table 15-12 describes the radius accounting configuration details.

Table 15-12 Radius Accounting Configuration

Field Name	Description
Server Selection Algorithm	The algorithm to select the RADIUS accounting server(s) to which accounting data must be sent. Values are: • first-n n Default • first-server • round-robin
Billing Version	The billing system version of RADIUS accounting servers.
Server Deadtime	The number of minutes after which communication must be attempted with a server that is not reachable.
Maximum Outstanding Messages	The maximum number of outstanding messages that can be queued with the AAA manager.
Fire and Forget	Indicates whether RADIUS Fire-and-Forget accounting is enabled for the AAA group.
Maximum Transmissions	The maximum number of transmissions attempted for a RADIUS accounting message, before it is declared FAILED.
Maximum Retries	The maximum number of attempts with the AAA server, before it is declared Not Responding and the detected dead server's consecutive failures count is incremented.
Maximum PDU Size (Bytes)	The maximum packet data unit size, in bytes, that can be accepted or generated.
Response Timeout	The time period, in seconds, to wait for a response from the RADIUS server, before resending the message.
Remote Address	Indicates whether the remote IP address lists are configured and the collection of accounting data for the addresses in these lists are enabled.
Archive Messages	Indicates whether archiving of the RADIUS accounting messages in the system (after retries to all available RADIUS accounting servers) is enabled.
APN To Be Included	The Access Point Name (APN) associated with the RADIUS accounting.
Interim Interval	The time interval (in seconds) between sending interim accounting records.
GTP Trigger Policy	The downlink volume that triggers interim RADIUS accounting.

Viewing the Radius Keepalive and Detect Dead Server Configuration Details for an AAA Group

To view the radius accounting/authentication Keepalive and Detect Dead Server Configuration details:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Accounting Keepalive and Detect Dead Server Configuration** or **Authentication Keepalive and Detect Dead Server Configuration**. The configuration details are displayed in the content pane.

Table 15-13 describes the radius accounting keepalive and detect dead server configuration details.

Table 15-13 Radius Accounting Keepalive and Detect Dead Server Configuration details

Field Name	Description
Keepalive Interval	The time interval (in seconds) between two keepalive access requests.
Keepalive Timeout	The time period to wait for a response from the RADIUS server, before resending the message. This value is displayed in seconds.
KeepAlive Maximum Retries	The maximum number of keepalive access requests to be sent, before the server is declared as not reachable.
Keepalive Consecutive Response	The number of consecutive accounting responses after which the server is declared as reachable.
Username	The accounting user name.
Calling Station ID	The calling station ID to be used for keepalive accounting.
Keepalive Password	The password to be used for authentication. This field is available only for authentication configuration.
Keepalive Allow Access Reject	Indicates the valid response for authentication request. This field is available only for authentication configuration.
Detect Dead Server Consecutive Failures	The number of consecutive failures for an AAA manager, before the status of an accounting server is changed from Active to Down.
Detect Dead Server KeepAlive	The number of seconds to wait for a response to any message, before the status of an accounting server is changed from Active to Down.

Viewing the RADIUS Attributes Configuration Details for an AAA Group

To view the radius attributes configuration details:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Attributes Configuration**. The configuration details are displayed in the content pane.

Table 15-14 describes the attributes configuration details.

Table 15-14 Radius Attributes Configuration details

Field Name	Description
NAS identifier	The AAA interface IP address used to identify the system.
Next HOP	Attribute name by which the system is identified in access request messages.
Backup NAS IP Address	The NAS IP address configured as the secondary or backup IP address to the RADIUS client.
Next HOP	The next hop IP address for the NAS IP address.
Input MPLS Label	Specifies the System's AAA MPLS input label.
Output MPLS Label	Specifies the system's AAA MPLS output label.

Viewing the RADIUS Accounting Attributes Configuration Details for an AAA Group

To view the RADIUS accounting attributes configuration details:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Groups** > *AAA Group* > **Radius Configuration** > **Accounting Attributes Configuration**. The configuration details are displayed in the content pane.

Table 15-15 describes the attributes configuration details.

Table 15-15 RADIUS Accounting Attributes Configuration details

Field Name	Description
NAS IP Address	Indicates whether RADIUS accounting attribute for NAS IP Address is enabled.
NAS Identifier	Indicates whether RADIUS accounting attribute for NAS Identifier is enabled.
IMSI	Indicates whether RADIUS accounting attribute for IMSI is enabled.
Service Type	Indicates whether RADIUS accounting attribute for service type is enabled.
Framed IP Address	Indicates whether RADIUS accounting attribute for Framed IP Address is enabled.
Framed IPv6 Prefix	Indicates whether RADIUS accounting attribute for Framed IPv6 Prefix is enabled.
Called Station ID	Indicates whether RADIUS authentication attribute for called station id is enabled.
Calling Station ID	Indicates whether RADIUS authentication attribute for calling station id is enabled.
User Name	Indicates enabled status for - name of the user being authenticated by the RADIUS server.
Class	Indicates whether RADIUS accounting attribute for class is enabled.
NAS Port ID	Indicates whether RADIUS accounting attribute for NAS Port ID is enabled.
Nas Port Type	Indicates whether RADIUS accounting attribute for NAS Port Type is enabled.
3GPP PDP Type	Indicates whether RADIUS accounting attribute for 3GPP PDP type is enabled.
3GPP CG Address	Indicates whether RADIUS accounting attribute for 3GPP CG address is enabled.
3GPP GPRS QoS Negotiated Profile	Indicates whether RADIUS accounting attribute for 3GPP GPRS QoS negotiated profile is enabled.
3GPP SGSN Address	Indicates whether RADIUS accounting attribute for 3GPP SGSN address is enabled.
3GPP GGSN Address	Indicates whether RADIUS accounting attribute for 3GPP GGSN address is enabled.
3GPP GGSN MCC MNC	Indicates whether RADIUS accounting attribute for 3GPP GGSN MCC MNC is enabled.
3GPP IMSI MCC MNC	Indicates whether RADIUS accounting attribute for 3GPP select mode is enabled.
3GPP Select Mode	Indicates whether RADIUS accounting attribute for 3GPP NSAPI is enabled.
3GPP NSAPI	Indicates whether RADIUS accounting attribute for 3GPP NSAPI is enabled.

Table 15-15 RADIUS Accounting Attributes Configuration details

Field Name	Description
3GPP SGSN MCC MNC	Indicates whether RADIUS accounting attribute for 3GPP SGSN MCC MNC is enabled.
3GPP Charging Characteristics	Indicates whether RADIUS accounting attribute for 3GPP charging characteristics is enabled.
3GPP Rat Type	Indicates whether RADIUS accounting attribute for 3GPP RAT type is enabled.
3GPP IMEISV	Indicates whether RADIUS accounting attribute for 3GPP imeisv is enabled.
3GPP MS Timezone	Indicates whether RADIUS accounting attribute for 3GPP ms timezone is enabled.
3GPP User Location Information	Indicates whether RADIUS accounting attribute for 3GPP user location information is enabled.
3GPP Session Stop Indicator	Indicates whether RADIUS accounting attribute for 3GPP Session Stop Indicator is enabled.
3GPP Charging ID	Indicates whether RADIUS accounting attribute for 3GPP charging ID is enabled.
Input Octets	Indicates whether RADIUS accounting attribute for accounting input octets is enabled.
Output Octets	Indicates whether RADIUS accounting attribute for accounting output octets is enabled.
Session Time	Indicates whether RADIUS accounting attribute for accounting session time is enabled.
Input Packets	Indicates whether RADIUS accounting attribute for accounting input packets is enabled.
Output Packets	Indicates whether RADIUS accounting attribute for accounting output packets is enabled.
Event Timestamp	Indicates whether RADIUS accounting attribute for event timestamp is enabled.
Session ID	Indicates whether RADIUS accounting attribute for session id is enabled.
Status Type	Indicates whether RADIUS accounting attribute for status type is enabled.
Authentication	Indicates whether RADIUS accounting attribute for authentication is enabled.
Delay Time	Indicates whether RADIUS accounting attribute for delay time is enabled.

Viewing the RADIUS Authentication Attributes Configuration Details for an AAA Group

To view the radius authentication attributes configuration details:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Authentication Attributes Configuration**. The configuration details are displayed in the content pane.

Table 15-16 describes the attributes configuration details.

Table 15-16 RADIUS Authentication Attributes Configuration details

Field Name	Description
NAS IP Address	Indicates whether RADIUS authentication attribute for NAS IP Address is enabled.
NAS Identifier	Indicates whether RADIUS authentication attribute for NAS Identifier is enabled.
IMSI	Indicates whether RADIUS authentication attribute for IMSI is enabled.
Service Type	Indicates whether RADIUS authentication attribute for service type is enabled.
Framed IP Address	Indicates whether RADIUS authentication attribute for Framed IP Address is enabled.
Framed IPv6 Prefix	Indicates whether RADIUS authentication attribute for Framed IPv6 Prefix is enabled.
Called Station ID	Indicates whether RADIUS authentication attribute for called station id is enabled.
Calling Station ID	Indicates whether RADIUS authentication attribute for calling station id is enabled.
Chap Challenge	Indicates if the Challenge Handshake Authentication Protocol challenge sent by the network access server to a PPP CHAP user, is enabled.
Nas Port Type	NAS-Port-Type (RADIUS IETF attribute 61) indicates the type of physical port the network access server (NAS) is using to authenticate the user.
NAS Port ID	NAS-Port-ID (RADIUS IEFT attribute 87) contains a text string that identifies the NAS port that is authenticating the user.
User Name	Indicates enabled status for - name of the user being authenticated by the RADIUS server.
3GPP PDP Type	Indicates whether RADIUS authentication attribute for 3GPP PDP type is enabled.
3GPP CG Address	Indicates whether RADIUS authentication attribute for 3GPP CG address is enabled.
3GPP GPRS QoS Negotiated Profile	Indicates whether RADIUS authentication attribute for 3GPP GPRS QoS negotiated profile is enabled.
3GPP SGSN Address	Indicates whether RADIUS authentication attribute for 3GPP SGSN address is enabled.

Table 15-16 RADIUS Authentication Attributes Configuration details

Field Name	Description
3GPP GGSN Address	Indicates whether RADIUS authentication attribute for 3GPP GGSN address is enabled.
3GPP GGSN MCC MNC	Indicates whether RADIUS authentication attribute for 3GPP GGSN MCC MNC is enabled.
3GPP IMSI MCC MNC	Indicates whether RADIUS authentication attribute for 3GPP select mode is enabled.
3GPP Select Mode	Indicates whether RADIUS authentication attribute for 3GPP NSAPI is enabled.
3GPP NSAPI	Indicates whether RADIUS authentication attribute for 3GPP NSAPI is enabled.
3GPP SGSN MCC MNC	Indicates whether RADIUS authentication attribute for 3GPP SGSN MCC MNC is enabled.
3GPP Charging Characteristics	Indicates whether RADIUS authentication attribute for 3GPP charging characteristics is enabled.
3GPP Rat Type	Indicates whether RADIUS authentication attribute for 3GPP RAT type is enabled.
3GPP IMEISV	Indicates whether RADIUS authentication attribute for 3GPP imeisv is enabled.
3GPP MS Timezone	Indicates whether RADIUS authentication attribute for 3GPP ms timezone is enabled.
3GPP User Location Information	Indicates whether RADIUS authentication attribute for 3GPP user location information is enabled.

Viewing the Radius Authentication Configuration Details for an AAA Group

To view the radius authentication configuration details for an AAA group:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Authentication Configuration**. The authentication configuration details are displayed in the content pane.

Table 15-17 describes the radius authentication configuration details.

Table 15-17 Radius Authentication Configuration

Field Name	Description
Server Selection Algorithm	The algorithm to select the RADIUS accounting server(s) to which accounting data must be sent. Values are: • first-server • round-robin
Server Deadtime	The time period after which the status of the authentication server must be changed from Down to Active.
Maximum Outstanding Messages	The maximum number of outstanding messages that can be queued with the AAA manager.
Authentication Maximum Retries	The maximum number of attempts with the AAA server, before it is declared Not Responding and the detected dead server's consecutive failures count is incremented.
Authentication Maximum Transmissions	The maximum number of transmissions attempted for a RADIUS authentication message, before it is declared FAILED.
Authentication Response Timeout	The time period to wait for a response from the RADIUS server, before resending the message. This value is displayed in seconds.
APN To Be Included	The APN associated with the RADIUS authentication.
Authenticate Null User Name	Indicates whether the authentication of user names that are blank or empty is enabled.
Modify NAS IP	Indicates whether the RADIUS authentication is attempted after NAS IP is modified.
Probe Interval	The time interval (in seconds) before sending another probe authentication request to a RADIUS server.
Probe Timeout	The time period (in seconds) to wait for a response from a RADIUS server before resending the authentication probe.
Probe Maximum Retries	The number of retries for RADIUS authentication probe response before the authentication is declared as failed.

Viewing the Charging Configuration Details for an AAA Group

To view the radius charging configuration details for an AAA group:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Charging Configuration**. The charging configuration details are displayed in the content pane.

Table 15-18 describes the charging configuration details.

Table 15-18 Radius Charging Configuration

Field Name	Description
Authentication Server Selection Algorithm	The algorithm to select the RADIUS server(s) for active charging service to ensure proper load distribution amongst the available servers used for authentication requests. Value could be one of the following: • first-server • round-robin
Accounting Server Selection Algorithm	The algorithm to select the RADIUS server(s) for active charging service to ensure proper load distribution amongst the available servers for accounting requests. Value could be one of the following: • first-n n Default • first-server • round-robin
Server Deadtime	The time period after which the status of the RADIUS server must be changed from Down to Active.
Maximum Outstanding Messages	The maximum number of outstanding messages that can be queued with the AAA manager.
Maximum Retries	The maximum number of attempts with the AAA server, before it is declared Not Responding and the detected dead server's consecutive failures count is incremented.
Response Timeout	The maximum number of retransmissions for RADIUS authentication requests.
Detect Dead Server Consecutive Retries	The number of consecutive failures for an AAA manager, before the status of an charging server is changed from Active to Down.

Viewing the Charging Trigger Configuration Details for an AAA Group

To view the radius charging trigger configuration details for an AAA group:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Charging Trigger**. The charging configuration details are displayed in the content pane.

Table 15-19 describes the charging trigger configuration details.

Table 15-19 Radius Charging Triggers Configuration

Field Name	Description
Serving Node Change	Indicates whether RADIUS trigger for serving node is enabled.
Radio Access Technology Change	Indicates whether RADIUS trigger for radio access technology change is enabled.
User Location Information Change	Indicates whether RADIUS trigger for user location information change is enabled.
Routing Area Information Change	Indicates whether RADIUS trigger for routing area information change is enabled.
Quality of Service Change	Indicates whether RADIUS trigger for quality of service change is enabled.
Mobile Station Timezone Change	Indicates whether RADIUS trigger for mobile station time zone change is enabled.

Viewing TACACS+ Group Configuration Details for an AAA Group

To view the TACACS+ group configuration details for a AAA group:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **AAA** > **AAA Groups**.The configuration details are displayed on the content pane. (The attributes that are displayed depend on the device type.)

Step 3 Expand a specific **TACACS+ Group** node and then **choose TACACS+ Configuration** under a specific AAA group node.

Table 15-20 describes the TACACS+ group configuration details and its associated TACACS+ Servers details.

Table 15-20 TACACS+ group Configuration

Field Name	Description
Group Name	The AAA group name.
Group Type	The AAA group type.
Source Interface	Specifies that the IP address of this specified interface is used for all outgoing TACACS+ packets.
VRF	The VRF used in this TACACS+ server group.
Acknowledge Broadcast Accounting	Specifies if accounting information can be broadcast to one or more AAA servers simultaneously.
Cache Expiry Time	Specifies the length of time, in hours, for a cache database profile entry to expire.
Cache Expiry Rule	Specifies how the expired cached database profile entries in this TACACS+ server group are to be used: • Enforce—Indicates not to use expired entries. • Failover—Indicates to use an expired entry if all other methods fail.
Cache Authentication Profile Name	The name of the cache authentication profile used in this TACACS+ server group.
Cache Authorization Profile Name	The name of the cache authorization profile used in this TACACS+ server group.
Associated TACACS+ Servers	
Server Address	The IP address or hostname of the TACACS+ server.
Port	The TCP port used to communicate with the TACACS+ server.
Server Name	The name of the associated TACACS+ Server.
Status	Specifies the operational state of the interface with the TACACS+ server.

Configuring AAA Groups

The following commands can be launched from the inventory by right-clicking and AAA group and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Navigation	Description
Create Diameter Accounting Server	Right-click the *AA group* > **Commands** > **group dialog box, select a group name** and then choose **Commands > Configuration > Create Diameter Accounting Server**	Use this command to create a new diameter accounting server.
Create Diameter Authentication Server	Right-click the *AA group* > **Commands** > **group dialog box, select a group name** and then choose **Commands > Configuration > Create Diameter Authentication Server**	Use this command to create a new diameter authentication server.
Delete AAA Group	Right-click the *AA group* > **Commands** > **group dialog box, select a group name** and then choose **Commands > Configuration > Delete AAA Group**	Use this command to delete an AAA group.
Modify AAA Group	Right-click the *AA group* > **Commands** > **group dialog box, select a group name** and then choose **Commands > Configuration > Modify AAA Group**	Use this command to modify the attributes of an AAA group.

Managing DWDM Networks

The Cisco IP over dense wavelength division multiplexing (IPoDWDM) solution enables the convergence of the IP and DWDM core networks of the service providers. It increases service flexibility, operational efficiency and reliability while lowering operating expenses (OpEx) and capital expenditures (CapEx).

Prime Network discovers and displays the following DWDM attributes in the Physical Inventory tree of the Vision client:

- DWDM controllers. The controller location is same as the DWDM interface.
- Loopback information for the DWDM controller.
- DWDM controller status.
- DWDM port properties—Wavelength, Laser Status, Tx Power, and Rx Power.
- DWDM controller card status (G.709 status).

Prime Network also provides commands that support DWDM and Synchronous Optical Network (SONET) controllers. These commands help in configuring the device and in displaying device details. The commands are described in Configuring and Viewing DWDM, page 16-14. (For information on the SONET commands, see Configuring Clock, page 26-55.)

The following topics describe how you can view and monitor IP over dense wavelength division multiplexing (DWDM) properties configured on network elements by using the Vision client. If you cannot perform an operation that is described in these topics, you may not have sufficient permissions; see Permissions for Managing DWDM, page B-16.

Viewing DWDM in Physical Inventory

The Vision client enables you to monitor a variety of DWDM properties in physical inventory, including forward error correction (FEC), G.709 status, and performance monitoring parameters.

To view DWDM properties in physical inventory:

Step 1 In the Vision client, double-click the device on which DWDM is configured.

Step 2 In the **Inventory** window, choose **Physical Inventory > Chassis** and navigate to the interface configured for DWDM. DWDM details are displayed in the DWDM area in the content pane as shown in Figure 16-1.

Figure 16-1 DWDM Properties in Physical Inventory

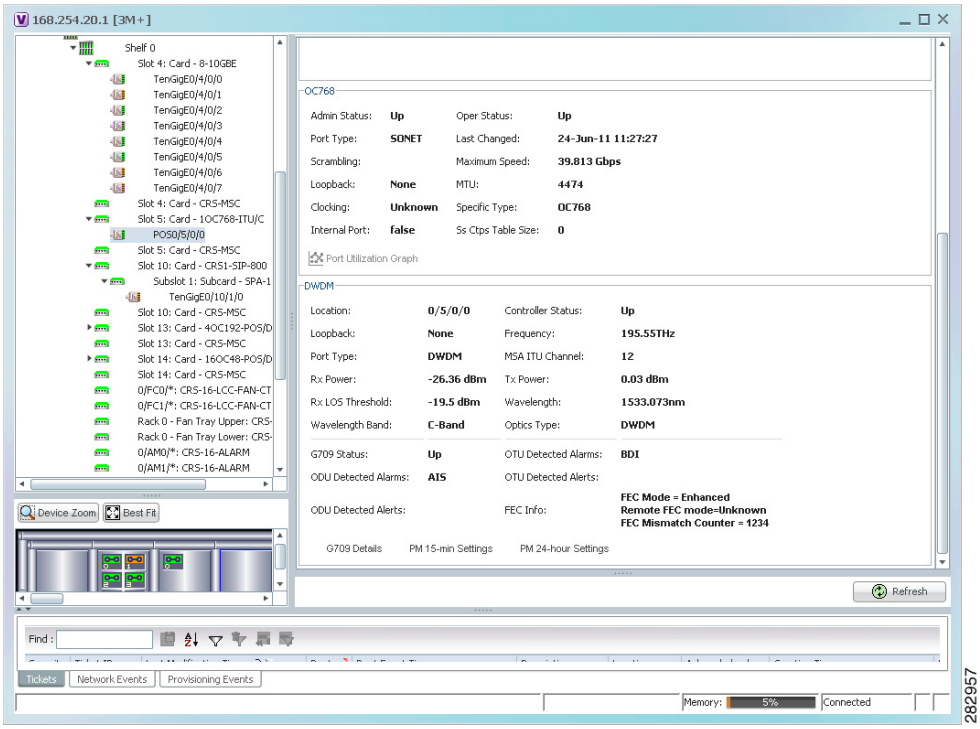


Table 16-1 describes the information displayed for DWDM.

Table 16-1 DWDM Properties in Physical Inventory

Field	Description
Location	Physical interface using the format *rack*/*slot*/*module*/*port* where: • *rack* is the chassis number of the rack. • *slot* is the physical slot number of the line card. • *module* is the module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. • *port* is the physical port number of the interface.
Controller Status	Status of the controller: Up or Down.
Loopback	Whether or not the DWDM controller is configured for loopback mode.
Frequency	Frequency of the channel in terahertz.
Port Type	The port type. In this case, DWDM.
MSA ITU Channel	Multi Source Agreement (MSA) ITU channel number.
Rx Power	Actual optical power at the receiving port.
Tx Power	Value of the transmit power level.
Rx LOS Threshold	Number of optical channel transport unit (OTU) loss of signal (LOS) alarms. If the receive optical power is less than or equal to this defined threshold, the optical LOS alarm is raised.
Wavelength	Wavelength corresponding to the channel number in nanometers.
Wavelength Band	Indicates the wavelength band: C-band or L-band.
Optics Type	Indicates the optics type: GE or DWDM.
G709 Properties	
G709 Status	Whether the G.709 wrapper is enabled or disabled: Up or Down.
OTU Detected Alarms	OTU overhead alarms.
ODU Detected Alarms	Optical channel data unit (ODU) alarms.
OTU Detected Alerts	OTU alerts.
ODU Detected Alerts	ODU alerts.
FEC Info	Indicates the: • FEC mode of the controller: Disabled, Enhanced, Standard, or Unknown. • FEC mode on the remote device: Disabled, Enhanced, Standard, or Unknown. • Number of sync word mismatches found during the tracking phase.
G709 Details	Click to view G709 properties. For more information, see Viewing G.709 Properties, page 16-4.

Table 16-1 DWDM Properties in Physical Inventory (continued)

Field	Description
PM 15-min Settings	Click to view 15-minute performance monitoring properties. For more information, see Viewing Performance Monitoring Configuration, page 16-10.
PM 24-hour Settings	Click to view 24-hour performance monitoring properties. For more information, see Viewing Performance Monitoring Configuration, page 16-10.

Viewing G.709 Properties

The Telecommunication Standardization Sector (ITU-T) Recommendation G.709 provides a standardized method for transparently transporting services over optical wavelengths end to end. A significant component of G.709 is the FEC code that improves performance and extends the distance that optical signals can span.

To view G.709 properties:

Step 1 In the Vision client, double-click the device on which DWDM is configured.

Step 2 In the **Inventory** window, choose **Physical Inventory > Chassis** and navigate to the interface configured for DWDM.

Step 3 In the content pane, click **G709 Details**. Figure 16-2 and Figure 16-3 provide examples of the G709 Info Properties windows. Most devices provide the information shown in Figure 16-2.

Figure 16-2 DWDM G709 Properties Window—Example 1

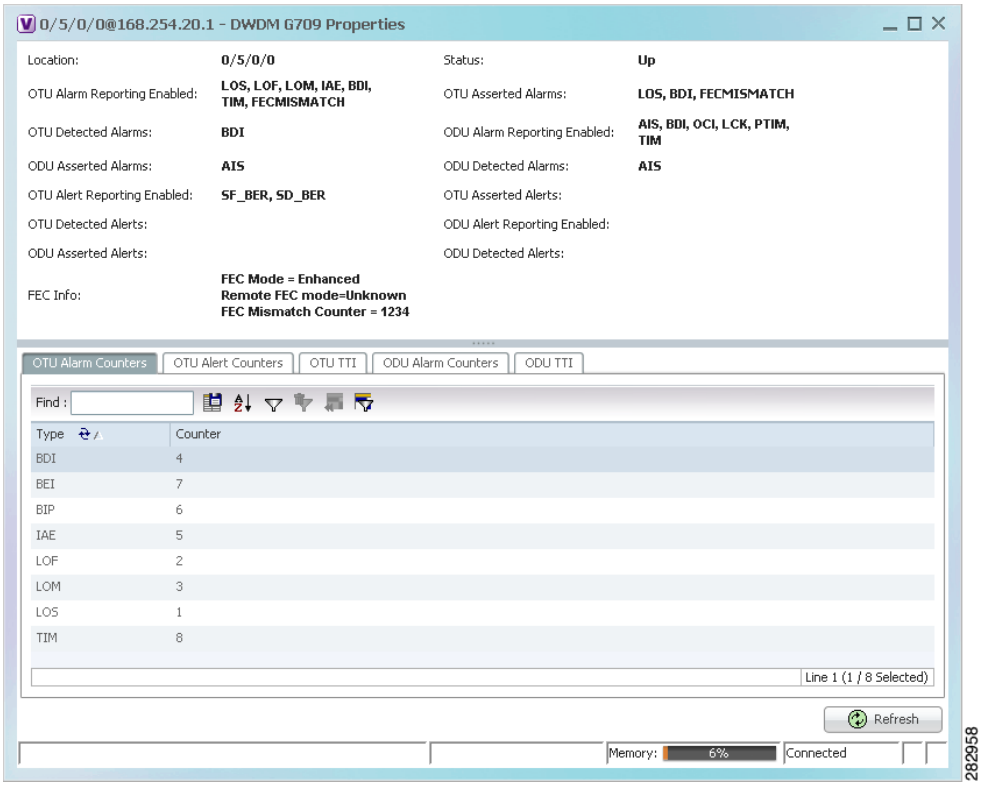


Figure 16-3 shows the tabs that are displayed for devices such as the Cisco 7600 series, where the ODU Alert Counters tab is displayed, but the ODU TTI and OTU TTI tabs are *not* displayed.

Figure 16-3 DWDM G709 Properties Window —Example 2

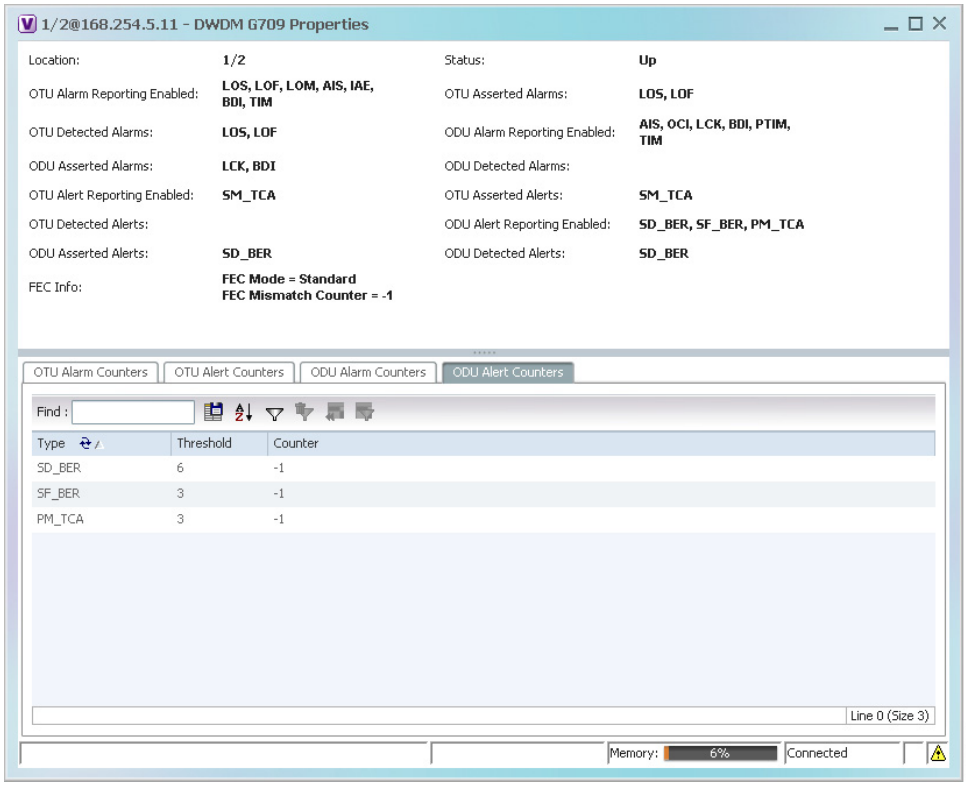


Table 16-2 describes the fields that are displayed above the tabs in the G709 Info Properties window.

Table 16-2 DWDM G709 Properties Window

Field	Description
Location	Physical interface using the format *rack*/*slot*/*module*/*port* where: • *rack* is the chassis number of the rack. • *slot* is the physical slot number of the line card. • *module* is the module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. • *port* is the physical port number of the interface.

Table 16-2 DWDM G709 Properties Window (continued)

Field	Description
OTU Alarms	
OTU Alarm Reporting Enabled for	The types of alarms enabled for reporting: • AIS—Alarm indication signal (AIS) alarms. • BDI—Backward defect indication (BDI) alarms. • BEI—Backward error indication (BEI) alarms. • BIP—Bit interleaved parity (BIP) alarms. • FECMISMATCH—FEC mismatch alarms. • IAE—Incoming alignment error (IAE) alarms. • LOF—Loss of frame (LOF) alarms. • LOM—Loss of multiple frames (LOM) alarms. • LOS—Loss of signal (LOS) alarms. • TIM—Type identifier mismatch (TIM) alarms.
OTU Asserted Alarms	OTU alarms indicated to be reported by the user.
OTU Detected Alarms	OTU alarms detected by the hardware.
ODU Alarms	
ODU Alarm Reporting Enabled for	The types of ODU alarms enabled for reporting: • AIS—Incoming SONET AIS error status. • BDI—Path termination BDI error status. • BEI—Backward error indication (BEI) error status. • BIP—Bit interleaved parity (BIP) error status. • LCK—Upstream connection locked (LCK) error status. • OCI—Open connection indication (OCI) error status. • PTIM—Payload TIM error status. • TIM—Data stream TIM error status.
ODU Asserted Alarms	ODU alarms indicated to be reported by the user.
ODU Detected Alarms	ODU alarms detected by the hardware.

Table 16-2 DWDM G709 Properties Window (continued)

Field	Description
OTU Alerts	
OTU Alert Reporting Enabled for	The types of alerts enabled for reporting: • SD-BER—Section Monitoring (SM) bit error rate (BER) is in excess of the signal degradation (SD) BER threshold. • SF-BER—SM BER is in excess of the signal failure (SF) BER threshold. • PM-TCA—Performance monitoring (PM) threshold crossing alert (TCA). • SM-TCA—SM threshold crossing alert.
OTU Asserted Alerts	OTU alerts indicated to be reported by the user.
OTU Detected Alerts	OTU alerts detected by the hardware.
ODU Alerts	
ODU Alert Reporting Enabled for	The types of ODU alerts enabled for reporting: • SD-BER—SM BER is in excess of the SD BER threshold. • SF-BER—SM BER is in excess of the SF BER threshold. • PM-TCA—PM threshold crossing alert. • SM-TCA—SM threshold crossing alert.
ODU Asserted Alerts	ODU alerts indicated to be reported by the user.
ODU Detected Alerts	ODU alerts detected by the hardware.
Other	
FEC Info	FEC properties: • FEC mode for the controller—Disable, Enhanced, Standard, or Unknown. • Remote FEC mode—FEC mode on the remote device: Disabled, Enhanced, Standard, or Unknown. • FEC mismatch counter—Number of sync word mismatches found during the tracking phase.
Status	G.709 wrapper administrative status: Up or Down.

Step 4 To view additional G.709 properties, click the required tab. Table 16-3 describes the information displayed in each tab. The information that is displayed depends on the selected network element.

Table 16-3 G709 Properties Window Tabs

Field	Description
OTU Alarm Counters Tab	
Type	Type of OTU alarm, such as BDI or BEI.
Counter	Number of alarms reported for each alarm type.

Table 16-3 G709 Properties Window Tabs (continued)

Field	Description
OTU Alert Counters Tab	
Type	Type of OTU alert, such as SD-BER or SF-BER.
Threshold	Threshold set for the type of alert.
Counter	Number of alerts reported for each alert type. A value of -1 indicates that no value has been set up.
ODU Alarm Counters Tab	
Type	Type of ODU alarm, such as AIS or BDI.
Counter	Number of alarms reported for each alarm type.
OTU TTI Tab (Displayed for most devices but not for those such as the Cisco 7600 series))	
Type	Type of OTU Trail Trace Identifier (TTI) configured: • Expected • Received • Sent
String Type	For each TTI type, the type of string: • ASCII • Hexadecimal
TTI String	For each TTI type, the specific TTI string configured.
ODU TTI Tab (Displayed for most devices but not for those such as the Cisco 7600 series)	
Type	Type of ODU TTI configured: • Expected • Received • Sent
String Type	For each TTI type, the type of string: • ASCII • Hexadecimal
TTI String	For each TTI type, the specific TTI string configured.

Table 16-3 G709 Properties Window Tabs (continued)

Field	Description
ODU Alert Counters Tab	
(Displayed for devices such as the Cisco 7600 series.)	
Type	Type of OTU alert, such as SD-BER or SF-BER.
Threshold	Threshold set for the type of alert.
Counter	Number of alerts reported for each alert type. A value of -1 indicates that no value has been set up.

Step 5 To close the G709 Info Properties window, click the upper right corner.

Viewing Performance Monitoring Configuration

Performance monitoring parameters are used to gather, store, set thresholds for, and report performance data for early detection of problems. Thresholds are used to set error levels for each performance monitoring parameter. During the accumulation cycle, if the current value of a performance monitoring parameter reaches or exceeds its corresponding threshold value, a threshold crossing alert (TCA) can be generated. The TCAs provide early detection of performance degradation.

The Vision client enables you to view the configuration settings for performance monitoring. Performance monitoring statistics are accumulated on a 15-minute basis, synchronized to the start of each quarter-hour. They are also accumulated on a daily basis starting at midnight. Historical counts are maintained for thirty-three 15-minute intervals and two daily intervals.

To view performance monitoring configuration settings:

Step 1 In the Vision client, double-click the device on which DWDM is configured.

Step 2 In the **Inventory** window, choose **Physical Inventory > Chassis** and navigate to the interface configured for DWDM.

Step 3 In the content pane, select the performance monitoring configuration settings you want to view:

- To view the performance monitoring 15-minute configuration settings, click **PM 15-min Settings**.
- To view the performance monitoring 24-hour configuration settings, click **PM 24-hour Settings**.

The Client DWDM PM Settings Properties window is displayed as shown in Figure 16-4.

Figure 16-4 Client DWDM PM Settings Properties Window

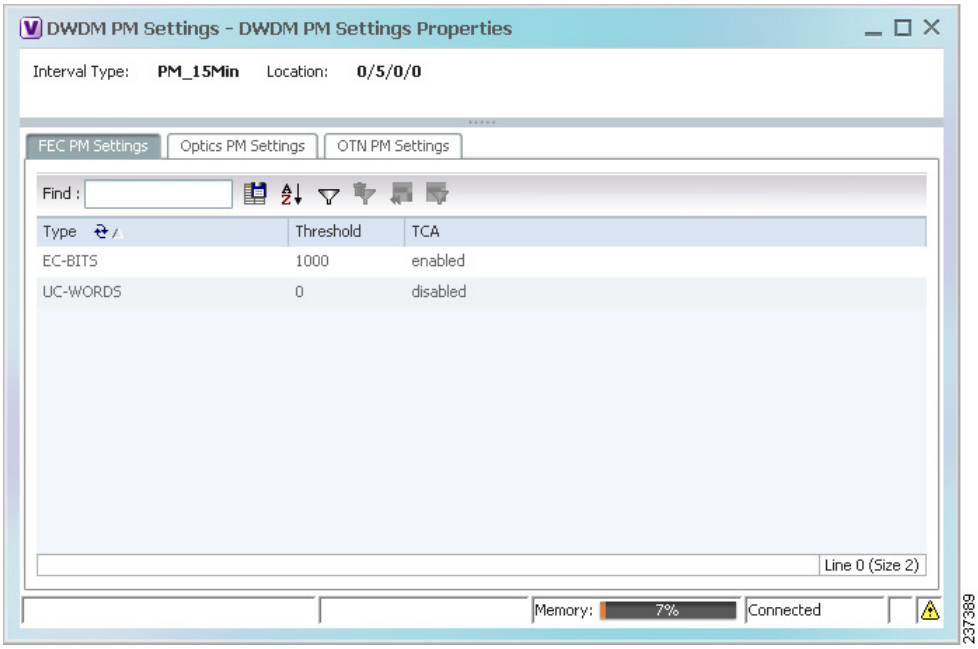


Table 16-4 describes the information displayed above the tabs in the Client DWDM PM Settings Properties window and in each of the tabs.

Table 16-4 Client DWDM PM Settings Properties Window and Tabs

Field	Description
Interval Type	The performance monitoring interval, either 15 minutes or 24 hours.
Location	Physical interface using the format *rack*/*slot*/*module*/*port* where: • *rack* is the chassis number of the rack. • *slot* is the physical slot number of the line card. • *module* is the module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. • *port* is the physical port number of the interface.
FEC PM Settings Tab	
Type	FEC performance monitoring parameter being tracked: • EC-BITS—The number of bit errors corrected (EC-BITS) in the DWDM trunk line during the performance monitoring time interval. • UC-WORDS—The number of uncorrectable words (UC-WORDS) detected in the DWDM trunk line during the performance monitoring time interval.
Threshold	Threshold for the performance monitoring parameter.
TCA	Whether TCA generation for the specified parameter on the DWDM controller is enabled or disabled.

Table 16-4 Client DWDM PM Settings Properties Window and Tabs (continued)

Field	Description
Optics PM Settings Tab	
Type	Optics performance monitoring parameter being tracked: • LBC—Laser bias current. • OPR—Optical power on the unidirectional port. • OPT—Transmit optical power in dBm.
Max Threshold	Maximum threshold configured for the parameter.
Max TCA	If enabled, indicates a TCA is generated if the value of the parameter exceeds the maximum threshold during the performance monitoring period. If disabled, TCAs are not generated if the maximum threshold is exceeded.
Min Threshold	Minimum threshold configured for the parameter.
Min TCA	If enabled, indicates a TCA is generated if the value of the parameter drops below the minimum threshold during the performance monitoring period. If disabled, TCAs are not generated if the value drops below the minimum threshold.

Table 16-4 Client DWDM PM Settings Properties Window and Tabs (continued)

Field	Description
OTN PM Settings Tab	
Type	OTN performance monitoring parameter being tracked: • bbe-pm-fe—Far-end path monitoring background block errors (BBE-PM). Indicates the number of background block errors recorded in the optical transport network (OTN) path during the performance monitoring time interval. • bbe-pm-ne—Near-end path monitoring background block errors (BBE-PM). • bbe-sm-fe—Far-end section monitoring background block errors (BBE-SM). Indicates the number of background block errors recorded in the OTN section during the performance monitoring time interval. • bbe-sm-ne—Near-end section monitoring background block errors (BBE-SM). • bber-pm-fe—Far-end path monitoring background block errors ratio (BBER-PM). Indicates the background block errors ratio recorded in the OTN path during the performance monitoring time interval. • bber-pm-ne—Near-end path monitoring background block errors ratio (BBER-PM). • bber-sm-fe—Far-end section monitoring background block errors ratio (BBER-SM). Indicates the background block errors ratio recorded in the OTN section during the performance monitoring time interval. • bber-sm-ne—Near-end section monitoring background block errors ratio (BBER-SM) • es-pm-fe—Far-end path monitoring errored seconds (ES-PM). Indicates the errored seconds recorded in the OTN path during the performance monitoring time interval. • es-pm-ne—Near-end path monitoring errored seconds (ES-PM). • es-sm-fe—Far-end section monitoring errored seconds (ES-SM). Indicates the errored seconds recorded in the OTN section during the performance monitoring time interval. • es-sm-ne—Near-end section monitoring errored seconds (ES-SM). • esr-pm-fe—Far-end path monitoring errored seconds ratio (ESR-PM). Indicates the errored seconds ratio recorded in the OTN path during the performance monitoring time interval. • esr-pm-ne—Near-end path monitoring errored seconds ratio (ESR-PM). • esr-sm-fe—Far-end section monitoring errored seconds ratio (ESR-SM). Indicates the errored seconds ratio recorded in the OTN section during the performance monitoring time interval. • esr-sm-ne—Near-end section monitoring errored seconds ratio (ESR-SM). • fc-pm-fe—Far-end path monitoring failure counts (FC-PM). Indicates the failure counts recorded in the OTN path during the performance monitoring time interval. • fc-pm-ne—Near-end path monitoring failure counts (FC-PM). • fc-sm-fe—Far-end section monitoring failure counts (FC-SM). Indicates the failure counts recorded in the OTN section during the performance monitoring time interval. • fc-sm-ne—Near-end section monitoring failure counts (FC-SM).

Table 16-4 Client DWDM PM Settings Properties Window and Tabs (continued)

Field	Description
Type (cont.)	• ses-pm-fe—Far-end path monitoring severely errored seconds (SES-PM). Indicates the severely errored seconds recorded in the OTN path during the performance monitoring time interval. • ses-pm-ne—Far-end path monitoring severely errored seconds (SES-PM). • ses-sm-fe—Far-end section monitoring severely errored seconds (SES-SM). Indicates the severely errored seconds recorded in the OTN section during the performance monitoring time interval. • ses-sm-ne—Near-end section monitoring severely errored seconds (SES-SM). • sesr-pm-fe—Far-end path monitoring severely errored seconds ratio (SESR-PM). Indicates the severely errored seconds ratio recorded in the OTN path during the performance monitoring time interval. • sesr-pm-ne—Near-end path monitoring severely errored seconds ratio (SESR-PM). • sesr-sm-fe—Far-end section monitoring severely errored seconds ratio (SESR-SM). Indicates the severely errored seconds ratio recorded in the OTN section during the performance monitoring time interval. • sesr-sm-ne—Near-end section monitoring severely errored seconds ratio (SESR-SM). • uas-pm-fe—Far-end path monitoring unavailable seconds (UAS-PM). Indicates the unavailable seconds recorded in the OTN path during the performance monitoring time interval. • uas-pm-ne—Near-end path monitoring unavailable seconds (UAS-PM). • uas-sm-fe—Far-end section monitoring unavailable seconds (UAS-SM). Indicates the unavailable seconds recorded in the OTN section during the performance monitoring time interval. • uas-sm-ne—Near-end section monitoring unavailable seconds (UAS-SM).
Threshold	Threshold configured for the parameter.
TCA	If enabled, indicates a TCA is generated if the value of the parameter crosses the threshold during the performance monitoring period. If disabled, TCAs are not generated if the value crosses the threshold.

Configuring and Viewing DWDM

The following commands can be launched from the inventory by right-clicking the appropriate node and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see Permissions for Managing DWDM, page B-16). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Navigation	Input Required and Notes
Controller Data	**Show >**	N/A; performed from command launch point
PM History Data		PM interval type: 15-min or 24-hour
		Interval number
RTPM Counters		PM interval type: 15-min or 24-hour
RTPM Threshold		PM interval type: 15-min or 24-hour
Wavelength Map		N/A; performed from command launch point
IM Trace Details		Card location (for example, 0/5/CPU0)
Device Log		N/A; performed from command launch point
Counters	**Clear >**	N/A; performed from command launch point
Channel	**Configure >**	Channel number
		Option: Set or reset channel
FEC Mode		G.709 FEC mode: Disabled, enhanced, or standard
G.709 ODU		ODU alarm type: ais, bdi, lck, oci, ptim, or tim
		Option: Enable or disable alarm type
G.709 OTU		OTU alarm type: bdi, fecmismatch, iae, lof, lom, los, sd-ber, sf-ber, or tim
		Option: Enable or disable alarm type

Command	Navigation	Input Required and Notes
G.709 TTI	**Configure >**	Optical channel unit type: ODU or OTU
		TTI type: Expected or sent
		TTI string type: ASCII or hex
		TTI string
		Option: Set or reset TTI string
G.709 Wrapper		Option: Disable or enable G.709 wrapper
Laser State		Laser state: Switch off or on
Loopback		Loopback value: Internal or line
		Option: Set or remove
PM FEC Data		PM interval type
		FEC alarm type: • Ec-bits—Bit errors corrected (BIEC); the number of bit errors corrected in the DWDM trunk line during the performance monitoring time interval • Uc-words—Uncorrectable words; the number of uncorrectable words detected in the DWDM trunk line during the performance monitoring time interval
		TCA options: Enable or disable TCA generation
		Threshold option. Set configures the value on the device; reset is the default. If you select blank, the threshold value is not used.
		Threshold value

Command	Navigation	Input Required and Notes
PM Optics Data	**Configure >**	PM interval: 15-min or 24-hour
		Optics alarm type: • lbc—Laser bias current • opr—Optical power on the unidirectional port • opt—Transmit optical power in dBm
		Maximum TCA option: Enable or disable
		Maximum threshold option: Choosing Set configures the value on the device; Reset is the default. If you select blank, the threshold value is not used.
		Maximum threshold
		Minimum TCA option: enable or disable
		Minimum threshold option: Choosing Set configures the value on the device; Reset is the default. If you select blank, the threshold value is not used.
		Minimum threshold
PM OTN Data		PM interval: 15-min or 24-hour
		OTN alarm type. For a list of types and their descriptions, see the OTN PN Settings Tab information in Table 16-4 on page 16-11.
		TCA option: Enable or disable
		Threshold option: Choosing Set configures the value on the device; Reset is the default. If you select blank, the threshold value is not used.
		Threshold value
Transmit Power		Transmit power in dBm
		Option: Set or reset transponder Tx threshold
Rx LOS Threshold		Rx LOS threshold value
		Option: Set or reset transponder Rx threshold

Managing MPLS Networks

The following topics describe how to view and manage aspects of Multiprotocol Label Switching (MPLS) services using the Vision client, including the MPLS service view, business configuration, and maps. The topics also describe the device inventory specific to MPLS VPNs, including routing entities, label switched entities (LSEs), BGP Neighbors, Multiprotocol BGP (MP-BGP), VRF instances, pseudowires, and TE tunnels. If you cannot perform an operation that is described in these topics, you may not have sufficient permissions; see Permissions for Managing MPLS Services, page B-18.

Viewing IPv6 Information (6VPE)

Prime Network supports IPv6 for:

- Gateways, clients, and units using IPv6.
- Communications between VNEs and devices in IPv6 environments, whether the device management IP address is IPv4 or IPv6.

- Polling and notification using the following protocols over IPv6:
  - SNMP v1, SNMPv2c, and SNMPv3
  - Telnet
  - SSHv2
  - ICMP
  - XML (for Cisco IOS XR devices)
  - HTTP (for Cisco UCS and VMware vCenter devices)
- All reports with devices that use IPv6 addresses.
- Fault management, including event processing and service alarm generation.

Prime Network supports correlation and path tracing for:

- 6PE and native IPv6 networks.
- IPv6 BGP address families.
- IPv6 GRE tunnels.

IPv6 VPN over MPLS, also known as 6VPE, uses the existing MPLS IPv4 core infrastructure for IPv6 transport to enable IPv6 sites to communicate over an MPLS IPv4 core network using MPLS label switch paths (LSPs). 6VPE relies on MP-BGP extensions in the IPv4 network configuration on the PE router to exchange IPv6 reachability information. Edge routers are configured to be dual-stacks running both IPv4 and IPv6, and use the IPv4-mapped IPv6 address for IPv6 prefix reachability exchange.

In 6VPE environments, Prime Network supports:

- Modeling of OSPFv3 routes between PE and CE devices.
- IPv6 addresses for BGP Neighbours for MP-BGP.
- Correlation and path tracing.

The Vision client displays IPv6 addresses when they are configured on PE and CE routers in the IP interface table. IPv6 addresses are:

- Displayed in the Vision client map pane for IPv6 links.
- Displayed in logical and physical inventory for routing and interface information, including IP, PPP, and High-Level Data Link Control (HDLC).
- Used in Cisco PathTracer to trace paths and present path trace results.

Table 17-1 describes where IPv6 information appears in logical and physical inventory.

Table 17-1 IPv6 Information in Inventory

Inventory Location	Description
Logical Inventory	
6rd Tunnels	The Tunnel Edges table displays IPv6 addresses and the IPv6 prefixes that are used to translate IPv4 addresses to IPv6 addresses. For more information, see Viewing 6rd Tunnel Properties, page 17-49.
Access Lists	• The Type field displays IPv6 for IPv6 access lists. • If an IPv6 access list is configured, the Access List Properties window displays IPv6 addresses in the Source, Destination, Source Wildcard, and Destination Wildcard fields.
Carrier Grade NAT	Carrier Grade NAT service types include 6rd and XLAT. For more information, see Viewing Carrier Grade NAT Properties in Logical Inventory, page 20-2.
GRE Tunnels	The IP Address field supports IPv6 addresses. For more information, see Viewing MPLS Pseudowire Over GRE Properties, page 26-31.
IS-IS	IS-IS properties support: • IPv6 address families in the Metrics tab. • IPv6 addresses in the Neighbours tab and the IS-IS Neighbour Properties window. For more information, see Viewing IS-IS Properties, page 18-132.
MPBGPs	• IP address family identifiers indicate the BGP peer address family: IPv4, IPv6, Layer 2 VPN, VPNv4, or VPNv6. • MP-BGP BGP Neighbour entries display IPv6 addresses. For information, see Viewing MP-BGP Information, page 17-48.
OSPFv3	IPv6 addresses are displayed for OSPF Neighbour interface addresses, OSPF interface internet addresses, OSPF Neighbour properties window, and OSPF interface properties window. For more information, see Viewing OSPF Properties, page 18-138.
Routing Entities	• IPv6 addresses appear in the IP Interfaces tab, the IPv6 Routing tab, and the interface properties window. • IPv6 addresses are displayed in the NDP Table tab and the ARP Entry Properties window. • VRRP groups using IPv6 display IPv6 addresses in the IP Interfaces Properties window in the VRRP group tab. For more information, see Viewing Routing Entities, page 17-32.
VRFs	IPv6 addresses appear in the IPv6 tab, Sites tab, VRF Properties window, and IP Interface Properties window. For more information, see Viewing VRF Properties, page 17-28.

Table 17-1 IPv6 Information in Inventory (continued)

Inventory Location	Description
Physical Inventory	
Port	IPv6 addresses appear in the Subinterfaces tab and interface properties popup window.

The IP addresses that appear depend on whether the interface has only IPv4 addresses, only IPv6 addresses, or both IPv4 and IPv6 addresses, as shown in Table 17-2.

Table 17-2 IP Addresses Displayed in the Interface Table and Properties Window

Addresses	Interface Table	Properties Window
IPv4 only	Primary IPv4 address	The primary IPv4 address and any secondary IPv4 addresses.
IPv6 only	Lowest IPv6 address	All IPv6 addresses.
IPv6 and IPv4	Primary IPv4 address	All IPv4 and IPv6 addresses.

Note the following when working with IPv6 addresses:

- MPLS label switching entries and Label Switching Entities (LSEs) do not display IPv6 addresses. However, the Neighbour Discovery Protocol (NDP) table does display IPv6 addresses.
- Prime Network supports all the textual presentations of address prefixes. However, the Vision client displays both the IP address and the subnet prefix, for example:

  `12AB::CD30:123:4567:89AB:CDEF, 12AB:0:0:CD30::/60`

Note Interfaces or subinterfaces that do not have IP addresses are not discovered and therefore are not shown in the Vision client.

Figure 17-1 shows a port inventory view of a port with IPv4 and IPv6 addresses. In this example, one IPv4 address and multiple IPv6 addresses are provisioned on the interface.

- The primary IPv4 address appears in the interface table and properties window. If secondary IPv4 addresses were provisioned on the interface, they would appear in the properties window.
- IPv6 addresses provisioned on the interface appear in the properties window and Sub Interfaces tab.

Figure 17-1 Port with IPv4 and IPv6 Addresses

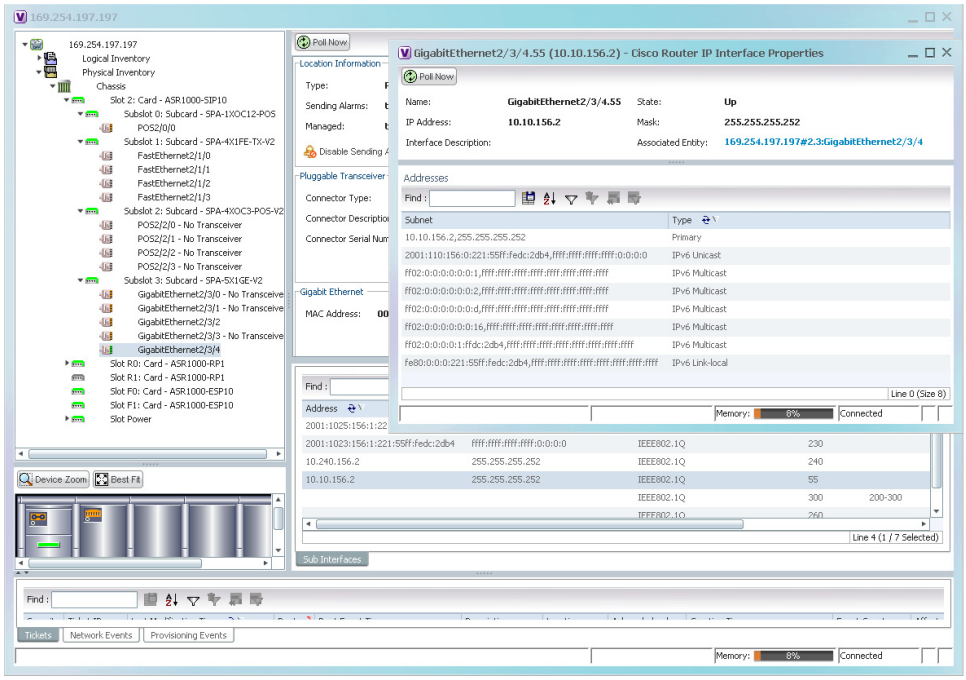
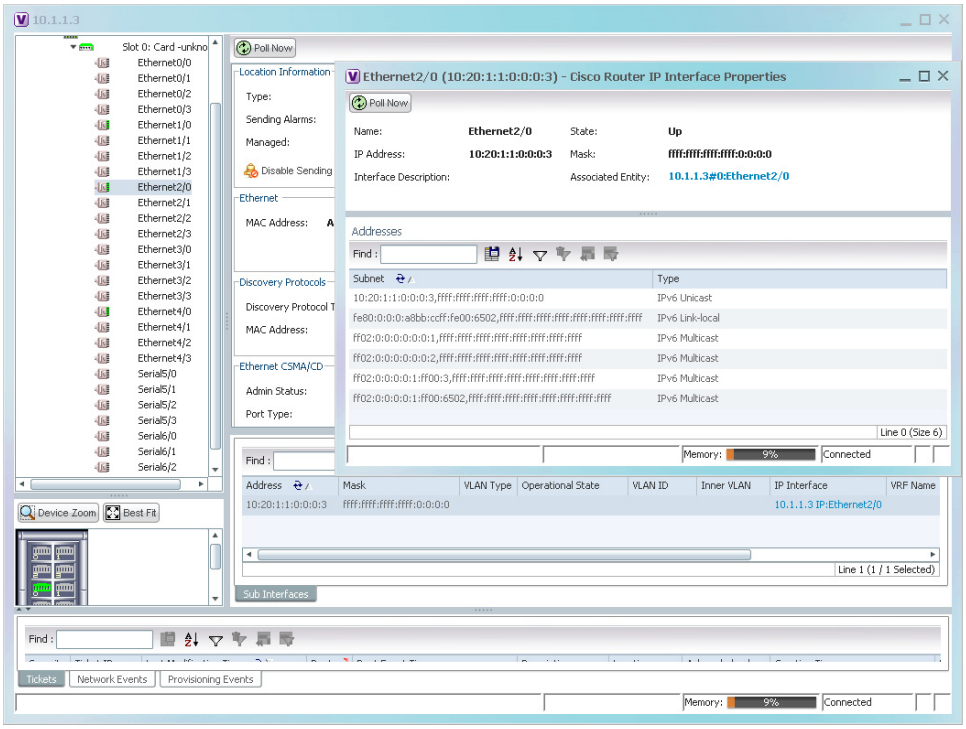


Figure 17-2 shows a port with only IPv6 addresses provisioned. In this example, the lowest IPv6 address is shown in the subinterface table, and all IPv6 addresses are shown in the interface properties window.

Figure 17-2 Port with IPv6 Addresses



Working with MPLS-TP Tunnels

MPLS-Transport Profile (MPLS-TP) is considered to be the next generation transport for those using SONET/SDH TDM technologies as they migrate to packet-switching technology. Although still under definition by the IETF, MPLS-TP provides:

- Predetermined and long-lived connections.
- Emphasis on manageability and deterministic behavior.
- Fast fault detection and recovery.
- Inband OAM.

MPLS-TP features include:

- Manually provisioned MPLS-TP LSPs.
- Reserved bandwidth for static MPLS-TP LSPs.
- One-to-one path protection for MPLS-TP LSPs.
- Working/Protected LSP switchover.
- Continuity Check (CC), Proactive Continuity Verification (CV), and Remote Defect Indication (RDI) based on BFD.
- New fault OAM functions resulting from the MPLS-TP standardization effort.

Prime Network automatically discovers network MPLS-TP tunnels from end to end, including LSPs, tunnel endpoints, and bandwidth. Network LSPs contain LSP endpoints and midpoints and are identified as working or protected.

Prime Network links the MPLS-TP tunnel components appropriately, provides a visual representation in Vision client maps, and displays the properties in logical inventory.

Prime Network employs warm start technology when rebooting. That is, when rebooting, Prime Network compares existing MPLS-TP tunnel information to topology changes that occur while Prime Network is down and updates MPLS-TP tunnel accordingly when Prime Network returns to operation.

The following options are available for working with MPLS-TP tunnels in the Vision client:

- Adding an MPLS-TP Tunnel, page 17-7
- Viewing MPLS-TP Tunnel Properties, page 17-9
- Viewing LSPs Configured on an Ethernet Link, page 17-13
- Viewing LSP Endpoint Redundancy Service Properties, page 17-15
- Applying an MPLS-TP Tunnel Overlay, page 17-17
- Viewing BFD Session Properties, page 17-50.

Adding an MPLS-TP Tunnel

Prime Network automatically discovers MPLS-TP tunnels, endpoints, and midpoints and enables you to add MPLP-TP tunnels to maps.

To add an MPLS-TP tunnel to a map:

Step 1 In the Vision client, display the map to which you want to add the MPLS-TP tunnel.

Step 2 Do either of the following:

- From the File menu, choose **Add to Map > MPLS-TP Tunnel**.
- In the main toolbar, click **Add to Map**, then choose **Add to Map > MPLS-TP Tunnel**.

The Add MPLS-TP Tunnel dialog box is displayed.

Step 3 Do either of the following:

- Choose a search category, enter a search string, then click **Go** to narrow search results to a range of MPLS-TP tunnels or a specific MPLS-TP tunnel. Search categories include:
  - Description
  - Name
  - System Name
- Choose **Show All** to display all the MPLS-TP tunnels.

Step 4 Select the MPLS-TP tunnel that you want to add to the map.

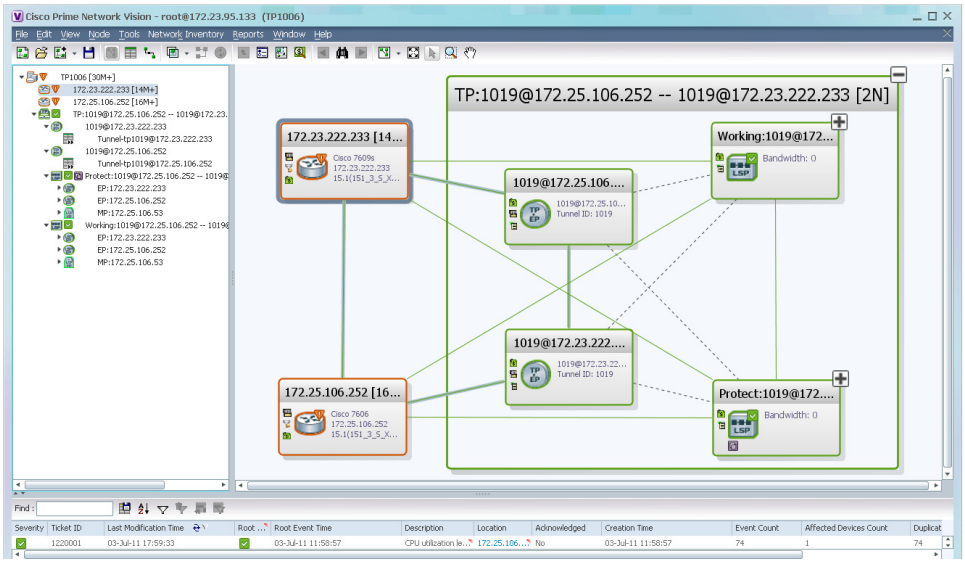
Step 5 Click **OK**.

The MPLS-TP tunnel is added to the map and to the navigation pane.

In Figure 17-3:

- The devices are on the left side of the map, and the MPLS-TP tunnel is displayed in a thumbnail on the right.
- The devices are connected to each other and to the MPLS-TP tunnel via tunnels.
- Physical links connect the devices to the Working and Protected LSPs.
- A redundancy service badge is displayed next to the Protected LSP in the navigation and map panes.
- In the thumbnail:
  - The tunnel endpoints are connected to each other via a tunnel.
  - A physical link connects the Working and Protected LSPs.
  - Business links connect the Working and Protected LSPs to each endpoint.

Figure 17-3 MPLS-TP Tunnel in Vision Map

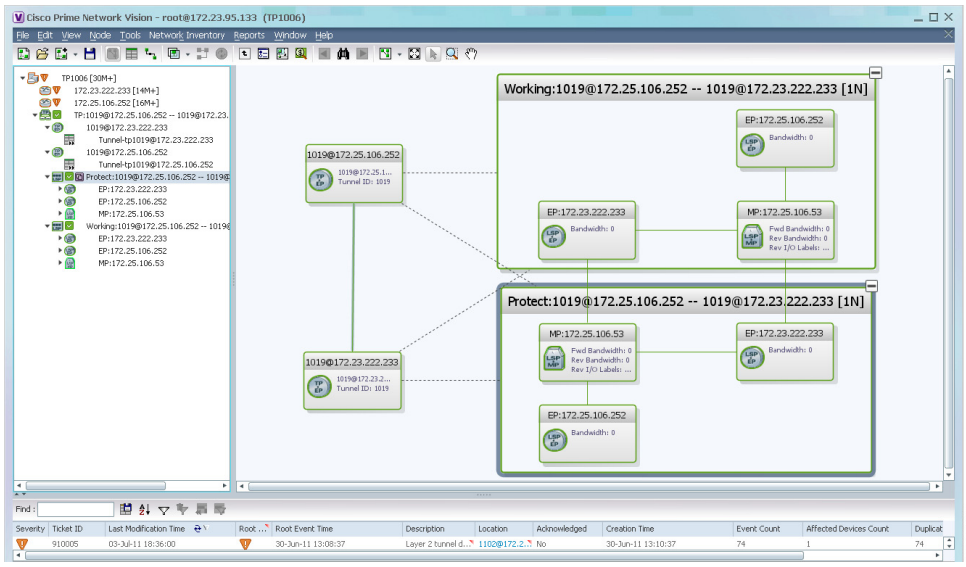


If an LSP is in lockout state, it is displayed with the lock badge ( ).

By expanding all aggregations in the MPLS-TP tunnel (see Figure 17-4), you can see components and links in the MPLS-TP tunnel, including:

- MPLS-TP tunnel endpoints
- LSP endpoints
- LSP midpoints

Figure 17-4 MPLS-TP Tunnel Expanded



If an LSP is configured for redundancy service, a redundancy service badge is applied to the secondary (backup) LSP in the navigation and map panes in the navigation and map panes.

For more information about LSP redundancy service, see Viewing LSP Endpoint Redundancy Service Properties, page 17-15.

Viewing MPLS-TP Tunnel Properties

Prime Network discovers and displays MPLS-TP attributes in the MPLS-TP branch in logical inventory as described in this topic.

Additional information about MPLS-TP tunnel properties are available in the following branches:

- Routing Entities—See Viewing Routing Entities, page 17-32.
- LSEs—See Viewing Label Switched Entity Properties, page 17-41.
- Pseudowires— See Viewing Pseudowire End-to-End Emulation Tunnels, page 17-58.

To view MPLS-TP tunnel properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > MPLS-TP > MPLS-TP Global**.

The routing information is displayed as shown in Figure 17-5.

Figure 17-5 MPLS-TP Tunnel Properties in Logical Inventory

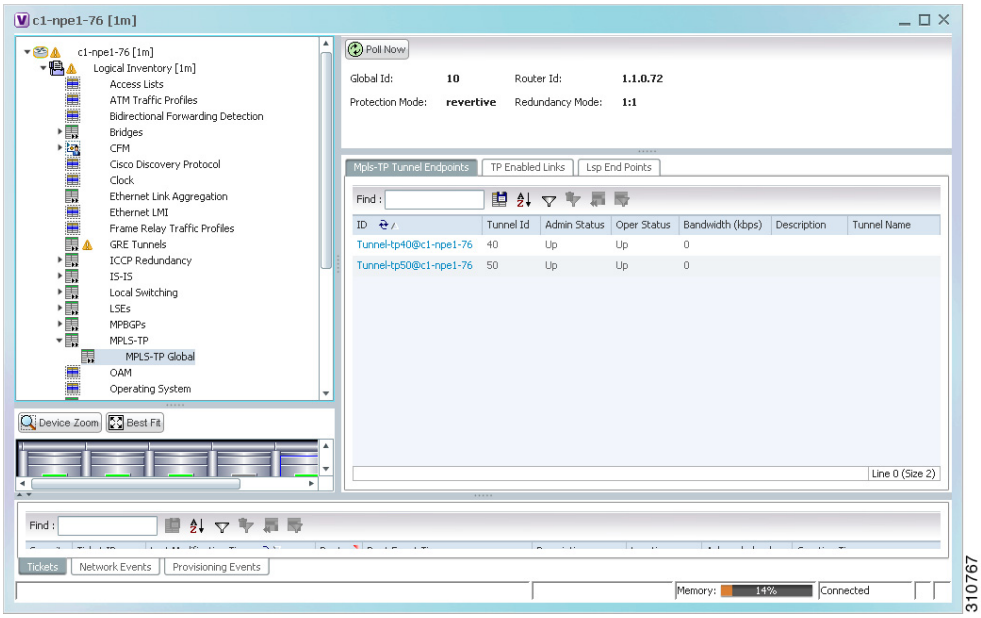


Table 17-3 describes the information that is available for MPLS-TP tunnels. The information that is displayed depends on the configuration.

Table 17-3 MPLS-TP Tunnel Properties in Logical Inventory

Field	Description
Global ID	Globally unique Attachment Interface Identifier (AII) for MPLS-TP derived from the Autonomous System Number (ASN) of the system hosting the PEs.
Router ID	MPLS-TP source node identifier for this element in the form of an IPv4 address.
Protection Mode	Whether the transmitting endpoint is in revertive or nonrevertive mode: • Revertive—If the protection mode is revertive and a failed path is restored, the traffic automatically returns, or reverts, to the original path. • Nonrevertive—If the protection mode is nonrevertive and a failed path is restored, the traffic does not return to the original path. That is, the traffic does not revert to the original path.
Redundancy Mode	Level of redundancy for the MPLS-TP tunnel: 1:1, 1+1, or 1:N.
MPLS-TP Tunnel Endpoints Tab	
ID	Tunnel endpoint identifier as a Tunnel-tp interface on the selected network element.
Tunnel ID	Unique tunnel identifier.
Admin Status	Administrative status of the tunnel: Up or Down.
Oper Status	Operational status of the tunnel: Up or Down.
Bandwidth (kbps)	Configured bandwidth (in Kb/s) for the tunnel.
Description	Tunnel description.
TP Enabled Links Tab	
Link ID	Identifier assigned to the MPLS-TP interface.
Interface	Hyperlink to the interface in physical inventory.
Next Hop	IP address of the next hop in the path.
LSP End Points Tab	
LSP ID	LSP identifier, derived from both endpoint identifiers and using the format *src-node-ID*::*src-tunnel-number*::*dest-node-ID*::*dest-tunnel-number* where: • *src-node-ID* represents the identifier of the node originating the signal exchange. • *src-tunnel-number* represents source tunnel identifier. • *dest-node-ID* represents the identifier of the target node. • *dest-tunnel-number* represents the destination tunnel identifier.
LSP Type	Indicates whether the LSP is active (Working) or backup (Protect).
In Label	Incoming label identifier.
Out Label	Outgoing label identifier.
Out Interface	Outgoing interface hyperlinked to the relevant entry in physical inventory.
Bandwidth (kbps)	Bandwidth specification in Kb/s.
Role (Oper Status)	Role of the LSP endpoint (Active or Standby) with the operational status (UP or DOWN).

Table 17-3 MPLS-TP Tunnel Properties in Logical Inventory (continued)

Field	Description
LSP Mid Points Tab	
LSP ID	LSP identifier, derived from both endpoint identifiers and using the format *src-node-ID*::*src-tunnel-number*::*dest-node-ID*::*dest-tunnel-number* where: • *src-node-ID* represents the identifier of the node originating the signal exchange. • *src-tunnel-number* represents source tunnel identifier. • *dest-node-ID* represents the identifier of the target node. • *dest-tunnel-number* represents the destination tunnel identifier.
LSP Type	Indicates whether the LSP is active (Working) or backup (Protect).
Forward In Label	Incoming label identifier in the forward direction (source to destination).
Forward Out Label	Label selected by the next hop device in the forward direction.
Reverse In Label	Incoming label identifier in the reverse direction (destination to source).
Reverse Out Label	Label selected by the next hop device in the reverse direction.
Forward Out Interface	Outgoing interface in the forward direction, hyperlinked to its entry in physical inventory.
Forward Bandwidth (kbps)	Bandwidth specification in Kb/s for the forward direction.
Reverse Out Link ID	Link identifier assigned to the outgoing interface in the reverse direction.
Reverse Out Interface	Outgoing interface in the reverse direction, hyperlinked to its entry in physical inventory.
Reverse Bandwidth	Bandwidth specification in Kb/s for the reverse direction.
Internal ID	Identifier associated with the parent entity of the link. Using an internal identifier ensures that individual LSP links do not participate in multiple network LSPs.

Step 3 To view additional MPLS-TP tunnel endpoint properties, double-click the required entry in the MPLS-TP Tunnel Endpoints table.

The MPLS-TP Tunnel Properties window is displayed as shown in Figure 17-6.

Figure 17-6 MPLS-TP Tunnel Properties Window

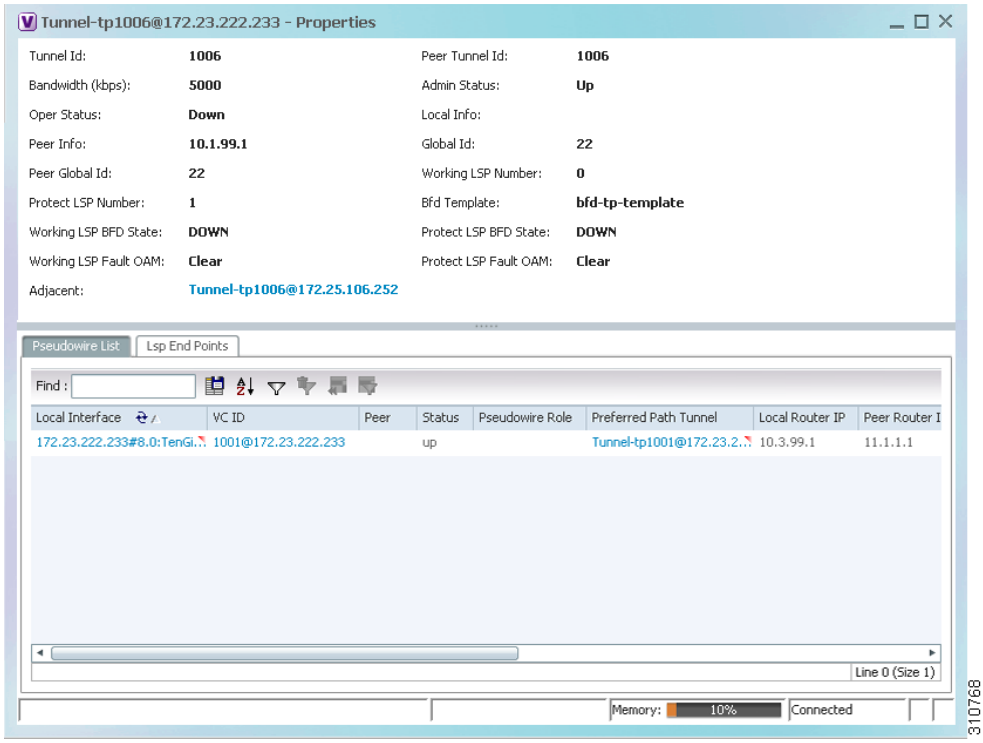


Table 17-4 describes the information available in the top portion of the MPLS-TP Tunnel Properties window. For information about the tabs that are displayed, see Table 17-3.

Table 17-4 MPLS-TP Tunnel Properties Window

Field	Description
Tunnel ID	Unique tunnel identifier.
Peer Tunnel ID	Unique identifier of peer tunnel.
Bandwidth (kbps)	Configured bandwidth (in Kb/s) for the tunnel.
Admin Status	Administrative status of the tunnel: Up or Down.
Oper Status	Operational status of the tunnel: Up or Down.
Local Info	MPLS-TP source node identifier for this element in the form of an IPv4 address.
Peer Info	MPLS-TP peer node identifier in the form of an IPv4 address.
Global ID	Globally unique Attachment Interface Identifier (AII) for MPLS-TP derived from the Autonomous System Number (ASN) of the system hosting the PEs.
Peer Global ID	Globally unique AII for the peer.
Working LSP Number	Number assigned to the working LSP. By default, the working LSP number is 0 and the protected LSP number is 1.
Protect LSP Number	Number assigned to the protected LSP. By default, the working LSP number is 0 and the protected LSP number is 1.
BFD Template	BFD template associated with this MPLS-TP tunnel.

Table 17-4 MPLS-TP Tunnel Properties Window (continued)

Field	Description
Working LSP BFD State	Configured state of the working LSP BFD template: Up or Down.
Protect LSP BFD State	Configured state of the protected LSP BFD template: Up or Down.
Working LSP Fault OAM	Indicates that a fault has been detected on the working LSP.
Protect LSP Fault OAM	Indicates that a fault has been detected on the protected LSP.
Tunnel Name	Tunnel name.
Adjacent	Hyperlink to the adjacent endpoint in logical inventory.

Viewing LSPs Configured on an Ethernet Link

A single Ethernet link can support a number of LSPs. The Vision client enables you to view all LSPs on a single Ethernet link and to identify the source and destination labels.

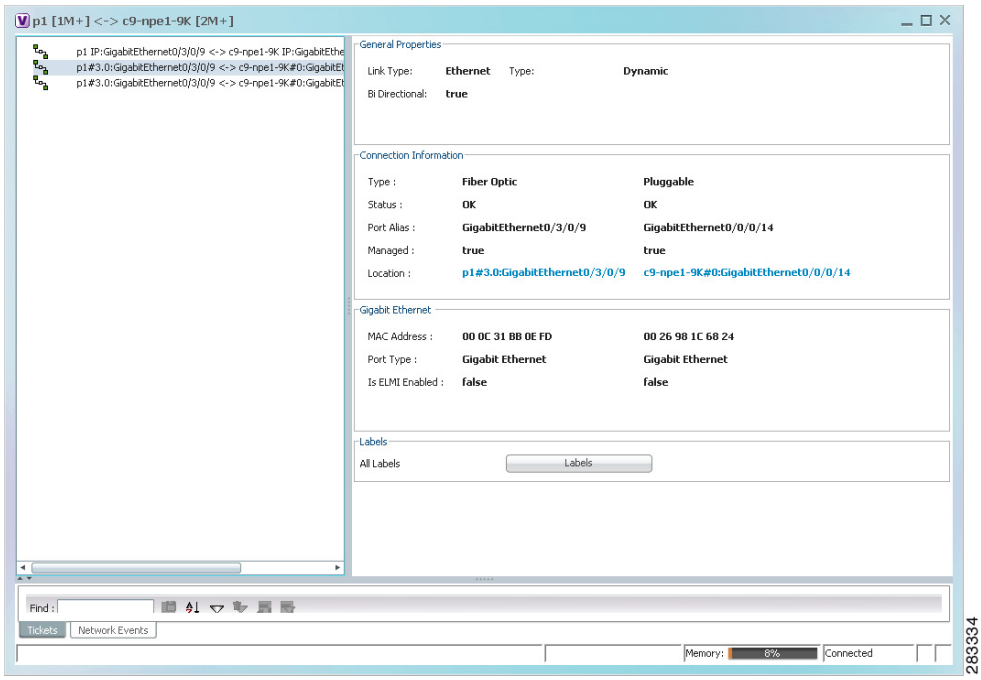
To view LSPs configured on an Ethernet link:

Step 1 In the map view, right-click the required link and choose **Properties**.

Step 2 In the link properties window, choose the required Ethernet link.

The link properties window refreshes and displays the Labels button as shown in Figure 17-7.

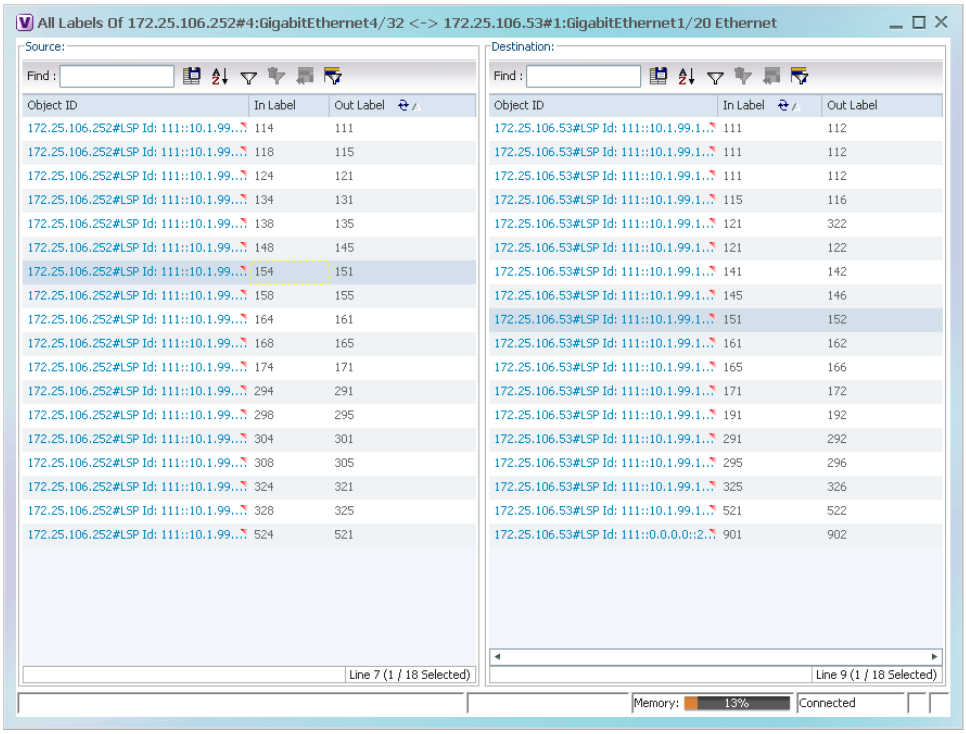
Figure 17-7 Link Properties Window with All Labels Button



Step 3 Click **Labels**.

The All Labels window is displayed as shown in Figure 17-8 with the LSP sources and destinations.

Figure 17-8 All Labels Table



Step 4 To identify a specific path, click an outgoing label in the Source table. The corresponding in label is selected in the Destination table.

Viewing MPLS-TE and P2MP-MPLS-TE links in a map

Using the link filter available in Prime Network, you can view only the MPLS-TE and P2MP-MPLS-TE links in a map.

Note The MPLS Point-to-Multipoint Traffic Engineering (P2MP TE) feature enables you to forward Multiprotocol Label Switching (MPLS) traffic from one source to multiple destinations.

To view the MPLS-TE and P2MP-MPLS-TE links in a map:

Step 1 Open the required map.

Step 2 Click the Link filter icon in the navigation menu.

Step 3 In the Link Filter window, select the **MPLS-TE** and **P2MP MPLS-TE** check boxes.

Step 4 Click **OK**. The map refreshes and displays only the **MPLS-TE** and **P2MP MPLS-TE** links.

Step 5 Right-click on the link and choose the **Properties** option.

Step 6 In the Link Properties window, the type of link is displayed in the **Link Type** field, which can be either **MPLS-TE** and **P2MP MPLS-TE** based on the link that you have selected. Additional details about the link such as the MPLS TE tunnel, operational status of the tunnel, TE tunnel type are displayed in the **Label Switching** section. For more information about the Link Properties window, see Viewing LSPs Configured on an Ethernet Link, page 17-13.

Viewing LSP Endpoint Redundancy Service Properties

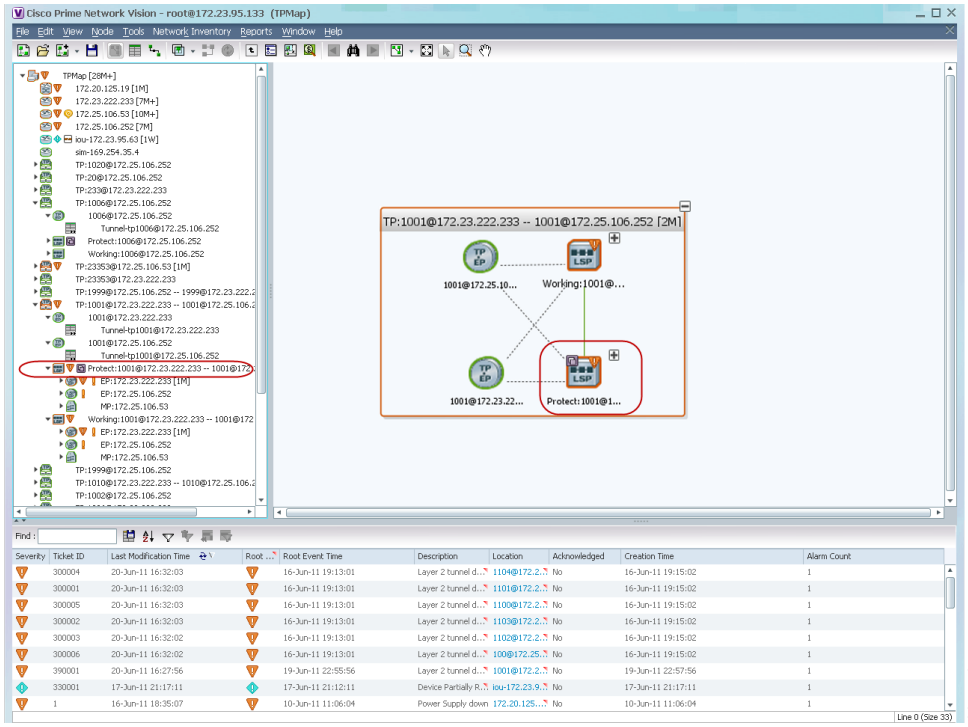
If an LSP endpoint in an MPLS-TP tunnel is configured for redundancy service, a redundancy service badge is applied to the secondary (backup) LSP endpoint in the navigation and map panes in the Vision client. Additional redundancy service details are provided in the LSP endpoint properties window and the inventory window for the element on which the MPLS-TP tunnel is configured.

To view LSP endpoint redundancy service properties:

Step 1 To determine if an LSP endpoint on an MPLS-TP tunnel is configured for redundancy service, expand the required MPLS-TP tunnel in the navigation or map pane.

If the LSP endpoint is configured for redundancy service, the redundancy service badge is displayed in the navigation and map panes as shown in Figure 17-9.

Figure 17-9 LSP Endpoint with Redundancy Service Badge



Step 2 To view properties for the LSP endpoint, navigate to and right-click the required endpoint in the map or navigation pane, and choose **Properties**.

The LSP endpoint properties window is displayed as shown in Figure 17-10.

Figure 17-10 LSP Endpoint Properties Window

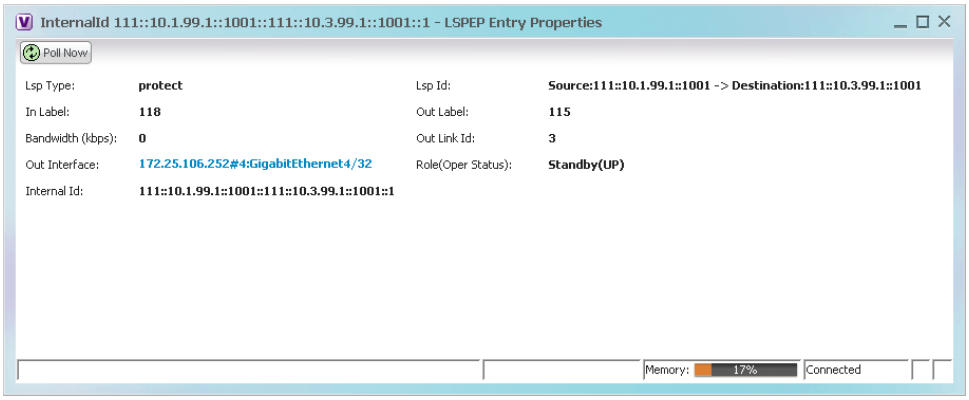


Table 17-5 describes the information displayed in the LSP Endpoint Properties window.

Table 17-5 LSP Endpoint Properties Window

Field	Description
LSP Type	Indicates whether the LSP is active (Working) or backup (Protected).
LSP ID	LSP identifier, derived from both endpoint identifiers and using the format *src-node-ID*::*src-tunnel-number*::*dest-node-ID*::*dest-tunnel-number* where: • *src-node-ID* represents the identifier of the node originating the signal exchange. • *src-tunnel-number* represents source tunnel identifier. • *dest-node-ID* represents the identifier of the target node. • *dest-tunnel-number* represents the destination tunnel identifier.
In Label	Incoming label identifier.
Out Label	Outgoing label identifier.
Bandwidth (kbps)	Bandwidth specification in Kb/s.
Out Link ID	Link identifier assigned to the outgoing interface.
Out Interface	Outgoing interface hyperlinked to the relevant entry in physical inventory.
Role (Oper Status)	Role of the LSP endpoint (Active or Standby) with the operational status (UP or DOWN)

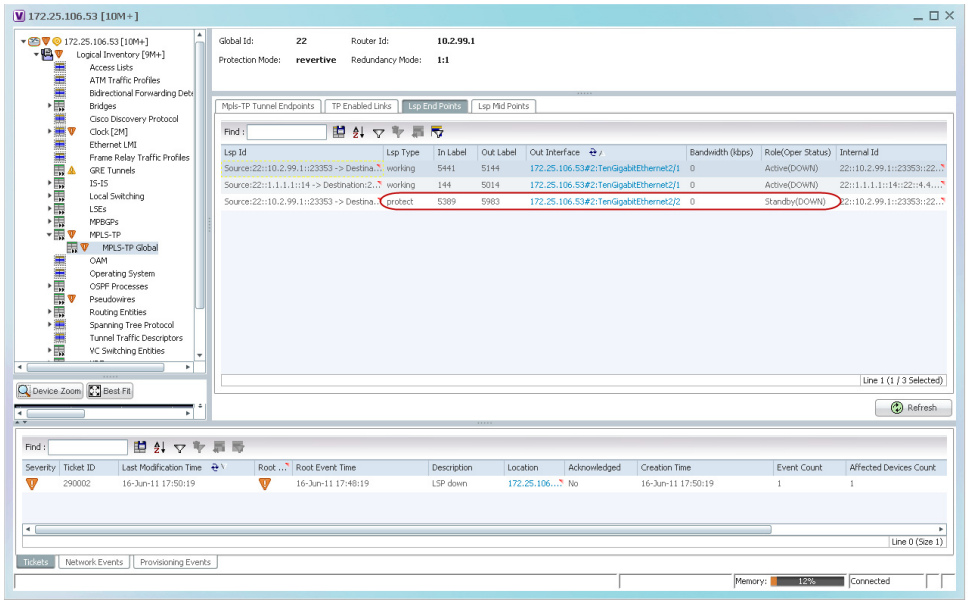
Step 3 To view LSP endpoint redundancy status in inventory, double-click the element on which the MPLS-TP tunnel is configured.

Step 4 Choose **Logical Inventory > MPLS-TP > MPLS-TP Global > LSP End Points**.

Step 5 The LSP End Points tab contains the following information related to LSP redundancy service (see Figure 17-11):

- Whether the LSP endpoint is Working or Protected.
- The LSP endpoint role, either Active or Standby.
- The operational status of the LSP endpoint, either Up or Down.

Figure 17-11 LSP End Points Tab in Logical Inventory



Applying an MPLS-TP Tunnel Overlay

You can select and display an overlay of a specific MPLS-TP tunnel on top of the devices displayed in a map view. The overlay is a snapshot of the network that visualizes the flows between the sites and tunnel peers. When an MPLS-TP tunnel is selected in the map, the following elements are highlighted in the map:

- Elements on which TP endpoints and LSPs are configured.
- Links that carry TP traffic.

All elements and links that are not part of the MPLS-TP tunnel are dimmed.

To apply an MPLS-TP tunnel overlay:

Step 1 In the Vision client, display the network map on which you want to apply an overlay.

Step 2 From the main toolbar, click **Choose Overlay Type** and choose **MPLS-TP tunnel**.

The Select MPLS-TP tunnel Overlay dialog box is displayed.

Step 3 Do one of the following:

- Choose a search category, enter a search string, then click **Go** to narrow the search results to a range of MPLS-TP tunnels or a specific MPLS-TP tunnel. Search categories include:
  - Description
  - Name
  - System Name

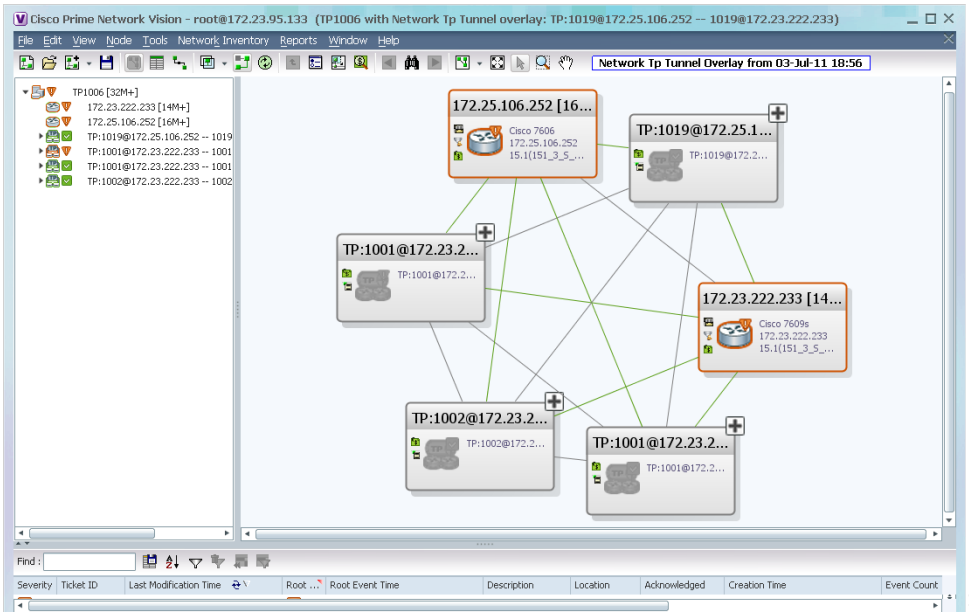
  The search condition is “contains.” Search strings are case-insensitive. For example, if you choose the Name category and enter “net,” the Vision client displays VPNs “net” and “NET” in the names whether net appears at the beginning, middle, or at the end of the name: for example, Ethernet.

- Choose **Show All** to display all MPLS-TP tunnels.

Step 4 Select the MPLS-TP tunnel overlay you want to apply to the map.

The elements and links used by the selected MPLS-TP tunnel are highlighted in the network map, and the MPLS-TP tunnel name is displayed in the window title bar as shown in Figure 17-12.

Figure 17-12 MPLS-TP Tunnel Overlay

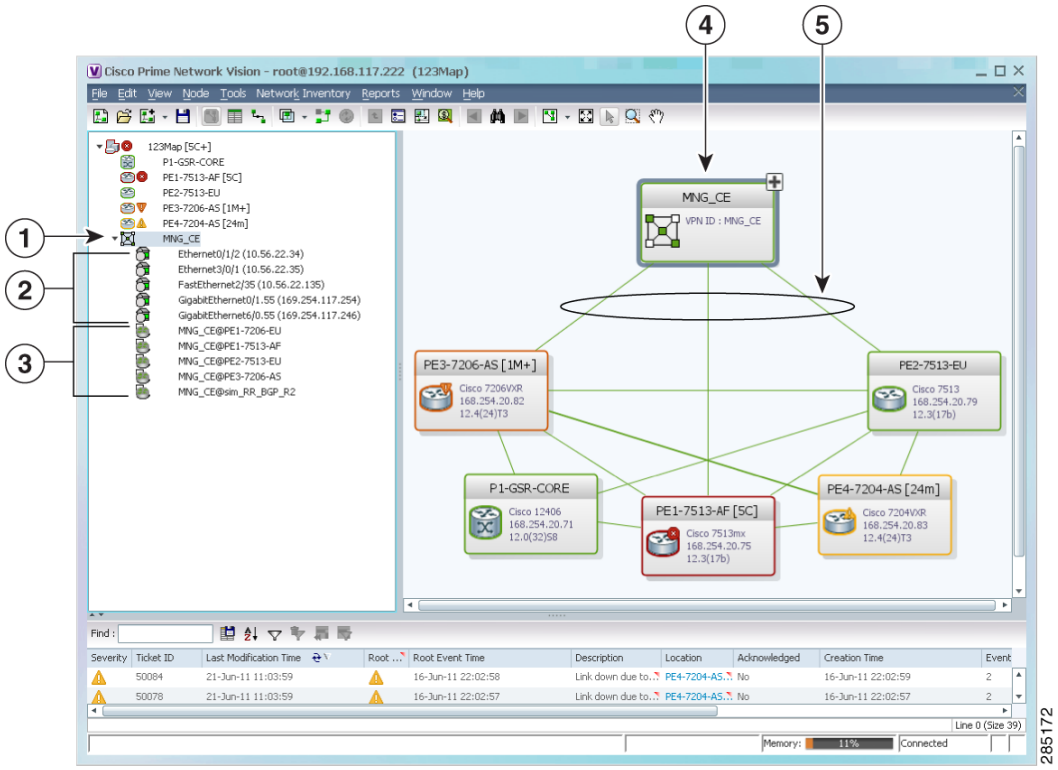


Note An overlay is a snapshot taken at a specific point in time and does not reflect changes that occur in the service. As a result, the information in an overlay can become stale. To update the overlay, click **Refresh Overlay** in the main toolbar.

Viewing VPNs

Figure 17-13 shows a VPN displayed in the Vision client map view. In this example, the VPN is selected in the navigation pane, so the VPN details, such as virtual routers and IP interfaces, are not shown in the map view.

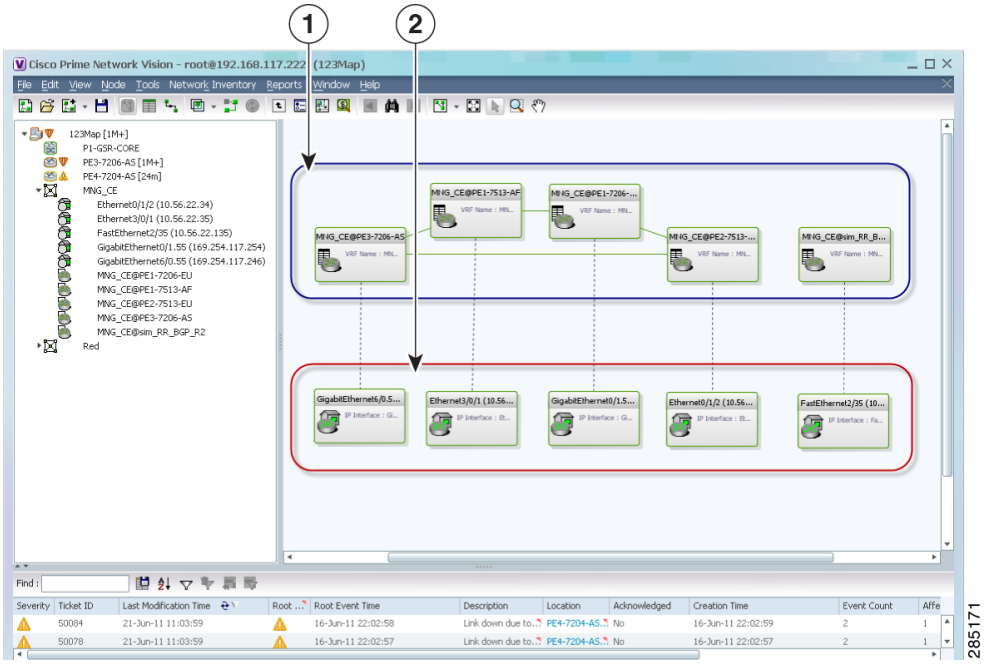
Figure 17-13 VPN in Vision Map



1	VPN in the navigation tree	**4**	VPN in the map view
2	Sites	**5**	VPN links
3	Virtual routers		

Figure 17-14 shows a VPN with details, including virtual routers and sites, in the Vision client map view.

Figure 17-14 VPN in Vision Map with VRFs and Sites



1	Virtual routers
2	Sites

The the Vision client navigation pane displays the VPN business elements in a tree-and-branch representation. Each business element is represented by an icon in a color that reflects the highest alarm severity. The icon might also have a management state badge or alarm. For more information about icon severity colors and badges, see Interpreting the Badges and Colors of an NE, page 11-9.

Table 17-6 shows the VPN icons in the Vision client map view.

The highest level of the navigation pane displays the root or map name. The branches display the VPN

Table 17-6 VPN Icons in Vision Map

Icon	Description
	Root (map name) or aggregation
	VPN
	Virtual router
	Site

and aggregated business elements as well as their names. The Layer 3 VPN sub-branch displays the virtual routers and sites contained in the VPN along with the names of the business elements. In addition, CE devices can be displayed in the Layer 2 and Layer 3 VPN sub-branches. If you select an aggregated business element in the navigation pane, the map view displays the business elements contained within the aggregated business element.

The the Vision client map view displays the VPN business elements and aggregated business elements loaded in the map view, along with the names of the business elements. In addition, the map view displays the VPN topology (between the virtual routers in the VPNs) and the topology and associations between other business elements. After you select the root in the navigation pane, the map view displays all the VPNs.

The Vision client presents tickets related to the map in the ticket area, which allows you to view and manage the VPN tickets.

Viewing Additional VPN Properties

The Vision client allows you to select any element in the navigation pane or map view and view additional underlying properties. To view additional properties for an object, either double-click it or right-click it and choose **Properties**. Table 17-7 shows the additional properties available for VPN entities.

Table 17-7 Displaying Additional VPN Properties

Object	Option	For Additional Information
VPN	• Double-click a VPN to view the participating VRFs, sites, and network elements in the navigation pane and map view. • Right-click a VPN and choose **Properties** to view the VPN Properties window.	Viewing VPN Properties, page 17-27
VRF	Double-click a VRF to view the VRF properties window.	Viewing VRF Properties, page 17-28

Table 17-7 Displaying Additional VPN Properties (continued)

Object	Option	For Additional Information
Site	Double-click a site to view the IP Interface Properties window	Viewing Site Properties, page 17-28
Link	Double-click a link to view the link properties window. The properties are dependent on the link type.	Viewing and Managing Links, page 7-20

Managing VPNs

The following topics describe:

- Creating a VPN, page 17-22
- Adding a VPN to a Map, page 17-23
- Removing a VPN from a Map, page 17-24
- Moving a Virtual Router Between VPNs, page 17-24

Creating a VPN

You can change business configurations by manually creating VPNs. The VPNs that are manually created do not contain virtual routers and sites.

To create a VPN:

Step 1 In the Vision client navigation pane, select the map root.

Step 2 From the File menu, choose **Add to Map > VPN > New**.

Step 3 In the Create VPN dialog box, enter the following:

- Name—A unique name for the new VPN.

  Note VPN business element names are case sensitive.

- Icon—To use a custom icon for the VPN, click the button next to the Icon field and navigate to the icon file.

  Note If a path is not specified to an icon, the default VPN icon is used (for more information about icons, see Table 17-6 on page 17-21).

- Description—(Optional) An additional VPN description.

Step 4 Click **OK**.

The new VPN is added to the VPN list in the Add VPN dialog box.

For more information about loading the newly created VPN in the service view map, see Adding a VPN to a Map, page 17-23.

Adding a VPN to a Map

You can add a VPN to a map view if the VPN was previously created by a user or discovered by Prime Network and are not currently displayed in the map.

Note Adding a VPN affects other users if they are working with the same map.

To add an existing VPN to a map:

Step 1 In the Vision client, display the map to which you want to add the VPN.

Step 2 Do either of the following:

- From the File menu, choose **Add to Map > VPN > Existing**.
- In the main toolbar, click **Add to Map**, then choose **Add to Map > VPN > Existing**.

The Add VPN dialog box is displayed.

Step 3 Do either of the following:

- Choose a search category, enter a search string, then click **Go** to narrow search results to a range of VPNs or a specific VPN. Search categories include:
  - Description
  - Name

  The search condition is “contains.” Search strings are case-insensitive. For example, if you choose the Name category and enter “net,” the Vision client displays VPNs “net” and “NET” in the names whether net appears at the beginning, middle, or at the end of the name.
- Choose **Show All** to display all the VPNs.

Step 4 Select the VPN that you want to add to the map.

Tip Press **Shift** or **Ctrl** to choose multiple adjoining or nonadjoining VPNs.

Step 5 Click **OK**.

The VPN is displayed in the navigation pane and the selected map or subnetwork in the Vision client window content pane. In addition, any tickets are displayed in the ticket area.

When a VPN service is added to a map, then a new link is available between the ethernet flow point that represents the pseudowire headend port and the site in the VPN to which it is connected.

If your network has a L3VPN connected to a pseudowire via a PWHe, then EVC will also include the L3VPN in the EVC that contains the pseudowire.

Removing a VPN from a Map

You can remove one or more VPNs from the current active map. This change does not affect other maps. Removing a VPN from a map does not remove it from the Prime Network database. The VPN will appear in the Add VPN dialog box, so you can add it back to the map at any time.

When removing VPNs from maps, keep the following in mind:

- Removing a VPN affects other users if they are working with the same map view.
- This option does not change the business configuration or database.
- You cannot remove virtual routers or sites from the map without removing the VPN.

To remove a VPN, in the Vision client pane or map view, right-click the VPN and choose **Remove from Map**.

The VPN is removed from the map view along with all VPN elements, such as connected CE devices. Remote VPNs (extranets) are not removed.

Note If the routing information changes after an overlay is applied, the changes do not appear in the current overlay. Click **Refresh Overlay** to update the routing information.

Moving a Virtual Router Between VPNs

You can move a virtual router (including its sites) from one VPN to another after you create a VPN and add it to the service view map.

Note Moving a virtual router moves all of its sites as well.

To move a virtual router:

Step 1 In the Vision client navigation pane or map, right-click the virtual router and choose **Edit > Move selected**.

Step 2 Right-click the required VPN in the navigation pane or map to where you want to move the virtual router and choose **Edit > Move here**.

Caution Moving a virtual router from one VPN to another affects all users who have the virtual router loaded in their service view map.

The virtual router and its sites are displayed under the selected VPN in the navigation pane and in the map.

Working with VPN Overlays

The following topics describe:

Applying VPN Overlays

You can select and display an overlay of a specific VPN on top of the devices displayed in a map view. The overlay is a snapshot of the network that visualizes the flows between the sites and tunnel peers. When one network VPN is selected in the network map, the PE routers, MPLS routers, and physical links that carry the LSP used by the VPN are highlighted in the network map. All the devices and links that are not part of the VPN are dimmed.

The VPN service overlay allows you to isolate the parts of a network that are being used by a particular service. This information can then be used for troubleshooting. For example, the overlay can highlight configuration or design problems when bottlenecks occur and all the site interlinks use the same link.

To apply a VPN overlay:

Step 1 In the Vision client, display the network map on which you want to apply an overlay.

Step 2 From the main toolbar, click **Choose Overlay Type** and choose **VPN**.

The Select VPN Overlay dialog box is displayed.

Step 3 Do one of the following:

- Choose a search category, enter a search string, then click **Go** to narrow the search results to a range of VPNs or a specific VPN. Search categories include:
  - Description
  - Name

  The search condition is “contains.” Search strings are case-insensitive. For example, if you choose the Name category and enter “net,” the Vision client displays VPNs “net” and “NET” in the names whether net appears at the beginning, middle, or at the end of the name: for example, Ethernet.
- Choose **Show All** to display all the VPNs.

Step 4 Select the VPN overlay that you want to apply to the map.

The PE routers, MPLS routers, and physical links used by the selected VPN are highlighted in the network map. The VPN name is displayed in the title of the window.

Note An overlay is a snapshot taken at a specific point in time and does not reflect changes that occur in the service. As a result, the information in an overlay can become stale. To update the overlay, click **Refresh Overlay** in the main toolbar.

Managing a VPN Overlay Display in the Map View

After a VPN overlay is applied to a map, you can manage its display by using the overlay tools in the main toolbar:

- To display the overlay, click **Show Overlay** on the main toolbar.
- To hide an active overlay, click **Hide Overlay** on the main toolbar.

Note The Show Overlay button is a toggle. When clicked, the overlay is displayed. When clicked again, the overlay is hidden.

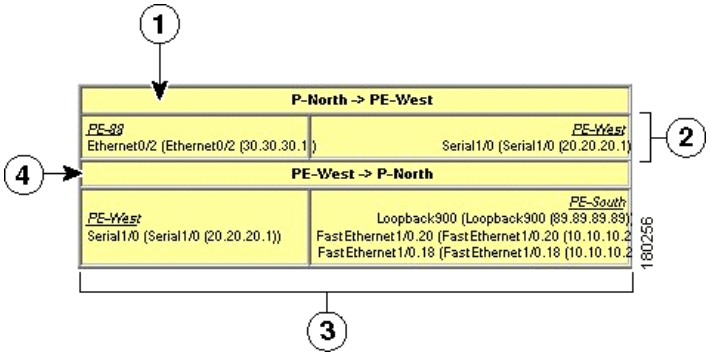
- To remove the VPN overlay, choose **Show Overlay Type > None**.

Displaying VPN Callouts in a VPN Overlay

You can display or hide the callouts for VPN links displayed in a VPN overlay to show the details of the sites that are interlinked through the selected links. The callouts (see Figure 17-15) enable you to view the VPN traffic links for a specific link (either bidirectional or unidirectional).

Note The link must be displayed in the VPN overlay and not dimmed for you to display the link callouts.

Figure 17-15 Callouts Window



1	Link details and direction. In this example, the link is from P-North to PE-West.	**3**	Details of sites using the link and interlinks. In this example, the site PE-West is linked to all sites on PE-South.
2	Details of the sites using the link and interlinks. In this example, the site PE-88 is linked to site PE-West.	**4**	Link details and the direction. In this example, the link is from PE-West to P-North.

To display or hide the callouts:

Step 1 In the Vision client window, display the map view with the VPN overlay.

Step 2 Right-click the required link in the map view and choose **Show Callouts**.

Step 3 To hide the callouts, right-click the link in the map view that is displaying the callouts and choose **Hide Callouts**.

Monitoring MPLS Services

The following topics provide details for viewing MPLS services and technologies:

Viewing VPN Properties

To view the properties of a VPN:

Step 1 In the Vision client navigation pane or map view, do either of the following:

- If the VPN icon is of the largest size, click the **Properties** button.
- Right-click the VPN and choose **Properties**.

The VPN Properties window displays the following information:

- Name—Name of the VPN.
- ID—Unique identifier assigned to the VPN.

Step 2 Click **Close** to close the VPN Properties dialog box.

Viewing Site Properties

The Vision client enables you to view site properties, including the interfaces that are configured on the PE device. The displayed properties reflect the configuration that Prime Network automatically discovered for the device.

To view site properties, in the Vision client navigation pane or map view, right-click the required site and choose **Properties**.

Table 17-8 describes the information that is displayed in the Router IP Interface Properties window:

Table 17-8 Router IP Interface Properties Window for Sites

Field	Description
Name	Name of the site, such as FastEthernet4/1.252.
State	Interface state, either Up or Down.
IP Address	IP address of the interface.
Mask	Network mask.
Interface Description	Description applied to the interface.
Associated Entity	Element and interface associated with the site, hyperlinked to its entry in physical inventory.
Addresses Table	
Subnet	IP address and subnet mask. **Note** If the site is an IPv6 VPN over MPLS with IPv6 addresses provisioned, the IPv6 addresses are displayed. For more information, see Viewing IPv6 Information (6VPE), page 17-1.
Type	Address type, such as Primary, Secondary, or IPv6 Unicast.

Viewing VRF Properties

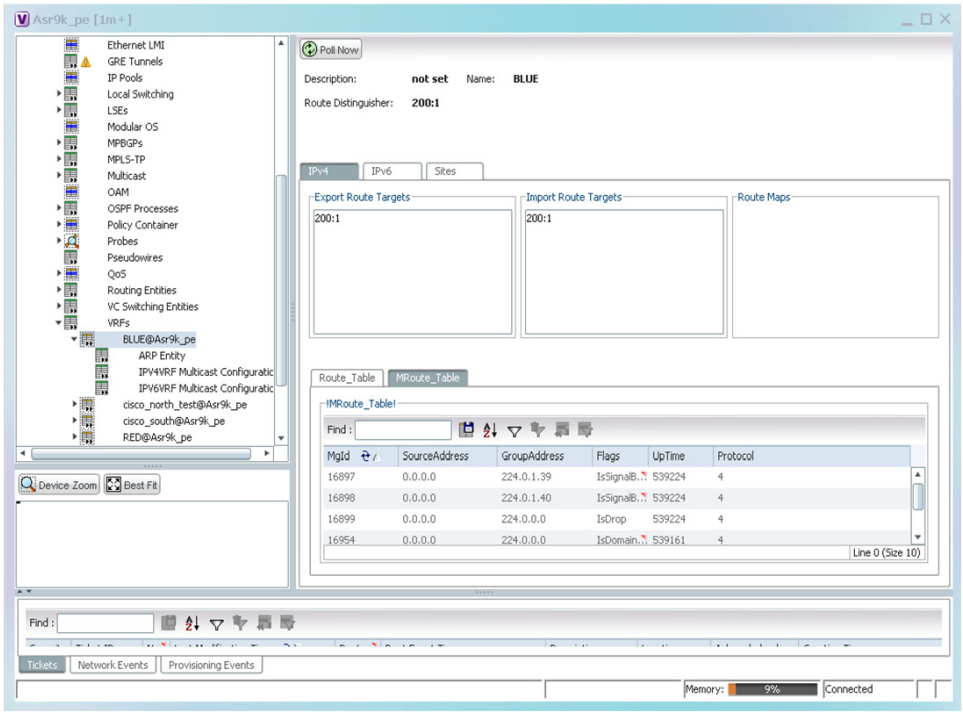
The Vision client enables you to view VRF properties, including the VRF route distinguisher, import and export route targets, and any provisioned sites and VRF routes.

To view VRF properties, do either of the following in map view:

- Double-click the element configured for VRFs.
- Expand the required VPN and double-click the virtual router.

The VRF properties window is displayed as shown in Figure 17-16.

Figure 17-16 VRF Properties



The VRF Properties window contains the VRF routing table for the device. The table is a collection of routes that are available or reachable to all the destinations or networks in the VRF. The forwarding table also contains MPLS encapsulation information.

Table 17-9 describes the information displayed in the VRF Properties window.

Note The VRF Properties window only displays properties and attributes that are provisioned in the VRF. You might not see all the fields and tabs described in Table 17-9.

Table 17-9 VRF Properties

Field	Description
Route Distinguisher	Route distinguisher configured in the VRF.
Name	VRF name.
Associate VNI	The **Associated VNI** field in the content pane displays the VXLAN ID associated with the VRF. You can click the link to go to the corresponding VNI row in the VNI Details pane.
Description	Description of the VRF.
IPv4 Tab	
Export Route Targets	IPv4 export route targets contained by the VRF.
Import Route Targets	IPv4 import route targets contained by the VRF.

Table 17-9 VRF Properties (continued)

Field	Description
Route Maps	Route maps for the VRF.
IPv6 Tab	
Export Route Targets	IPv6 export route targets contained by the VRF.
Import Route Targets	IPv6 import route targets contained by the VRF.
Route Maps	Route maps for the VRF.
Routing Tables	
Destination	Destination of the specific network.
Prefix Length	Length of the network prefix in bits.
Next Hop	Next routing hop.
Outgoing Interface	Name of the outgoing interface; displayed if the Routing Protocol type is local.
Type	Route type: Direct (local), Indirect, or Static.
Routing Protocol	Routing protocol used to communicate with the other sites and VRFs: BGP or local.
BGP Next Hop	Border Gateway Protocol (BGP) next hop. This is the PE address from which to continue to get to a specific address. This field is empty when the routing entry goes to the CE.
Bottom In Label	Innermost label that is expected when MPLS traffic is received.
Bottom Out Label	Innermost label sent with MPLS traffic.
Outer Label	Outermost or top label in the stack used for MPLS traffic.
MRoute_Table	
Source Address	The source IP address from where the multicast information is sent.
Group Address	The group IP address of the multicast.
Flags	The flag information pertaining to the multicast.
Up Time	The amount of time the interface has been active.
Protocol	The protocol information, which can be 4 or 6.
Sites Tab	
Name	Site name.
IP Address	IP address of the interface.
Mask	Subnet mask.
State	State of the subinterface: Up or Down.
Associated Entity	Element and interface associated with the site, hyperlinked to its entry in physical inventory.
Description	Interface description.
Input Access List	Access list applied to the inbound traffic.
Output Access List	Access list applied to the outbound traffic.

Table 17-9 VRF Properties (continued)

Field	Description
Rate Limits	If a rate limit is configured on an IP interface, the limit is shown as an IP interface property. This option is checked when a rate limit is defined on the IP interface, meaning the access list is a rate limit access list. IP interface traffic is measured and includes the average rate, normal burst size, excess burst size, conform action, and exceed action. **Note** Double-clicking a row displays the properties of the IP interface. When a rate limit is configured on the IP interface, the Rate Limits tab is displayed. For more information about rate limits, see Viewing Rate Limit Information, page 17-38. **Note** The Input Access, Output Access, and Rate Limits parameters apply only to certain operating systems, such as Cisco IOS.
IP Sec Map Name	IP Security (IPsec) map name.
Site Name	Name of the business element to which the interface is attached.

Viewing VRF Multicast Configuration details

To view global multicast configuration details for a VRF:

Step 1 Right-click on the required device and select **Inventory**.

Step 2 In the **Inventory** window, choose **Logical Inventory > VRFs >** *vrf* (where *vrf* is the required VRF) **> IPV4VRF Multicast Configuration** or **IPV6VRF Multicast Configuration**. The route policies configured on the device are displayed in the content pane.

Table 17-10 describes the information that is displayed in the Router IP Interface Properties window:

Table 17-10 Global Multicast Configuration Details

Field	Description
VPN ID	The VPN ID configured for the VRF.
RoutePolicy	The name of the multicast route policy.
BgpAD	The BgpAd enabled on the device.
MdtSourceif	The Multicast Distribution Tree (MDT) source interface.
MdtPartioned	The MDT partitioned permission.
NSF	The non-stop forwarding (NSF) information configured for the VRF.
MdtAddress	The MDT address.
MdtData	The MDT data that can be handled.
Address Family	The address family, which can be IPV4 or IPV6.
RP Address	The rendezvous point (RP) address configured for the VRF.

Viewing VRF Egress and Ingress Adjacents

The Vision client enables you to view the exporting and importing Neighbours by displaying the VRF egress and ingress adjacents. In addition, you can view the connectivity between the VRFs for the route targets and view their properties. For example, if VRF A retrieved route target import X, you can view all VRFs that export X as a route target whether it is in the same or another VPN.

To display the VRF egress and ingress adjacents, you can use either an element configured for VRFs or a virtual router:

- To use an element configured for VRFs:
  a. Double-click the element configured for VRFs.
  b. In the **Inventory** window, choose **Logical Inventory > VRFs >** *vrf* where *vrf* is the required VRF.
  c. Right-click the required VRF and choose **Show VRF Egress Adjacents** or **Show VRF Ingress Adjacents**.
- To use a virtual router, right-click the required VRF in the navigation pane, and choose **Show VRF Egress Adjacents** or **Show VRF Ingress Adjacents**.

Table 17-11 describes the information displayed in the Adjacents window.

Table 17-11 VRF Adjacents Properties Window

Field	Description
Name	VRF name.
Route Distinguisher	Route distinguisher configured in the VRF.
VRF V6 Table	IPv6 route distinguisher if IPv6 is configured.

Viewing Routing Entities

To view routing entities:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > Routing Entities > Routing Entity**.

The routing information is displayed as shown in Figure 17-17.

Figure 17-17 Routing Entity Table

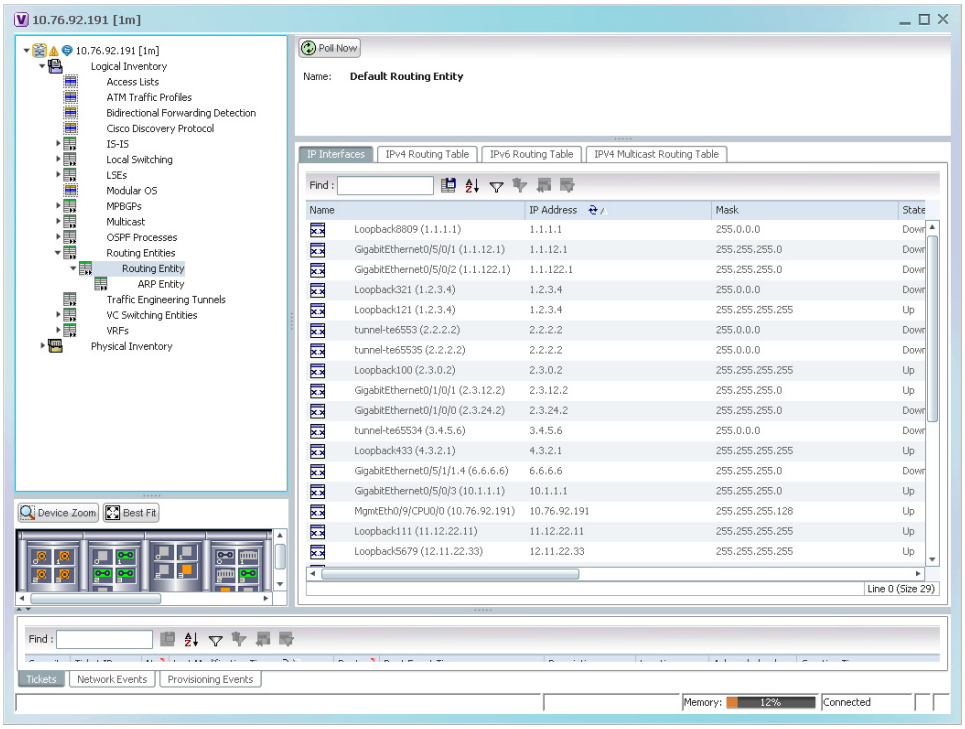


Table 17-12 describes the information that is displayed in the Routing Entity table.

Table 17-12 Routing Entity Table

Field	Description
Name	Name of the routing entity.
IP Interfaces Tab	
Name	Site name.
IP Address	IP address of the interface.
Mask	Network mask.
State	State of the subinterface: Up or Down.
Associated Entity	Interface associated with the routing entity, hyperlinked to its location in physical inventory.
Description	Description of the interface.
Input Access List	If an input access list is assigned to an IP interface, the list is shown as an IP interface property, and a hyperlink highlights the related access list in the Access List table. When an access list is assigned to the inbound traffic on an IP interface, the actions assigned to the packet are performed.

Table 17-12 Routing Entity Table (continued)

Field	Description
VRRP Group	If a VRRP group is configured on an IP interface, the information is shown as an IP interface property. This option is checked when a rate limit is defined on the IP interface. **Note** Double-clicking a row displays the properties of the IP interface. When a VRRP group is configured on an IP interface, the VRRP Groups tab is displayed in the IP Interface Properties window. For more information, see Viewing VRRP Information, page 17-39.
Output Access List	If an output access list is assigned to an IP interface, the list is shown as an IP interface property, and a hyperlink highlights the related access list in the Access List table. When an access list is assigned to the outbound traffic on an IP interface, the actions assigned to the packet are performed.
Rate Limits	If a rate limit is configured on an IP interface, the limit is shown as an IP interface property. This option is checked when a rate limit is defined on the IP interface, meaning the access list is a rate limit access list. IP interface traffic is measured and includes the average rate, normal burst size, excess burst size, conform action, and exceed action. **Note** Double-clicking a row displays the properties of the IP interface. When a rate limit is configured on the IP interface, the Rate Limits tab is displayed. For more information, see Viewing Rate Limit Information, page 17-38. **Note** The Input Access, Output Access, and Rate Limits parameters apply only to certain operating systems, such as Cisco IOS.
IP Sec Map Name	IP Security (IPsec) crypto map name.
Site Name	Name of the business element to which the interface is attached.
IPv4 and IPv6 Routing Table Tabs	
Destination	Destination of the specific network.
Outgoing If Name	Name of the outgoing interface.
Type	Routing type: Direct, Indirect, Static, Other, Invalid, or Unknown.
Next Hop	IP address from which to continue to get to a specific address. This field is empty when the routing entry goes to a PE router.
Prefix Length	Length of the network prefix in bits.
Route Protocol Type	Routing protocol used to communicate with other routers.
IPv4 and IPv6 Multicast Routing Tabs	
Source Address	The source IP address from where the multicast information is sent.
Group Address	The group IP address of the multicast.
Flags	The flag information pertaining to the multicast.
Up Time	The amount of time the interface has been active.
Protocol	The protocol information, which can be 4 or 6.
IPv4 and IPv6 BGP Label Routing Table Tabs	
Destination	Destination of the specific network

Table 17-12 Routing Entity Table (continued)

Field	Description
Prefix Length	Length of the network prefix in bits
Next Hop	Next routing hop
Incoming Label	Incoming BGP label identifier
Outgoing Interfaces	Name of the outgoing interface
Outgoing label	Outgoing label for the network.
Type	Route type: Direct (local), Indirect, or Static
Routing Protocol	Routing protocol used to communicate with the other sites: BGP

Viewing IPv4 Label in BGP Routes

The labeled BGP IPv4 (RFC 3107) enables BGP to distribute MPLS label along the routes it advertises. The label mapping information for a particular route is added in the same BGP update message that is used to distribute the route itself. The label mapping information is carried as a part of the Network Layer Reachability Information (NLRI) in the multiprotocol extension attributes. Hence, the use of any other label distribution protocol is eliminated.

The outer label again identifies the LSP and the inner label identifies the MPLS service. In this case, the RFC 3107 edge device replaces the outer label with two labels, generating a three-label stack.

In Prime Network, the IPv4 BGP Label Routing table displays incoming and outgoing labels. Path tracer follows a service that relies on RFC 3107 and it reflects the BGP label in the MPLS label stack.

RFC3107 is supported on the following device types: ASR9K, ASR901, ASR903, and ME3600/3800X.

To view the BGP label information:

Step 1 Double-click the required element in the Vision client.

Step 2 Choose **Logical Inventory** > **Routing Entities** > **Routing Entity**.

Step 3 In the IPv4 BGP Label Routing table, view the details of incoming and outgoing labels.

Table 17-13 describes the information in the IPv4 BGP Label Routing Table tab.

Table 17-13 IPv4 BGP Label Routing Table Properties

Field	Description
Destination	Destination of the specific network
Prefix Length	Length of the network prefix in bits
Next Hop	Next routing hop
Incoming Label	Incoming BGP label identifier
Outgoing Interfaces	Name of the outgoing interface
Outgoing label	Outgoing label for the network.

Field	Description
Type	Route type: Direct (local), Indirect, or Static
Routing Protocol	Routing protocol used to communicate with the other sites: BGP

Viewing the ARP Table

To view the ARP table:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > Routing Entities > Routing Entity > ARP**.

Table 17-14 describes the information that is displayed in the ARP table.

Table 17-14 ARP Table

Field	Description
MAC	Interface MAC address.
Interface	Interface name.
IP Address	Interface IP address.
State	Interface state: • Dynamic—The entry was learned by the device according to network traffic. • Static—The entry was learned by a local interface or from a user configuring a static route. • Other—The entry was learned by another method not explicitly defined. • Invalid—In SNMP, this type is used to remove an ARP entry from the table.

Viewing the NDP Table

Neighbor Discovery Protocol (NDP) is used with IPv6 to discover other nodes, determine the link layer addresses of other nodes, find available routers, and maintain reachability information about the paths to other active Neighbour nodes.

NDP functionality includes:

- Router discovery
- Autoconfiguration of addresses (stateless address autoconfiguration [SLAAC])
- IPv6 address resolution (replaces Address Resolution Protocol [ARP])
- Neighbour reachability (neighbour unreachability detection [NUD])
- Duplicate address detection (DAD)
- Redirection

To view the NDP table:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > Routing Entities > Routing Entity > ARP Entity**.

Step 3 Click the **NDP Table** tab.

Figure 17-18 shows an example of the NDP Table tab.

Figure 17-18 NDP Table in Logical Inventory

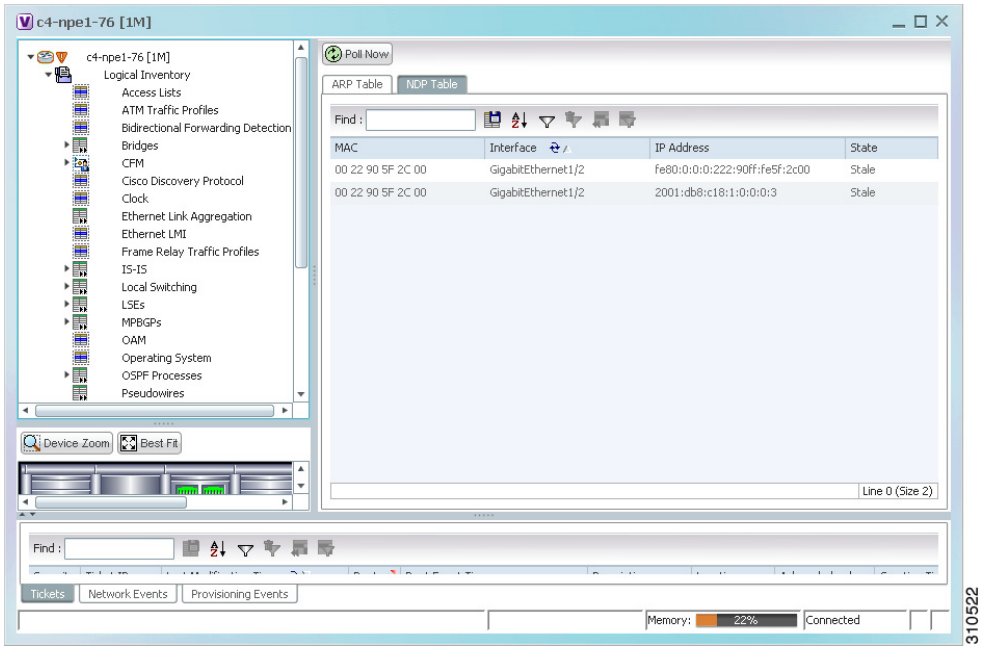


Table 17-15 describes the information displayed for NDP.

Table 17-15 NDP Table

Field	Description
MAC	Interface MAC address.
Interface	Interface name.
IP Address	Interface IPv6 address.
Type	Entry type: • ICMP (Incomplete)—Address resolution is being performed on the entry. A Neighbour solicitation (NS) message has been sent to the solicited-node multicast address of the target, but the corresponding Neighbour advertisement (NA) message has not yet been received. • REACH (Reachable)—Positive confirmation was received via an NA that the forward path to the Neighbour was functioning properly. While in REACH state, the device takes no special action as packets are sent. • STALE—Too much time has elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent. • DELAY—Too much time has elapsed since the last positive confirmation was received that the forward path was functioning properly. If no reachability confirmation is received within a specified amount of time, the device sends an NS message and changes the state to PROBE. • PROBE—A reachability confirmation is actively sought by resending Neighbour solicitation messages until a reachability confirmation is received.

Viewing Rate Limit Information

To view rate limit information:

Step 1 Right-click the required element in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > Routing Entities > Routing Entity**.

Step 3 In the IP Interfaces tab, double-click the required interface to view the IP interface properties. If a rate limit is configured on the IP interface, the Rate Limits tab is displayed.

Note Rate Limit information applies only to certain operating systems, such as Cisco IOS.

Table 17-16 describes the information that is displayed in the Rate Limits tab of the IP Interface Properties dialog box.

Table 17-16 Rate Limits Information

Field	Description
Type	Rate limit direction, either Input or Output.
Max Burst	Excess burst size in bytes.
Normal Burst	Normal burst size in bytes.
Bit Per Second	Average rate in bits per second.
Conform Action	Action that can be performed on the packet if it conforms to the specified rate limit (rule), for example, continue, drop, change a bit, or transmit.
Exceed Action	Action that can be performed on the packet if it exceeds the specified rate limit (rule), for example, continue, drop, change a bit, or transmit.
Access List	Hyperlink that highlights the related access list in the Access List table.

Viewing VRRP Information

Virtual Router Redundancy Protocol (VRRP) is a non-proprietary redundancy protocol that is designed to increase the availability of the static default gateway servicing hosts on the same subnet. This increased reliability is achieved by advertising a *virtual router* (a representation of master and backup routers acting as a group) as a default gateway to the hosts instead of one physical router. Two or more physical routers are then configured to stand for the virtual router, with only one doing the actual routing at any given time. If the current physical router that is routing the data on behalf of the virtual router fails, another physical router automatically replaces it. The physical router that forwards data on behalf of the virtual router is called the master router; physical routers standing by to take over for the master router if needed are called backup routers.

To view VRRP information:

Step 1 Double-click the required element in the Vision client.

Step 2 In logical inventory, choose **Logical Inventory > Routing Entities > Routing Entity**.

Step 3 In the IP Interfaces tab, double-click the required interface to view the IP interface properties. If VRRP is configured on the IP interface, the VRRP Groups tab is displayed.

Figure 17-19 VRRP Properties in IP Interface Properties Window

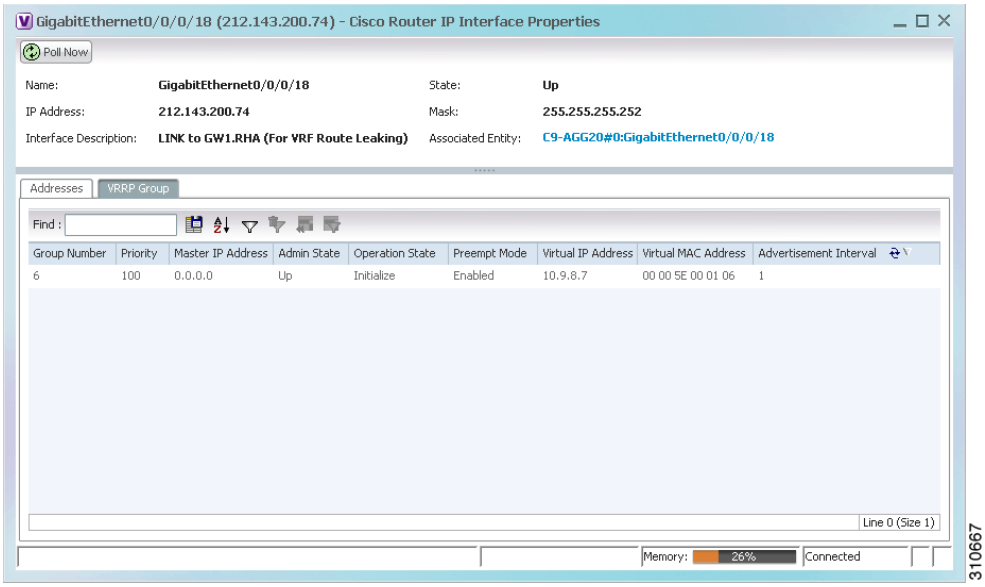


Table 17-17 describes the information in the VRRP Groups tab.

Table 17-17 VRRP Group Properties

Field	Description
Group Number	Number of the VRRP group associated with the interface.
Priority	Value that determines the role each VRRP router plays and what happens if the master virtual router fails. Values are 1 through 254, with lower numbers having priority over higher numbers.
Master IP Address	IP address of the VRRP group, taken from the physical Ethernet address of the master virtual router.
Admin State	Administrative status of the VRRP group: Up or Down.
Operation State	State of the VRRP group: Master or Backup.
Preempt Mode	Whether or not the router is to take over as the master virtual router for a VRRP group if it has a higher priority than the current master virtual router: Enabled or Disabled.
Virtual IP Address	IP address of the virtual router.
Virtual MAC Address	MAC address of the virtual router.
Advertisement Interval	Amount of time (in seconds) between successive advertisements by the master virtual router.

Viewing Label Switched Entity Properties

Logical inventory can display any or all of the following tabs for label switched entities, depending on the configuration:

- Label Switching Table—Describes the MPLS label switching entries used for traversing MPLS core networks.
- LDP Neighbours—Details all MPLS interface peers that use the Label Distribution Protocol (LDP). LDP enables Neighbouring provider (P) or PE routers acting as label switch routers (LSRs) in an MPLS-aware network to exchange label prefix binding information, which is required to forwarding traffic. The LSRs discover potential peers in the network with which they can establish LDP sessions in order to negotiate and exchange the labels (addresses) to be used for forwarding packets.

  Two LDP peer discovery types are supported:

  – Basic discovery—Used to discover directly connected LDP LSRs. An LSR sends hello messages to the all-routers-on-this-subnet multicast address, on interfaces for which LDP has been configured.

  – Extended discovery—Used between indirectly connected LDP LSRs. An LSR sends targeted hello messages to specific IP addresses. Targeted sessions are configured because the routers are not physically connected, and broadcasting would not reach the peers. The IP addresses of both peers are required for extended discovery.

  If two LSRs are connected with two separate interfaces, two LDP discoveries are performed.
- MPLS Interfaces—Contains information on MPLS interfaces and whether traffic engineering tunnels are configured on an interface.
- MPLS Label Range—Identifies whether MPLS uses static or dynamic routing, and the label range.
- Traffic Engineering LSPs—Describes the MPLS traffic engineering Label Switched Paths (LSPs) provisioned on the switch entity. MPLS traffic engineering LSP, an extension to MPLS TE, provides flexibility when configuring LSP attributes for MPLS TE tunnels.
- VRF Table—Describes MPLS paths that terminate locally at a VRF.

To view information for label switched entities:

Step 1 Double-click the required device in the Vision client.

Step 2 In the logical inventory window, choose **Logical Inventory > LSEs > Label Switching**.

Table 17-18 describes the information that is displayed for label switched entities.

Table 17-18 Label Switching Properties in Logical Inventory

Field	Description
Local LDP ID	Local Label Distribution Protocol (LDP) identifier.
LDP Process State	State of the LDP process, such as Running, Down, or Unknown.
MPLS Interfaces	
ID	Identifier for MPLS interface, as a combination of IP address and interface name.
Distribution Protocol Type	Distribution protocol used: Null, LDP, TDP (Tag Distribution Protocol), RSVP, or TDP and LDP.

Table 17-18 Label Switching Properties in Logical Inventory (continued)

Field	Description
MPLS TE Properties	Whether or not traffic engineering (TE) properties are configured on the interface: • Checked—MPLS TE properties are configured on the interface. • Unchecked—MPLS TE properties are not configured on the interface.
Discovery Protocols	Discovery protocols used on the interface.
Label Switching Table	
Incoming Label	Incoming MPLS label identifier.
Action	Type of switching action: Null, Pop, Swap, Aggregate, Untagged, or Act. If an action is defined as Pop, an outgoing label is not required. If an action is defined as Untagged, an outgoing label is not present.
Outgoing Label	Outgoing label.
Out Interface	Name of the outgoing interface, displayed as a hyperlink to the port subinterface in physical inventory.
IP Destination	Destination IP address.
Destination Mask	Subnet mask of the destination.
Next Hop	IP address of the next hop in the path. The IP address is used for resolving the MAC address of the next MPLS interface that you want to reach.
VRF Table	
Incoming Label	Incoming VRF label identifier.
Action	Type of switching action: Null, Pop, Swap, Aggregate, Untagged, or Act.
VRF	VRF name, hyperlinked to its location in logical inventory.
IP Destination	Destination IP address.
Destination Mask	Subnet mask of the destination.
Next Hop	IP address of the next hop in the path. The IP address is used for resolving the MAC address of the next MPLS interface that you want to reach.
Out Interface	Name of the outgoing interface, displayed as a hyperlink to the port subinterface in physical inventory.
Traffic Engineering LSPs	
LSP Name	Label switched path (LSP) name.
LSP Type	Segment type: Head, Midpoint, or Tail.
Source Address	Source IP address.
Destination Address	Destination IP address.
In Label	Incoming label, if not a head segment.
In Interface	Incoming interface, if not a head segment.
Out Interface	Outgoing interface, if not a tail segment.

Table 17-18 Label Switching Properties in Logical Inventory (continued)

Field	Description
Out Label	Outgoing label, if not a tail segment.
Average Bandwidth (Kbps)	Current bandwidth (in Kb/s) used to automatically allocate the tunnel's bandwidth.
LSP ID	LSP identifier.
Burst (Kbps)	Tunnel bandwidth burst rate, in Kb/s.
Peak (Kbps)	Tunnel bandwidth peak rate, in Kb/s.
FRR TE Tunnel	Fast Reroute (FRR) TE tunnel name, hyperlinked to the routing entity in logical inventory.
FRR TE Tunnel State	State of the FRR TE tunnel: • Active—A failure exists in the primary tunnel and the backup is in use. • Not Configured—The primary tunnel has no designated backup tunnel. • Ready—The primary tunnel is in working condition.
MPLS Label Range	
MPLS Label Type	Type of MPLS label: Dynamic or Static.
Minimum Label Value	Lowest acceptable MPLS label in the range.
Maximum Label Value	Highest acceptable MPLS label in the range.
LDP Neighbours	
LDP ID	Identifier of the LDP peer.
Transport IP Address	IP address advertised by the peer in the hello message or the hello source address.
Session State	Current state of the session: Transient, Initialized, Open Rec, Open Sent, or Operational.
Protocol Type	Protocol used by the peer to establish the session: LDP, TDP, or Unknown.
Label Distribution Method	Method of label distribution: Downstream, Downstream On Demand, Downstream Unsolicited, or Unknown.
Session Keepalive Interval	Length of time (in milliseconds) between keepalive messages.
Session Hold Time	The amount of time (in milliseconds) that an LDP session can be maintained with an LDP peer, without receiving LDP traffic or an LDP keepalive message from the peer.
Discovery Sources	Whether the peer has one or more discovery sources: • Checked—Has one or more discovery sources. • Unchecked—Has no discovery sources. **Note** To see the discovery sources in the LDP Neighbor Properties window, double-click the row of the peer in the table.

Step 3 Double-click an entry in any of the tables to view additional properties for that entry.

Table 17-19 Additional Properties Available from Label Switching in Logical Inventory

Double-click an entry in this tab...	To display this window...
Label Switching Table	Label Switching Properties
LDP Neighbors	LDP Peer Properties
MPLS Interfaces	MPLS Link Information - MPLS Properties
MPLS Label Range	MPLS Label Range Properties
Traffic Engineering LSPs	Tunnel Properties
VRF Table	MPLS Aggregate Entry Properties

Multicast Label Switching (mLADP)

Multicast Label Distribution protocol (mLDP) provides extensions to the Label Distribution Protocol (LDP) for the setup of point-to-multipoint (P2MP) and multipoint-to-multipoint (MP2MP) Label Switched Paths (LSPs) in MPLS networks. A P2MP LSP allows traffic from a single root (or ingress) node to be delivered to a number of leaf (or egress) nodes.

A MP2MP LSP allows traffic from multiple ingress nodes to be delivered to multiple egress nodes. Only a single copy of the packet will be sent on any link traversed by a multipoint LSP. Container is the holder of MPLS MLDP databases and neighbors instances for Multicast.

Viewing MLDP Database Information

To view the MLDP database information:

Step 1 Double-click the required device in the Vision client.

Step 2 In the logical inventory window, choose **Logical Inventory > LSEs > Label Switching > Multicast Label Switching > Databases**. The database information is displayed in the **MLDP Databases** content pane.

Step 3 Select a database from the content pane, right-click and choose the **Properties** option. The **MLDP Database Properties** dialog box is displayed. You can click on the tabs to view more details.

Table 17-20 describes the information that is displayed for **MLDP Database Properties** dialog box.

Table 17-20 MLDP Database Properties Dialog Box

Field	Description
LSM ID	The unique ID assigned to a LSP.
Tunnel Type	The tunnel type.
FEC Root	The root IP address of the MDT.
Opaque Value	The stream information that uniquely identifies the tree to the root. To receive label switched multicast packets, the Egress Provider Edge (PE) indicates to the upstream router (the next hop closest to the root) which label it uses for the multicast source by applying the label mapping message.
Is Root	Indicates whether Forwarding Equivalence Class (FEC) is the root.
Downstream Clients Tab	
Egress Interface Name	The egress interface name.
Associated Entity	The entity associated with the LSP. Click this link to view the associated entity details.
Uptime	The amount of time from when the interface is active.
Table ID	The unique Table ID of the label through which the packet was received.
Ingress State	The status of the ingress interface, which can be **Enabled** or **Disabled**.
PPMP State	The status of the Point-to-Point Multipoint, which can be **Enabled** or **Disabled**.
Local Label	The label used to identify the label stack of the route within the local VPN network.

Viewing the MLDP Neighbors Information

To view information of MLDP neighbors:

Step 1 Double-click the required device in the Vision client.

Step 2 In the logical inventory window, choose **Logical Inventory > LSEs > Label Switching > Multicast Label Switching > MLDP Neighbors**. The MLDP peer information is displayed in the **MLDP Peers** content pane.

Step 3 Select a peer id from the content pane, right-click and choose the **Properties** option. The **Peer ID Properties** dialog box is displayed.

Table 17-21 describes the information that is displayed for **Peer ID Properties** dialog box.

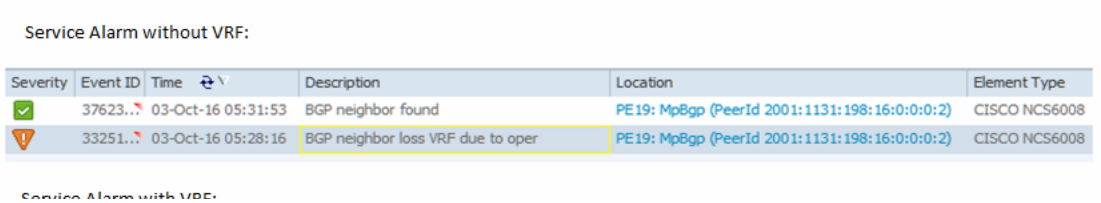
Table 17-21 Peer ID Properties Dialog Box

Field	Description
Peer ID	The IP address of the MLDP peer.
Capabilities	The capabilities supported by the LDP LSR.
MLDP GR	Indicates whether graceful restart is enabled for the LDP. **Note** LDP graceful restart provides a control plane mechanism to ensure high availability and allows detection and recovery from failure conditions while preserving Non Stop Forwarding (NSF) services.
Path Count	The number of LSP's configured.
Uptime	The amount of time from when the peer id is working.
Peer Paths tab	
IP Address	The IP address of the MLDP peer.
Interface Name	The interface name.
Associated Entity	The link to the associated entity, which when clicked will highlight the associated **Default routing entity** record under the **Routing Entity** node.
Protocol	The protocol type used for communication.
Peer Adjacent List	
IP Address	The IP address of the MLDP peer.
Interface Name	The interface name.
Associated Entity	The link to the associated entity, which when clicked will highlight the associated **Default routing entity** record under the **Routing Entity** node.

Viewing BGP Neighbor Service Alarm with VRF Name

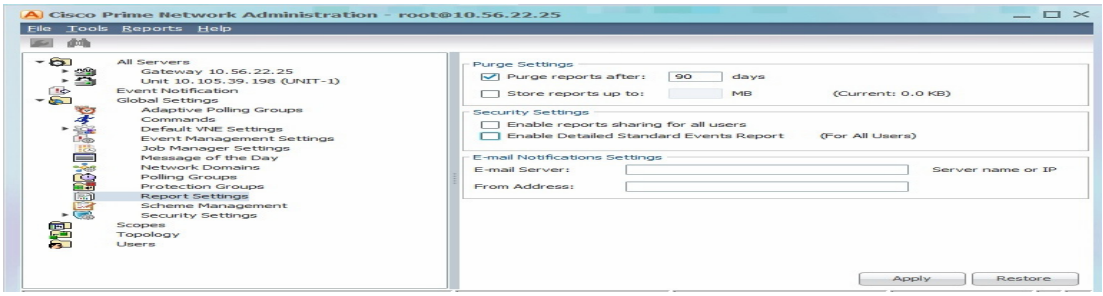
BGP neighbor loss VRF due to oper and BGP neighbor found service alarms are raised on the BGP links for any mis-configurations that shuts down physical interfaces or any other scenario that might break the BGP neighborship. If a BGP neighbor service alarm is configured with the VRF, the VRF name is displayed as part of the Location links for a **BGP neighbor loss VRF due to oper** and **BGP neighbor found** service alarms. For example, Figure 17-20 shows the BGP neighbor service alarms displayed with the VRF Name.

Figure 17-20 Service Alarm with VRF Name



To view the VRF details, click the links available in the **Location** field. For example, the following figure 17-21, shows a link properties of a BGP Service alarm with VRF Name.

Figure 17-21 Link Properties with VRF Information



Viewing MP-BGP Information

The MP-BGP branch displays information about a router's BGP neighbors and cross-connect VRFs.

Note If there are multiple MP-BGP links between two devices, the Vision client displays each link in the content pane map view.

To view MP-BGP information:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > MPBGPs > MPBGP**.

Table 17-22 describes the information that is displayed for MP-BGP.

Table 17-22 MP-BGP Information in Logical Inventory

Field	Description
Local AS	Identifier of the autonomous system (AS) to which the router belongs.
BGP Identifier	BGP identifier, represented as an IP address.
Cross VRFs Tab	
VRF Name	Name of the VRF.
Cross VRF Routing Entries	Group of cross VRFs that share a single destination.
BGP Neighbors Tab	
Peer AS	Identifier of the AS to which the remote peer belongs.
Peer State	State of the remote peer: Active, Connect, Established, Open Confirm, Open Sent, or Null.
Peer Address	Remote peer IP address.
AFI	Address family identifier: IPv4, IPv6, L2VPN, VPNv4, or VPNv6. Address Type identifier: Unicast, Multicast, Labeled-unicast, Vpls, MDT, EVPN.
AF Peer State	Address family peer state: Established or Idle.
Peer Up/Down Since	Specifies a BGP Peer Up/Down time property. **Note** Use **Poll Now** to view the latest value.
Peer BGP ID	Identifier of the remote peer, represented as an IP address.
Local BGP ID	Local peer IP address.
VRF Name	Remote peer VRF name.
BGP Neighbor Type	Neighbor type: Null, Client, or Non Client.
Hold Time (secs)	Established hold time in seconds.
Keepalive (secs)	Established keepalive time in seconds.
BGP Neighbor Entry	BGP neighbor IP address.

Viewing 6rd Tunnel Properties

IPv6 rapid deployment (6rd) is a mechanism that allows stateless tunneling of IPv6 over IPv4. For information on the devices that support 6rd, refer to *Cisco Prime Network 5.2 Supported VNEs*.

To view 6rd tunnel properties:

Step 1 In the Vision client, double-click the required device.

Step 2 In the **Inventory** window, choose **Logical Inventory > 6rd Tunnels**.

The 6rd tunnel properties are displayed as shown in Figure 17-22.

Figure 17-22 6rd Tunnel Properties in Logical Inventory

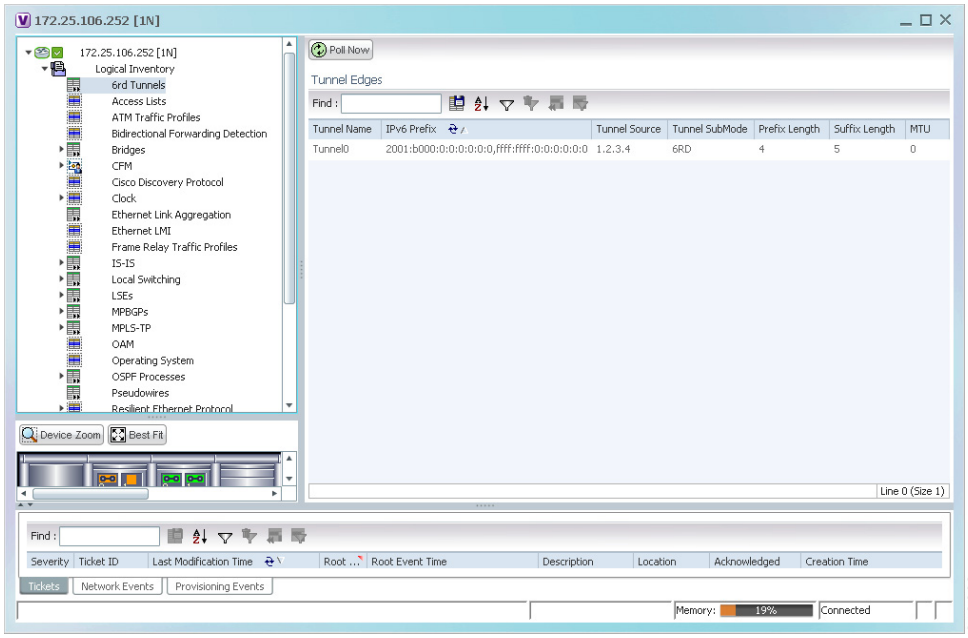


Table 17-23 describes the information displayed for 6rd tunnels.

Table 17-23 6rd Tunnel Properties in Logical Inventory

Field	Description
Tunnel Name	6rd tunnel name.
IPv6 Prefix	IPv6 prefix used to translate the IPv4 address to an IPv6 address.
Source Address	Tunnel IPv4 source IP address.
Tunnel SubMode	Tunnel type: • 6rd—Static IPv6 interface. • 6to4—IPv6 address with the prefix embedding the tunnel source IPv4 address. • Auto-tunnel—IPv4-compatible IPv6 tunnel. • ISATAP—Overlay tunnel using an Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) address.
Prefix Length	IPv4 prefix length used to derive the delegated IPv6 prefix.
Suffix Length	IPv4 suffix length used to derive the delegated IPv6 prefix.
MTU	Maximum transmission unit (MTU) configured on the 6rd IPv4 tunnel.

Viewing BFD Session Properties

Bidirectional Forwarding Detection (BFD) is used to detect communication failures between two elements, or endpoints, that are connected by a link, such as a virtual circuit, tunnel, or LSP. BFD establishes sessions between the two endpoints over the link. If more than one link exists, BFD establishes a session for each link.

Prime Network supports BFD with the following protocols: BGP, IPv4 (static), IPv6 (static), IS-IS, LAG (Ether channel), MPLS TE, MPLS-TP, and OSPF.

To view BFD session properties that are configured on an element:

Step 1 In the Vision client, double-click the required device.

Step 2 In the **Inventory** window, choose **Logical Inventory > Bidirectional Forwarding Detection**.

The properties for BFD sessions are displayed as shown in Figure 17-23.

Figure 17-23 BFD Session Properties

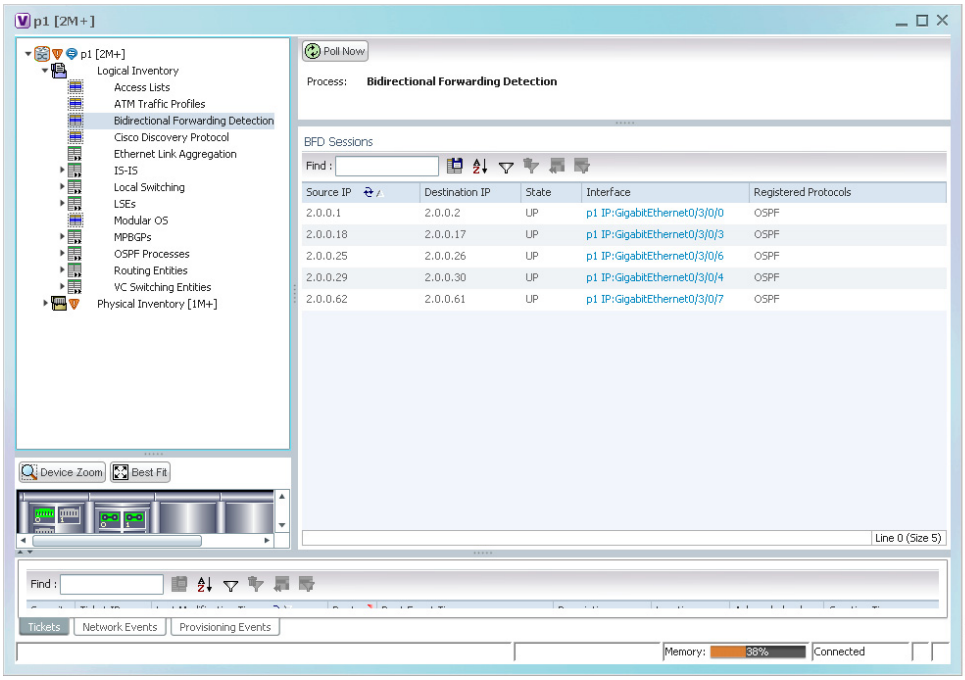


Table 17-24 describes the information displayed for BFD sessions.

Table 17-24 BFD Session Properties

Field	Description
Process	Process name, such as Bidirectional Forwarding Detection.
Process State	Process state, such as Running.
BFD Sessions Table	
Source IP	Source IP address of the session.
Destination IP	Destination IP address of the session.
State	Session state, such as Up or Down.
Interface	Interface used for BFD communications, hyperlinked to the routing entity in logical inventory.
Registered Protocols	Routing protocol being monitored for communication failures, such as BGP or OSPF.

For MPLS-TP BFD sessions, the information in Table 17-25 is displayed.

Table 17-25 MPLS-TP BFD Session Properties in Logical Inventory

Field	Description
Process	Process name: Bidirectional Forwarding Detection.
Process State	Process state, such as Running.
MPLS-TP BFD Sessions Table	
Interface	Interface used for BFD communications, hyperlinked to the routing entity in logical inventory.
LSP Type	Type of LSP: Working or Protected.
State	Session state: Up or Down.
Registered Protocols	Routing protocol being monitored for communication failures: MPLS-TP.

Step 3 To view additional properties, double-click the required entry in the Sessions table.

Table 17-26 describes the information that is displayed in the Session Properties window.

Table 17-26 Session Properties Window

Field	Description
Source IP	Source IP address of the session.
Destination IP	Destination IP address of the session.
State	Session state: Up or Down.
Interface	Hyperlink to the routing entity in logical inventory.
Registered Protocols	Routing protocol being monitored for communication failures.
Offload Host	BFD offload property: Software (applicable when configuring BFD on BVI interface). Displays BFD session hosted in software.
Protocols Table	
Protocol	Protocol used for this session.
Interval	Length of time (in milliseconds) to wait between packets that are sent to the neighbor.
Multiplier	Number of times a packet is missed before the neighbor is declared down.

BFD Single-Hop Authentication

The BFD Single-Hop Authentication feature enables authentication for single-hop Bidirectional Forwarding Detection (BFD) sessions between two directly connected devices. This feature supports Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1) authentication types. The BFD templates can be configured only if the BFD sessions are enabled.

BFD Templates Support

BFD (Bidirectional Forwarding Detection Templates) are the new features added in CPT devices. Prime Network uses the below Telnet or CLI Command to get the BFD templates in existing CPT devices.

Show running-config|section bfd-template

Cerent Trap Support

Cerent traps are alarms supported for CPT devices. There are 170 traps supported .There are various kinds of traps supported which are listed below:

- Communications
- Equipment
- Environmental
- Integrity Violation
- Quality of Service

The alarms can be categorized by their severity such as Critical, Major, Minor, Not Reported and Not Alarmed. Examples of each severity categories are as follows:

- Critical- Equipment failure
- Major- High Voltage, Battery Failure
- Minor- Loss of frame, Loss of signal
- Not Reported- Unqualified PPM Inserted
- Not Alarmed- Transit Node Clock Traceable

Change Settings in Cisco Transport Controller (CTC)

Any configurations settings made in CPT should be done through CTC. To receive traps in a particular server, that server IP needs to be entered in the device through CTC. Most of the traps are on device dependencies.

CMP Tool

The default trap format can be used to send the alarms through CMP tool which can be generated in Prime Network. The default trap format is given as follows:

<key name="trap"><key name=""><entry name="">sendtrap -V2 10.105.39.217 -ccellbus -r162 -o1.3.6.1.2.1.1.3.0 -mt1166470595 -o1.3.6.1.6.3.1.1.4.1.0 -md1.3.6.1.4.1.3607.6.10.30.0.1670 -o1.3.6.1.4.1.3607.6.10.100.10.20 -mo03/Nov/2001 -o1.3.6.1.4.1.3607.6.10.20.30.20.1.80.1.1670 -mi50 -o1.3.6.1.4.1.3607.6.10.20.30.20.1.20.1.1670 -mi50 -o1.3.6.1.4.1.3607.6.10.20.30.20.1.60.1.1670 -mi1 -o1.3.6.1.4.1.3607.6.10.20.30.20.1.30.1.1670 -mi0 -o1.3.6.1.4.1.3607.6.10.20.30.20.1.40.1.1670 -mi1 -o1.3.6.1.4.1.3607.6.10.20.30.20.1.50.1.1670 -mi0 -o1.3.6.1.4.1.3607.6.10.20.30.20.1.100.1.1670 -md1.3.6.1.4.1.3607.6.10.30.0.2110 -o1.3.6.1.4.1.3607.6.10.20.30.20.1.120.1.1670 -mi30 -o1.3.6.1.4.1.3607.6.10.20.30.20.1.130.1.1670 -mi10 -o1.3.6.1.4.1.3607.6.10.20.30.20.1.140.1.1670 -mi10 -o1.3.6.1.6.3.18.1.3.0 -ma10.104.120.46</entry></key></key>

Link and Port Parameters

The link and port parameters are scripts which can be navigated from **Device->Port->Interface-> right click Commands->Configuration->Scripts**. The link and port parameters are supported for the following auto populated UI attributes:

Ethernet Parameter Configuration

- MTU
- Link State
- Expected Speed
- Expected Duplex
- Operating Flow Control
- Carrier Delays
- Auto Negotiation

Port Parameter Configuration

- Port Name
- Admin State
- AINS Soak
- Reach
- Wavelength

L2 Parameter Configuration

- CDP
- DOTIX
- DTP
- LACP
- PAGP
- VTP
- STP

The following are the configuration scripts supported,

- Add Loopback
- Remove Loopback
- Configure CDP
- Configure Ethernet
- Configure L2 Control Protocol
- Configure Port Parameters
- Show Ethernet Parameters
- Show L2 Control Parameters
- Show Port Parameters

Viewing Configuration Scripts in Prime Network

Add Loopback

To view the **Add Loopback** script:

Step 1 Model the device in **Cisco Prime Network Administration**.

Step 2 Launch the Cisco Prime Network Vision client and choose **Inventory**

Step 3 In the physical inventory window, choose **Physical inventory >IPortConnector >Commands > Configuration >Add Loopback**

Step 4 Select the value **Loopback** from the **Attribute** combo box.

Step 5 Click on **Execute Now** button.

Step 6 Verify if **Loopback** is successfully added.

Remove Loopback

To view the **Remove Loopback** script:

Step 1 Model the device in **Cisco Prime Network Administration**.

Step 2 Launch the Cisco Prime Network Vision client and choose **Inventory**

Step 3 In the physical inventory window, choose **Physical inventory >IPortConnector >Commands > Configuration >Remove Loopback**

Step 4 Click on **Execute Now** button.

Step 5 Verify if **Loopback** is successfully removed.

Configure CDP

To view the **Configure CDP** script:

Step 1 Model the device in **Cisco Prime Network Administration**.

Step 2 Launch the Cisco Prime Network Vision client and choose **Inventory**

Step 3 In the physical inventory window, choose **Physical inventory >IPortConnector >Commands > Configuration >Configure CDP**

Step 4 Select the value **CDP** from the **Attribute** combo box.

Step 5 Click on **Execute Now** button.

Step 6 Verify if **CDP** is successfully configured.

Configure Ethernet

To view the **Configure Ethernet** script:

Step 1 Model the device in **Cisco Prime Network Administration**.

Step 2 Launch the Cisco Prime Network Vision client and choose **Inventory**

Step 3 In the physical inventory window, choose **Physical inventory >IPortConnector >Commands > Configuration >Configure Ethernet**

Step 4 Select the value **Admin Status** from the **Attribute** combo box.

Step 5 Click on **Execute Now** button.

Step 6 Verify if **Ethernet** is successfully configured.

Configure L2 Control Protocol

To view the **Configure L2 Control Protocol** script:

Step 1 Model the device in **Cisco Prime Network Administration**.

Step 2 Launch the Cisco Prime Network Vision client and choose **Inventory**

Step 3 In the physical inventory window, choose **Physical inventory >IPortConnector >Commands > Configuration >Configure L2 Control Protocol**

Step 4 Select the value **STP** from the **Attribute** combo box.

Step 5 Click on **Execute Now** button.

Step 6 Verify if **L2 Control Protocol** is successfully configured.

Configure Port Parameters

To view the **Configure Port Parameters** script:

Step 1 Model the device in **Cisco Prime Network Administration**.

Step 2 Launch the Cisco Prime Network Vision client and choose **Inventory**

Step 3 In the physical inventory window, choose **Physical inventory >IPortConnector >Commands > Configuration >Configure Port Parameters**

Step 4 Select the value **Reach** from the **Attribute** combo box.

Step 5 Click on **Execute Now** button.

Step 6 Verify if **Port Parameters** are successfully added.

Show Port Parameters

To view the **Show Port Parameters** script:

Step 1 Model the device in **Cisco Prime Network Administration**.

Step 2 Launch the Cisco Prime Network Vision client and choose **Inventory**

Step 3 In the physical inventory window, choose **Physical inventory >IPortConnector >Commands > Configuration >Show Port Parameters**

Step 4 Click on **Execute Now** button.

Step 5 Verify if all **Port Parameters** are listed.

Show Ethernet Parameters

To view the **Show Ethernet Parameters** script:

Step 1 Model the device in **Cisco Prime Network Administration**.

Step 2 Launch the Cisco Prime Network Vision client and choose **Inventory**

Step 3 In the physical inventory window, choose **Physical inventory >IPortConnector >Commands > Configuration >Show Ethernet Parameters**

Step 4 Click on **Execute Now** button.

Step 5 Verify if **Show Ethernet Parameters** are listed.

Show L2 Control Parameters

To view the **Show L2 Control Parameters** script:

Step 1 Model the device in **Cisco Prime Network Administration**.

Step 2 Launch the Cisco Prime Network Vision client and choose **Inventory**

Step 3 In the physical inventory window, choose **Physical inventory >IPortConnector >Commands > Configuration >Show L2 Control Parameters**.

Step 4 Click on **Execute Now** button.

Step 5 Verify if all **L2 Control Parameters** are listed.

Show Configure Ethernet

To view the **Show Configure Ethernet** script:

Step 1 Model the device in **Cisco Prime Network Administration**.

Step 2 Launch the Cisco Prime Network Vision client and choose **Inventory**

Step 3 In the physical inventory window, choose **Physical inventory >IPortConnector >Commands > Configuration >Show Configure Ethernet**

Step 4 Click on **Execute Now** button.

Step 5 Verify if all the **configured Ethernets** are listed.

Viewing Cross-VRF Routing Entries

Cross-VRF routing entries display routing information learned from the BGP neighbors (BGP knowledge base).

To view properties for cross-VRF routing entries:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > MPBGPs > MPBGP**.

Step 3 Click the **Cross VRFs** tab.

Step 4 Double-click the required entry in the list of cross-VRFs.

The Cross VRF Properties window is displayed, containing the information described in Table 17-27.

Table 17-27 Cross-VRF Properties Window

Field	Description
Name	Cross-VRF name.
Cross VRF Routing Entries Table	
Destination	IP address of the destination network.
Prefix	Length of the network prefix in bits.
Next Hop	IP address of the next hop in the path.
Out Going VRF	Outgoing VRF identifier, hyperlinked to its entry in logical inventory.
Out Tag	Outgoing virtual router tag, such as 50 or no tag.
In Tag	Incoming virtual router tag, such as 97 or no tag.

Viewing Pseudowire End-to-End Emulation Tunnels

The Pseudowires branch in logical inventory displays a list of the Layer 2 tunnel edge properties (per edge), including tunnel status and VC labels.

To view pseudowire properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > Pseudowires**.

The Tunnel Edges table is displayed and contains the information described in Table 17-28.

Table 17-28 Pseudowires Branch Tunnel Edges Table

Field	Description
Local Interface	Name of the subinterface or port. Strings, such as Aggregation Group, EFP, VLAN, and VSI, are included in the interface name, and the entry is hyperlinked to the relevant entry in logical or physical inventory: • Aggregation groups are linked to Ethernet Link Aggregation in logical inventory. • ATM interfaces are linked to the port in physical inventory and the ATM interface. • ATM VCs are linked to the port in physical inventory and the Port IP Properties table. • CEM groups are linked to the port in physical inventory and the CEM Group table. • EFPs are linked to the port in physical inventory and the EFPs table. • IMA groups are linked to IMA Groups in logical inventory. • Local switching entities are linked to Local Switching Entity in logical inventory. • VLANs are linked to Bridges in logical inventory. • VSIs are linked to the VSI entry in logical inventory.
VC ID	Tunnel identifier, hyperlinked to the PTP Layer 2 MPLS Tunnel Properties window.
SAII	Specifies the Source Access Individual Identifier (SAII) of the tunnel. **Note** The SAII attribute can be configured only if the Pseudowire type is FEC129 TYPE II.
TAII	Specifies the Target Attachment Individual Identifier (TAII) of the tunnel. **Note** The TAII can be configured only if the Pseudowire type is FEC129 TYPE II.
Pseudowire Type	Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, SAToP or FEC129 TYPE II.
Peer	Details of the selected peer, hyperlinked to the peer pseudowire tunnel in logical inventory.
Status	Operational state of the tunnel: Up or Down.
Pseudowire Role	If the pseudowire is in a redundancy configuration, indicates whether its role is as the primary or secondary pseudowire in the configuration. If the pseudowire is not configured for redundancy, this field is blank.
Preferred Path Tunnel	Path to be used for MPLS pseudowire traffic.
Local Router IP	IP address of this tunnel edge, which is used as the MPLS router identifier.
Peer Router IP	IP address of the peer tunnel edge, which is used as the MPLS router identifier.
Local MTU	Size, in bytes, of the MTU on the local interface.
Remote MTU	Size, in bytes, of the MTU on the remote interface.
Local VC Label	MPLS label that is used by this router to identify or access the tunnel. It is inserted into the MPLS label stack by the local router.
Peer VC Label	MPLS label that is used by this router to identify or access the tunnel. It is inserted into the MPLS label stack by the peer router.

Table 17-28 Pseudowires Branch Tunnel Edges Table (continued)

Field	Description
Signaling Protocol	Protocol used by MPLS to build the tunnel, for example, LDP or TDP.
Peer Status	Status of the peer link.
Associated EVC Name	Specifies the name of the associated Ethernet Virtual Circuits (EVC)

Viewing MPLS TE Tunnel Information

Prime Network automatically discovers MPLS TE tunnels and enables you to view MPLS TE tunnel information in inventory.

To view MPLS TE tunnel information:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > Traffic Engineering Tunnels**.

Table 17-29 describes the information that is displayed in the Tunnel Edges table.

Table 17-29 Tunnel Edges Table

Field	Description
Name	Name of the TE tunnel; for Cisco devices it is the interface name.
Tunnel Type	Whether the tunnel is Point-to-Point or Point-to-Multipoint.
Tunnel Destination	IP address of the device in which the tunnel ends.
Administrative Status	Administrative state of the tunnel: Up or Down.
Operational Status	Operational state of the tunnel: Up or Down.
Outgoing Label	TE tunnel's MPLS label distinguishing the LSP selection in the next device.
Description	Description of the tunnel.
Outgoing Interface	Interface through which the tunnel exits the device.
Bandwidth (KBps)	Bandwidth specification for this tunnel in Kb/s.
Setup Priority	Tunnel priority upon path setup.
Hold Priority	Tunnel priority after path setup.
Affinity	Tunnel preferential bits for specific links.
Affinity Mask	Tunnel affinity bits that should be compared to the link attribute bits.
Auto Route	Whether or not destinations behind the tunnel are routed through the tunnel: Enabled or disabled.
Lockdown	Whether or not the tunnel can be rerouted: • Enabled—The tunnel cannot be rerouted. • Disabled—The tunnel can be rerouted.

Table 17-29 Tunnel Edges Table (continued)

Field	Description
Path Option	Tunnel path option: • Dynamic—The tunnel is routed along the ordinary routing decisions after taking into account the tunnel constraints such as attributes, priority, and bandwidth. • Explicit—The route is explicitly mapped with the included and excluded links.
Average Rate (Kbps)	Average bandwidth for this tunnel (in Kb/s).

Table 17-29 Tunnel Edges Table (continued)

Field	Description
Burst (Kbps)	Burst flow specification (in Kb/s) for this tunnel.
Peak Rate (Kbps)	Peak flow specification (in Kb/s) for this tunnel.
LSP ID	LSP identifier.
Policy Class	Value of Policy Based Tunnel Selection (PBTS) configured. Values range from 1-7.
FRR	TE Fast Reroute (FRR) status: Enabled or Disabled.
Type	

The Traffic Engineering LSPs tab in the LSEs branch in logical inventory displays TE tunnel LSP information.

For details about the information displayed for TE tunnel LSPs, see Traffic Engineering LSPs, page 17-42.

Configuring VRFs

The following commands configure routes that are available or reachable to all the destinations or networks in the VRF. These commands are launched by right-clicking the VRF node and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see Permissions for Managing MPLS Services, page B-18). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Description
Modify VRF **Delete VRF**	Configures VRF properties, including the VRF route distinguisher, import and export route targets, and any provisioned sites and VRF routes.

Configuring IP Interfaces

The following IP interface commands are launched by right-clicking **Routing Entities >** *routing entity* and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see Permissions for Managing IP and MPLS Multicast, page B-20). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Description
Create Interface **Modify Interface** **Delete Interface** **Configure Secondary IP Address** **Delete Secondary IP Address**	Configures an IP interface for the selected routing entity

Auto-IP in PN

Prime network supports AUTO-IP feature in 5.3 Release. Auto-IP is an IP address configured on the interface using the Auto-IP ring command. The Auto-IP feature enables node insertion, removal and movement to any location within a ring without the need for reconfiguring the existing nodes manually. When enabled on the physical interface or the sub interface, you can discover the devices in the Auto-IP ring automatically.

Configuring Auto-IP

To configure Auto-IP, configure one of the routers in the ring as a seed router. Normally an edge router is configured as a seed router, and the Auto-IP address of the seed router is same as the IP address of the router interface in which the Auto-IP is enabled. The device, in which the Auto-IP configured with priority value 2, becomes the owner interface and assigns the IP address to the non-owner interface (Priority value for non-owner interface is 0) in the ring topology. The Link Layer Discovery Protocol (LLDP) must be enabled on the device before enabling the auto-IP functionality on a node interface.

Note When you configure Auto-IP feature on the devices, by default, the priority value is 1.

Configuring MPLS-TP

The following MPLS-TP commands are launched by right-clicking the appropriate node and choosing **MPLS-TP Global > Commands > Configuration**. Your permissions determine whether you can run these commands (see Permissions for Managing MPLS Services, page B-18). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Note To run the Global Configuration, BFD Configuration, and Link Configuration commands on the Cisco Carrier Packet Transport (CPT) System, right-click the device in the Vision client list or map view, and click **Logical Inventory > CPT Context Container**.

Command	Description
Tunnel Ping **Tunnel Trace** **LSP Ping** **LSP Trace** **LSP Lockout** **LSP Path Lockout** **LSP Path No Lockout**	These actions are performed at the command the launch point. LSP Path Lockout can be accessed at both the tunnel level and endpoint level. If you run the command at the tunnel level, you must indicate whether the Lsp is protected or working.
Add Global Configuration **Update Global Configuration** **Remove Global Configuration**	Configure Global configuration with Router-id, Global-id, Fault OAM refresh timer value, Wait before restoring timer value. The remove operation is performed at the command the launch point.
BFD Global Configuration	BFD minimum interval and multiplier.
Add Link Configuration Remove Link Configuration	MPLS-TP link number, Next hop router address. Only the link number is require for the remove operation.
Add BFD Template Configuration **Remove BFD Template Configuration**	Template type and name, interval type and value, For compute hold down Check/UnCheck Multiplier, multiplier value. The remove operation requires a template type and name.
Show BFD Template **Show BFD Template at Tunnel**	Show BFD Template requires a template name. The Show BFD Template at Tunnel is performed at the command launch point.
Add Label Range Configuration **Remove Label Range Configuration**	Minimum and maximum values for dynamic and static labels. The remove operation is performed at the command launch point.

Locking/Unlocking MPLS-TP Tunnels in Bulk

An MPLS-TP network has one or multiple LSPs running between endpoint devices. If you want to shutdown one of the interfaces in the network, the MPLS-TP packet must be diverted through an alternative LSP. This can be achieved by locking the interface. Before attempting to lock or unlock a tunnel, ensure that MPLS-TP tunnels have been configured for the link. Also, ensure that you have the appropriate rights (Configurator and above) to lock or unlock a tunnel.

The MPLS-TP bulk lockout/unlock option in Prime Network allows you to lock or unlock multiple MPLS-TP tunnels on different VNEs at the same time.

Your permissions determine whether you can run these commands (see Permissions for Managing MPLS Services, page B-18). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Locking MPLS-TP Tunnels

To lock MPLS-TP tunnels in bulk:

Step 1 In the map view, right-click the required link and choose **Properties**.

Step 2 In the link properties window, right-click on the required physical link and choose the **Show MPLS-TP tunnels** option. The MPLS-TP tunnels' commands dialog box is displayed, which lists all the tunnels in the selected link.

Step 3 In the MPLS-TP tunnels' commands dialog box, choose the tunnels that you want to lock and select the **Lock Out** option in the **Commands** field.

Step 4 Click **Execute Now**. You are prompted to confirm the lockout operation.

Step 5 Click **Yes** to confirm. A message is displayed confirming that the selected tunnels have been locked. The status of the tunnel is automatically updated as Lockout(UP) after this operation.

Unlocking MPLS-TP Tunnels

To unlock MPLS-TP tunnels in bulk:

Step 1 In the map view, right-click the required link and choose **Properties**.

Step 2 In the link properties window, right-click on the required physical link and choose the **Show MPLS-TP tunnels** option. The MPLS-TP tunnels' commands dialog box is displayed, which lists all the tunnels in the selected link.

Step 3 In the MPLS-TP tunnels' commands dialog box, select the locked tunnels that you want to unlock and select the **Unlock** option in the **Commands** field.

Step 4 Click **Execute Now**. You are prompted to confirm the unlock operation.

Step 5 Click **Yes** to confirm. A message is displayed confirming that the selected tunnels have been unlocked. The status of the tunnels is automatically updated as Active(UP) after this operation.

Note If you attempt to unlock a tunnel that is not locked, a message is displayed indicating that there are no valid tunnels to perform the unlock operation.

Linear Protection for MPLS-TP

As explained earlier, MPLS-TP is the transport profile that fulfills the deployment in the network for the MPLS technology. This technology provides fast protection switching for end-to-end segments wherein the protection switching time is generally less than 50 milliseconds.

Protection switching is a mechanism wherein route and resources of a protection path are reserved for a selected working path or set of working paths.

Linear protection provides rapid and simple protection switching because it can operate between any pair of points within the network. For every working Label Switched Paths (LSP) in the network, there is a protected LSP that is not related to any other working entity. When a working LSP fails, the protected LSP is ready to take up transmission of data.

In Prime Network, the following commands are available for linear protection:

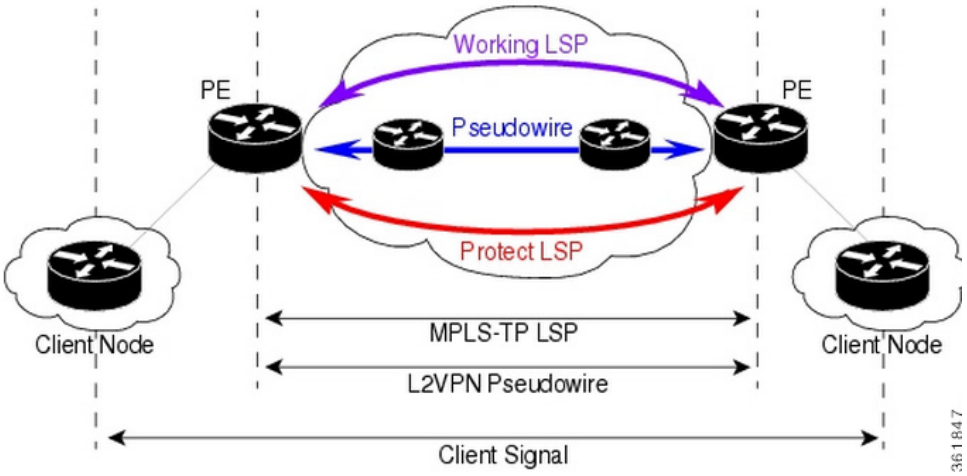
- Force Switch (Lockout)—This command is used to switch normal traffic from a working LSP to a protected LSP. This command can only be applied on a working LSP. If Force Switch is enabled, then the Working LSP becomes standby and the Protected LSP becomes active.
- Manual Switch—This command is used to switch normal traffic from a working LSP to a protected LSP. This command can be applied only on a working LSP. If Manual Switch is enabled, then the working LSP becomes standby and the protected LSP becomes active.

Note The Force Switch and Manual Switch commands are both used to switch traffic from the working LSP to the protected LSP. However, if the Manual Switch command is used, and there is a failure in the protecting LSP, then the working LSP becomes active. In case of the Force Switch command, then the working LSP does not become active if there is a failure in the protecting LSP.+

- Lockout of Protecting (Lockout)—This command is used to switch traffic from the protected LSP to the working LSP. This command can be applied only on a protected LSP. If Lockout of Protecting is enabled, then the working LSP becomes active and the protected LSP becomes standby.
- Clear Force Switch (no Lockout)—This command is used to clear the force switch on a working LSP after which the working LSP becomes active and the protected LSP becomes standby.
- Clear Manual Switch—This command is used to clear the manual switch made on a working LSP, after which the working LSP becomes active and the protected LSP becomes standby.
- Clear Lockout of Protecting (no Lockout)—This command is used to clear the lockout of protecting made on a protected LSP. The working LSP becomes standby and the protected LSP becomes active after this command is executed.

Figure 17-24 depicts the MPLS-TP topology along with the working and protected LSPs:

Figure 17-24 Linear Protection for MPLS-TP



Note In the above figure, you can find working and protected LSPs between two routers. In case of maintenance or network upgrade, the Force Switch and Manual Switch commands can be used to shut down the working LSP link. Similarly, the Lockout of Protecting command can be used to shut down the protected LSP link.

To switch traffic using the Force Switch or Manual Switch command:

Step 1 In the map view, right-click the required link and choose **Properties**. A list of tunnels for the selected link is displayed.

Step 2 Right-click on the required physical link and choose the **Manage MPLS-TP tunnels** option. The MPLS-TP tunnels' commands dialog box is displayed.

Note If there are no MPLS-TP tunnels configured for the selected link, then a message indicating the absence of MPLS-TP tunnels is displayed.

Step 3 In the MPLS-TP tunnels' commands dialog box, select the working LSP tunnel and select **Force Switch (Lockout)** or **Manual Switch** in the **Commands** field.

Step 4 Click **Execute Now**. You are prompted to confirm the operation.

Step 5 Click **Yes** to confirm. The status of the working LSP is updated as **Standby** and the status of the protected LSP is updated as **Active** after this operation.

To switch traffic using the Lockout of Protecting command:

Step 1 In the map view, right-click the required link and choose **Properties**. A list of tunnels for the selected link is displayed.

Step 2 Right-click on the required physical link and choose the **Manage MPLS-TP tunnels** option. The MPLS-TP tunnels' commands dialog box is displayed.

Step 3 In the MPLS-TP tunnels' commands dialog box, select the protected LSP tunnel and select **Lock of Protecting** in the **Commands** field.

Step 4 Click **Execute Now**. You are prompted to confirm the operation.

Step 5 Click **Yes** to confirm. The status of the working LSP is updated as **Active** and the status of the protected LSP is updated as **Standby** after this operation.

To clear the Force Switch or Manual switch on a working LSP:

Step 1 In the map view, right-click the required link and choose **Properties**. A list of tunnels for the selected link is displayed.

Step 2 Right-click on the required physical link and choose the **Manage MPLS-TP tunnels** option. The MPLS-TP tunnels' commands dialog box is displayed.

Step 3 In the MPLS-TP tunnels' commands dialog box, select the working LSP tunnel that has been locked and select **Clear Force Switch** or **Clear Manual Switch** in the **Commands** field.

Step 4 Click **Execute Now**. You are prompted to confirm the operation.

Step 5 Click **Yes** to confirm. The status of the working LSP is updated as **Active** and the status of the protected LSP is updated as **Standby** after this operation.

To clear the Lockout of Protecting on a protected LSP:

Step 1 In the map view, right-click the required link and choose **Properties**. A list of tunnels for the selected link is displayed.

Step 2 Right-click on the required physical link and choose the **Manage MPLS-TP tunnels** option. The MPLS-TP tunnels' commands dialog box is displayed.

Step 3 In the MPLS-TP tunnels' commands dialog box, select the protected LSP tunnel that has been locked and select **Clear Lockout of Protecting** in the **Commands** field.

Step 4 Click **Execute Now**. You are prompted to confirm the operation.

Step 5 Click **Yes** to confirm. The status of the protected LSP is updated as **Active** and the status of the working LSP is updated as **Standby** after this operation.

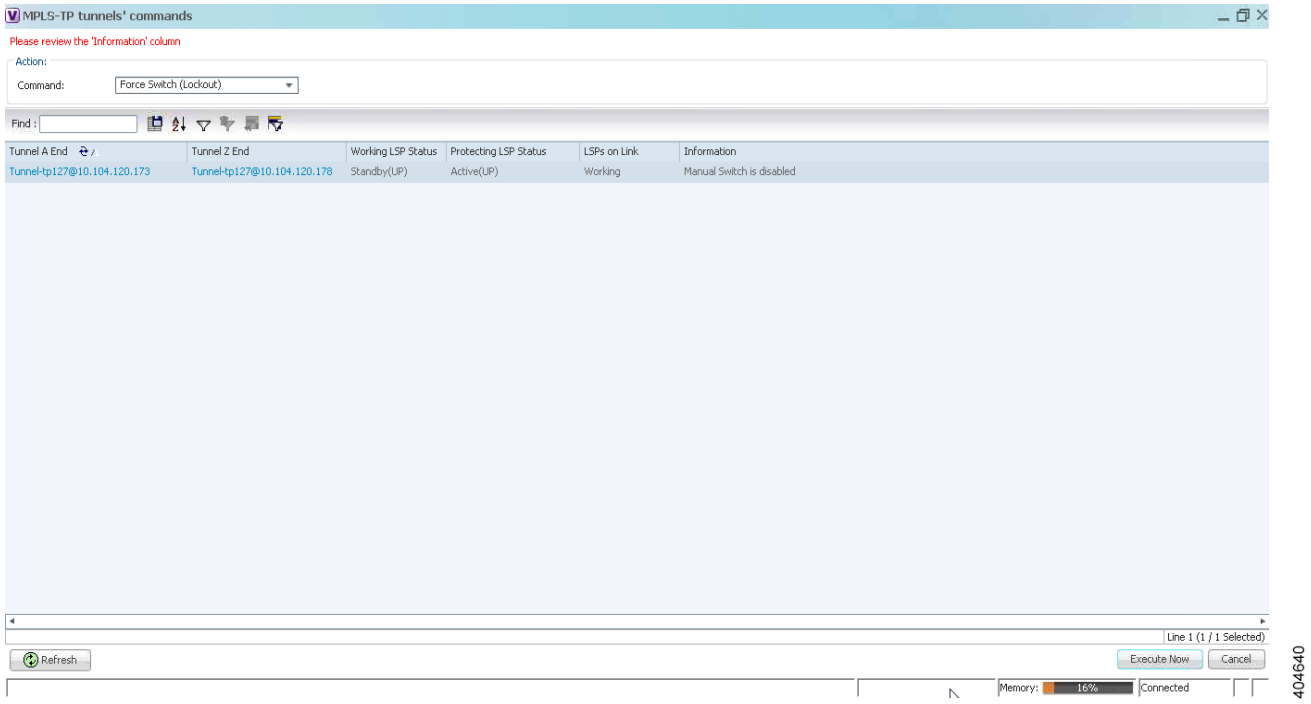
Visualization Status Enhancements- MPLS TP Tunnel

In the MPLS TP Tunnel, the following visualization status enhancements have been carried out:

Non Eligible LSPs

If the tunnel is not configured with protected LSP, i.e., the tunnel is configured with working LSP (Active-UP); the information column displays the value as Protected LSP is not configured. See Figure 17-26.This information is displayed for all non-eligible LSPs which are not eligible for bulk flow operations like FS, LOP, MS, LOCK.

Figure 17-25 Viewing the Working LSPs and Protected LSPs



In the above Figure 17-25, both the status of **Working LSP** and the **Protected LSP** are in up state. So, the **Information** field is blank.

Lockout State

In the Lockout State, information value has been changed. If the **Working LSP** is down, it displays **Working LSP is Locked Out**. If the **Protected LSP** is down, it displays that the **Protected LSP is Locked Out**

Figure 17-26 Viewing the Lockout States of LSP

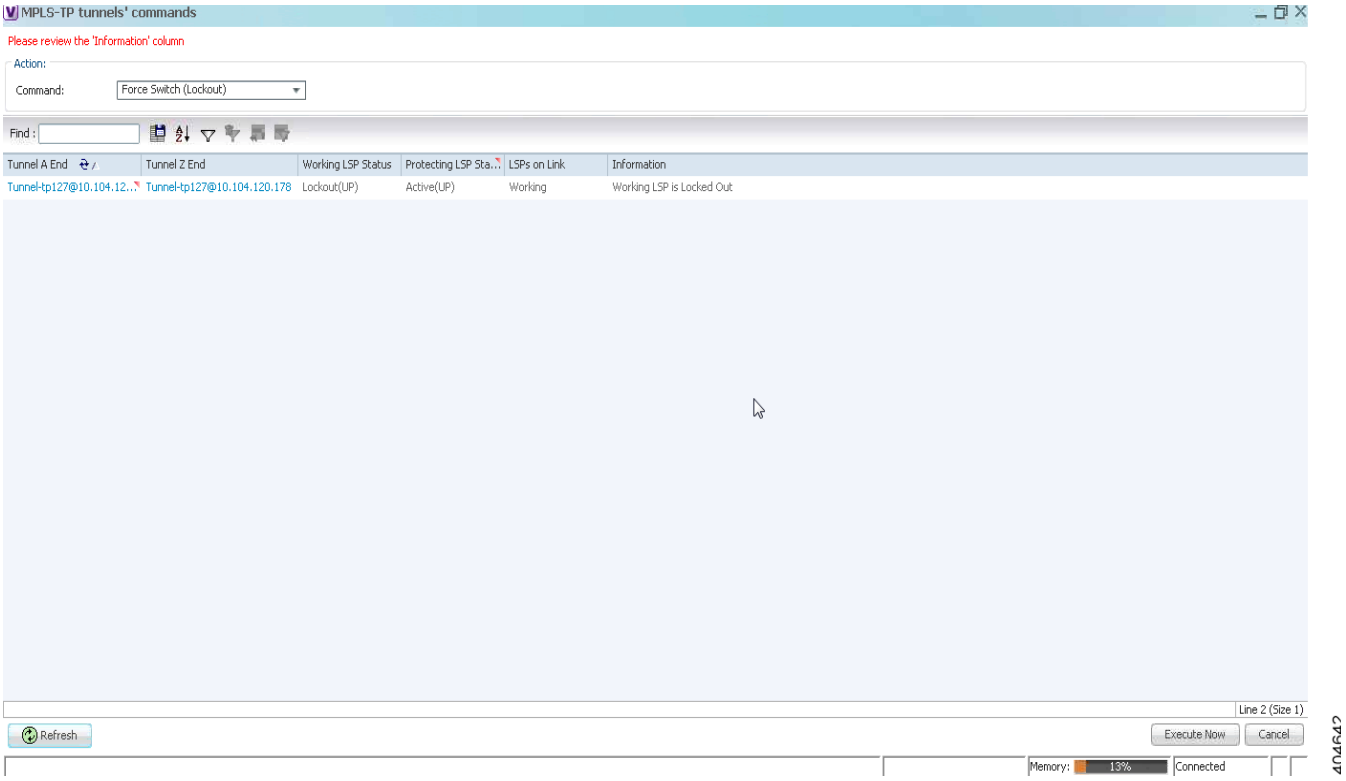
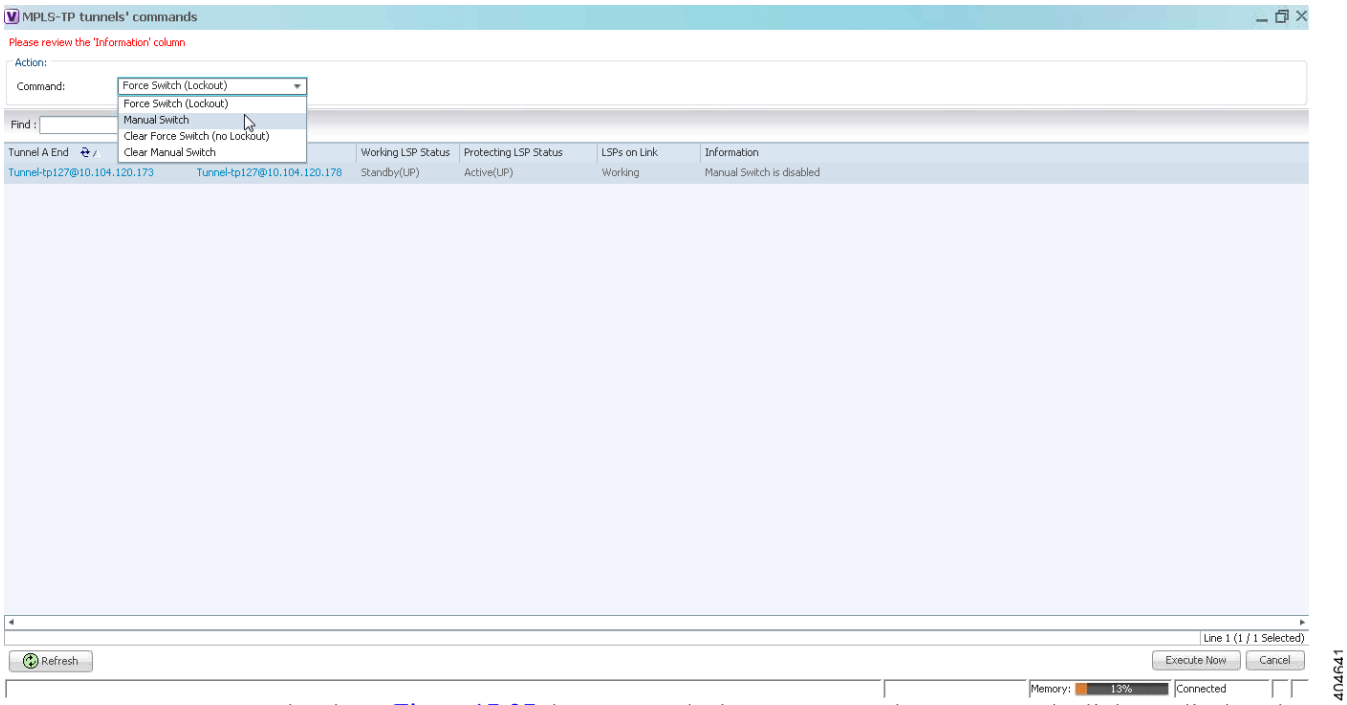


Figure 17-27 Viewing the Commands for Eligible LSPs



In the above Figure 17-27 the commands that are executed on LSPs on the link are displayed.

It will be enabled only when an eligible LSP is working/protected on the link.

Other Descriptions displayed in the Information Column are :

- If only the Working LSP is configured, you will not be allowed to Lock the Working LSP since, there is no Protected member to carry the traffic; the information column displays the value as Protected LSP is not configured.
- If both the “Working LSP EndPoints” and “Protected LSP EndPoints” are configured in the same physical link, which informs that this tunnel will not be allowed for performing the Lockout operations; the information column displays the value as Both LSPs are configured on the same physical link.
- If the device's Software Version in which the “Manual Switch” feature is disabled; the information column displays the value as Manual switch is disabled.
- If both the Working (Active) and Protected LSPs are in Down state; the information column displays the value as Working and protected LSPs are down.
- If the tunnel is not eligible for any Linear Protection operations as it is disabled, the information column displays the value as Linear Protection is disabled.

Configuring MPLS-TE

The following table lists commands you can use to configure MPLS-TE and how to launch these commands. You can preview a command before executing it, or schedule it to run at a later time. You may be prompted to enter your device access credentials while executing a command.

Your permissions determine whether you can run these commands (see Permissions for Managing MPLS Services, page B-18). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*. (You can also add support for new commands by downloading and installing Prime Network Device Packages (DPs); see the *Cisco Prime Network 5.3 Administrator Guide*.)

Command	Navigation	Description
Configure MPLS-TE Global	**LSEs >** *right-click* **Label Switching > Commands > Configuration**	Configures MPLS at the device level or an interface level. Contains information on MPLS interfaces and whether traffic engineering tunnels are configured.
Configure MPLS-TE Interface	**Routing Entities > Routing Entity >** *IP Interfaces tab, right-click the required interface* **> Commands > Configuration**	

Configuring MPLS

The following table lists commands you can use to configure MPLS and how to launch these commands. You can preview a command before executing it, or schedule it to run at a later time. You may be prompted to enter your device access credentials while executing a command.

Your permissions determine whether you can run these commands (see Permissions for Managing MPLS Services, page B-18). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*. (You can also add support for new commands by downloading and installing Prime Network Device Packages (DPs); see the *Cisco Prime Network 5.3 Administrator Guide*.)

Command	Navigation	Description
Configure MPLS Discovery	**LSEs >** *right-click* **Label Switching > Commands > Configuration**	Configures MPLS LDP discovery parameters to discover core MPLS networks. This also includes specifying the discovery method.
Configure MPLS Label Range		Configures MPLS static and dynamic label range.
Enable MPLS on Interface	**LSEs > Label Switching >** right-click the selected ID in the **MPLS Interface** tab > **Commands > Configuration**	Enables/disables MPLS protocol on an interface. Contains information on MPLS interfaces and whether traffic engineering tunnels are configured on an interface.
Disable MPLS on Interface		

Configuring RSVP

The following RSVP commands manage a reserved-bandwidth path between hosts or the end systems to predetermine and ensure Quality of Service (QoS) for their data transmission. You can preview a command before executing it, or schedule it to run at a later time. You may be prompted to enter your device access credentials while executing a command.

Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*. (You can also add support for new commands by downloading and installing Prime Network Device Packages (DPs); see the *Cisco Prime Network 5.3 Administrator Guide*.)

Command	Navigation	Description
Configure RSVP	**LSEs >** *right-click* **Label Switching > Commands > Configuration**	Configures RSVP on a device or an interface.
Delete RSVP		
Enable RSVP On Interface **Disable RSVP On Interface**	**Routing Entities > Routing Entity > IP Interfaces** *tab, right-click the required interface* **> Commands > Configuration**	

Configuring BGP

The following BGP commands configure the routing protocol to communicate with the other sites and VRFs. BGP neighbors should be configured as part of BGP routing. At least one neighbor and at least one address family must be configured to enable BGP routing.

You can preview a command before executing it, or schedule it to run at a later time. You may be prompted to enter your device access credentials while executing a command.

Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*. (You can also add support for new commands by downloading and installing Prime Network Device Packages (DPs); see the *Cisco Prime Network 5.3 Administrator Guide*.)

Command	Navigation	Description
Create BGP Router **Modify BGP Router** **Delete BGP Router**	**MPBGPs** > *right-click* **MPBGP > Commands > Configuration > Create BGP Router** **MPBGPs** > *right-click* **MPBGP > Commands > Configuration > Modify BGP Router** **MPBGPs** > *right-click* **MPBGP > Commands > Configuration > Delete BGP Router**	Configures BGP routing and establish a BGP routing process with AS number and Router ID
Create BGP Address Family	**MPBGPs > MPBGP >** *right-click on the BGP neighbour in the content pane* **> Commands > Configuration > Create BGP Address Family**	Enter various address family configuration modes that uses IPv4, IPv6, L2VPN, VPNV4 or VPNV6 address prefixes.
Create BGP Neighbour	**MPBGPs > MPBGP >** *right-click on the BGP neighbour in the content pane* **> Commands > Configuration > Create BGP Neighbour**	Places the router in Neighbour configuration mode for BGP routing and configures the Neighbour IP address as a BGP peer.
Modify BGP Neighbour **Delete BGP Neighbour**	**MPBGPs > MPBGP >** *right-click on the BGP neighbour in the content pane* **> Commands > Configuration >**	

Configuring VRRP

The following VRRP commands configure the VRRP protocol on routers. These commands configures transparent failover at the first-hop IP router, enabling a group of routers to form a single virtual router. You can preview a command before executing it, or schedule it to run at a later time. You may be prompted to enter your device access credentials while executing a command.

Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*. (You can also add support for new commands by downloading and installing Prime Network Device Packages (DPs); see the *Cisco Prime Network 5.3 Administrator Guide*.)

Command	Navigation	Description
Create VRRP Group **Delete VRRP Interface**	**Routing Entities > Routing Entity > IP Interfaces** *tab, right-click the required interface* **> Commands > Configuration**	Configure a group of routers to form a single virtual router. Example is using VRRP group as default router on the client. The LAN clients can be configured with the virtual router as their default gateway thus avoiding single point of failure, which was the case in dynamic discovery protocol.
Modify VRRP Group **Delete VRRP** **Show VRRP**	**Routing Entities >** *Routing Entity* **> IP Interfaces** *tab, double-click on the VRRP configured interface > select* **VRRP Group** *tab* **>** *right-click on required group.*	

Configuring Bundle Ethernet

Configure a bundle of one or more ports to form a single link using bundle ethernet commands.

The following table lists the supported bundle ethernet commands. You can preview a command before executing it, or schedule it to run at a later time. You may be prompted to enter your device access credentials while executing a command.

Your permissions determine whether you can run these commands (see Appendix B, "Permissions Required to Perform Tasks Using the Prime Network Clients"). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*. (You can also add support for new commands by downloading and installing Prime Network Device Packages (DPs); see the *Cisco Prime Network 5.3 Administrator Guide*.)

Command	Navigation	Description
Configure Bundle Ethernet	**Physical Inventory** > **Chassis** > *Slot* > *Ethernet Port* > **Commands > Configuration**	Configuring an Ethernet link bundle involves creating a bundle and adding member interfaces to that bundle.

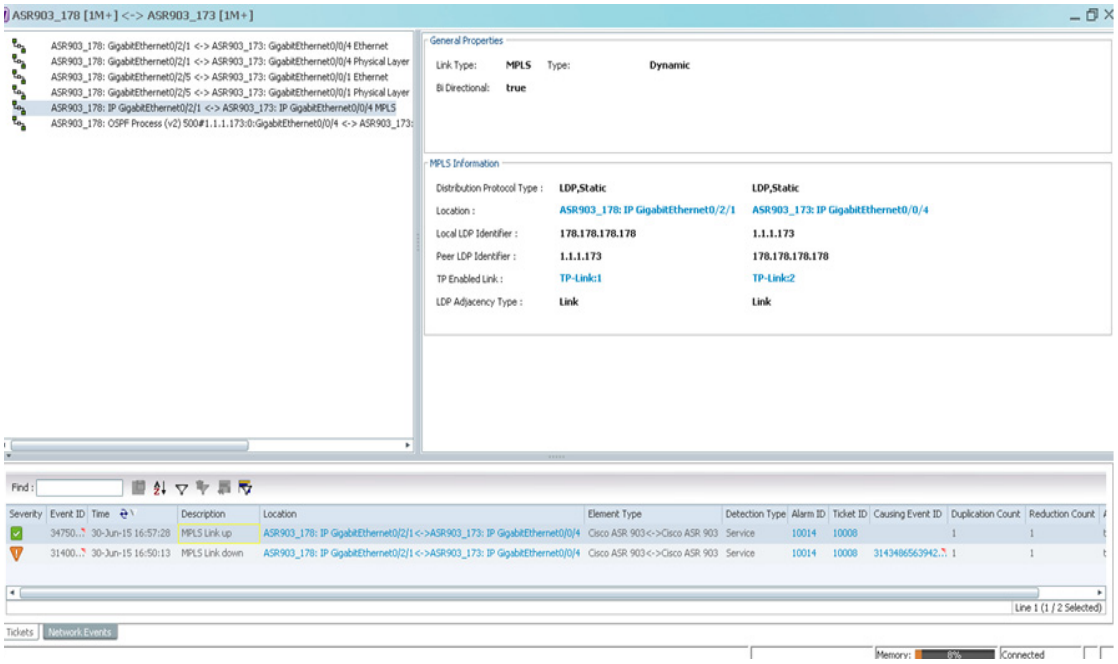
Viewing MPLS LDP, Static Information

The Multi-Protocol Label Switching (MPLS) is a scalable, protocol-independent transport. In an MPLS network, data packets are assigned labels. The packet-forwarding decisions are made solely based on the contents of this label, without the need of examining the packet itself. This enables creating end-to-end circuits across any type of transport medium using any protocol.

Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) enables peer label switch routers (LSRs) in an MPLS network to exchange label binding information for supporting hop-by-hop forwarding in an MPLS network.

As part of the topological link support, Prime Network started supporting two new service alarms **MPLS Link down** and **MPLS Link up**, besides MPLS-TP inventory information. These alarms are raised on the MPLS links during misconfigurations of physical links or shut down of physical interfaces. To view the service alarms supported by Prime Network, refer Cisco Prime Network Supported Service Alarms

Figure 17-28 Viewing MPLS link configured with LDP and Static



Working with FEC 129-based Pseudowire

The following topics describe how to use the Vision client to monitor FEC 129-based pseudowires:

- FEC 129-based Pseudowire, page 17-76
- Viewing FEC 129-based Pseudowire from Logical Inventory, page 17-76
- Viewing FEC 129 links from Topology View, page 17-80
- FEC 129-based Pseudowire Service Discovery, page 17-82
- Viewing FEC 129 Type II-based Pseudowire Tunnel from Pseudowire Map View, page 17-83
- Viewing FEC 129 Type II-based Pseudowire Tunnels from Virtual Connection Map View, page 17-84
- Viewing FEC 129 Type I-based Pseudowire Tunnel from VPLS Map view, page 17-85
- Viewing FEC 129 Type I-based Pseudowire Tunnels from Virtual Connection Map View, page 17-86

FEC 129-based Pseudowire

A pseudowire (PW) is a Layer 2 circuit or a service that emulates the essential attributes of a telecommunication service (such as T1 line) over an MPLS packet-switched network (PSN).

Pseudowires can be established between two provider edges (PEs) as a single segment (SS) or multisegment (MS) pseudowire.

The Cisco Prime Network supports FEC 129 pseudowire configured in a single segment mode.

The single segment pseudowire (SS-PW) pseudowire originates and terminates on the edge of the same MPLS PSN, especially within the same autonomous system (AS). The pseudowire label is unchanged between the originating and terminating provider edge (T-PE) devices.

The FEC 129 pseudowire uses Source Attachment Individual Identifier (SAII), Target Attachment Individual Identifier (TAII), and Attachment Group Identifier (AGI) to make a key along with the existing attributes such as tunnel ID and peer router IP.

The FEC 129-based pseudowire can be classified into two types based on the attachment circuit:

- Type I—The attachment circuit for type I would be VSI, which in turn connected to bridges on either ends. You can identify the Type I pseudowires uniquely with the AGI, SAII, and TAII values.
- Type II—The attachment circuit for type II would be Ethernet on which EFP is configured. You can identify the Type II pseudowire uniquely with the SAII and TAII values.

  In order to configure FEC 129 Type II pseudowire, an Ethernet interface with EFP already configured, is selected. Under this Ethernet interface (which becomes SAII), you can configure the TAII with the target attachment identifier statement. If the configured target identifier matches a source identifier advertised by a remote PE device by way of a BGP auto discovery message, then the pseudowire between that source and target pair is signaled. If there is no match between an advertised source identifier and the configured target identifier, the pseudowire is not established.

The following topic explain how to view the FEC 129 pseudowire from the inventory view:

- Viewing FEC 129 Type I-based Pseudowire from VSI Inventory, page 17-78

Viewing FEC 129-based Pseudowire from Logical Inventory

To view the FEC 129-based pseudowire information in the logical inventory:

Step 1 Right-click the required device in the Vision client and choose Inventory.

Step 2 In the Inventory window, choose **Logical Inventory** > **Pseudowires**.

Note The AGI, SAII, and TAII are the new attributes supported for the FEC 129-based pseudowires.

The **Pseudowire Tunnel Edges** table is displayed and contains the information described in Table 17-30.

Table 17-30 Pseudowire Tunnel Edges Table

Field	Description
Local Interface	Name of the subinterface or port. Strings, such as Aggregation Group, EFP, VLAN, and VSI, are included in the interface name, and the entry is hyperlinked to the relevant entry in logical or physical inventory.
VC ID	Tunnel identifier, hyperlinked to the PTP Layer 2 MPLS Tunnel Properties window. **Note** For the FEC 128 pseudowire, VC ID is populated whereas for the FEC 129 pseudowire, VC ID is not populated.
AGI	Attachment Group Identifier (AGI). An identifier common to a group of pseudowires that may be connected. The AGI carries VPLS ID of the local PE router VPLS instance. The VPLS ID must be the same for all the PEs in the same VPLS instance.
SAII	Specifies the Source Attachment Individual Identifier (SAII) of the tunnel. The SAII attribute is configured for FEC 129 Type I and II pseudowires.
TAII	Specifies the Target Attachment Individual Identifier (TAII) of the tunnel. The TAII attribute is configured for FEC 129 Type I and II pseudowires.
Pseudowire Type	Type of pseudowire, in this case Ethernet.
Peer	Details of the selected peer, hyperlinked to the peer pseudowire tunnel in logical inventory.
Status	Operational state of the tunnel: Up or Down.
Pseudowire Role	If the pseudowire is in a redundancy configuration, indicates whether its role is as the primary or secondary pseudowire in the configuration. If the pseudowire is not configured for redundancy, this field is blank.
Preferred Path Tunnel	Path to be used for MPLS pseudowire traffic.
Local Router IP	IP address of local tunnel edge, which is used as the MPLS router identifier.
Peer Router IP	IP address of the peer tunnel edge, which is used as the MPLS router identifier.
Local MTU	Size, in bytes, of the MTU on the local interface.
Remote MTU	Size, in bytes, of the MTU on the remote interface.
Local VC Label	MPLS label that is used by this router to identify or access the tunnel. It is inserted into the MPLS label stack by the local router.
Peer VC Label	MPLS label that is used by this router to identify or access the tunnel. It is inserted into the MPLS label stack by the peer router.
Signaling Protocol	Protocol used by MPLS to build the tunnel, for example, LDP or TDP.
Peer Status	Status of the peer link.
Associated EVC Name	Specifies the name of the associated Ethernet Virtual Circuits (EVC).

Viewing FEC 129 Type I-based Pseudowire from VSI Inventory

To view the FEC 129 Type I-based pseudowire from VSI logical inventory:

Step 1 To view VSI properties in the Vision client, open the **VSI Properties** window in either of the following ways:

- Double-click the required VNE and, in the **Inventory** window, choose **Logical Inventory > VSIs >** *vsi*.
- In the navigation pane, expand the VPLS instance, right-click the required VPLS forward, and choose **Inventory** or **Properties**.

Table 17-31 describes the information that is displayed for the selected VSI.

Note The AGI, SAII, and TAII are the new attributes supported for the FEC 129 pseudowires.

Table 17-31 VSI Properties in Logical Inventory

Field	Description
VSI Name	VSI name.
VPN ID	VPN identifier used in an MPLS network to distinguish between different VPLS traffic.
VSI Mode	VSI mode: Point-to-Point (default) or Multipoint.
Discovery Mode	VSI discovery mode: Auto-BGP.
Operational State	VSI operational status: Up or Down.
Administrative State	VSI administrative status: Up or Down.
Local Bridge	Local bridge, hyperlinked to the bridge in logical inventory.
Pseudowires Table	
Pseudowire ID	Pseudowire identifier, hyperlinked to the Tunnel Edges table under Pseudowires in logical inventory.
VC ID	Pseudowire virtual circuit identifier. **Note** For the FEC 128 pseudowire, VC ID is populated whereas for the FEC 129 pseudowire, VC ID is not populated.
AGI	Attachment Group Identifier (AGI). An identifier common to a group of pseudowires that may be connected. The AGI carries VPLS ID of the local PE router VPLS instance. The VPLS ID must be the same for all the PEs in the same VPLS instance.
SAII	Specifies the Source Access Individual Identifier (SAII) of the tunnel. The SAII attribute is configured for FEC 129 Type I and II pseudowires.
TAII	Specifies the Target Attachment Individual Identifier (TAII) of the tunnel. The TAII attribute is configured for FEC 129 Type I and II pseudowires.
Peer IP	IP address of the pseudowire peer.
Autodiscovery	The pseudowire was automatically discovered using BGP (auto-BGP). In this case, the value is True.
Split Horizon	SSH pseudowire policy that indicates whether or not packets are forwarded to the MPLS core. In this case, the value is True.

Viewing FEC 129 links from Topology View

Viewing FEC 129 Pseudowire Properties from Topology View

On adding the two associated VNEs to the map, a link is formed between them. This is the topology view and this link depicts the logical association between the associated VNES. Hovering over this link displays all the logical links (or protocols) configured between these peers.

To view the FEC 129 link:

Step 1 In the Vision client map view, select a link connected to two devices and open the link quick view window.

Step 2 Click the link between the two VNEs. Identify the FEC 129 pseudowires based on the unique identifiers as mentioned in the Viewing FEC 129-based Pseudowire from Logical Inventory, page 17-76.

Note If the link is down, it will be displayed in Red and the active links are displayed as green.

Step 3 To view the FEC 129 properties in detail, click **Properties** in the link properties window.

Step 4 Select the FEC 129 Type I or II link and the link properties are displayed.

Table 17-32 describes the information that is displayed for the FEC 129 link.

Table 17-32 FEC 129 Link Properties

Field	Description
General Properties	
Link Type	Link protocol. In this case, PW.
Type	Type of link: Dynamic or Static.
Bi Directional	Whether the link is bidirectional: True or False.
FEC 129 Properties	Properties are displayed for both ends of the MLPPP link.
ID	Pseudowire identifier, hyperlinked to the VLAN entry in Bridges in logical inventory.
Peer	Identifier of the pseudowire peer, hyperlinked to the entry in the Pseudowire Tunnel Edges table in logical inventory.
AGI	Attachment Group Identifier (AGI). An identifier common to a group of pseudowires that may be connected. The AGI carries VPLS ID of the local PE router VPLS instance. The VPLS ID must be the same for all the PEs in the same VPLS instance. **Note** The FEC 129 Type I topology displays AGI in addition to SAII and TAII.
SAII	Specifies the Source Attachment Individual Identifier (SAII) of the tunnel. The SAII attribute is configured for FEC 129 Type I and II pseudowires.
Tunnel Status	Operational state of the tunnel: Up or Down.
TAII	Specifies the Target Attachment Individual Identifier (TAII) of the tunnel. The TAII attribute is configured for FEC 129 Type I and II pseudowires.
Peer Router IP	IP address of the peer router for this pseudowire.
Pseudowire Type	Type of pseudowire, in this case, Ethernet.
Pseudowire Role	If the pseudowire is in a redundancy configuration, then the pseudowire role indicates whether its a primary pseudowire or a secondary pseudowire in the configuration. If the pseudowire is not configured for redundancy, the field is blank.
Preferred Path Tunnel	Specifies the path that has to be used for MPLS pseudowire traffic.
Local Router IP	Specifies the IP address of the tunnel edge, which is used as the router identifier.
Local MTU	Specifies the byte size of the MTU on the local interface.
Remote MTU	Specifies the byte size of the MTU on the remote interface.
Local VC Label	Specifies the MPLS label that is used by the local router to identify or access the tunnel. It is inserted in the MPLS label stack by the local router.
Peer VC Label	Specifies the MPLS label that is used by the peer router to identify or access the tunnel. It is inserted in the MPLS label stack by the peer router.
Signaling Protocol	Specifies the protocol that is used to build the tunnel, such as the LDP or TDP.
Peer Status	Specifies the status of the peer link.

FEC 129-based Pseudowire Service Discovery

The Cisco Prime Network delivers FEC 129-based discovery for various support services such as bridge domains, pseudowires, Virtual Connections, and VPLS.

The Cisco Prime Network release supports the following service discoveries:

- Bridge Domain Discovery—Discovers bridges domains such as I-Bridges, B-Bridges, and regular bridges that are not associated to VFIs or pseudowires. For more information, refer to Working with PBB-VPLS.
- Pseudowire Discovery—Discovers pseudowires in any one of the following ways:
  - Pseudowires that are associated to I-Bridges and B-Bridges in addition to regular bridges.

Note As specified in the Bridge Domain discovery, the regular bridges associated to pseudowires, cannot be discovered from the Bridge Domain services.

  - All the pseudowires that are associated to Ethernet such as FEC 128, FEC 129 Type II, which in turn has an EFP configured. This service discovers the end-to-end pseudowire peers (FEC 128 or FEC 129 Type II) along with the Ethernet attachments.

Note The FEC 129 Type II end-to-end tunnels are identified from the Pseudowire service using the SAII and TAII values.

- VPLS Discovery—Discovers VPLS in any one of the following ways:
  - VFIs associated to I-Bridges, B-Bridges, and regular bridges.

Note As specified in the Bridge Domain discovery, the regular bridges associated to VFIs, cannot be discovered from the Bridge Domain services.

  - VFIs associated to pseudowires such as FEC 128, FEC 129 Type I pseudowires (pseudowires which are attached to VFIs which in turn attached to bridges (B-Bridges)) are discovered. This service discovers the end-to-end VFIs, which on expanding from the VPLS map view, displays the end-to-end pseudowire peers (FEC 128 or FEC 129 type I pseudowires).

Note The FEC 129 Type I end-to-end tunnels are identified from the VPLS service using the Attachment Group Identifier (AGI) value along with SAII and TAII values.

Note In order to view the B-bridges attached to the VFIs, the bridges must be selected from the Bridge Domain service.

- Virtual Connection or EVC Discovery—Creates an end-to-end complex circuit representing the network associations in the core network of all the above discovered elements. Using the Virtual Connection map view, the complete topology of the pseudowire is displayed instead of selecting each plugin separately from the VPLS or pseudowire map view.
  - FEC 129 Type I—Instead of selecting FEC 129 Type I pseudowires and their associated VFIs (from the VPLS service) and the associated B-bridges (from the bridge domain service), the FEC-129 type 1 end-to-end tunnels can be viewed as a single instance from the Virtual Connection service.
    The FEC 129 Type I end-to-end tunnels are identified using the AGI value along with SAII and TAII values.
  - FEC 129 Type II—The FEC 129 Type II end-to-end tunnels and the Ethernet attachments can be viewed as a single instance from the Virtual Connections service.
    The FEC 129 Type II end-to-end tunnels are identified using the SAII and TAII values.

The following topics explain how to view the FEC 129-based pseudowire from service discovery:

- Viewing FEC 129 Type II-based Pseudowire Tunnel from Pseudowire Map View, page 17-83
- Viewing FEC 129 Type II-based Pseudowire Tunnels from Virtual Connection Map View, page 17-84
- Viewing FEC 129 Type I-based Pseudowire Tunnel from VPLS Map view, page 17-85
- Viewing FEC 129 Type I-based Pseudowire Tunnels from Virtual Connection Map View, page 17-86

Viewing FEC 129 Type II-based Pseudowire Tunnel from Pseudowire Map View

To discover the links between the FEC Type II pseudowires:

Step 1 Choose **Add to Map > Pseudowire** to open the **Add Pseudowire to Specific plugins** dialog box.

Step 2 In the **Add Pseudowire to Specific plugins** dialog box, select **Show All** to display the list of pseudowires.

Step 3 To view a specific FEC Type II pseudowire, filter using the pseudowire ID (SAII or TAII) to identify the FEC Type II pseudowire.

Step 4 Click **OK** to add the selected FEC 129 type II pseudowire to the map.

Step 5 The selected pseudowire component in the map displays the following links. Click the expand (+) icon to view the links:

- Association between the EFP of one router (for example, router 1) to the FEC 129 type II pseudowire.
- Link between the two associated FEC 129 type II pseudowires that are peers.
- Association between the FEC 129 type II pseudowire of the other router (for example, router 2) to the EFP.

Viewing FEC 129 Type II-based Pseudowire Tunnels from Virtual Connection Map View

The Virtual Connection view displays the logical association between the FEC 129 type II pseudowires in a single view.

To view the end-to-end connection between the FEC 129 type II pseudowire peers:

Step 1 Open the **Add Virtual Connection to Specific plugin** dialog box in either of the following ways:

- In the toolbar, choose **Add to Map > Virtual Connection**.
- In the menu bar, choose **File > Add to Map > Virtual Connection**.

Step 2 In the **Add Virtual Connection to Specific plugins** dialog box, select the virtual connection that you want to view.

Step 3 To view a specific FEC type II pseudowire, filter using the pseudowire ID (SAII or TAII) to identify the FEC Type II pseudowire.

Step 4 Click **OK** to add the selected virtual connection component to the map.

Step 5 For the selected virtual connection component in the map, you can view the following FEC 129 Type II pseudowire information:

- Viewing FEC 129 Type II Pseudowire Links from Virtual Connection View, page 17-84
- Viewing FEC 129 Type II Pseudowire Properties from Virtual Connection View, page 17-84

Viewing FEC 129 Type II Pseudowire Links from Virtual Connection View

To view the end-to-end connection between the FEC 129 type II pseudowire peers:

Step 1 Click the expand (+) icon to view the links:

- Association between the EFP of one router (for example, router 1) to the FEC 129 type II pseudowire.
- Link between the two associated FEC 129 type II pseudowires that are peers.
- Association between the FEC 129 type II pseudowire of the other router (for example, router 2) to the EFP.

Viewing FEC 129 Type II Pseudowire Properties from Virtual Connection View

To view the FEC 129 type II pseudowire properties:

Step 1 Right-click the selected virtual connection component in the map.

Step 2 Click the **Properties** tab to display the EVC hyperlink.

Step 3 Click the EVC hyperlink to view the EVC terminating points.

Viewing FEC 129 Type I-based Pseudowire Tunnel from VPLS Map view

The FEC 129 Type I pseudowires are associated to VFIs, which in turn are associated to PBB bridges (that is VFIs are attached to B-bridges, and B-bridges are attached to I-bridges on both the FEC 129 Type I pseudowire peers).

The following services help in viewing the components involved in forming the FEC 129 Type I-based pseudowire topology:

- **VPLS** view—You can view the FEC 129 Type I pseudowires that are attached to the VFIs from the **VPLS** view. These VFIs are in turn attached to the PBB bridges. To view the VFIs, refer Viewing VPLS, page 17-85.
- **Bridge Domain** view—From the bridge domains service, you can view the PBB bridges (I-bridges linked to the B-bridges). To view the bridge domains, refer Viewing Bridge domains, page 17-85.

Note In addition to PBB bridges, regular bridges, with no associations to pseudowires or VFIs, can also be discovered in the **Bridge Domain** service.

Viewing VPLS

To view the VFIs:

Step 1 Choose **Add to Map** > **VPLS** to open the **Add VPLS Instance to *map*** dialog box.

Step 2 In the **Add VPLS Instance to *map*** dialog box, select **Show All** to display the list of VPLS instances.

Step 3 Add the required VPLS instance from the VPLS list. It can be filtered either using the VPN-id or the names of the associated VFIs.

Step 4 Once the VPLS instance is added to the map, it displays the link between the two associated VFIs. On further expanding these VFI components, you can view the associated FEC 129 Type 1 pseudowire peers, linked to these VFIs on either ends.

Step 5 Click the link between the two associated FEC 129 Type 1 pseudowire peers to display the topology link properties window. This link is specific to these FEC 129 Type 1 pseudowire peers.
Unlike the Map view, topology properties which display all the topology links between the two VNEs are added to the map. Refer Viewing FEC 129 links from Topology View, page 17-80.

Viewing Bridge domains

To view the bridge domains associated to the VFIs, follow the steps provided below:

Step 1 Open the **Add Bridge Domain** dialog box in one of the following ways:

- Choose **File Add to Map > Bridge Domain**.
- In the toolbar, click **Add to Map** and choose **Bridge Domain**.

Note The Bridge Domains must be added to the map containing the VPLS instances to view the associations between them.

Step 2 In the **Add Bridge Domain** dialog box, select **Show All** to display the list of bridge domains.

Step 3 For both the peers, select the PBB bridges associated to the VFIs. The bridges can be filtered using the name of the bridges.

Note I-SID can also be used for filtering I-bridges.

Step 4 On adding the PBB-bridges to the map:

- A link is formed between the associated VPLS plugin and the B-bridges for both the peers.
- A link is formed between the I-bridges and the B-bridges for both the peers.

Viewing FEC 129 Type I-based Pseudowire Tunnels from Virtual Connection Map View

The Virtual Connection view displays the logical association between the FEC 129 type I pseudowire peers in a single view.

To view the end-to-end connection between the FEC 129 type I pseudowire peers:

Step 1 Open the **Add Virtual Connection to Specific plugin** dialog box in either of the following ways:

- In the toolbar, choose **Add to Map > Virtual Connection**.
- In the menu bar, choose **File > Add to Map > Virtual Connection**.

Step 2 In the **Add Virtual Connection to Specific plugins** dialog box, select the FEC 129 type I-based pseudowire virtual connection that you want to view.

Step 3 To view a specific FEC type I pseudowire, filter using the I-SID, VPN-id, or the names of the associated VFIs to identify the FEC Type I pseudowire.

Step 4 Click **OK** to add the selected virtual connection component to the map.

Step 5 You can view the following FEC 129 Type I pseudowire information for the selected virtual connection component added to the map:

- Viewing FEC 129 Type I Pseudowire Links from Virtual Connection View, page 17-86
- Viewing FEC 129 Type I Pseudowire Properties from Virtual Connection View, page 17-87

Viewing FEC 129 Type I Pseudowire Links from Virtual Connection View

To view the end-to-end connection between the FEC 129 Type I-based pseudowire peers:

Step 1 Click the Expand (+) icon to view the associated components and the links:

- Association between the VPLS instances. Click the Expand (+) icon on the VPLS instances.
- Association between the VFIs, which on further expansion, displays the corresponding components.
- Association between the FEC-129 Type I-based pseudowire peers. To view the topology **Link Properties** window, click the link between the two associated FEC 129 Type I-based pseudowire peers.

If the above topology has PBB bridges configured on either ends, then the following are displayed in addition to the above components and links:

- Association between the I-bridges and the B- bridges (of both the FEC 129 Type I pseudowire peers).
- Association between the B-bridges and the VPLS instances. For further viewing the components attached to the VPLS instances, navigate to Step 1.

Viewing FEC 129 Type I Pseudowire Properties from Virtual Connection View

To view the virtual connection properties of FEC 129 type I pseudowire peers:

Step 1 Right-click the selected virtual connection component in the map.

Step 2 Click the **Properties** tab to display the EVC hyperlink.

Step 3 Click the EVC hyperlink to view the EVC terminating points.

Managing Carrier Ethernet Configurations

The following topics describe how you can use the Vision client to monitor Carrier Ethernet services. If you cannot perform an operation that is described in these topics, you may not have sufficient permissions; see Permissions for Managing Carrier Ethernet, page B-12.

Viewing CDP Properties

Cisco Discovery Protocol (CDP) is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices.

In Logical Inventory

To view CDP properties:

Step 1 In the Vision client, double-click the device whose CDP properties you want to view.

Step 2 In the **Inventory** window, click **Logical Inventory > Cisco Discovery Protocol**.

The CDP properties are displayed in logical inventory as shown in Figure 18-1.

Figure 18-1 CDP in Logical Inventory

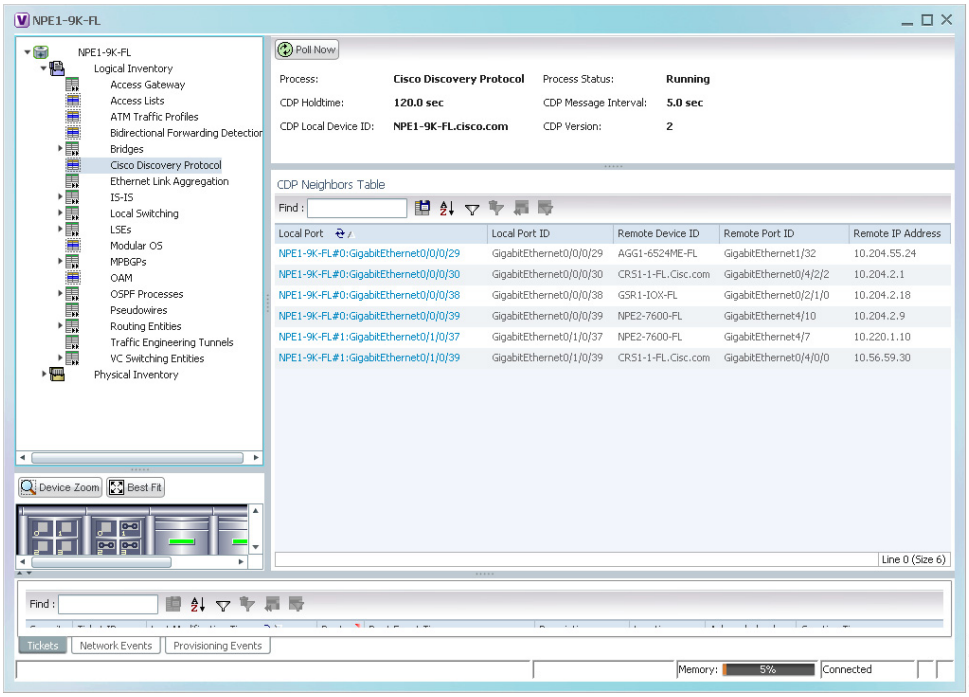


Table 18-1 describes the CDP instance properties that are displayed.

Table 18-1 CDP Properties in Logical Inventory

Field	Description
Process	Process name; in this case, Cisco Discovery Protocol
Process Status	Process status: Running or Disabled.
CDP Holdtime	Specifies the amount of time a receiving device should hold the information sent by a device before discarding it.
CDP Message Interval	Interval between CDP advertisement transmissions.
CDP Local Device ID	Local device identifier.
CDP Version	CDP version: 1 or 2.
CDP Neighbors Table	
Local Port	Local port name.
Local Port ID	Local port identifier.
Remote Device ID	Remote device identifier.
Remote Port ID	Remote port identifier.
Remote IP Address	Remote IP address.

In Physical Inventory

To view CDP on a Layer 2 port:

Step 1 In the Vision client, double-click the device with the Layer 2 port with the CDP information you want to view.

Step 2 In the **Inventory** window, select the required port under Physical Inventory.

The CDP information is displayed in the Discovery Protocols area in the Vision client content pane:

- Discovery Protocol Type—CDP
- Info—Up or Down

Viewing Link Layer Discovery Protocol Properties

Link Layer Discovery Protocol (LLDP) stores and maintains the local device information, including a list of devices directly connected to the device.

In Logical Inventory

To view LLDP properties:

Step 1 In the Vision client, double-click the device with the LLDP information you want to view.

Step 2 In the **Inventory** window, choose **Logical Inventory > Link Layer Discovery Protocol**.

The LLDP properties are displayed in logical inventory as shown in Figure 18-2.

Figure 18-2 LLDP in Logical Inventory

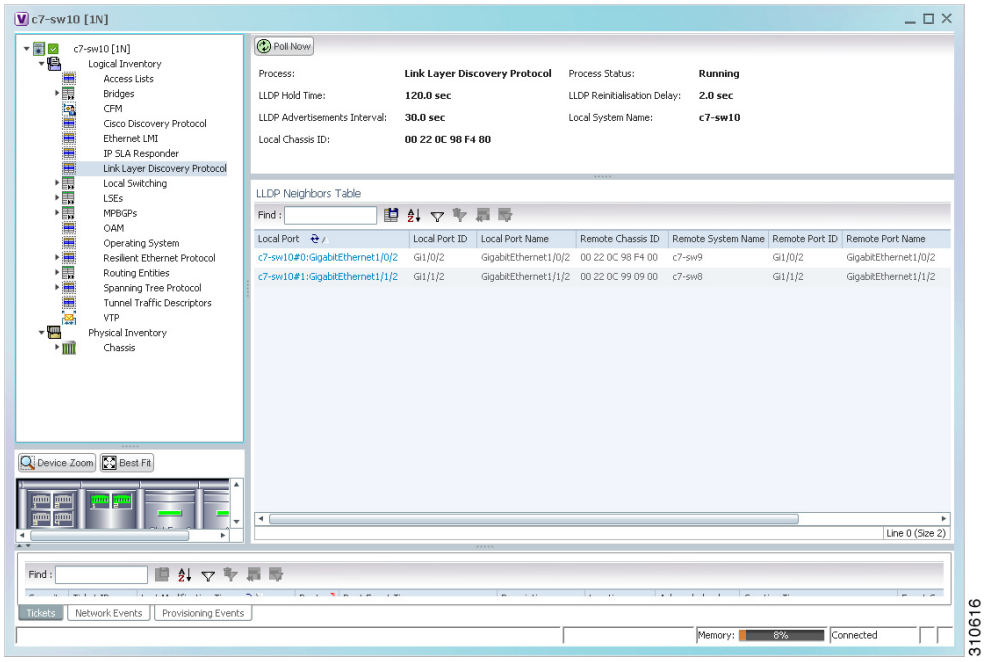


Table 18-2 describes the properties that are displayed for LLDP.

Table 18-2 Link Layer Discovery Protocol Properties

Field	Description
Process	Process; in this case, Link Layer Discovery Protocol
Process Status	Process status: Running or Disabled.
LLDP Hold Time	LLDP advertised hold time in seconds.
LLDP Reinitialization Delay	LLDP interface reinitialization delay in seconds
LLDP Advertisements Interval	LLDP advertisements interval in seconds.
Local System Name	Local system name.
Local Chassis ID	Local chassis identifier.

Table 18-2 Link Layer Discovery Protocol Properties (continued)

Field	Description
LLDP Neighbors Table	
Local Port	Local port.
Local Port ID	Local port identifier.
Local Port Name	Local port name.
Remote System Name	Remote system name.
Remote Chassis ID	Remote chassis identifier.
Remote Port ID	Remote port identifier.
Remote Port Name	Remote port name.
Remote Management IP	Remote management IP address.

In Physical Inventory

To view LLDP on a Layer 2 port:

Step 1 In the Vision client, double-click the device with the Layer 2 port with LLDP information you want to view.

Step 2 In the **Inventory** window, select the required port under Physical Inventory.

The LLDP information is displayed in the Discovery Protocols area in the Vision client content pane:

- Discovery Protocol Type—LLDP
- Info—Tx (Enabled or Disabled), Rx (Enabled or Disabled).

Note If the LLDP transmit is disabled on the interface using CLI and you click the Poll Now button, the LLDP **Info-Tx** field is disabled.

Viewing Spanning Tree Protocol Properties

Spanning Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

To view Spanning Tree properties:

Step 1 In the Vision client, double-click the element whose STP properties you want to view.

Step 2 In the **Inventory** window, choose **Logical Inventory > Spanning Tree Protocol**.

Step 3 STP properties are displayed in logical inventory as shown in Figure 18-3.

Figure 18-3 STP in Logical Inventory

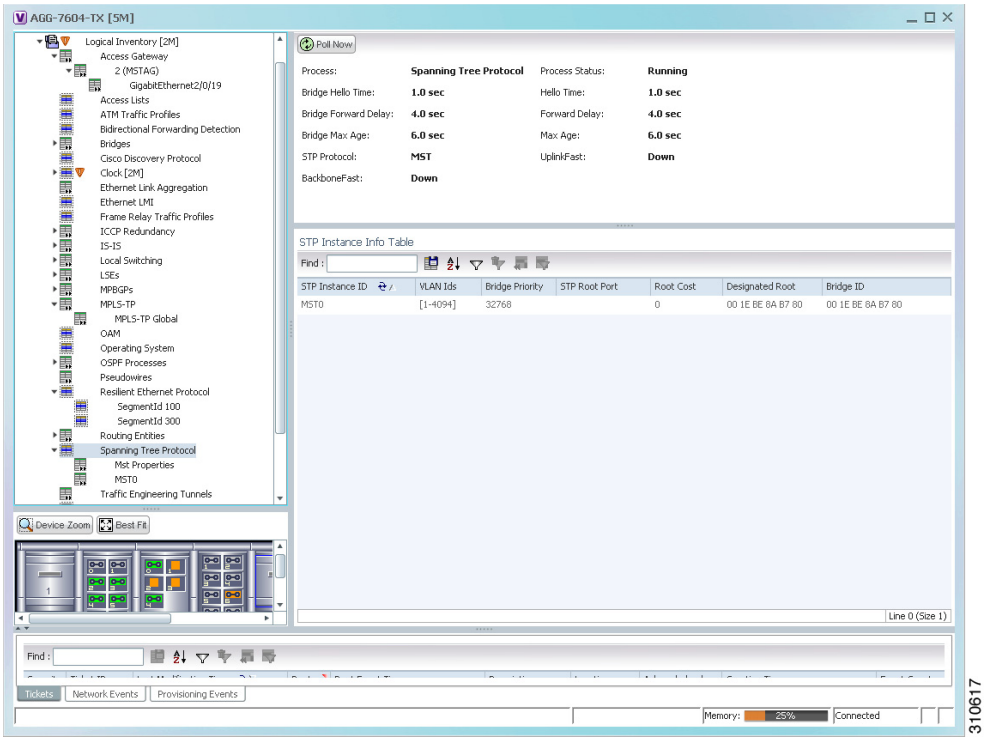


Table 18-3 describes the properties that are displayed for STP.

Table 18-3 STP Properties

Field	Description
Process	Process; in this case, Spanning Tree Protocol.
Process Status	Process status: Running or Disabled.
Bridge Hello Time	Hello message keepalive interval (in seconds) when the port is the root.
Hello Time	Current hello time (in seconds).
Bridge Forward Delay	When the port is the root and in listening or learning state, amount of time to wait (in seconds) before proceeding to the forwarding state.
Forward Delay	Current bridge forward delay (in seconds).
Bridge Max Age	When the port is the root, maximum age of learned Spanning Tree Protocol port information (in seconds).
Max Age	Current maximum age (in seconds).
STP Protocol	STP version: MST, RSTP, PVSTP, MSTP, or RPVST.
UplinkFast	PVSTP Uplink Fast function status: Up or Down.
BackboneFast	PVSTP BackboneFast function status: Up or Down.
STP Instance Info Table	
STP Instance ID	STP instance name.
VLAN ID	VLAN identifiers.
Bridge Priority	Bridge priority.

Table 18-3 STP Properties (continued)

Field	Description
STP Root Port	Hyperlinked entry to the STP port in logical or physical inventory.
Root Cost	Root cost value for this bridge.
Designated Root	MAC address of the designated root.
Bridge ID	Bridge identifier (MAC address).
Bridge Hello Time	Hello message keepalive interval (in seconds) when the port is the root.
Hello Time	Current hello time (in seconds).
Bridge Forward Delay	When the port is the root and in the listening or learning state, amount of time to wait (in seconds) before proceeding to the forwarding state.
Forward Delay	Current bridge forward delay (in seconds).
Bridge Max Age	When the port is the root, maximum age of learned Spanning Tree Protocol port information (in seconds).
Max Age	Current maximum age (in seconds).

Step 4 To view the properties of an STP instance, do one of the following:

- Double-click the required instance.
- Click the required entry in logical inventory under the Spanning Tree Protocol branch.

Table 18-4 describes the information that is displayed in the STP Instance Information Properties window.

Table 18-4 STP Instance Information Properties

Field	Description
STP Instance ID	STP instance identifier.
VLAN ID	VLAN identifier.
Bridge Priority	Bridge priority.
Bridge ID	Bridge identifier (MAC address).
Root Cost	Root cost value for this bridge.
Designated Root	MAC address of the designated root.
Bridge Hello Time	Hello message keepalive interval (in seconds) when the port is the root.
Hello Time	Current hello time (in seconds).
Bridge Forward Delay	When the port is the root and in listening or learning state, amount of time to wait (in seconds) before proceeding to the forwarding state.
Forward Delay	Current bridge forward delay (in seconds).
Bridge Max Age	When the port is the root, the maximum age of learned Spanning Tree Protocol port information (in seconds).
Max Age	Current maximum age (in seconds).
STP Protocol Specification	Specific STP protocol type or variant used for this instance, such as Rapid PvSTP.
Is Root	Whether or not the port is the root: True or False.

Table 18-4 STP Instance Information Properties (continued)

Field	Description
Ports Info Table	
STP Port	Hyperlinked entry to the STP port in physical inventory.
Port State	STP port state: Disabled, Blocking, Listening, Learning, or Forwarding,
Port Role	Port role: Unknown, Backup, Alternative, Designated, Root, or Boundary.
Port Priority	Default 802.1p priority assigned to untagged packets arriving at the port.
Port Path Cost	Port path cost, which represents the media speed for this port.
Point To Point Port	Whether or not the port is linked to a point-to-point link: True or False.
Edge Port	Whether or not the port is an edge port; that is, whether it is connected to a nonbridging device: True or False.
MST Port Hello Time	This field is displayed in the Ports Info Table only for MST. In seconds, the interval between hello BPDUs sent by root switch configuration messages. The range is 1 to 10 seconds.
Port Identifier	STP port identifier.
Portfast	Whether or not STP PortFast is enabled on the port: Up or Down.
Designated Port Identifier	Designated STP port identifier.
Designated Bridge	STP designated bridge.
BPDU Filter	BPDU Filter status: Up or Down.
BPDU Guard	BPDU Guard status: Up or Down.

Step 5 To view MSTP properties, choose the required MSTP entry in logical inventory under Spanning Tree Protocol.

Table 18-5 describes the information that is displayed for MSTP.

Table 18-5 MSTP Properties in Logical Inventory

Field	Description
MST Force Version	Force version used: MST, PVSTP, RSTP, STP, or Unknown.
MST Cfg ID Rev Level	Revision level used by the selected device and negotiated with other devices.
MST Cfg ID Name	MSTP instance name.
MST Max Instances	Maximum number of MSTP instances.
MST Cfg ID Fmt Sel	Configuration format used by this device and negotiated with other devices.
MST External Root Cost	External root cost of the MSTP instance.

The following topics describe how to view STP properties related to:

- VLAN domain views and overlays—See Viewing STP Information in VLAN Domain Views and VLAN Overlays, page 18-83.
- VLAN service link properties—See Viewing STP Properties for VLAN Service Links, page 18-84.

Viewing Resilient Ethernet Protocol Properties (REP)

Cisco Resilient Ethernet Protocol (REP) technology is implemented on Cisco Carrier Ethernet switches and intelligent service edge routers. REP is a segment protocol, and a REP segment is a chain of ports connected to each other and configured with the same segment identifier. Each end of a segment terminates on an edge switch. The port where the segment terminates is called the edge port.

Prime Network discovers and displays REP Segments (identified by a REP segment identifier that is locally configured on the network element) along with Global REP configuration details.

You can also view the REP port roles (open, alternate, and failed) in the Vision client map. The REP port role is displayed as a tool-tip between the REP enabled trunk ports in the Ethernet links. Using the Vision client, you can identify if the segment is open or closed.

The map displays the forwarding direction (REP port roles) along the Physical links within VLAN overlays. It also displays the forwarding direction along the VLAN links among the switching elements within the VLAN logical domain topology.

REP implementation supports the following faults:

- A REP Port Role change to Failed service event will be generated when a REP port role is change from Alternate or Open to Failed.
- A REP Port Role change to OK clearing service event will be generated when a REP port role is change from Failed to Alternate or Open.

Correlation to these service events to physical layer events (for example Link down or Port down) is also performed.

You can view REP properties in logical inventory.

Step 1 In the Vision client, double-click the device configured for REP.

Step 2 In the **Inventory** window, choose **Logical Inventory > Resilient Ethernet Protocol**.

Figure 18-4 shows an example of REP in logical inventory.

Figure 18-4 REP in Logical Inventory

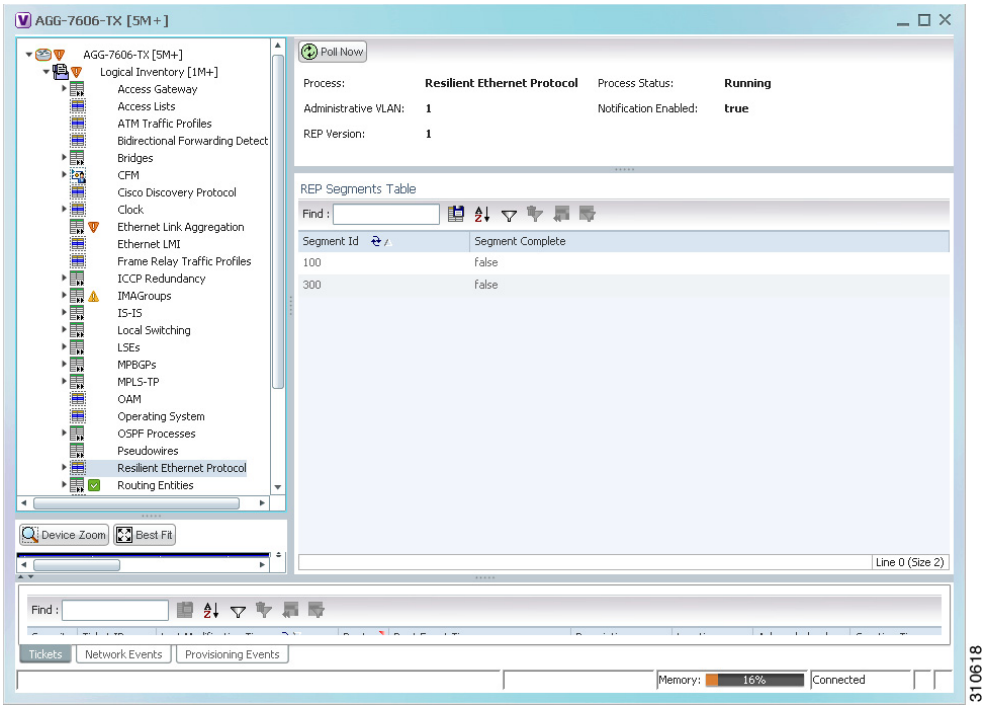


Table 18-6 describes the information that is displayed for REP.

Table 18-6 REP Properties

Field	Description
Process	Process name; in this case, Resilient Ethernet Protocol.
Process Status	State of the REP process, such as Running or Down.
Administrative VLAN	Administrative VLAN used by REP to transmit its hardware flooding layer messages. Values range from 1 to 4094.
Notification Enabled	Whether or not notification is enabled: True or False.
REP Version	Version of REP being used.
REP Segments Table	
Segment ID	Segment identifier.
Segment Complete	Whether the segment is complete; that is, that no port in the segment is in a failed state: True or False.

Step 3 To view REP segment properties, double-click the required entry in the REP Segments table.

Figure 18-5 shows an example of REP segment properties in logical inventory.

Figure 18-5 REP Segment Properties

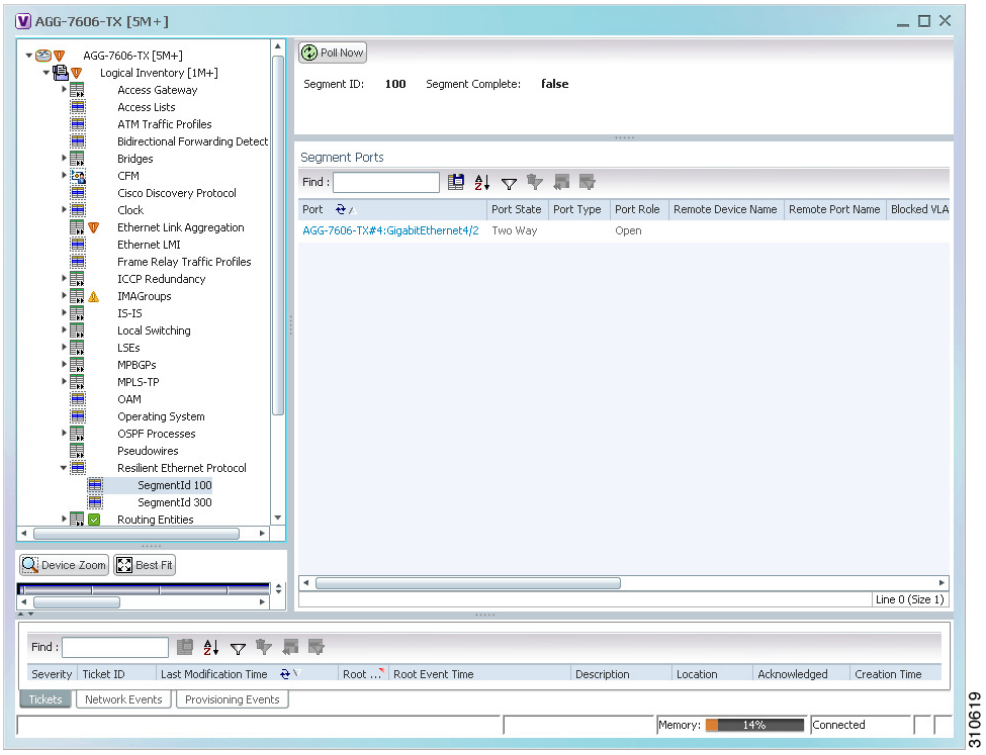


Table 18-7 describes the information that is displayed for REP segments.

Table 18-7 REP Segment Properties

Field	Description
Segment ID	Segment identifier.
Segment Complete	Whether the segment is complete; that is, that no port in the segment is in a failed state: True or False.
Segment Ports Table	
Port	Hyperlinked entry to the port in physical inventory.
Port State	Current operational link state of the REP port: None, Init Down, No Neighbor, One Way, Two Way, Flapping, Wait, or Unknown.
Port Type	Port type: Primary Edge, Secondary Edge, or Intermediate.
Port Role	Role or state of the REP port depending on its link status and whether it is forwarding or blocking traffic: Failed, Alternate, or Open.
Remote Device Name	Name of the neighbor device that this port is connected to on this segment. This value can be null.
Remote Port Name	Name of the neighbor port on the neighbor bridge that this port is connected to on this segment. This value can be null.
Blocked VLANs	VLANs that are blocked on this port.
Configured Load Balancing Blocked VLANs	List of VLANs configured to be blocked at this port for REP VLAN load balancing.
Preemptive Timer	Amount of time, in seconds, that REP waits before triggering preemption after the segment is complete. The entry can range from 0 to 300, or be Disabled. The value Disabled indicates that no time delay is configured, and that the preemption occurs manually. This property applies only to REP primary edge ports.
LSL Ageout Timer	Using the Link Status Layer (LSL) age-out timer, the amount of time, in milliseconds, that the REP interface remains up without receiving a hello from a neighbor.
Remote Device MAC	MAC address of the neighbor bridge that this port is connected to on this segment. This value can be null.

The following topics describe how to view REP properties related to VLANs:

- VLAN domain views and overlays—See Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 18-80.
- VLAN service link properties—See Viewing REP Properties for VLAN Service Links, page 18-81.

Viewing HSRP Properties

Hot Standby Router Protocol (HSRP) is a protocol that provides backup to a router in case of failure. Using HSRP, several routers are connected to the same Ethernet network segment and work together to present the appearance of a single virtual router. The routers share the same IP and MAC addresses; therefore in the event of failure of one router, the hosts on the LAN will be able to continue forwarding packets to a consistent IP and MAC address.

HSRP groups are configured on IP interfaces. An IP interface is modeled by the VNE through the IPInterface DC. The IPInterface DC maintains the HSRP related information by the use of HSRP group entries. Ethernet DCs, which are used to model Ethernet ports, maintain MAC addresses of the HSRP groups.

To view HSRP properties:

Step 1 Double-click the required element in the Vision client.

Step 2 In logical inventory, choose **Logical Inventory > Routing Entities > Routing Entity**.

Step 3 In the IP Interfaces tab, double-click the required interface to view the IP interface properties. If HSRP is configured on the IP interface, the HSRP Group tab is displayed as shown in Figure 18-6.

Figure 18-6 HSRP Group Information

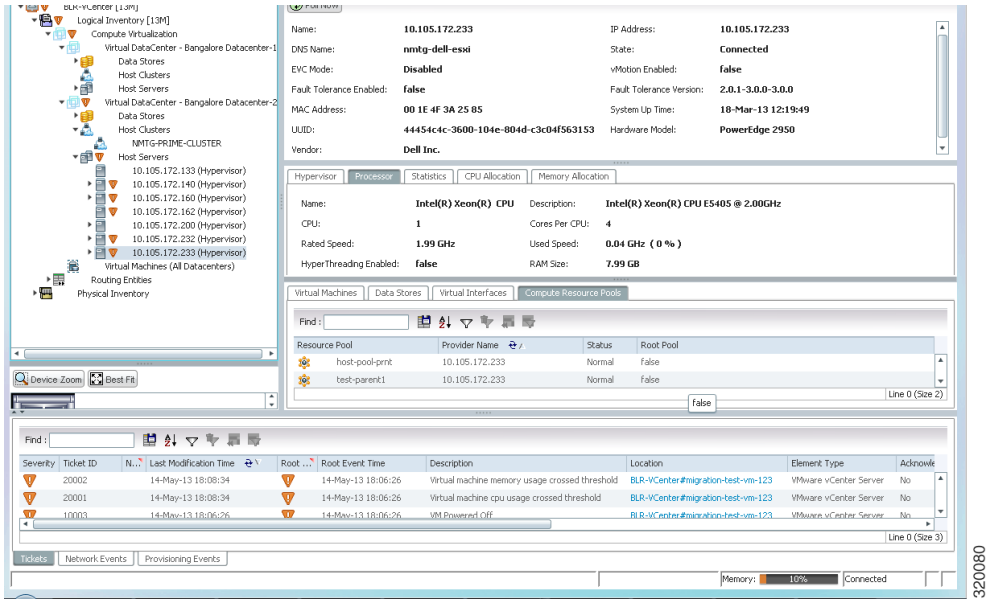


Table 18-8 describes the information in the HSRP Group tab.

Table 18-8 HSRP Group Properties

Field	Description
Group Number	Number of the HSRP group associated with the interface.
Version	Version of the HSRP group.
Port Name	Port on which the HSRP is configured.
Priority	Value that determines the role each HSRP router plays. Values are 1 through 254, with higher numbers having priority over lower numbers.
Coupled Router	The partnet router.
State	State of the HSRP group: Active or Standby.
Virtual IP Address	Virtual IP address assigned to the active router.
Virtual MAC Address	Virtual MAC address assigned to the active router.

Viewing Access Gateway Properties

In an access network, an access gateway configuration ensures loop-free connectivity in the event of various failures by sending statically configured bridge protocol data units (BPDUs) toward the access network. Using statically configured BPDUs enables the gateway device to act appropriately when notified of the following topology changes:

- Failure of a link in the access network.
- Failure of a link between the access network and the gateway device.
- Failure of an access device.
- Failure of a gateway device.

To view access gateway properties:

Step 1 Double-click the element configured for access gateway.

Step 2 In the **Inventory** window, choose **Logical Inventory > Access Gateway >** *access-gateway*. The group name is appended by either MSTAG or REPAG, indicating the group type Multiple Spanning Tree Access Gateway or Resilient Ethernet Protocol Access Gateway.

Figure 18-7 shows an example of an access gateway entry in logical inventory.

Figure 18-7 Access Gateway in Logical Inventory

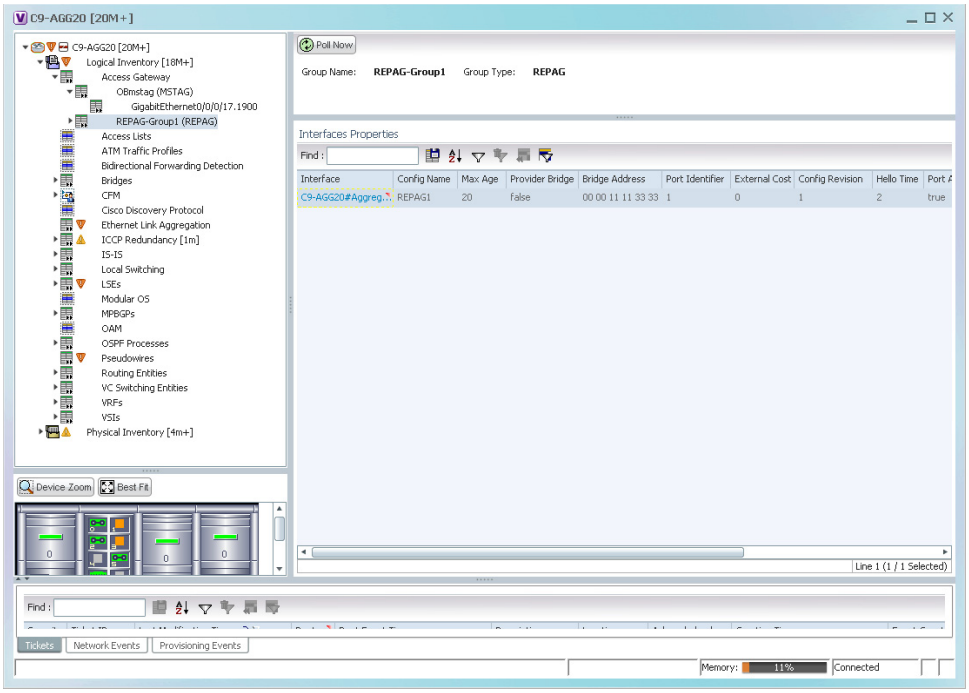


Table 18-9 describes the information that is displayed for an access gateway.

Table 18-9 Access Gateway Properties in Logical Inventory

Field	Description
Group Name	Access gateway group name.
Group Type	Group type: MSTAG or REPAG.
Interface Properties	
Interface	Hyperlink to the interface in physical inventory on which access gateway is configured.
Config Name	Name of the MSTP region. The default value is the MAC address of the switch, formatted as a text string using the hexadecimal representation specified in IEEE Standard 802.
Max Age	In seconds, the maximum age for the bridge. Values range from 6 to 40 seconds.
Provider Bridge	Whether the current instance of the protocol is in 802.1ad mode: True or False.
Bridge Address	Bridge identifier for the interface.
Port Identifier	Port identifier for the interface.
External Cost	External path cost on the current port. Values range from 1 to 200000000.
Config Revision	Number of the configuration revision.

Table 18-9 Access Gateway Properties in Logical Inventory (continued)

Field	Description
Hello Time	Current hello time (in seconds)
Port Active	Whether or not the port is active: True or False.
BPDUs Sent	Number of BPDUs sent.
Reversion Control Enabled	Whether reversion control is enabled: True or False.

Step 3 Choose an access gateway instance to view instance properties.

Figure 18-8 shows an example of the information displayed for an access gateway instance.

Figure 18-8 Access Gateway Instance in Logical Inventory

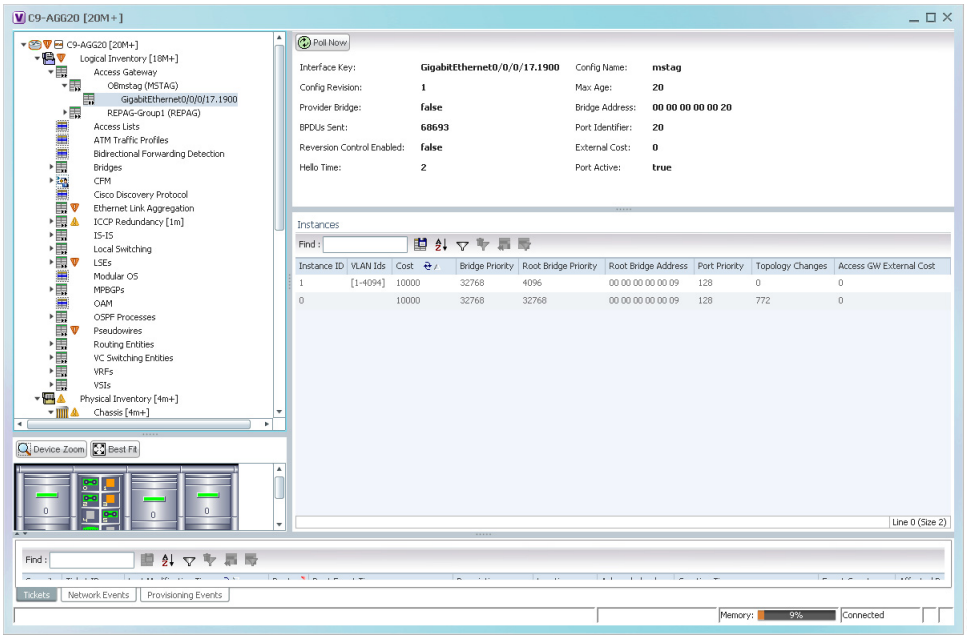


Table 18-10 describes the information that is displayed for an access gateway instance.

Table 18-10 Access Gateway Instance Properties

Field	Description
Interface Key	Hyperlink to the interface in physical inventory on which access gateway is configured.
Config Name	Name of the MSTP region. The default value is the MAC address of the switch, formatted as a text string using the hexadecimal representation specified in IEEE Standard 802.
Config Revision	Number of the configuration revision.
Max Age	In seconds, the maximum age for the bridge. Values range from 6 to 40 seconds.

Table 18-10 Access Gateway Instance Properties (continued)

Field	Description
Provider Bridge	Whether the current instance of the protocol is in 802.1ad mode: True or False.
Bridge Address	Bridge identifier for the current switch.
BPDUs Sent	Number of BPDUs sent.
Port Identifier	Port identifier for the interface.
Reversion Control Enabled	Whether reversion control is enabled: True or False.
External Cost	External path cost on the current port. Values range from 1 to 200000000.
Hello Time	Current hello time (in seconds)
Port Active	Whether or not the port is active: True or False.
Instances Table	
Instance ID	Access gateway instance identifier.
VLAN ID	VLAN identifiers.
Cost	Path cost for this instance.
Bridge Priority	Priority associated with current bridge.
Root Bridge Priority	Priority associated with the root bridge.
Root Bridge Address	Address of the root bridge.
Port Priority	Priority of the interface for this instance.
Topology Changes	Number of times the topology has changed for this instance.
Access GW External Cost	External root cost of this instance.

Working with Ethernet Link Aggregation Groups

Ethernet link aggregation groups (LAGs) provide the ability to treat multiple switch ports as one switch port. The port groups act as a single logical port for high-bandwidth connections between two network elements. A single link aggregation group balances the traffic load across the links in the channel.

LAG links are discovered automatically for devices that support LAG technology and use VNEs that model Link Aggregation Control Protocol (LACP) attributes.

You can create static links between Ethernet LAGs by choosing a LAG and the desired port channel for the A or Z side as described in Adding a Static Link When a Network Link is Missing, page 4-13.

If a physical link within the link aggregation group fails, the following actions occur:

- Traffic that was previously carried over the failed link is moved to the remaining links.

  Most protocols operate over single ports or aggregated switch ports and do not recognize the physical ports within the port group.

- An aggregation service alarm is generated.

  The aggregation service alarm indicates the percentage of links within the aggregation that have failed. For example, if an Ethernet link aggregation group contains four Ethernet links and one fails, the aggregation service alarm indicates that 25% of the links are down.

Viewing Ethernet LAG Properties

To view a device's Ethernet LAG properties, the device must be configured to receive SNMP traps as described in the *Cisco Prime Network 5.3 Administrator Guide*. To view properties for Ethernet link aggregation groups:

Step 1 In the Vision client, double-click the device with the link aggregation group you want to view.

Step 2 In the **Inventory** window, choose **Logical Inventory > Ethernet Link Aggregation**.

The link aggregation properties are displayed as shown in Figure 18-9.

Figure 18-9 Ethernet Link Aggregation in Logical Inventory

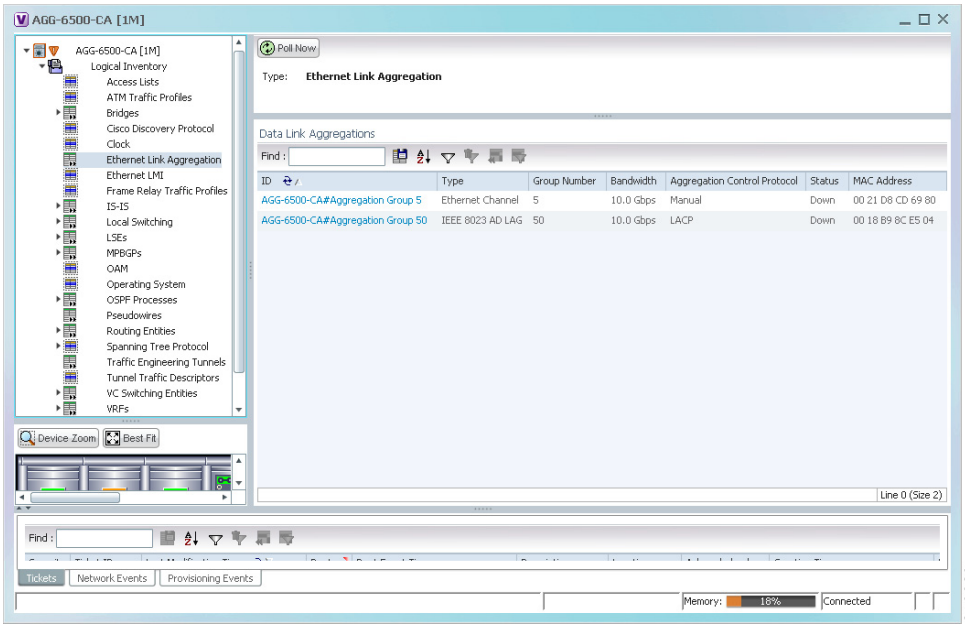


Table 18-11 describes the aggregation group properties that are displayed in the Data Link Aggregations table.

Table 18-11 Data Link Aggregations Table

Field	Description
ID	Aggregation identifier. Double-click the entry to view the properties for that aggregation.
Type	Aggregation group type: Ethernet Channel or IEEE 802.3 AD LAG.
Group Number	Aggregation group number.
Bandwidth	Aggregation bandwidth.

Table 18-11 Data Link Aggregations Table (continued)

Field	Description
Aggregation Control Protocol	Aggregation control protocol: Manual, Link Aggregation Control Protocol (LACP), or Port Aggregation Protocol (PagP).
Status	Aggregation status: Up or Down.
MAC Address	Aggregation MAC address.
Link Type	The type of ethernet bundle link, namely ICL and transport. • ICL link type represents the ethernet link bundle between Cisco ASR 9000 device and satellite chassis or between two satellite chassis. • Transport link type represents the ethernet link bundle between two Cisco ASR 9000 devices.
Non Revertive	Specifies the currently active but a lower priority port to remain active port even after a higher priority port is capable of being operational (if non revertive is enabled). By default, non revertive is disabled.
Load Balance	Load balance type which uses Source and Destination MAC address, Source IP address, or Destination IP address.

Step 3 To view properties for a specific aggregation, double-click the group identifier.

The information that is displayed depends on the type of aggregation:

- For Ethernet Channel aggregations, see Table 18-12.
- For IEEE 802.3 AD aggregations, see Table 18-13.

Table 18-12 LAG Ethernet Channel Properties

Field	Description
Group Number	Aggregation group number.
Bandwidth	Aggregation bandwidth in b/s.
Control Protocol	Aggregation control protocol: Manual, Link Aggregation Control Protocol (LACP), or Port Aggregation Protocol (PagP).
MAC Address	Aggregation MAC address.
Administrative State	Aggregation administrative status: Up or Down.
Operational State	Aggregation operational status: Up or Down.
Adjacent	Adjacent group, hyperlinked to the group in logical inventory.
mLACP Properties	mLACP properties are displayed if the aggregation group is associated with an ICCP redundancy group.
ICCP Redundancy Group	ICCP redundancy group associated with this aggregation group, hyperlinked to the relevant entry in logical inventory.
mLACP Role	Role of the LAG in the redundancy group: Active or Standby.
mLACP Operational System MAC	MAC address used in a dual-homed environment that is selected by ICCP from one of the configured system MAC addresses for one of the points of attachment (PoAs).

Table 18-12 LAG Ethernet Channel Properties (continued)

Field	Description
mLACP Operational System Priority	Priority used in a dual-homed environment that is selected by ICCP from the configured system priority on one of the PoAs.
mLACP Failover Option	Configured mLACP failover mode: Revertive or Nonrevertive.
mLACP Max Bundle	Maximum number of links allowed per bundle.
Aggregated Ports Table	
ID	Aggregated port identifier, hyperlinked to the interface in physical inventory.
Type	Aggregation type, such as Layer 2 VLAN.
Mode	VLAN mode, such as Trunk.
Native VLAN ID	VLAN identifier (VID) associated with this VLAN. The range of VLANs is 1 to 4067.
VLAN Encapsulation Type	Type of encapsulation configured on the VLAN, such as IEEE 802.1Q.
Allowed VLANs	List of VLANs allowed on this interface.
VLAN Encapsulation Admin Type	VLAN administration encapsulation type, such as IEEE 802.1Q.
Subinterfaces Table	
Address	IP address of the subinterface.
Mask	Subnet mask applied to the IP address.
VLAN Type	Type of VLAN, such as Bridge or IEEE 802.1Q.
Operational State	Operational state of the subinterface: Up or Down.
VLAN ID	VLAN identifier.
Inner VLAN	CE-VLAN identifier.
IP Interface	IP interface configured as part of the subinterface, hyperlinked to the routing entity or VRF in logical inventory.
VRF Name	VRF associated with the subinterface.
Is MPLS	Whether the subinterface is enabled for MPLS: True or False. This column is displayed when at least one interface is MPLS-enabled.
Tunnel Edge	Whether this is a tunnel edge: True or False.
VC	Virtual circuit identifier, hyperlinked to the VC Table when the subinterface is configured for ATM VC.
Binding	Hyperlinked entry to the specific bridge in logical inventory.
EFPs Table	
EFP ID	EFP identifier.
Operational State	EFP operational state: Up or Down.
VLAN	VLAN associated with this EFP.
Inner VLAN	CE-VLAN identifier.
Translated VLAN	Translated, or mapped, VLAN identifier.
Translated Inner VLAN	Translated, or mapped, inner VLAN identifier.

Table 18-12 LAG Ethernet Channel Properties (continued)

Field	Description
Binding	Hyperlinked entry to the specific bridge in logical inventory.
Description	Description for the EFP.

Table 18-13 LAG IEEE 802.3 AD Properties

Field	Description
Group Number	Aggregation group number.
Bandwidth	Aggregation bandwidth.
Control Protocol	Aggregation control protocol: Manual, Link Aggregation Control Protocol (LACP), or Port Aggregation Protocol (PagP).
MAC Address	Aggregation MAC address.
Administrative State	Aggregation administrative status: Up or Down.
Operational State	Aggregation operational status: Up or Down.
Dot3ad Agg Partner System Priority	Priority of the partner system.
Dot3ad Agg MAC Address	Aggregation MAC address.
Adjacent	Displays the adjacent ethernet link aggregation for the selected Data Link Aggregation ID.
Dot3ad Agg Actor Admin Key	Actor administrative key.
Dot3ad Agg Actor System Priority	Actor system priority.
Dot3ad Agg Partner Oper Key	Partner operational key.
Dot3ad Agg Actor Oper Key	Actor operational key.
Dot3ad Agg Collector Max Delay	Maximum delay (in microseconds) for either delivering or discarding a received frame by the frame collector.
Dot3ad Agg Actor System ID	Actor system identifier, in the form of a MAC address.
Dot3ad Agg Partner System ID	Partner system identifier, in the form of a MAC address.
mLACP Properties	mLACP properties are displayed if the aggregation group is associated with an ICCP redundancy group.
ICCP Redundancy Group	ICCP redundancy group associated with this aggregation group, hyperlinked to the relevant entry in logical inventory.
mLACP Role	Role of the LAG in the redundancy group: Active or Standby.
mLACP Operational System MAC	MAC address used in a dual-homed environment that is selected by ICCP from one of the configured system MAC addresses for one of the points of attachment (PoAs).
mLACP Operational System Priority	Priority used in a dual-homed environment that is selected by ICCP from the configured system priority on one of the PoAs.
mLACP Failover Option	Configured mLACP failover mode: Revertive or Nonrevertive.
mLACP Max Bundle	Maximum number of links allowed per bundle.
Aggregated Ports Table	
ID	Port identifier, hyperlinked to the interface in physical inventory.
Type	Type of VLAN, such as Layer 2 VLAN.
Discovery Protocols	Discovery protocols used on this port.

Table 18-13 LAG IEEE 802.3 AD Properties (continued)

Field	Description
Subinterfaces Table	
Address	IP address of the subinterface.
Mask	Subnet mask applied to the IP address.
VLAN Type	Type of VLAN, such as Bridge or IEEE 802.1Q.
Operational State	Operational state of the subinterface: Up or Down.
VLAN ID	VLAN identifier.
Inner VLAN	CE-VLAN identifier.
IP Interface	IP interface configured as part of the subinterface, hyperlinked to the routing entity or VRF in logical inventory.
VRF Name	VRF associated with the subinterface.
VC	Virtual circuit identifier, hyperlinked to the VC Table when the subinterface is configured for ATM VC.
Binding	Hyperlinked entry to the specific bridge in logical inventory.
EFPs Table	
EFP ID	EFP identifier.
Operational State	EFP operational state: Up or Down.
VLAN	VLAN associated with this EFP.
Inner VLAN	CE-VLAN identifier.
Translated VLAN	Translated, or mapped, VLAN identifier.
Translated Inner VLAN	Translated, or mapped, inner VLAN identifier.
Binding	Hyperlinked entry to the specific bridge in logical inventory.
Description	Description for the EFP.
LACP Port Entries	
Aggregated Port	Port on which the aggregation is configured, hyperlinked to the entry in physical inventory.
Dot3ad Agg Port Partner Admin Port Priority	Administrative port priority for the partner.
Dot3ad Agg Port Partner Admin Key	Administrative key for the partner port.
Dot3ad Agg Port Partner Oper Port Priority	Priority assigned to the aggregation port by the partner.
Dot3ad Agg Port Actor Oper State	Local operational state for the port.
Dot3ad Agg Port Actor Admin State	Local administrative state as transmitted by the local system in LACP data units (LACPDUs).
Dot3ad Agg Port Selected Agg ID	Selected identifier for the aggregation port.
Dot3ad Agg Port Partner Oper Key	Operational key for the partner port.
Dot3ad Agg Port Partner Admin State	Partner administrative state.
Dot3ad Agg Port Actor Port Priority	Priority assigned to the local aggregation port.
Dot3ad Agg Port Partner Oper State	Partner administrative state as transmitted by the partner in the most recently transmitted LAPCDU.
Dot3ad Agg Port Attached Agg ID	Identifier of the aggregator that the port is attached to.

Table 18-13 LAG IEEE 802.3 AD Properties (continued)

Field	Description
Dot3ad Agg Port Actor Admin Key	Administrative key for the local port.
Dot3ad Agg Port Actor Port	Number assigned to the local aggregation port.
Dot3ad Agg Port Partner Oper Port	Number assigned to the aggregation port by the partner.
Dot3ad Agg Port Actor Oper Key	Operational for the local port.
Dot3ad Agg Port Partner Admin Port	Administrative value of the port for the partner.

Viewing mLACP Properties

The Vision client supports the discovery of Multichassis LACP (mLACP) configurations on devices configured for them, and displays mLACP configuration information, such as redundancy groups and properties, in inventory.

To view mLACP properties:

Step 1 In the Vision client, double-click the element configured for mLACP.

Step 2 In the **Inventory** window, choose **Logical Inventory > ICCP Redundancy**.

In response, the Vision client lists the Inter-Chassis Communication Protocol (ICCP) redundancy groups configured on the device as shown in Figure 18-10.

Figure 18-10 ICCP Redundancy in Logical Inventory

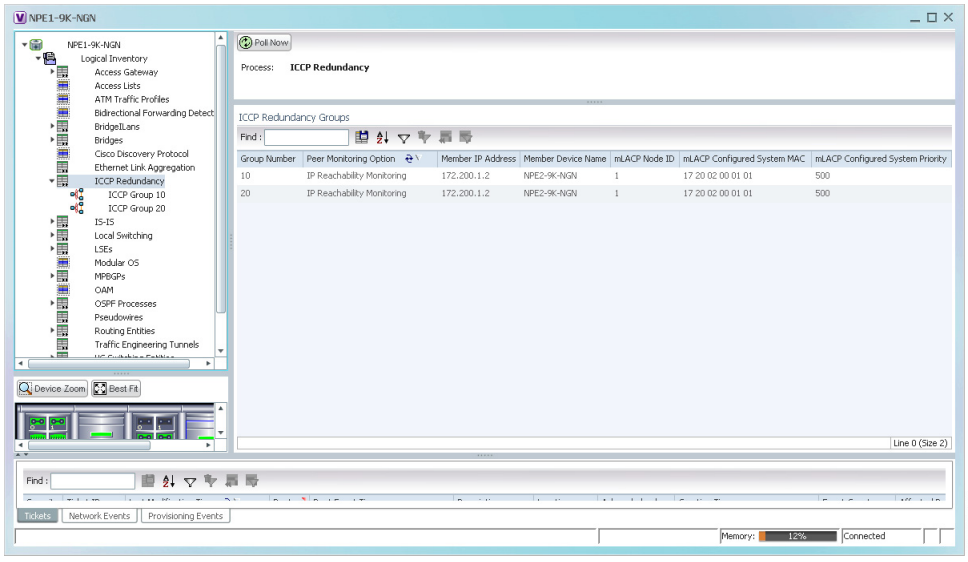


Table 18-14 describes the information displayed in the ICCP Redundancy Groups table.

Table 18-14 ICCP Redundancy Groups in Logical Inventory

Field	Description
Group Number	ICCP group identifier.
Peer Monitoring Option	Method used to monitor the peer: BFD or IP Reachability Monitoring.
Member IP Address	IP address of the neighbor PoA device.
Member Device Name	Name of the neighbor PoA device.
mLACP Node ID	Identifier used by this member of the mLACP redundancy group.
mLACP Configured System MAC	System MAC address of the redundancy group advertised to other members of the mLACP redundancy group and used for arbitration.
mLACP Configured System Priority	System priority advertised to other mLACP members of the redundancy group.

Step 3 To view additional information about an ICCP redundancy group, do either of the following:

- In the logical inventory window navigation pane, choose **Logical Inventory ICCP Redundancy >** *ICCP-group*.
- In the logical inventory content pane, right-click the required group in the ICCP Redundancy Groups table and choose **Properties**.

The ICCP Redundancy Group Properties window is displayed with the Backbone Interfaces and Data Link Aggregations tabs as shown in Figure 18-11.

Figure 18-11 ICCP Redundancy Group Properties Window

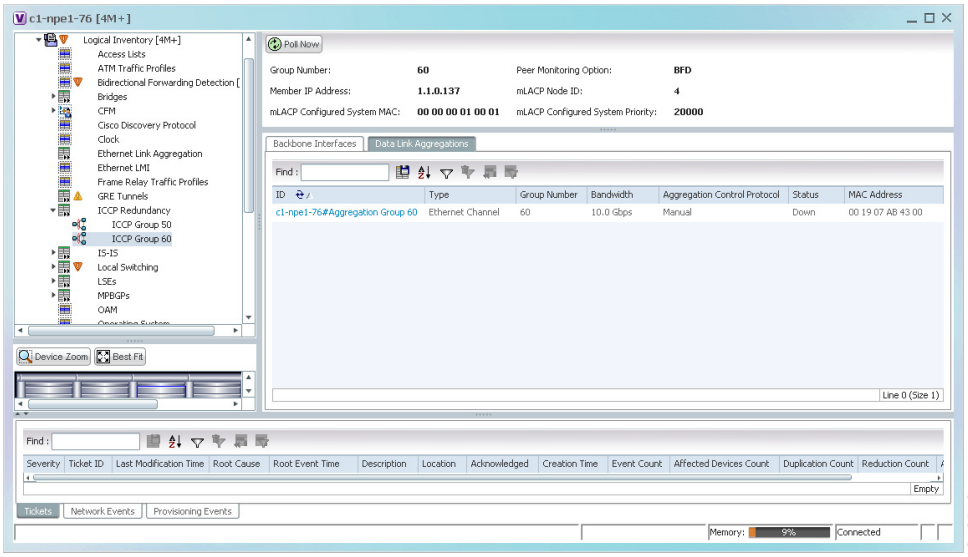


Table 18-15 describes the information available in the ICCP Redundancy Group Properties window.

Table 18-15 ICCP Redundancy Group Properties Window

Field	Description
Group Number	ICCP group identifier.
Peer Monitoring Option	Method used to monitor the peer: BFD or IP Reachability Monitoring.
Member IP Address	IP address of the neighbor PoA device.
Member device name	Name of the neighbor PoA device.
mLACP Node ID	Identifier used by this member of the mLACP redundancy group.
mLACP Configured System MAC	System MAC address of the redundancy group advertised to other members of the mLACP redundancy group and used for arbitration.
mLACP Configured System Priority	System priority advertised to other mLACP members of the redundancy group.
Backbone Interfaces Tab	
ID	Backbone interface defined for the redundancy group, hyperlinked to the relevant entry in logical inventory.
Status	Status of the backbone interface: Up, Down, or Unknown.
Data Link Aggregations Tab	
ID	Link aggregation group associated with the redundancy group, hyperlinked to the relevant entry in logical inventory.
Type	Aggregation group type: Ethernet Channel or IEEE 802.3 AD LAG.
Group Number	Aggregation group number.
Bandwidth	Aggregation bandwidth.
Aggregation Control Protocol	Aggregation control protocol: Manual, LACP, or PAgP.
Status	Aggregation status: Up or Down.
MAC Address	Aggregation MAC address.

Step 4 To view additional mLACP properties, double-click the entry for the required link aggregation group in the Data Link Aggregations tab.

mLACP information is displayed in the Link Aggregation Group Properties window, as described in the following tables:

- Table 18-12—LAG Ethernet Channel Properties
- Table 18-13—LAG IEEE 802.3 AD Properties

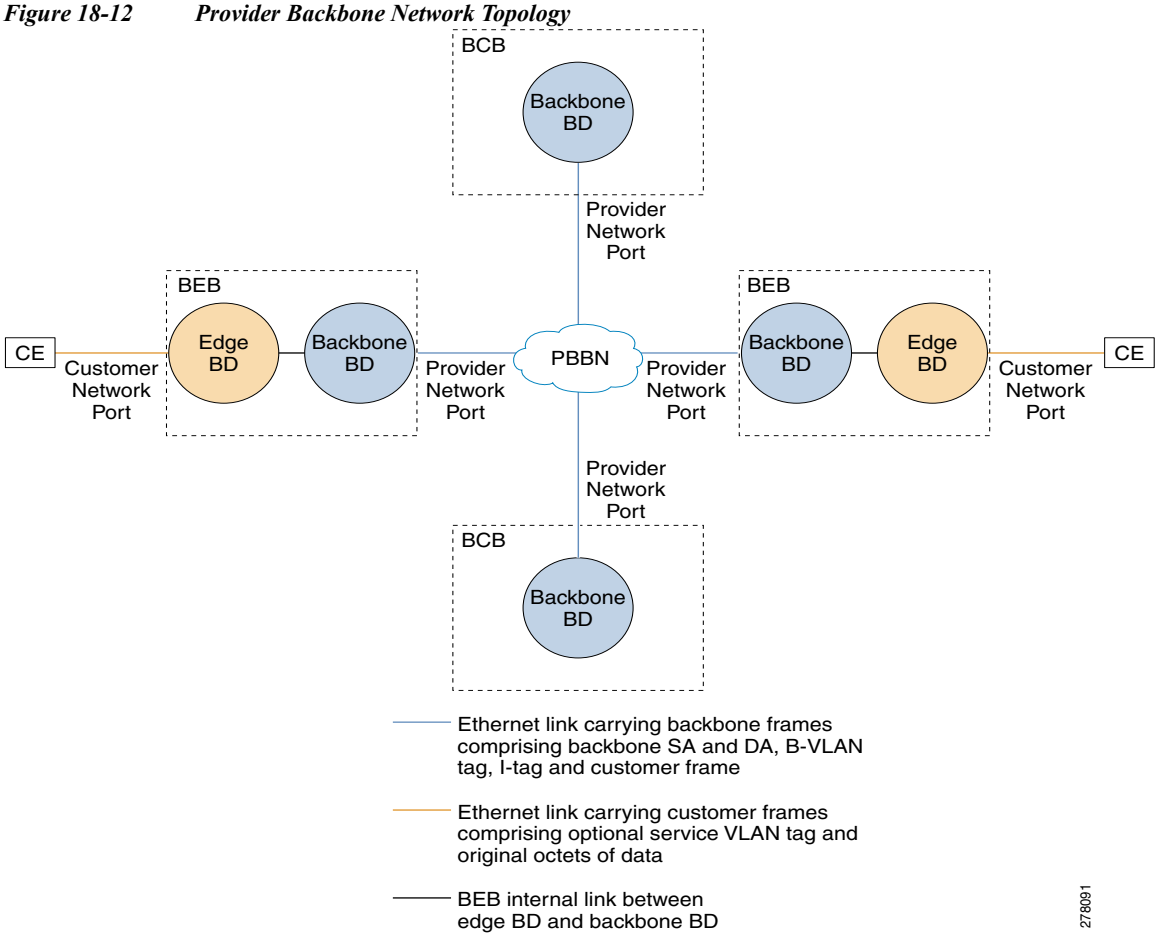
Monitoring Provider Backbone Bridges

The Provider Backbone Bridge (PBB) specified by IEEE 802.1ah-2008, provide a way to increase the number of service provider supported Layer 2 service instances beyond the number supported by QinQ and VPLS. PBB adds a backbone VLAN tag and backbone destination and source MAC addresses to encapsulate customer Ethernet frames and create a MAC tunnel across core switches.

The PBB network comprises of a set of architecture and protocols for routing over a provider's network. The PBB network interconnects multiple provider bridge networks without losing each customer's individual VLANs. The PBB network encapsulates and decapsulates end-user traffic on a Backbone Edge Bridge (BEB) at the edge of the Provider Backbone Bridged Network (PBBN). A Backbone Core Bridge (BCB)-based network provides internal transport of the IEEE 802.1ah encapsulated frames within the PBBN.

Figure 18-12 shows a typical provider backbone network topology.

Figure 18-12 Provider Backbone Network Topology



BFD Templates Support

BFD (Bidirectional Forwarding Detection Templates) are the new features added in CPT devices. Prime Network uses Telnet Command to get the BFD templates in existing CPT devices.

Telnet /CLI Command for listing the BFD template

Show running-config|section bfd-template

Cerent Trap Support

Cerent trap alarms are supported for CPT devices. There are 170 traps supported.

Change Settings in CTC (Cisco Transport Controller)

Any configurations settings made in CPT should be done through CTC. To receive traps in a particular server, that server IP needs to be entered in the device through CTC. Most of the traps are on device dependencies.

Link and Port Parameters

Configuration of Ethernet loopback is used to add and remove loopback. Link and Port parameters have been used for Prime Network configuration scripts in both TLI and Telnet. The link and port parameters are supported for the following: Ethernet Parameter Configuration

- MTU
- Link State
- Expected Speed
- Expected Duplex
- Operating Flow Control
- Carrier Delays
- Auto Negotiation

Port Parameter Configuration

- Port Name
- Admin State
- AINS Soak
- Reach
- Wavelength

L2 Parameter Configuration

- CDP
- DOTIX
- DTP
- LACP
- PAGP
- VTP
- STP

The following are the configuration scripts supported,

- Add Loopback
- Remove Loopback
- Configure CDP
- Configure Ethernet
- Configure L2 Control Protocol
- Configure Port Parameters
- Show Ethernet Parameters
- Show L2 Control Parameters
- Show Port Parameters

This chapter describes the following topics:

Working with PBB-EVPN

Ethernet Virtual Private Network (EVPN) is a solution for secure and private connectivity of multiple sites within an organization. The EVPN service extends the benefits of Ethernet technology to the WAN. This service is delivered over Multiprotocol Label Switching (MPLS) networks.

EVPN allows you to manage routing over a virtual private network, providing complete control and security. EVPN introduces a solution for multipoint L2VPN services with advanced multi-homing capabilities, using BGP for distributing customer or client MAC address reachability information over the MPLS/IP network. EVPN advertises each customer MAC address as BGP routes, therefore allowing BGP policy control over MAC addresses.

The PBB-EVPN solution combines Ethernet Provider Backbone Bridging (PBB - IEEE 802.1ah) with Ethernet VPN, where provider edges (PEs) perform as PBB Backbone Edge Bridge (BEB). The PEs receive 802.1Q Ethernet frames from their attachment circuits. These frames are encapsulated in the PBB header and forwarded over the Internet Protocol / Multi-protocol label switching (IP/MPLS) core. On the egress side (EVPN PE), the PBB header is removed after MPLS disposition, and the original 802.1Q Ethernet frame is delivered to the customer equipment.

The PE routers perform these functions:

- Learns customer or client MAC addresses (C-MACs) over the attachment circuits in the data-plane, per normal bridge operation.
- Learns remote C-MAC to backbone MAC (B-MAC) bindings in the data-plane from traffic ingress from the core.
- Advertises local B-MAC address reachability information in BGP to all other PE nodes in the same set of service instances. Note that every PE has a set of local B-MAC addresses that uniquely identify the device.

- Builds a forwarding table from the received remote BGP advertisements, associating remote B-MAC addresses with remote PE IP addresses.

PBB-EVPN scales well for large network with millions of customer MAC addresses by constraining customer MAC address in access. Only B-MAC addresses are advertised in core, making the number of BGP routes exchanged manageable.

This section describes the following topics:

- EVPN Instance, page 18-30
- Ethernet Segment, page 18-30

EVPN Instance

E-VPN Instance (EVI) identifies a VPN in the MPLS/IP network. There can only be one EVI per core bridge.

Ethernet Segment

Ethernet Segment is a site connected to one or more PEs. The Ethernet Segment can be a single device like a Customer Edge (CE) or an entire network, such as:

- Single-Homed Device (SHD)
- Multi-Homed Device (MHD) using Ethernet Multi-chassis Link Aggregation Group
- Single-Homed Network (SHN)
- Multi-Homed Network (MHN)

The Ethernet segment is uniquely identified by a 10-byte global Ethernet Segment Identifier (ESI).

You can view the following properties in the PBB-EVPN network:

- Viewing PBB-EVPN Core Bridge Properties, page 18-30
- Viewing EVPN Container Properties, page 18-34
- Viewing EVPN Properties, page 18-35
- Viewing Ethernet Segment Container Properties, page 18-36
- Viewing Ethernet Segment Properties, page 18-38

Viewing PBB-EVPN Core Bridge Properties

To view the PBB-EVPN core bridge properties:

Step 1 Double-click the required device in the Vision client.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **Bridges** to view the list of bridges.

Step 3 Select a PBB-EVPN bridge to view the properties.

Table 18-16 describes the information displayed for PBB-EVPN bridge properties.

Table 18-16 PBB-EVPN Core Bridge Properties

Field	Description
Name	PBB bridge name.
Type	Specifies the type of bridge. There can be two types of bridges: • I-Bridge—Interfaces with the customer edge. • B-bridge—Interfaces with the core network. The PBB-EVPN core bridge is a B-bridge
VLAN ID	VLAN identifier configured for the subscriber.
VSI	VSI information, hyperlinked to the VSI entry in logical inventory.
Evi	Specifies an unique route distinguisher per customer. There can only be one Evi per core bridge.
MMRP Enabled	Denotes Multiple MAC Registration Protocol (MMRP). It allows multicast traffic in bridged LANs. **Note** The MMRP is disabled by default in the EVPN network.
Pseudowires Tab	
ID	Pseudowire identifier, hyperlinked to the VLAN entry in Bridges in logical inventory.
Peer	Identifier of the pseudowire peer, hyperlinked to the entry in the Pseudowire Tunnel Edges table in logical inventory.
SAII	Specifies the Source Access Individual Identifier (SAII) of the tunnel. **Note** The SAII attribute can be configured only if the Pseudowire type is FEC129 TYPE II.
Tunnel Status	Operational state of the tunnel: Up or Down.
TAII	Specifies the Target Attachment Individual Identifier (TAII) of the tunnel. **Note** The TAII can be configured only if the Pseudowire type is FEC129 TYPE II.
Peer Router IP	IP Address of the peer router for this pseudowire.
Pseudowire Type	Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, SAToP or FEC129 TYPE II.
Pseudowire Role	If the pseudowire is in a redundancy configuration, then the pseudowire role indicates whether its a primary pseudowire or a secondary pseudowire in the configuration. If the pseudowire is not configured for redundancy, the field is blank.
Preferred Path Tunnel	Specifies the path that has to be used for MPLS pseudowire traffic.

Table 18-16 PBB-EVPN Core Bridge Properties (continued)

Field	Description
Local Router IP	Specifies the IP address of the tunnel edge, which is used as the router identifier.
Local MTU	Specifies the byte size of the MTU on the local interface.
Remote MTU	Specifies the byte size of the MTU on the remote interface.
Local VC Label	Specifies the MPLS label that is used by the local router to identify or access the tunnel. It is inserted in the MPLS label stack by the local router.
Peer VC Label	Specifies the MPLS label that is used by the peer router to identify or access the tunnel. It is inserted in the MPLS label stack by the peer router.
Signaling Protocol	Specifies the protocol that is used to build the tunnel, such as the LDP or TDP.
Peer Status	Specifies the status of the peer link.
Associated EVC Name	Specifies the name of the associated Ethernet Virtual Circuits (EVC).
I-Bridge Associations Tab	
I-SID	Specifies a 24-bit identifier that represents the backbone service instance.
I-Bridge	Specifies the exchange identification (XID) in the I-Bridge component. The XID is hyperlinked to the relevant bridge in the logical inventory.

Viewing PBB-EVPN Customer Bridge Properties

To view the PBB-EVPN customer bridge properties:

Step 1 Double-click the required device in the Vision client.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **Bridges** to view the list of bridges.

Step 3 Select a PBB-EVPN customer bridge to view the properties.

Table 18-17 describes the information displayed for PBB-EVPN customer bridge properties.

Table 18-17 PBB-EVPN Customer Bridge Properties

Field	Description
Name	PBB bridge name.
Type	Specifies the type of bridge. The PBB-EVPN customer bridge is an I-bridge
VLAN ID	VLAN identifier configured for the subscriber.

Table 18-17 PBB-EVPN Customer Bridge Properties (continued)

Field	Description
I-SID	Specifies a 24-bit identifier that represents the backbone service instance.
B-Bridge	Specifies the XID of the B-Bridge component. The XID is hyperlinked to the relevant bridge in logical inventory.
Pseudowires Tab	
ID	Pseudowire identifier, hyperlinked to the VLAN entry in Bridges in logical inventory.
Peer	Identifier of the pseudowire peer, hyperlinked to the entry in the Pseudowire Tunnel Edges table in logical inventory.
SAII	Specifies the Source Access Individual Identifier (SAII) of the tunnel. **Note** The SAII attribute can be configured only if the Pseudowire type is FEC129 TYPE II.
Tunnel Status	Operational state of the tunnel: Up or Down.
TAII	Specifies the Target Attachment Individual Identifier (TAII) of the tunnel. **Note** The TAII can be configured only if the Pseudowire type is FEC129 TYPE II.
Peer Router IP	IP address of the peer router for this pseudowire.
Pseudowire Type	Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, SAToP or FEC129 TYPE II.
Pseudowire Role	If the pseudowire is in a redundancy configuration, then the pseudowire role indicates whether its a primary pseudowire or a secondary pseudowire in the configuration. If the pseudowire is not configured for redundancy, the field is blank.
Preferred Path Tunnel	Specifies the path that has to be used for MPLS pseudowire traffic.
Local Router IP	Specifies the IP address of the tunnel edge, which is used as the router identifier.
Local MTU	Specifies the byte size of the MTU on the local interface.
Remote MTU	Specifies the byte size of the MTU on the remote interface.
Local VC Label	Specifies the MPLS label that is used by the local router to identify or access the tunnel. It is inserted in the MPLS label stack by the local router.
Peer VC Label	Specifies the MPLS label that is used by the peer router to identify or access the tunnel. It is inserted in the MPLS label stack by the peer router.
Signaling Protocol	Specifies the protocol that is used to build the tunnel, such as the LDP or TDP.
Peer Status	Specifies the status of the peer link.

Table 18-17 PBB-EVPN Customer Bridge Properties (continued)

Field	Description
Associated EVC Name	Specifies the name of the associated EVC.
EFPs Tab	
EFP ID	EFP identifier.
Operational State	EFP operational state.
VLAN	VLAN identifier.
Inner VLAN	CE-VLAN identifier.
Translated VLAN	Translated VLAN identifier.
Translated Inner VLAN	Translated CE-VLAN identifier.
Binding Port	Hyperlinked entry to the port in physical inventory.
Description	Brief description of the EFP.
Ingress Policy	The name of the ingress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates.
Egress Policy	The name of the egress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates.
Service Control Policy	Specifies the policy for a port or operation.
MMRP Participants	
Associated MMRP Participant	Specifies an entry that is hyperlinked to an associated MMRP service for that bridge.

Viewing EVPN Container Properties

To view the EVPN container properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **EVPN** to view the EVPN container properties.

Table 18-18 describes the information displayed for the EVPN container properties.

Table 18-18 EVPN Container Properties

Field	Description
EVI	The EVI identifies a VPN (Virtual Private Network) in the MPLS/IP network. There can only be one EVI per core bridge.
Bridge Domain	Maintains a forwarding database of MAC addresses from packets received from its interfaces. The bridge domain is hyperlinked to the relevant core bridge in the logical inventory.

Table 18-18 EVPN Container Properties (continued)

Field	Description
EVPN Type	Specifies the type of bridges.There can be two types of bridges: • PBB-EVPN • BD
Route Distinguisher	Creates a unique 96-bit VPNv4 address to distinguish routes within a single internet service provider's (ISP) MPLS network.
Multicast Label	Specifies a 20-bit multicast label in the MPLS packet to make forwarding decisions and to pre-establish a path for switch-labeled packets at the Layer 2.
Unicast Label	Specifies a 20-bit unicast label in MPLS packet to make forwarding decisions and to pre-establish a path for switch-labeled packets at the Layer 2.
Route Distinguisher (Auto)	The Route Distinguisher (Auto) is generated by default as a combination of Loopback IP Address and EVI.
Route Target (Auto)	Communicates the VPN route to the PE routers.

Viewing EVPN Properties

To view the EVPN properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **EVPN** to display the EVPN container properties.

Step 3 Double-click an EVI to view its EVPN properties.

Table 18-19 describes the information displayed for EVPN properties.

Table 18-19 EVPN Properties

Field	Description
EVI	The EVI identifies a VPN in the MPLS/IP network. There can only be one EVI per core bridge.
Bridge Domain	Maintains a forwarding database of MAC addresses from packets received from its interfaces. The bridge domain is hyperlinked to the relevant core bridge in the logical inventory.
EVPN Type	Specifies the type of bridges. There can be two types of bridges: • PBB-EVPN • BD
Route Distinguisher	Creates a unique 96-bit VPNv4 address to distinguish routes within a single ISP-MPLS network.

Table 18-19 EVPN Properties

Field	Description
Multicast Label	Specifies a 20-bit multicast label in MPLS packet to make forwarding decisions and to pre-establish a path for switch-labeled packets at the Layer 2.
Unicast Label	Specifies a 20-bit unicast label in MPLS packet to make forwarding decisions and to pre-establish a path for switch-labeled packets at the Layer 2.
Route Distinguisher (Auto)	The Route Distinguisher (Auto) is generated by default as a combination of Loopback IP Address and EVI.
Route Target (Auto)	Communicates the VPN route to the PE routers.
EVPN BMAC Address Entries Tab	
MAC Address	It is an unique identifier of the bridge clients in a PE router for an EVPN instance.
Next HOP	Specifies the peer router associated to each EVPN instance.
MPLS Label	Enables the MPLS network data packets to make packet forwarding decisions. This allows the data packets to create end-to-end circuits across any type of transport medium, using any protocol.
Import Route Targets Tab	
Route Target	The PE imports routes with specific prefixes or subnet masks based on the Route Target.
Export Route Targets Tab	
Route Target	The Route Target attribute defines the prefixes that are exported on the PE routers.

Viewing Ethernet Segment Container Properties

The Ethernet segment is a site that is connected to one or more Provider Edge Switches (PEs). The Ethernet segment can be a single device such as a customer edge or an entire network. The Ethernet segment in a network can be of the following types:

- Single-homed device (SHD)
- Multi-homed device (MHD)
- Single-homed network (SHN)
- Multi-homed network (MHN)

The Ethernet segment is unique and identified by a 10-byte global Ethernet Segment Identifier (ESI).

To view the Ethernet segment container properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **Ethernet Segments** to view the Ethernet segment container properties.

Table 18-20 describes the information displayed for PBBe VPN Ethernet segment container properties.

Table 18-20 Ethernet Segment Container Properties

Field	Description
Interface Name	Name of the interface that is connected to the Ethernet segment.
Associated Interface	Associated Name of the interface that is connected to the Ethernet segment.
ES ID	The Ethernet Segment Identifier (ES ID) is a 10-byte field. It identifies the unique Ethernet segment in the core network of the PE routers.
Source MAC Address	Specifies the Ethernet Segment MAC Address.
Access Topology Mode	Specifies one of the following network types: • Single Home Device (SH) • Single Home Network (SHN) • Dual Home Device (DHD) • Dual Home Network (DHN) • Multi Home Network (MHN) The default value is MHN.
Access Topology Flow Mode	Specifies the flow of traffic in a network. The flow mode can be one of the following options: • Active/Active per-flow • Active/Active per-service
I-SID Primary Services	Specifies the type of primary customer service interfaces provided by the I-Bridge Backbone Edge Bridge (IB-BEB). The primary customer service interfaces can be one of the following types: • Port based • S-tagged • I-tagged
I-SID Secondary Services	Specifies the type of secondary customer service interfaces provided by the IB-BEB bridge. The secondary customer service interfaces can be one of the following types: • Port based • S-tagged • I-tagged
Total I-SID Count	Specifies the total number of elected and non-elected ports.
Elected I-SIDs	Specifies the Elected Service Identifiers (I-SID) list.
Non-Elected I-SIDs	Specifies the Non-Elected Service Identifiers (I-SID) list.

Table 18-20 Ethernet Segment Container Properties (continued)

Field	Description
MAC Flushing Mode	Specifies the MAC flush over Multiple VLAN Registration Protocol (MVRP). The possible values in the MAC Flushing Mode field can be one of the following: • Spanning Tree Protocol - Topology Change Notification (STP-TCN) • MVRP The default value is STP-TCN.
Peering Timer	Specifies the interface-specific peering timer in seconds. The default value is 45 seconds.
Recovery Timer	Specifies the interface-specific recovery timer in seconds. The range is 20 to 3600 seconds. The default value is 20 seconds.
Flush Again Timer	Specifies the interface-specific MAC flush again timer in seconds. The range is 0 to 120 seconds. The default value is 60 seconds.

Viewing Ethernet Segment Properties

To view the Ethernet segment properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **Ethernet Segments** to view the Ethernet segment container properties.

Step 3 Double-click an interface to view its PBBe VPN Ethernet segment properties.

Table 18-21 describes the information displayed for PBBe VPN Ethernet segment properties.

Table 18-21 Ethernet Segment Properties

Field	Description
Interface Name	Name of the interface that is connected to the Ethernet segment.
Associated Interface	Associated Name of the interface that is connected to the Ethernet segment.
ES ID	The Ethernet Segment Identifier (ES ID) is a 10-byte field. It identifies the unique Ethernet segment in the core network of the PE routers.
Source MAC Address	Specifies the Ethernet Segment MAC Address.
Access Topology Mode	Specifies one of the following network types: • Single Home Device (SH) • Single Home Network (SHN) • Dual Home Device (DHD) • Dual Home Network (DHN) • Multi Home Network (MHN) The default value is MHN.

Table 18-21 Ethernet Segment Properties (continued)

Field	Description
Access Topology Flow Mode	Specifies the flow of traffic in a network. The flow mode can be one of the following options: • Active/Active per-flow • Active/Active per-service
I-SID Primary Services	Specifies the type of primary customer service interfaces provided by the IB-BEB bridge. The primary customer service interfaces can be one of the following types: • Port based • S-tagged • I-tagged
I-SID Secondary Services	Specifies the type of secondary customer service interfaces provided by the IB-BEB bridge. The secondary customer service interfaces can be one of the following types: • Port based • S-tagged • I-tagged
Total I-SID Count	Specifies the total number of elected and non-elected ports.
Elected I-SIDs	Specifies the Elected Service Identifiers (I-SID) list.
Non-Elected I-SIDs	Specifies the Non-Elected Service Identifiers (I-SID) list.
MAC Flushing Mode	Specifies the MAC flush over MVRP. The possible values in the MAC Flushing Mode field can be one of the following: • STP-TCN • MVRP The default value is STP-TCN.
Peering Timer	Specifies the interface-specific peering timer in seconds. The default value is 45 seconds.
Recovery Timer	Specifies the interface-specific recovery timer in seconds. The range is 20 to 3600 seconds. The default value is 20 seconds.
Flush Again Timer	Specifies the interface-specific MAC flush again timer in seconds. The range is 0 to120 seconds. The default value is 60 seconds.
Redundancy Group Entries	
IP Address	Identifies the redundancy group IP address that is associated to an Ethernet segment.
Is Self	Specifies whether the redundancy group IP Address belongs to a local border gateway protocol (BGP).

Working with PBB-VPLS

The Virtual Private LAN service (VPLS) is a class of VPN that supports the connection of multiple sites in a single bridged domain over a managed MPLS network. The VPLS is a multipoint service and it can also transport non-IP traffic. All customer premises at a VPLS instance appear to be on the same local area network regardless of their actual locations. The VPLS uses an Ethernet interface to the customer.

A VPLS network consists of the following three main components.

- Customer Edges
- Provider Edges
- IP/MPLS core network

This section consists of the following topics:

Viewing PBB-VPLS Core Bridge Properties

To view the PBB-VPLS bridge properties:

Step 1 Double-click the required device in the Vision client.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **Bridges** to view the list of bridges.

Step 3 Select a PBB-VPLS bridge to view the properties.

Table 18-22 describes the information displayed for PBB-VPLS bridge properties.

Table 18-22 PBB-VPLS Bridge Properties

Field	Description
Name	PBB bridge name.
Type	Specifies the type of bridge. There can be two types of bridges: I-Bridge—Interfaces with the customer edge. B-bridge—Interfaces with the core network.
VLAN ID	Specifies the VLAN identifier of the subscriber.
VSI	VSI information, hyperlinked to the VSI entry in logical inventory.
Evi	Specifies a unique route distinguisher per customer. There can only be one EVI per core bridge.
MMRP Enabled	Denotes Multiple MAC Registration Protocol (MMRP). It allows multicast traffic in bridged LANs. **Note** The MMRP is enabled in the VPLS network.
Pseudowires Tab	

Table 18-22 PBB-VPLS Bridge Properties (continued)

Field	Description
ID	Pseudowire identifier, hyperlinked to the VLAN entry in Bridges in logical inventory.
Peer	Identifier of the pseudowire peer, hyperlinked to the entry in the Pseudowire Tunnel Edges table in logical inventory.
SAII	Specifies the Source Access Individual Identifier (SAII) of the tunnel. **Note** The SAII attribute can be configured only if the Pseudowire type is FEC129 TYPE II.
Tunnel Status	Operational state of the tunnel: Up or Down.
TAII	Specifies the Target Attachment Individual Identifier (TAII) of the tunnel. **Note** The TAII can be configured only if the Pseudowire type is FEC129 TYPE II.
Peer Router IP	IP address of the peer router for this pseudowire.
Pseudowire Type	Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, SAToP or FEC129 TYPE II.
Pseudowire Role	If the pseudowire is in a redundancy configuration, then the pseudowire role indicates whether its a primary pseudowire or a secondary pseudowire in the configuration. If the pseudowire is not configured for redundancy, the field is blank.
Preferred Path Tunnel	Specifies the path that has to be used for MPLS pseudowire traffic.
Local Router IP	Specifies the IP address of the tunnel edge, which is used as the router identifier.
Local MTU	Specifies the byte size of the MTU on the local interface.
Remote MTU	Specifies the byte size of the MTU on the remote interface.
Local VC Label	Specifies the MPLS label that is used by the local router to identify or access the tunnel. It is inserted in the MPLS label stack by the local router.
Peer VC Label	Specifies the MPLS label that is used by the peer router to identify or access the tunnel. It is inserted in the MPLS label stack by the peer router.
Signaling Protocol	Specifies the protocol that is used to build the tunnel, such as the LDP or TDP.
Peer Status	Specifies the status of the peer link.
Associated EVC Name	Specifies the name of the associated EVC.
VPLS I-Bridge Associations Tab	

Table 18-22 PBB-VPLS Bridge Properties (continued)

Field	Description
I-SID	Specifies a 24-bit identifier that represents the backbone service instance.
I-Bridge	Specifies the exchange identification (XID) in the I-Bridge component. The XID is hyperlinked to the relevant bridge in the logical inventory.

Viewing PBB-VPLS Customer Bridge Properties

The PBB-VPLS customer bridges communicates directly with the customer edge. Multiple customer bridges can communicate with the core bridge.

To view the PBB-VPLS customer bridge properties:

Step 1 Double-click the required device in the Vision client.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **Bridges**.

Step 3 Select a PBB-VPLS customer bridge to view the properties.

Table 18-22 describes the information displayed for PBB-VPLS bridge properties.

Table 18-23 PBB-VPLS Customer Bridge Properties

Field	Description
Name	PBB customer bridge name.
Type	Specifies the type of bridge. There can be two types of bridges: I-Bridge—Interfaces with the customer edge. B-bridge—Interfaces with the core network.
VLAN ID	Specifies the VLAN identifier of the subscriber.
I-SID	Specifies a 24-bit identifier that represents the backbone service instance.
B-Bridge	Specifies the XID of the B-Bridge component. The XID is hyperlinked to the relevant bridge in logical inventory.
Pseudowires Tab	
ID	Pseudowire identifier, hyperlinked to the VLAN entry in Bridges in logical inventory.
Peer	Identifier of the pseudowire peer, hyperlinked to the entry in the Pseudowire Tunnel Edges table in logical inventory.

Table 18-23 PBB-VPLS Customer Bridge Properties

Field	Description
SAII	Specifies the Source Access Individual Identifier (SAII) of the tunnel. **Note** The SAII attribute can be configured only if the Pseudowire type is FEC129 TYPE II.
Tunnel Status	Operational state of the tunnel: Up or Down.
TAII	Specifies the Target Attachment Individual Identifier (TAII) of the tunnel. **Note** The TAII can be configured only if the Pseudowire type is FEC129 TYPE II.
Peer Router IP	IP address of the peer router for this pseudowire.
Pseudowire Type	Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, SAToP or FEC129 TYPE II.
Pseudowire Role	If the pseudowire is in a redundancy configuration, then the pseudowire role indicates whether its a primary pseudowire or a secondary pseudowire in the configuration. If the pseudowire is not configured for redundancy, the field is blank.
Preferred Path Tunnel	Specifies the path that has to be used for MPLS pseudowire traffic.
Local Router IP	Specifies the IP address of the tunnel edge, which is used as the router identifier.
Local MTU	Specifies the byte size of the MTU on the local interface.
Remote MTU	Specifies the byte size of the MTU on the remote interface.
Local VC Label	Specifies the MPLS label that is used by the local router to identify or access the tunnel. It is inserted in the MPLS label stack by the local router.
Peer VC Label	Specifies the MPLS label that is used by the peer router to identify or access the tunnel. It is inserted in the MPLS label stack by the peer router.
Signaling Protocol	Specifies the protocol that is used to build the tunnel, such as the LDP or TDP.
Peer Status	Specifies the status of the peer link.
Associated EVC Name	Specifies the name of the associated EVC.
EFPs Tab	
EFP ID	EFP identifier.
Operational State	EFP operational state.
VLAN	VLAN identifier.
Inner VLAN	CE-VLAN identifier.
Translated VLAN	Translated VLAN identifier.
Translated Inner VLAN	Translated CE-VLAN identifier.

Table 18-23 PBB-VPLS Customer Bridge Properties

Field	Description
Binding Port	Hyperlinked entry to the port in physical inventory.
Description	Brief description of the EFP.
Ingress Policy	The name of the ingress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates.
Egress Policy	The name of the egress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates.
Service Control Policy	Specifies the policy for a port or operation.
MMRP Participants Tab	
Associated MMRP Participant	Specifies an entry that is hyperlinked to an associated MMRP service for that bridge.

Working with PBB-MMRP

Multiple MAC registration protocol (MMRP) is a data link layer 2 protocol that registers group MAC addresses on multiple switches. The MMRP allows multicast traffic in bridged LANs and provides a mechanism to achieve the following:

- Register or unregister group membership information across the bridges attached to the same LAN.
- Register or unregister individual MAC address information across the bridges attached to the same LAN.
- Communicate the registration information across all the bridges that support extended filtering services in the bridged network.

MMRP operates on the services provided by the Multiple Registration Protocol (MRP). It allows bridges, switches or other similar devices to register or unregister attribute values such as VLAN identifiers and multicast the group membership information across a large LAN.

You can view the following properties in the PBB-MMRP network:

- Viewing MMRP Container Properties, page 18-44
- Viewing MMRP Registration Properties, page 18-46

Viewing MMRP Container Properties

To view MMRP container properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **MMRP** to view the container properties.

Table 18-24 describes the information displayed for the MMRP container properties.

Table 18-24 MMRP Container Properties

Field	Description
Flood Time	Specifies the flood time to enable the flooding of traffic for the whole core bridge when the MMRP feature is first enabled on the core bridge. The range is 3 to 600 seconds.
Leave All Time	Specifies the minimum time in seconds for the Leave All timer parameter to check how often Leave All messages are sent for all the active ports. The range is 5 to 30 seconds. The default value is 10 seconds.
Leave Time	Specifies the leave time for all the active ports. The range is 1 to 90 seconds. The default value is 30 seconds.
Join Time	Specifies the maximum time for controlling the interval between transmit opportunities that are applied to the applicant state machine for all active ports.
Periodic Transmit	Specifies the periodic transmit interval of Multiple MAC Registration Protocol Data Units (MMRPDU) on all active ports. The range is 2 to10 seconds.
MMRP Participants Tab	
Peer IP Address	Specifies the neighbor Peer IP address.
PW ID	Specifies the associated Pseudowire ID.
Bridge Domain	Specifies the associated B-Bridge domain.
Participant Type	Specifies the node participating in MMRP. In PBB-MMRP, each IB-PE router in B-domain is a participant. The possible value is FULL.
Flood Optimization	Specifies if the flood optimization is enabled between two point-to-point peers. The possible value is Yes.
Participant State	Specifies the state of the Participant. The possible value is Normal.
Registrar State	Specifies the state of the Registrar. The Registrar listens to the MRPDUs and registers the applicants. The possible value is Normal.
Leave State	Specifies the state of one or more remote IB-PE routers that must leave the group B-MAC address flooding tree.
Join State	Specifies the state of one or more remote IB-PE routers that must join the group B-MAC address flooding tree.
Last Peer	Specifies the last peer.
Failed Registrations	Specifies the number of failed registrations when the PE bridges join the network.

Viewing MMRP Registration Properties

To view the MMRP registration properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **MMRP** to view the container properties.

Step 3 Double-click any row to view its registration properties.

Table 18-25 describes the information displayed for MMRP registration properties.

Table 18-25 MMRP Registration Properties

Field	Description
Peer IP Address	Specifies the neighbor peer IP address.
PW ID	Specifies the associated pseudowire ID.
Bridge Domain	Specifies the associated B-Bridge domain
Participant Type	Specifies the participating node in MMRP. In PBB-MMRP, each IB-PE router in B-domain is a participant. The possible value is FULL.
Point To Point	Specifies if flood optimization is enabled between two point-to-point peers. The possible value is Yes.
Applicant State	Announces the group B-MAC address and triggers MRPDU propagation. The possible values can be one of the following: • Normal • Quiet Active
Registrar State	Specifies the state of the Registrar. The Registrar listens to the MRPDUs and registers the applicants. The possible value is Normal.
Leave	Specifies the state of one or more remote IB-PE routers that must leave the group B-MAC address flooding tree.
Join	Specifies the state of one or more remote IB-PE routers that must join the group B-MAC address flooding tree.
Last Peer	Specifies the last peer.
Failed Registrations	Specifies the number of failed registrations when the PE bridges join the network.
Registered Neighbours Tab	
I-SID	Specifies a 24-bit identifier that represents the backbone service instance.
B-MAC	Specifies the bridge MAC Address.
Participant State	Specifies the state of the Participant. The default value is Normal.
Registrar State	Specifies the state of the Registrar. The Registrar listens to the MRPDUs and registers the applicants. The possible value is In.

Monitoring PBB-based Support Service Discovery

The Cisco Prime Network delivers PBB-based discovery for various support services over VLAN, VPLS, EVC, and pseudowires.

The Cisco Prime Network supports the following service discoveries:

- VLAN Discovery—Discovers bridges domains such as I-Bridges, B-Bridges, and regular bridges that are unassociated.
- VPLS Discovery—Discovers VFIs and their associations between I-Bridges and B-Bridges.
- Pseudowire Discovery—Discovers pseudowires and their associations between I-Bridges and B-Bridges.
- EVC Discovery—Creates an end-to-end complex circuit representing the network associations in the core network of the above discovered elements.

The PBB specified by IEEE 802.1ah-2008, provides a way to increase the number of service provider supported Layer 2 service instances beyond the number supported by QinQ and VPLS. PBB adds a backbone VLAN tag, and backbone destination and source MAC addresses to encapsulate customer Ethernet frames and create a MAC tunnel across core switches. The PBB network interconnects multiple provider bridge networks without losing each customer's individual VLANs.

The Prime Network PBB-based support service discovery recognizes service entities in the network. Service discovery are either network data discovered by Prime Network VNEs or other underlying services discovered by other service discoveries. The network data is stored and cached (in memory) in Snapshots on the Prime Network gateway machine. After which, the data is transformed into service data, and then stored in the Prime Network database.

The Prime Network PBB-based support services can be discovered either by using a full discovery mode or a notification-based discovery mode.

The Prime Network supports the following PBB-based support services:

- PBB-based VLAN Discovery, page 18-47
- PBB-based EVC Discovery, page 18-48
- Discovering PBB-links Between I-Bridge and B-Bridge, page 18-49
- PBB-based Pseudowire Discovery, page 18-49
- PBB-based VPLS Discovery, page 18-50

PBB-based VLAN Discovery

Prime Network discovers and allows you to display maps with a network-level view of VLANs.

A VLAN entity consists of one or more bridges and the corresponding EFP elements. When the VLAN discovery is initiated, it identifies VLANs that are considered as part of a switching entity.

Associated and Unassociated Bridges

Generally, all the bridges are categorized as associated or unassociated based on their association with the type of switching entities such as pseudowire and VPLS. In the Provider Backbone configuration, the VLANs identified by VLAN discovery are considered as a part of associated bridges and the VLANs that are not identified are considered as a part of unassociated bridges. For example, if a regular bridge

is associated with a pseudowire or a VPLS, then it is classified as an associated bridge. Otherwise, it is classified as an unassociated bridge. However, the I-Bridges and B-Bridges are always considered as a part of unassociated bridges irrespective of their association with the switching entities.

Discovering Unassociated Domains

To discover the VLAN service configured in a network, a component called VLAN data plug-in collects information related to VLAN from various devices. The data plug-in holds all the data related to the bridges in a centralized location. To discover an unassociated bridge, for example, an I-bridge or a B-bridge, it is essential to verify whether the plug-in has information related to the I-bridge or the B-bridge, or any other additional I-bridge PBB information. To verify, see Verifying Bridge domains, page 18-48. Based on the information collected, a discovery plug-in is created, and the plug-in receives the necessary data from the VLAN plug-in to create the VLAN instances.

Verifying Bridge domains

To verify the bridge domains, follow the steps provided below:

Step 1 Create a new map in the **Vision** client. For example, VLAN.

Step 2 Add bridges to the map.

Step 3 Right-click one of the bridges and choose **Inventory**.

Step 4 Verify the bridge type in the **Inventory** window.

Step 5 Open the **Add Bridge Domain** dialog box in one of the following ways:

- Choose **File Add to Map > Bridge Domain**.
- In the toolbar, click **Add to Map** and choose **Bridge Domain**.

Step 6 In the **Add Bridge Domain** dialog box, select **Show All** to display the list of bridge domains.

Step 7 Verify whether the bridge that you identified in the **Inventory** window is listed in the Bridge Domain list.

Note The bridges of type I-Bridges or B-Bridges are considered as the bridge domains. These I-Bridges or B-Bridges are added in the Bridge Domain list.

PBB-based EVC Discovery

PBB-based EVC discovery is dependent on the following discovery processes:

- VPLS Discovery
- Network VLAN Discovery
- Network Pseudowire Discovery
- Bridge Domain Discovery

EVC discovery plug-in is responsible for handling Carrier Ethernet technologies such as VPLS, VLAN, bridge domains, cross connect, and pseudowires. This plug-in connects all the domains together in a map from the Vision client.

For more information on the Ethernet services, refer to Working with Ethernet Services in the Cisco Prime Network 5.3 User Guide.

PBB-based EVC Multiplexing

Every EVC should be created with the following rules:

- Every network element, for example, I-Bridge, B-Bridge, pseudowire, or VPLS that is discovered in the inventory should definitely be part of at least one EVC.
- If a network element is associated with the I-Bridge, EVC is created for each I-SID (I-Bridge unique identifier).
- If no I-Bridges are associated, then the EVC is created based on the association between the B-Bridge and VPLS.
- EVC creation for regular bridges works in the same way as that of Prime Network 5.3.

Prime Network supports EVC multiplexing to create an EVC. EVC creation involves the following processes:

- Discovers all dependent discoveries such as VLAN, VPLS, or pseudowires.
- Notifications for each discovery are received by related processors and the Information Model Objects (IMOs) are processed to loaders for creating building blocks based on the associations between the network elements.
- Segmenter collects building blocks from all the above mentioned discoveries and creates segments based on the associations.
- Every segment created is processed based on the rules specified above and creates a complex virtual circuit.

Discovering PBB-links Between I-Bridge and B-Bridge

The PBB I-Bridge interfaces with the customer edge and the B-bridge interfaces with the core network.

To discover the link between the I-Bridge and the B-Bridge, follow the steps provided below:

Step 1 Create a new map in the Vision client. For example, VLAN.

Step 2 Open the **Add Bridge Domain** dialog box in one of the following ways:

- Choose **File Add to Map > Bridge Domain**.
- In the toolbar, click **Add to Map** and choose **Bridge Domain**.

Step 3 In the **Add Bridge Domain** dialog box, select **Show All** to display the list of bridge domains.

Step 4 From the bridge domains, select an I-Bridge and a B-Bridge and click **OK**.

Step 5 Add the selected bridges to the map. The map displays the PBB links between the newly added bridges.

PBB-based Pseudowire Discovery

A pseudowire is a point-to-point connection between pairs of provider edge (PE) routers.

Discovering PBB-links Between Pseudowire and I-Bridge/B-Bridge

To discover the link between the pseudowire and the I-Bridge or B-Bridge, follow the steps provided below:

Step 1 Create a new map in the Vision client. For example, Pseudowire.

Step 2 Open the **Add Bridge Domain** to *domain* dialog box in one of the following ways:

- Choose **File Add to Map > Bridge Domain**.
- In the toolbar, click **Add to Map** and choose **Bridge Domain**.

Step 3 In the **Add Bridge Domain** dialog box, select **Show All** to display the list of bridge domains.

Step 4 From the bridge domains, select an I-Bridge and a B-Bridge and click **OK** to add the selected bridges to the map.

Step 5 Choose **Add to Map > Pseudowire** to open the **Add Pseudowire** to *map* dialog box.

Step 6 In the **Add Pseudowire** to *map* dialog box, select **Show All** to display the list of pseudowires.

Step 7 Add any pseudowire from the list to the map.

Step 8 The map displays the link between the pseudowires and the bridge domains.

PBB-based VPLS Discovery

Prime Network provides Virtual Private LAN Service (VPLS) plug-in to gather VPLS relevant information in a network.

The VPLS plug-in gathers VPLS relevant information from all the VNEs, including the VFIs or VSIs, to create a VPLS service. A VPLS instance representing the VPLS configuration is created on the network. The VPLS snapshot finds out VNEs that are running to retrieve potential VFIs and VSIs. The bridge domains that are connected to the VSIs are attached to VPLS instances to create connection between the VPLS and the Network VLANs.

Based on data gathered, the VPLS discovery constructs the VPLS instances. This discovery can be viewed from the client GUI. A map in the GUI represents VPLS instances in addition to regular VNEs. Thereby, the bridges connected to VSI or VFI are discovered and connected. The VPLS container sends notifications when an VPLS instance is added, modified, or deleted.

Discovering PBB-links Between VPLS and I-Bridge/B-Bridge

To discover the link between the VPLS and the I-Bridge or B-Bridge, follow the steps provided below:

Step 1 Create a new map in the Vision client. For example, VPLS.

Step 2 Open the **Add Bridge Domain** to *domain* dialog box in one of the following ways:

- Choose **File Add to Map > Bridge Domain**.
- In the toolbar, click **Add to Map** and choose **Bridge Domain**.

Step 3 In the **Add Bridge Domain** dialog box, select **Show All** to display the list of bridge domains.

Step 4 From the bridge domains, select an I-Bridge and a B-Bridge and click **OK** to add the selected bridges to the map.

Step 5 Choose **Add to Map > VPLS** to open the **Add Vpls Instance** to *map* dialog box.

Step 6 In the **Add Vpls Instance** to *map* dialog box, select **Show All** to display the list of VPLS instances.

Step 7 Add a VPLS instance from the VPLS instances list.
The map displays the link between the VPLS instance and bridge domains.

Viewing EFP Properties

The Vision client provides information about EFPs in a number of ways. For example:

- EFP names displayed in Vision client maps add EFP and the managed element name to the interface name, such as GigabitEthernet4/0/1 EFP: 123@c4-npe5-67.
- If you select an EFP in the navigation pane in the Vision client and then click **Show List View**, an Ethernet Flow Points table lists the network element, port, and network VLAN associated with the EFP.

To view additional EFP properties:

Step 1 In the Vision client map view, select the required EFP in the navigation pane or in the map pane and then do either of the following:

- Right-click the EFP and choose **Properties**.
- Choose **Node > Properties**.

Figure 18-13 shows an example of the EFP Properties window.

Figure 18-13 EFP Properties Window

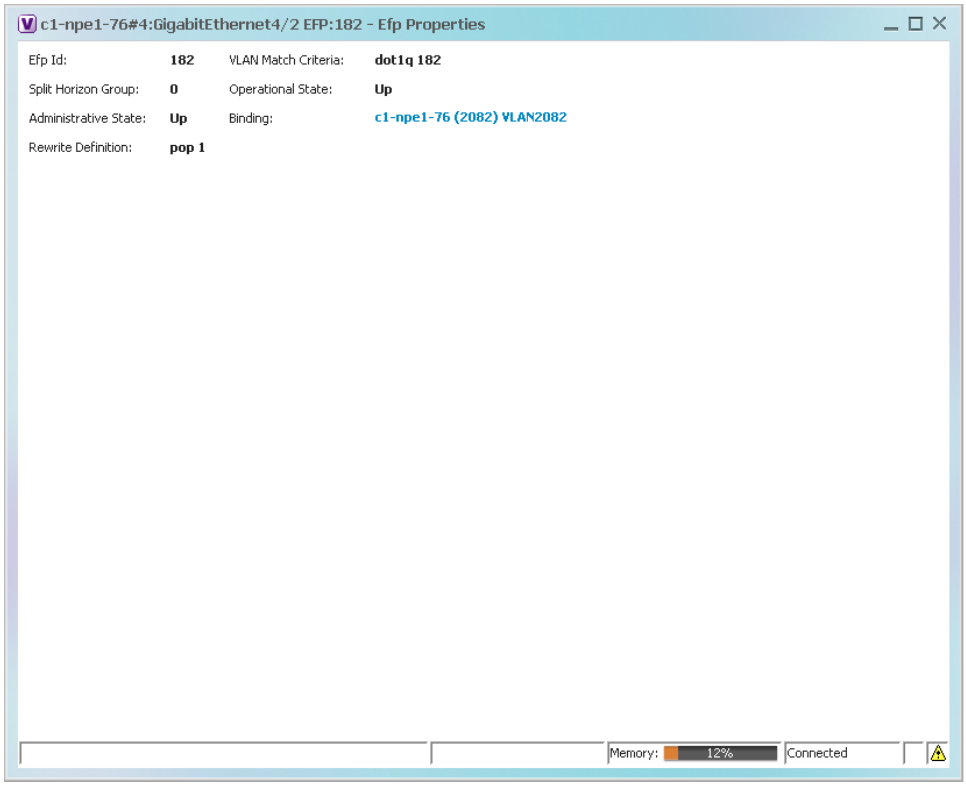


Table 18-26 describes the information displayed in the EFP Properties window.

Table 18-26 EFP Properties Window

Field	Description
EFP ID	Identifier for the EFP.
VLAN Match Criteria	Match criteria configured on the EFP for forwarding decisions.
Split Horizon Group	Split horizon group to which the EFP is associated. If no split horizon group is defined, the value is null. If only one split horizon group exists and it is enabled for the EFP, the value is the default group 0.
Operational State	Operational status of the EFP: Up or Down.
Administrative State	Administrative status of the EFP: Up or Down.
Binding	Hyperlinked entry to the relevant item in logical inventory, such as a pseudowire or bridge.
Rewrite Definition	Rewrite command configured on the EFP: **pop**, **push**, or **translate**.

Step 2 Click the hyperlink entry in the Binding field to view the related properties in logical inventory.

In this example, clicking the hyperlink displays the relevant bridge in logical inventory, as shown in Figure 18-14.

Figure 18-14 Bridge Associated with EFP in Logical Inventory

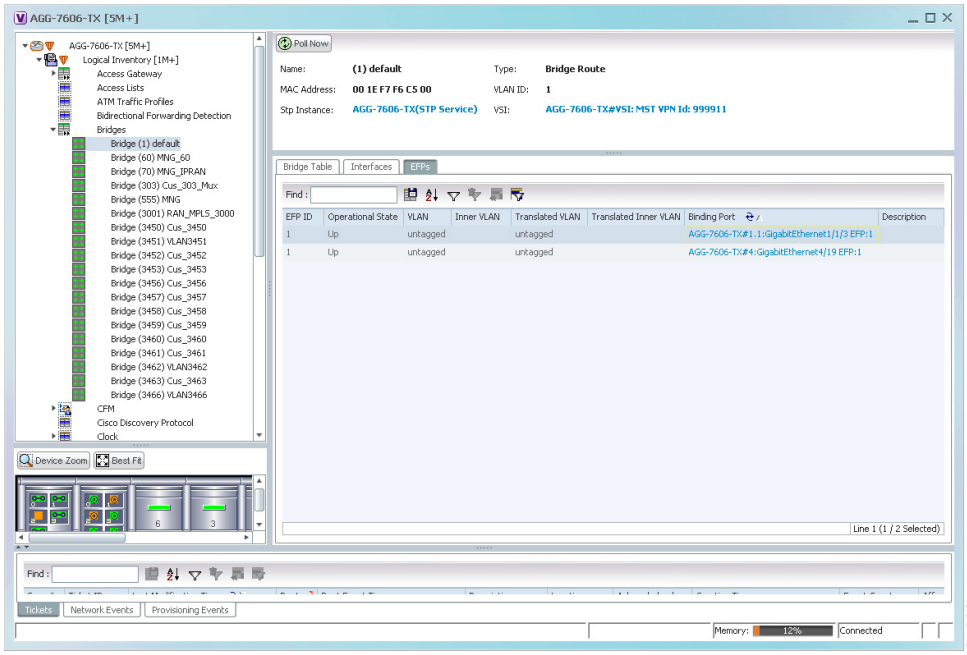


Table 18-27 describes the information displayed for an EFP associated with a bridge.

Table 18-27 EFP Associated with a Bridge in Logical Inventory

Field	Description
Name	VLAN bridge name.
Type	VLAN bridge type.
MAC Address	VLAN bridge MAC address.
VLAN ID	VLAN bridge VLAN identifier.
STP Instance	STP instance information, hyperlinked to the STP entry in logical inventory.
VSI	VSI information, hyperlinked to the VSI entry in logical inventory.
EFPs Table	
EFP ID	EFP identifier.
Operational State	EFP operational state: Up or Down.
VLAN	VLAN associated with this EFP.
Inner VLAN	CE-VLAN identifier.
Translated VLAN	Translated, or mapped, VLAN identifier.
Translated Inner VLAN	Translated, or mapped, inner VLAN identifier.
Binding	Hyperlinked entry to the specific interface and EFP entry in physical inventory.
Description	Description for the EFP.

Step 3 To view EFP properties in physical inventory, navigate to the required interface in one of the following ways:

- In the bridge entry in logical inventory, click the hyperlinked entry in the Binding field.
- Use the procedure described in Viewing and Renaming Ethernet Flow Domains, page 18-60 to navigate to the individual interface.
- In physical inventory, navigate to and then select the required interface.

The EFPs tab is displayed in the content pane next to the Subinterfaces tab as shown in Figure 18-15.

Figure 18-15 EFPs Tab in Physical Inventory

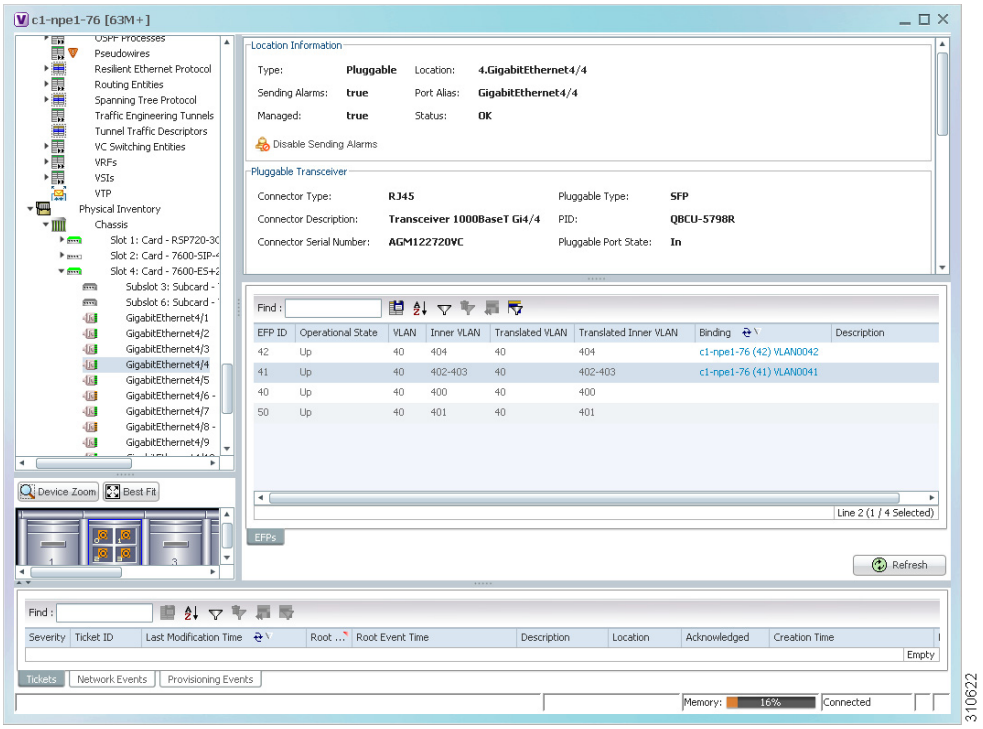


Table 18-28 describes the information displayed in the EFPs tab.

Table 18-28 EFPs Tab

Field	Description
EFP ID	EFP identifier.
Operational State	EFP operational state.
VLAN	VLAN identifier.
Inner VLAN	CE-VLAN identifier.
Translated VLAN	Translated VLAN identifier.
Translated Inner VLAN	Translated CE-VLAN identifier.
Binding	Hyperlinked entry to the specific bridge or pseudowire in logical inventory.
Description	Configured description for the EFP.

Connecting a Network Element to an EFP

You can add and connect network elements to an EFP under an existing aggregation for VLAN, VPLS, Pseudowire, and Ethernet Service.

To connect network elements to an EFP:

Step 1 Select an EFP node under the VLAN/VPLS/Pseudowire/Ethernet Service aggregation node and choose **File > Add to Map > Network Element**.

Step 2 In the Add Network Element dialog box, search for the desired network elements and choose the network element that you want to add.

The selected network element appears under the aggregation node in the navigation pane.

Step 3 Right-click the EFP node and choose **Topology > Connect CE Device**.

Step 4 Right-click the network element that you added and choose **Topology > Connect to** *EFP*.

The map view displays a link between the EFP and the added network element. If required, you can remove the link, by right-clicking the link and choosing **Remove Link**.

Step 5 To hide or show the connected network elements, right-click the EFP node and choose **Hide Connected Devices** or **Show CE device**.

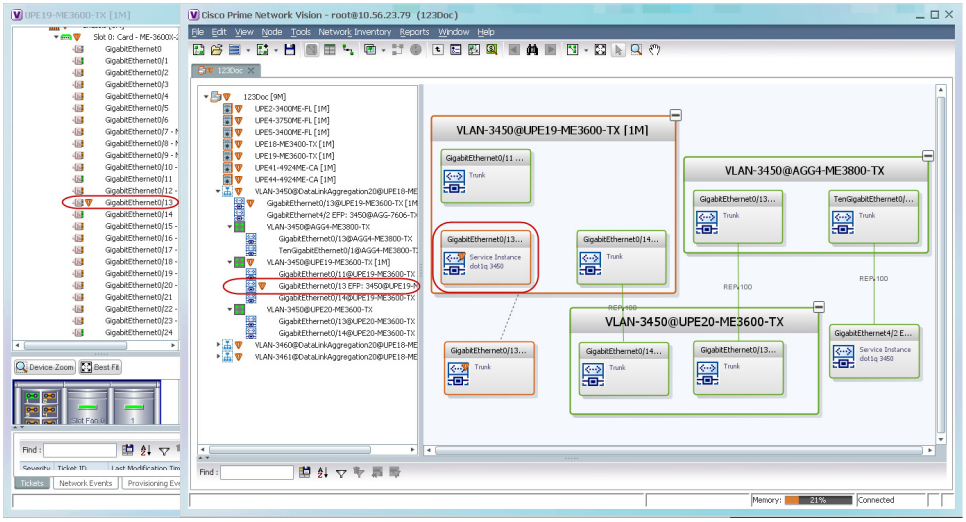
Understanding EFP Severity and Ticket Badges

Severity and ticket badges are displayed on EFP icons as follows:

- If the VLAN EFP element represents a configuration, such as a service instance on a Cisco 7600 device or an enhanced port on a Cisco ASR 9000 device, and is associated directly with a network VLAN or a bridge domain switching entity, the severity and ticket badges are based on the underlying service instance or enhanced port configuration.

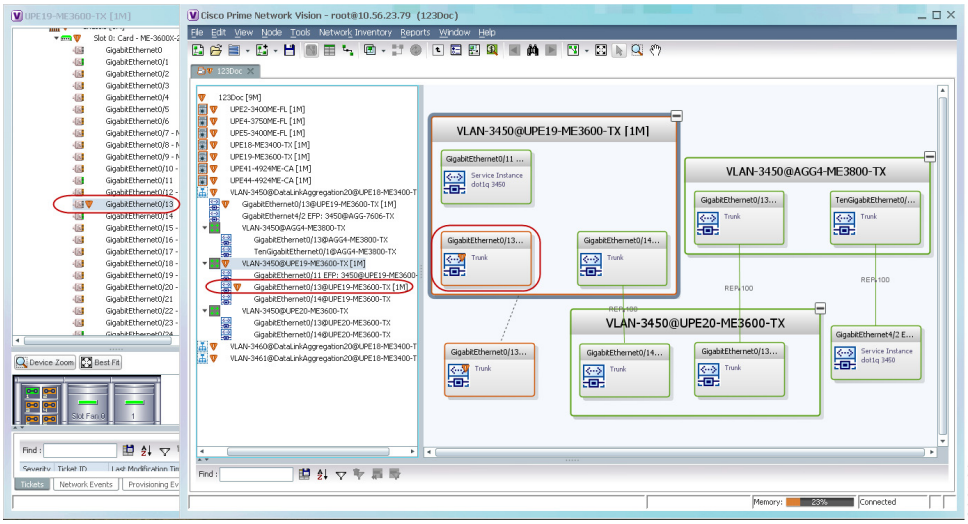
  Figure 18-16 shows an example of a ticket badge based on a service instance.

Figure 18-16 EFP Severity and Ticket Badges Based on Underlying Service Instance



- If the Ethernet flow point element represents a VLAN interface for a regular switch port, the severity and ticket badges are based on the corresponding port, as shown in Figure 18-17.

Figure 18-17 EFP Severity and Ticket Badges Based on Corresponding Port



Viewing EVC Service Properties

Certain EVC service properties are configured as port attributes. These attributes determine the degree of service transparency and protect the service provider's network from protocol control traffic. For information on the devices for which Prime Network discovers and models these key EVC service properties, refer to *Cisco Prime Network 4.1 Supported VNEs*.

Shared Switching Entities and EVC Service View

Some switching entities that the Vision client discovers are concurrently part of a network VLAN and VPLS/EoMPLS instance. These switching entities are referred to as *shared switching entities*.

The Vision client displays the switching entity information for shared switching entities only under the VPLS instances in the EVC service view.

To view EVC port-related properties for the supported devices and software versions:

Step 1 In the Vision client, double-click the required device.

Step 2 In the **Inventory** window, choose **Physical Inventory > Chassis >** *module* **>** *port*.

Figure 18-18 shows an example of a port in physical inventory configured with these EVC properties.

Figure 18-18 EVC Port Properties in Physical Inventory

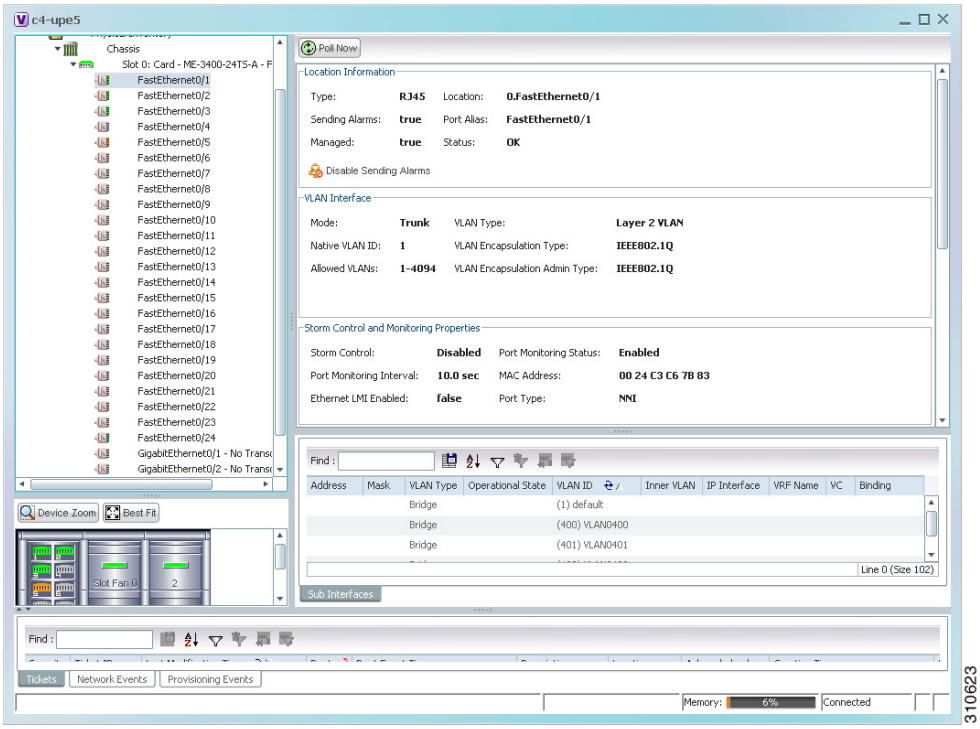


Table 18-29 describes the information displayed for these properties.

Table 18-29 EVC Port Properties in Physical Inventory

Field	Description
Storm Control and Monitoring Properties Area	
Storm Control	Status of storm control on the port: Enabled or Disabled.
Port Monitoring Status	Status of port monitoring: • Enabled—The switch sends keepalive messages on user network interfaces (UNIs) and enhanced network interfaces (ENIs) and does not send keep alive messages on network node interfaces (NNIs). • Disabled—The switch does not send keepalive messages.
Port Monitoring Interval	Keepalive interval in seconds. The default value is ten seconds.
Storm Control Level	Representing a percentage of the total available bandwidth of the port, the threshold at which additional traffic of the specified type is suppressed until the incoming traffic falls below the threshold.
Storm Control Type	Type of storm the port is configured for protection from: Broadcast, Multicast, or Unicast.
Security Properties Areas	
Port Security	Status of security on the port: Enabled or Disabled.
MAC Address Limit	Maximum number of MAC addresses allowed on the interface.

Table 18-29 EVC Port Properties in Physical Inventory (continued)

Field	Description
Aging Type	Type of aging used for automatically learned addresses on a secure port: • Absolute—Times out the MAC address after the specified age-time has been exceeded, regardless of the traffic pattern. This is the default for any secured port, and the age-time value is set to 0. • Inactivity—Times out the MAC address only after the specified age-time of inactivity from the corresponding host has been exceeded.
Aging Time	Length of time, in minutes, that a MAC address can remain on the port security table.
Violation Mode	Action that occurs when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected: • Protect—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value • Restrict—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment. • Shutdown—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

Viewing the Virtual Connections for a Port

In Prime Network, you can view the related virtual connections for an ethernet port or LAG port. In other words, you can view a list of Ethernet Virtual Connections (EVCs) to which the selected port is linked to. The virtual connections can be of type L2 (if the virtual connection is a L2 service) or L3 (if the virtual connection is an L3 service or combination of L2 and L3 service).

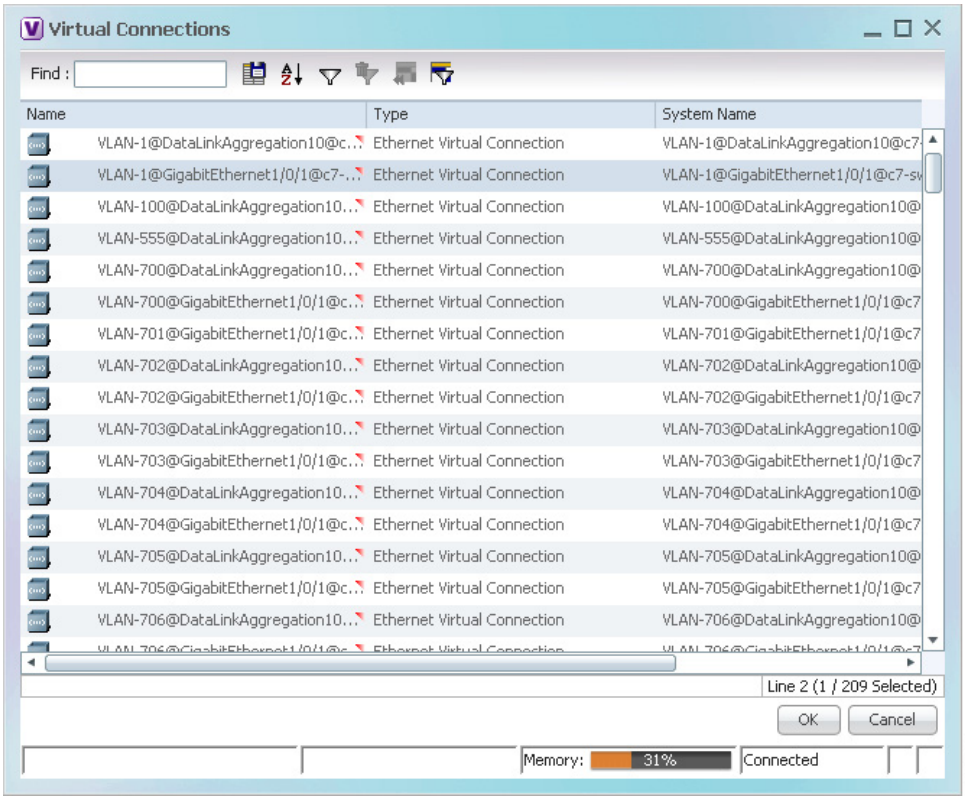
To view the related virtual connections for an ethernet port:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Physical Inventory** > **Chassis** > *slot* > port.

Step 3 Right-click on the selected port and choose **Get Virtual Connections**. The **Virtual Connections** window is displayed as shown in Figure 18-19.

Figure 18-19 Virtual Connections



Note If no related virtual connections are available for a port, then a message indicating that there are no virtual connections for the port is displayed.

Step 4 In the Virtual Connections window, select the relevant connections and click **OK**. A temporary map that contains the selected connections is created and displayed in the Prime Network Vision window.

You can also view the virtual connections for an ethernet link aggregation.

To view the related virtual connections for an ethernet link aggregation:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **Ethernet Link Aggregation**. The link aggregation details are displayed in the content pane.

Step 3 In the Data Link Aggregations section, Right-click the ID and select **Get Virtual Connections**. The Virtual Connections window is displayed.

Step 4 Select the relevant connections and click **OK** to create a temporary map for the connections.

Viewing and Renaming Ethernet Flow Domains

An Ethernet flow domain represents an Ethernet access domain. The Ethernet flow domain holds all network elements between the CE (inclusive, if managed by the SP), up to the SP core (exclusive). This includes CE, access, aggregation, and distribution network elements.

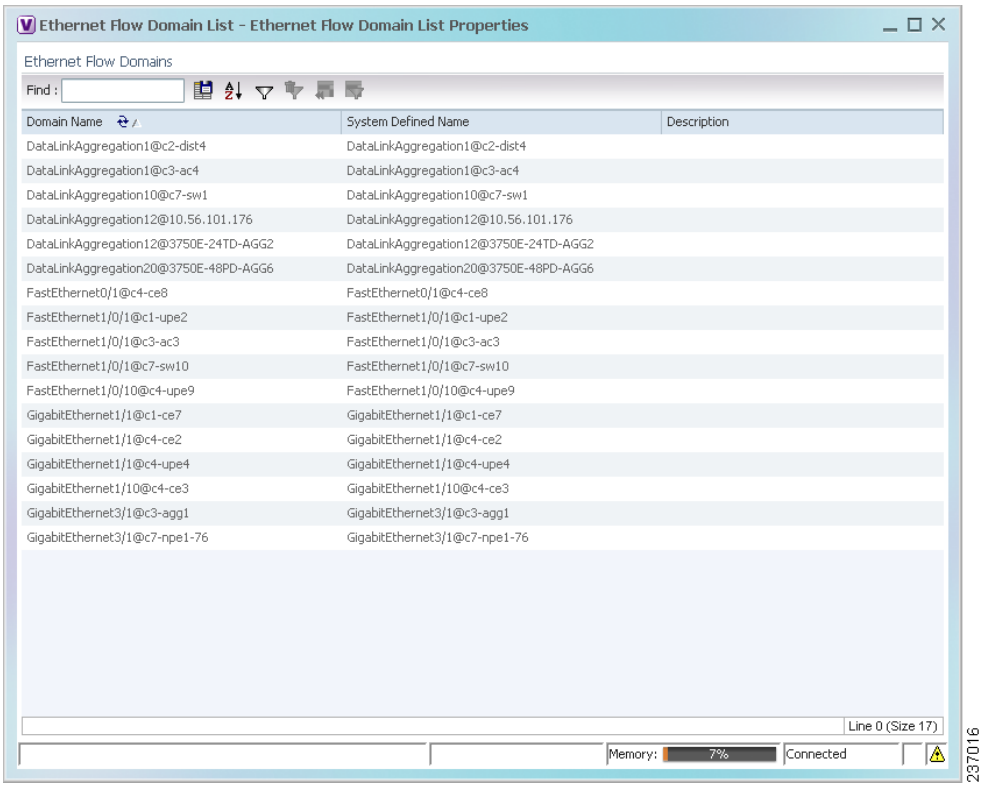
An Ethernet flow domain can have no N-PEs (flat VLAN) or one or more N-PEs (N-PE redundancy configuration). The Ethernet flow domain is defined using physical connectivity at the port level, and not at the network element level. STP is used to mark the root bridge, root or blocked ports, and blocked VLAN links.

To view Ethernet flow domains:

Step 1 In the Vision client, choose **Network Inventory > Ethernet Flow Domains**.

The Ethernet Flow Domain List window is displayed with the domain name, the system-defined domain name, and a brief description for each Ethernet flow domain as shown in Figure 18-20.

Figure 18-20 Ethernet Flow Domain List Properties Window



Step 2 To rename an Ethernet flow domain:

a. Right-click the required domain, then choose **Rename**.

b. In the Rename Node dialog box, enter a new name for the domain.

c. Click **OK**.

The window is refreshed, and the new name is displayed.

Step 3 To view Ethernet flow domain properties, do either of the following:

- Right-click the required domain, then choose **Properties**.
- Double-click the required domain.

The Ethernet Flow Domain Properties window is displayed as shown in Figure 18-21.

Figure 18-21 Ethernet Flow Domain Properties Window

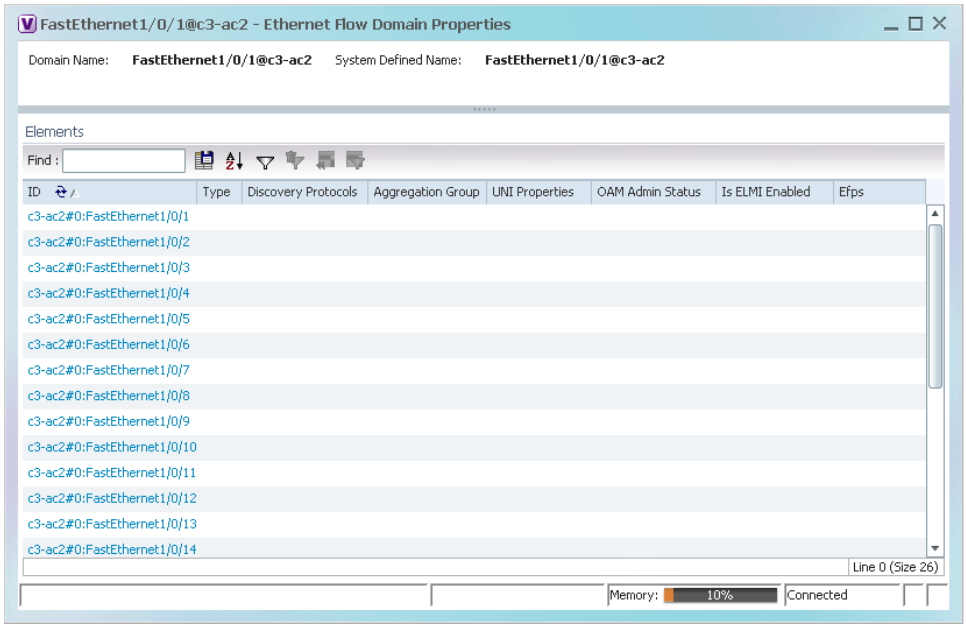


Table 18-30 describes the information displayed in the Ethernet Flow Domain Properties window.

Note Not all fields are available in all tables. The table contents depend on the domain type, such as FastEthernet.

Table 18-30 Ethernet Flow Domain Properties Window

Field	Description
Domain Name	Name of the selected domain.
System Defined Name	Domain name as identified by the most dominant device and its lowest port name lexicographically.
Elements Table	
ID	Interface identifier, hyperlinked to the interface in physical inventory.
Type	Aggregation group type: Ethernet Channel (EtherChannel), or IEEE 802.3 AD LAG (IEEE 802.3 link aggregation group).
Discovery Protocols	Discovery protocols used on the interface.
Is ELMI Enabled	Whether or not Ethernet LMI is enabled on the interface: True or False.

Step 4 To navigate to the individual interface or link aggregation group, click an interface identifier or group.

The interface or link aggregation group properties are displayed in the inventory window.

Working with VLANs

The following topics provide information and procedures for working with VLANs. The Vision GUI client supports a VLAN overlay which, when applied, highlights the network elements and links that a VLAN (and its associated VLANs) traverse. The overlay displays STP and REP link and port information. Using overlays is described in Displaying VLANs By Applying VLAN Overlays to a Map, page 18-77.

Understanding VLAN and EFD Discovery

When you start the Prime Network gateway the first time, the Prime Network waits for two topology cycles to complete before discovering new VLANs, VLAN associations, and EFDs. The default configured time for two topology cycles to complete is one hour, but might be configured for longer periods of time on large setups. This delay allows the system to stabilize, and provides the time needed to model devices and discover links.

During this delay, Prime Network does not add VNEs or apply updates to existing VLANs or EFDs.

After the initial delay has passed, Prime Network discovers new VLANs, VLAN associations, and EFDs, applies updates to existing VLANs, VLAN associations, and EFDs, and updates the database accordingly.

When you restart the gateway, Prime Network uses the persisted topology information instead of waiting two topology cycles, thus improving the discovery time for new VLANs, VLAN associations, and EFDs.

Understanding VLAN Elements

The following concepts are important to understand when working with the representation of edge EFPs inside VLANs:

VLAN Elements in the Vision Client

Table 18-31 describes the icons that the Vision client uses to represent VLAN elements.

Table 18-31 VLAN Elements and Icons in the Vision Window

Element	Associated Network Element	Icon
Network VLAN	None	
Switching entity	Bridge	
Ethernet Flow Point (EFP)	Ethernet port	

VLANs

Prime Network discovers and allows you to display maps with a network-level view of VLANs.

In Prime Network, a VLAN entity consists of one or more switching entities and the corresponding EFP elements.

A network VLAN represents the virtual LAN. The network VLAN holds its contained switching entities and can be associated to a customer. The network VLAN also holds the Ethernet flow points that are part of the network VLAN but not part of any switching entity. For example, a port that tags ingress flows after which the flow moves to a different VLAN.

Switching Entities

A switching entity represents a device-level Layer 2 forwarding entity (such as a VLAN or bridge domain) that participates in a network VLAN. A switching entity is associated to a network VLAN according to its relationship to the same Ethernet Flow Domain (EFD) and the VLAN identifier.

If you right-click a switching entity in the Vision client and then choose **Inventory**, the inventory window is displayed with the corresponding bridge selected in Logical Inventory.

A switching entity typically contains EFP elements.

Ethernet Flow Points

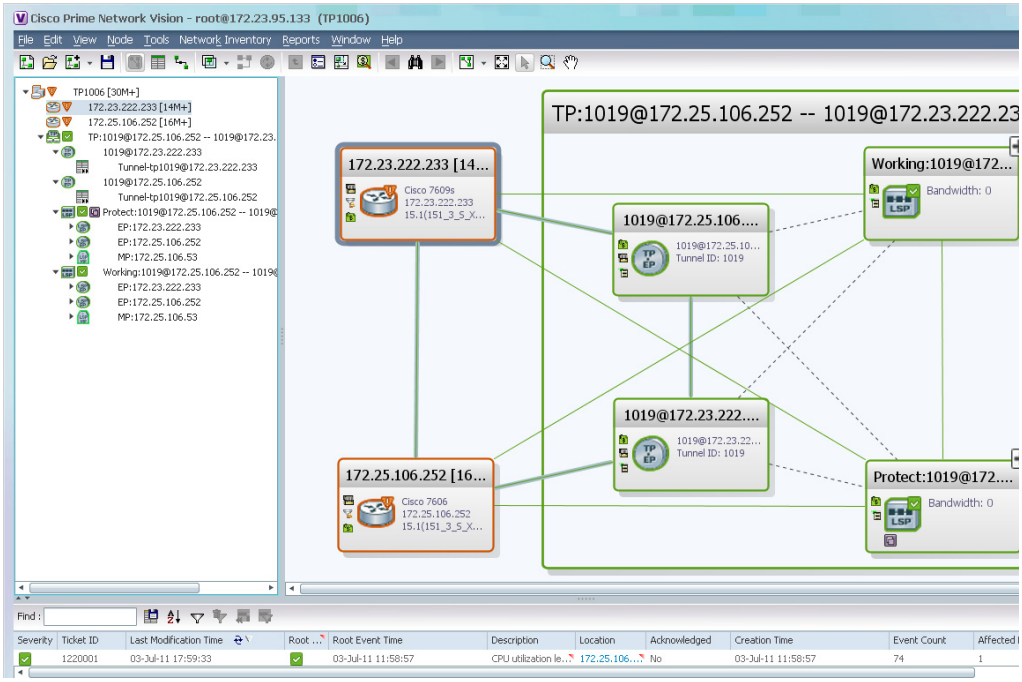
An Ethernet flow point (EFP) can represent a port that is configured for participation in a specific VLAN.

If you right-click an EFP in the Vision client and then choose **Inventory**, the inventory window is displayed with the corresponding port selected in Physical Inventory.

EFPs that are located in a switching entity represent Ethernet ports that are configured as switch ports (in either Access, Trunk, or Dot1Q tunnel mode).

Figure 18-22 shows an example of EFPs configured as switch ports in the Vision client.

Figure 18-22 EFPs Configured as Switch Ports

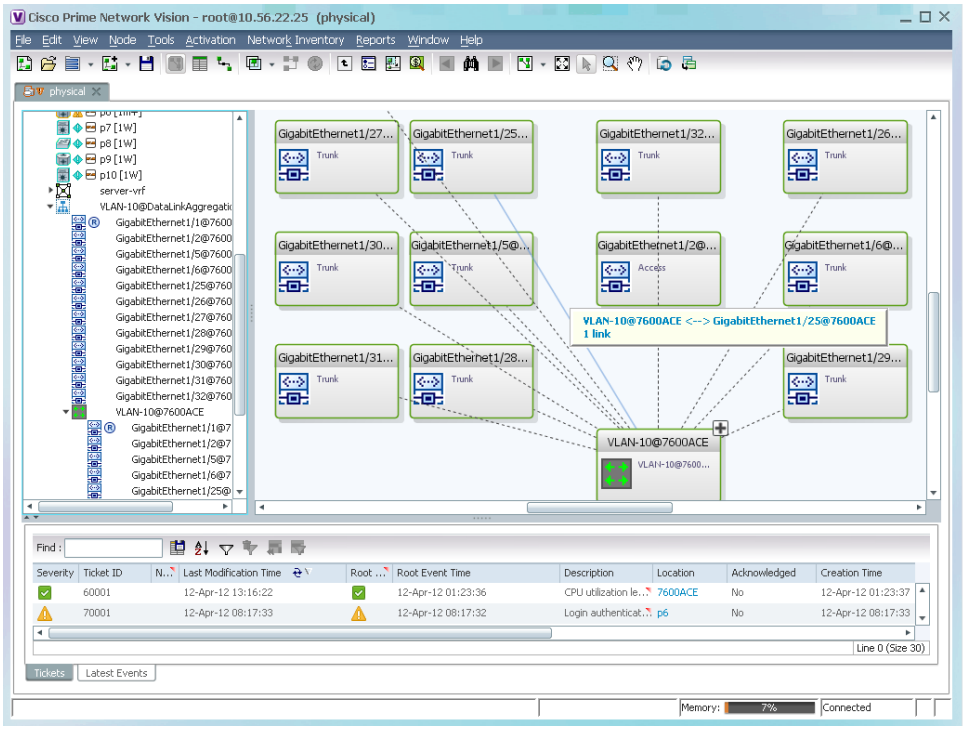


EFPs that are located directly inside a VLAN represent one of the following:

- Termination point EFPs—Ethernet ports that are at the edge of a Layer 2 domain flow, such as a VLAN, on which traffic enters a Layer 3 domain or a different Layer 2 domain, such as EoMPLS (for example, in Cisco 7600 series, Cisco GSR, and Cisco ASR 9000 series devices).

  These EFPs are typically connected to a switching entity inside the VLAN by a VLAN link, as shown in Figure 18-23.

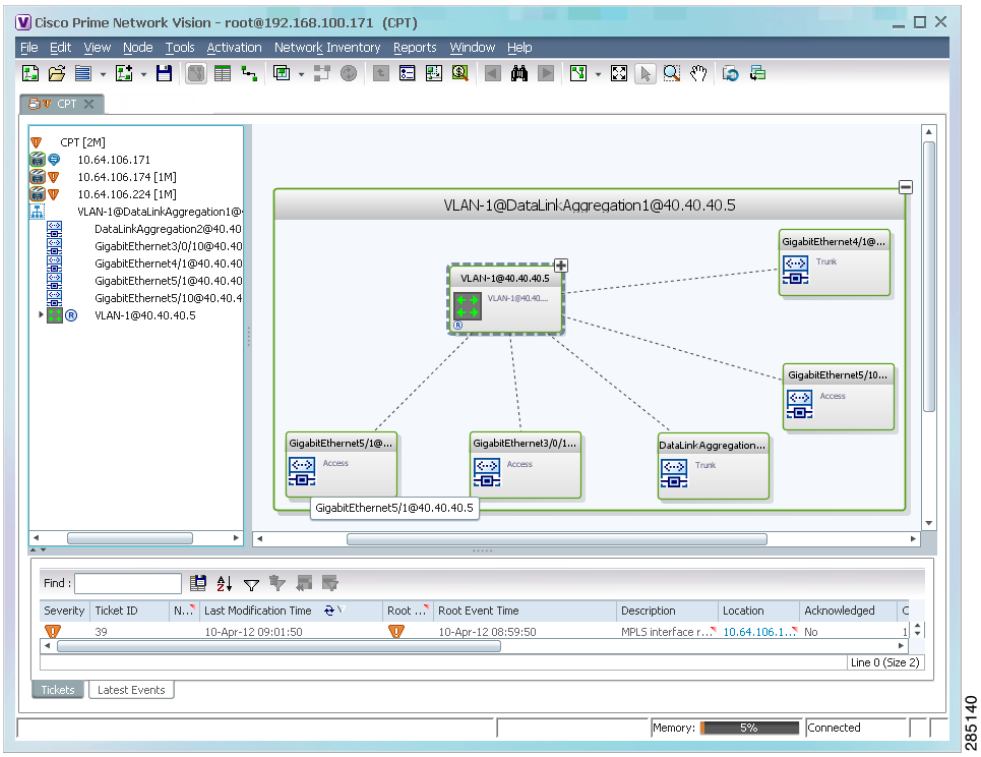
Figure 18-23 Termination Point EFP Inside a VLAN



- Edge EFPs—A subset of EFPs that exist inside a switching entity but that are not connected to other EFPs and that represent edge EFPs in the context of the VLAN.

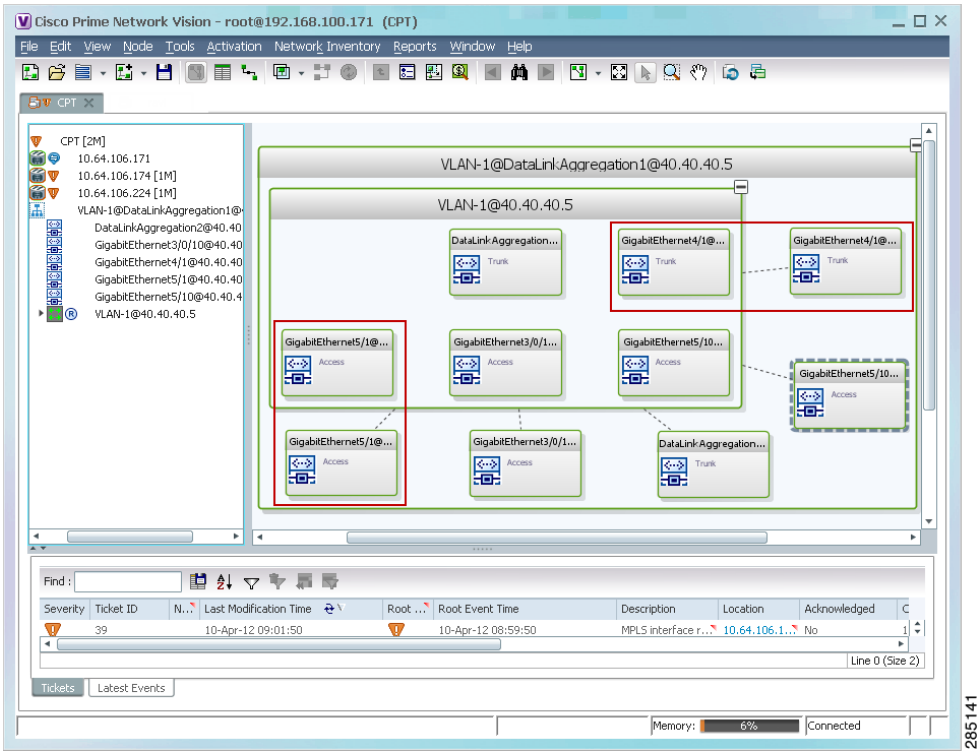
In the Vision client, edge EFPs are displayed directly under the VLAN at the same level as their switching entities and are connected to their corresponding switching entities by a dotted link, as shown in Figure 18-24.

Figure 18-24 Edge EFP Inside a VLAN



An edge EFP can be displayed both inside and outside of its switching entity, as shown (highlighted with a red outline) in Figure 18-25:

Figure 18-25 Edge EFPs Displayed Inside and Outside of Switching Entities



You can delete EFPs and switching entities that have a reconciliation icon by right-clicking them and choosing **Delete**. After all switching entities and EFPs are deleted from a network VLAN, the empty network VLAN is automatically deleted from the Vision client after a few minutes.

Switching Entities Containing Termination Points

For certain devices (for example, the Cisco 7600 series, Cisco GSR series, and Cisco ASR 9000 series devices), the related switching entities can contain Ethernet flow point elements that serve as termination points on different network VLANs. If a single map contains both the switching entities and the network VLANs, a link is displayed between them.

Adding and Removing VLANs from a Map

Adding VLANs to a Map

You can add VLANs to a map if the VLANs were previously discovered by Prime Network and are not currently displayed in the map.

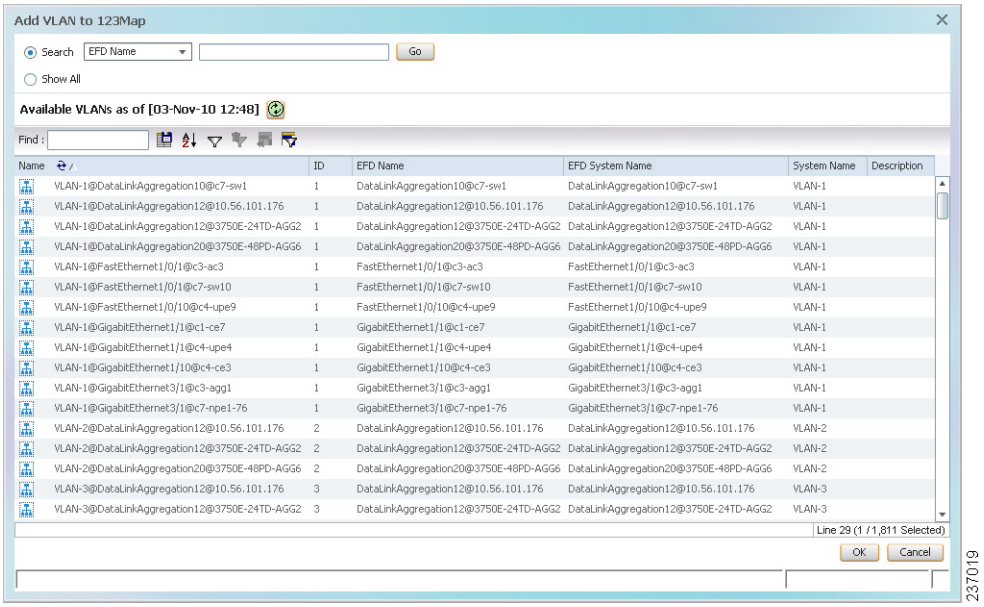
Note Adding VLANs affects other users if they are working with the same map.

To add VLANs to a map:

Step 1 In the Vision client, display the map to which you want to add the VLANs.

Step 2 Choose **File > Add to Map > VLAN**. The Add VLAN to *map* dialog box is displayed as shown in Figure 18-26.

Figure 18-26 Add VLAN Dialog Box



Step 3 In the Add VLAN dialog box, do either of the following:

- Choose a search category, enter a search string, then click **Go** to narrow the VLAN display to a range of VLANs or a specific VLAN.

  The search condition is "contains." Search strings are case-insensitive. For example, if you choose the Name category and enter "net," the Vision client displays VPNs "net" and "NET" in the names whether net appears at the beginning, middle, or at the end of the name: for example, Ethernet.

- Choose **Show All** to display all the VLANs.

Step 4 Select the VLANs that you want to add to the map.

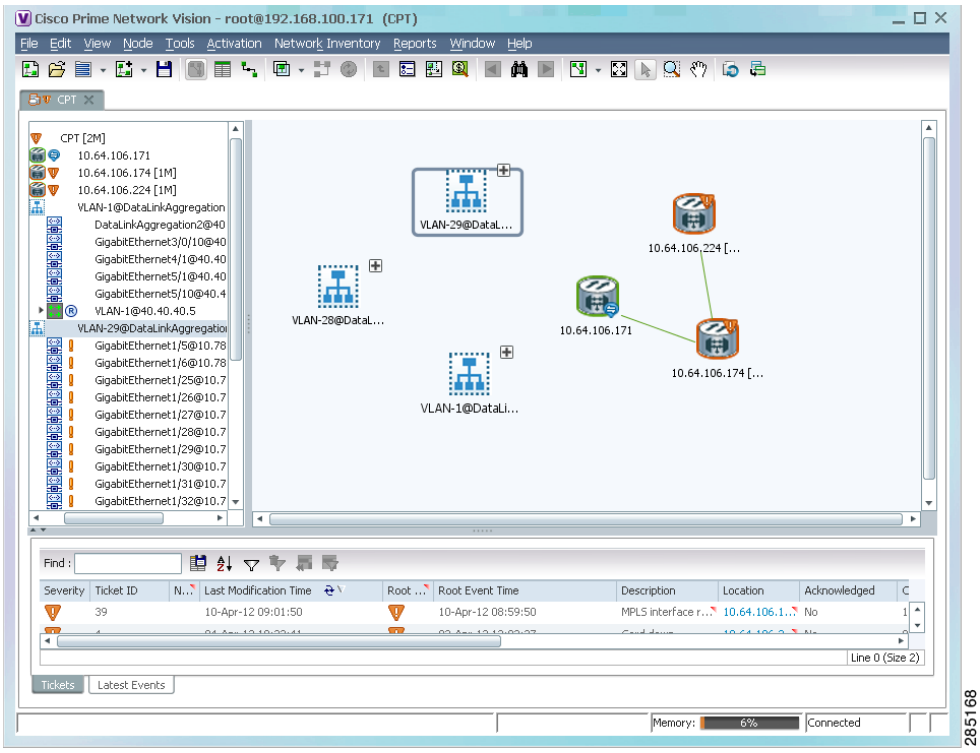
Tip Press **Shift** or **Ctrl** to choose multiple adjoining or nonconsecutive VLANs.

Step 5 Click **OK**.

The VLANs are displayed in the Vision client content pane as shown in Figure 18-27.

Any tickets that apply to the VLANs are displayed in the ticket pane.

Figure 18-27 VLANs in Map View



After you add a VLAN to a map, you can use the Vision client to view its switching entities and Ethernet flow points. For more information, see:

- Viewing and Renaming Ethernet Flow Domains, page 18-60
- Viewing EFP Properties, page 18-51

You can view additional information about REP and STP in logical inventory, VLAN domain views, and VLAN overlays.

For REP, see:

- Viewing Resilient Ethernet Protocol Properties (REP), page 18-9
- Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 18-80
- Viewing REP Properties for VLAN Service Links, page 18-81

For STP, see:

- Viewing Spanning Tree Protocol Properties, page 18-5
- Viewing STP Information in VLAN Domain Views and VLAN Overlays, page 18-83
- Viewing STP Properties for VLAN Service Links, page 18-84

Removing VLANs From a Map

You can remove one or more VLANs from the current map. This change does not affect other maps. Removing a VLAN from a map does not remove it from the Prime Network database. You can add the VLAN to the map at any time.

When removing VLANs from maps, keep the following in mind:

- Removing a VLAN affects other users who are working with the same map view.
- This option does not change the business configuration or database.
- You cannot remove virtual routers or sites from the map without removing the VLAN.

To remove a VLAN, in the Vision client navigation pane or map view, right-click the VLAN and choose **Remove from Map**.

The VLAN is removed from the navigation pane and map view along with all VLAN elements such as connected CE devices. Remote VLANs (extranets) are not removed.

Viewing VLAN Mappings

VLAN mapping, or VLAN ID translation, is used to map customer VLANs to service provider VLANs. VLAN mapping is configured on the ports that are connected to the service provider network. VLAN mapping acts as a filter on these ports without affecting the internal operation of the switch or the customer VLANs.

If a customer wants to use a VLAN number in a reserved range, VLAN mapping can be used to overlap customer VLANs by encapsulating the customer traffic in IEEE 802.1Q tunnels.

To view VLAN mappings:

Step 1 In the Vision client, double-click the device with VLAN mappings configured.

Step 2 In the **Inventory** window, choose **Physical Inventory > Chassis >** *slot* **>** *port*.

Step 3 Click **VLAN Mappings** next to the Subinterfaces tab in the lower portion of the content pane.

The VLAN Mappings tab is displayed as shown in Figure 18-28.

Figure 18-28 VLAN Mappings Tab in Physical Inventory

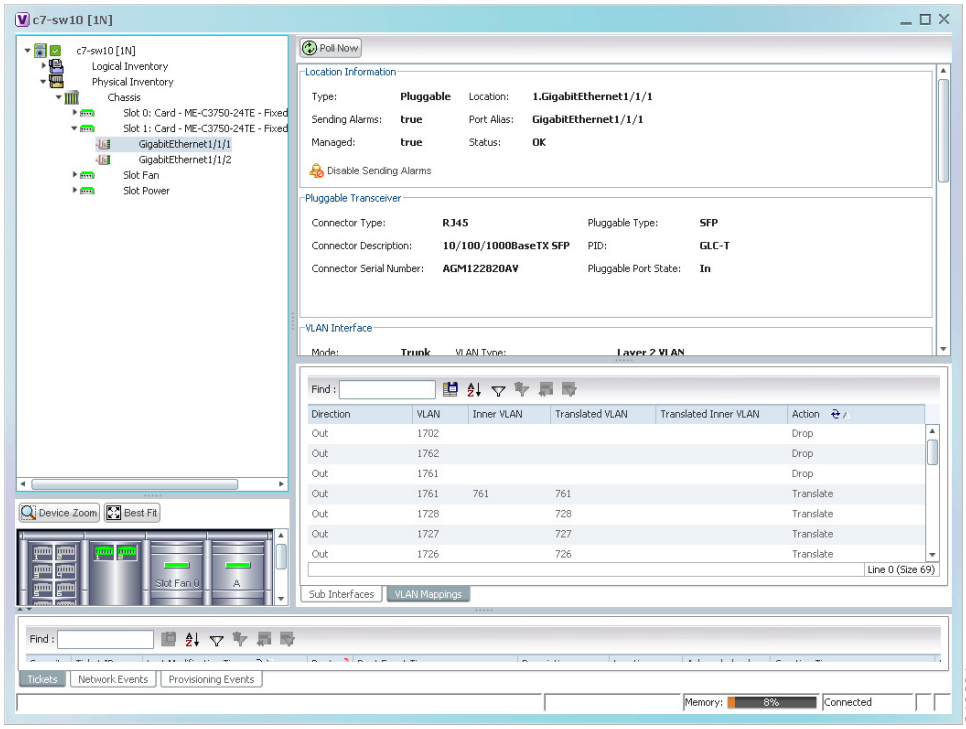


Table 18-32 describes the information that is displayed in the VLAN Mappings table.

Table 18-32 VLAN Mappings Table

Field	Description
Direction	Whether the VLAN mapping is defined in the incoming or outgoing direction: In or Out.
VLAN	Customer-side VLAN identifier.
Inner VLAN	Used for two-to-one mappings, the customer-side inner VLAN identifier.
Translated VLAN	Translated, or mapped, service-provider side VLAN identifier.
Translated Inner VLAN	Translated, or mapped, service-provider side inner VLAN identifier.
Action	Action taken if the VLAN traffic meets the specified mapping: Translate or Drop.

Working with Associated VLANs

Prime Network discovers associations between network VLANs and displays the information in the Vision client. Network VLAN associations are represented by VLAN service links, and can be any of the tag manipulation types described in Table 18-33.

Table 18-33 Types of Tag Manipulations in VLAN Associations

VLAN Tag Manipulation	Description	Example
One-to-one	One VLAN tag is translated to another VLAN tag.	VLAN tag 100 > VLAN tag 200
Two-to-two	• Two VLAN tags exist and both are translated to other tags. • Two VLAN tags exist, but tag manipulation is applied only to the outer tag.	• Inner tag 100, Outer tag 101 > Inner tag 200, Outer tag 201 • Inner tag 100, Outer tag 101 > Inner tag 100, Outer tag 201
One-to-two	One VLAN tag exists and an additional tag is inserted into the packet.	VLAN tag 100 > Inner tag 100, Outer tag 101

When working with VLANs, you can:

- Add an associated VLAN—See Adding an Associated VLAN, page 18-72.
- View properties for associated VLANs—See Viewing Associated Network VLAN Service Links and VLAN Mapping Properties, page 18-74.

Adding an Associated VLAN

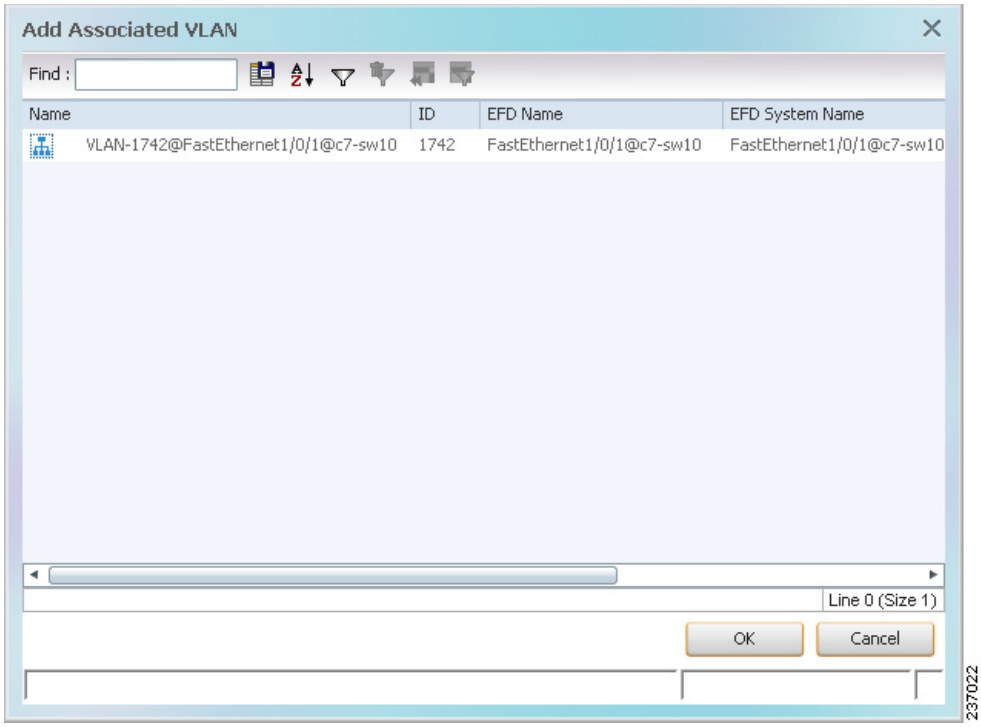
To add an associated VLAN to an existing VLAN in a map:

Step 1 In the Vision client, select the required VLAN in the map view.

Step 2 Right-click the VLAN and choose **Add Associated VLAN**.

The Add Associated VLAN table is displayed as shown in Figure 18-29.

Figure 18-29 Add Associated VLAN Window



In this example, the selected network VLAN has one associated VLAN: VLAN-1742.

Table 18-34 describes the information displayed in the Add Associated VLAN table.

Table 18-34 Add Associated VLAN Table

Field	Description
Name	Name of the VLAN.
ID	VLAN identifier.
EFD Name	Name of the Ethernet flow domain.
EFD System Name	Name that Prime Network assigns to the EFD.
System Name	Name that Prime Network assigns to the VLAN.
Description	Brief description of the VLAN.

Step 3 Select the required VLAN in the Add Associated VLAN table, then click **OK**.

The associated network VLAN is added to the map in the Vision client.

Viewing Associated Network VLAN Service Links and VLAN Mapping Properties

After you add an associated network VLAN, you can:

- View the associated network VLAN service links in the Vision client in the thumbnail view.
- View VLAN mapping properties in the Link Properties window.

To view associated network VLAN service links and VLAN mapping properties:

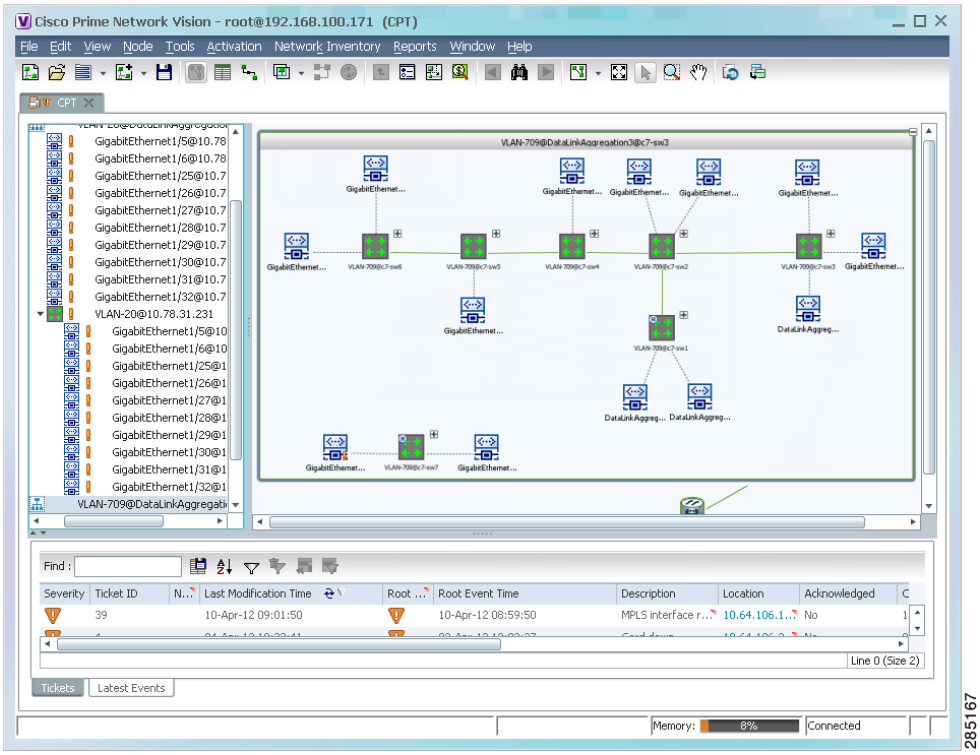
Step 1 Select the required network VLAN in the map view.

Step 2 Right-click the VLAN, then choose **Show Thumbnail**.

Figure 18-30 shows an example of a network VLAN in a thumbnail.

The VLAN service links are displayed as 5.3 between the associated network VLANs. The links represent the connections between the Ethernet flow points that are part of each network VLAN.

Figure 18-30 VLAN Service Links Between Associated Network VLANs

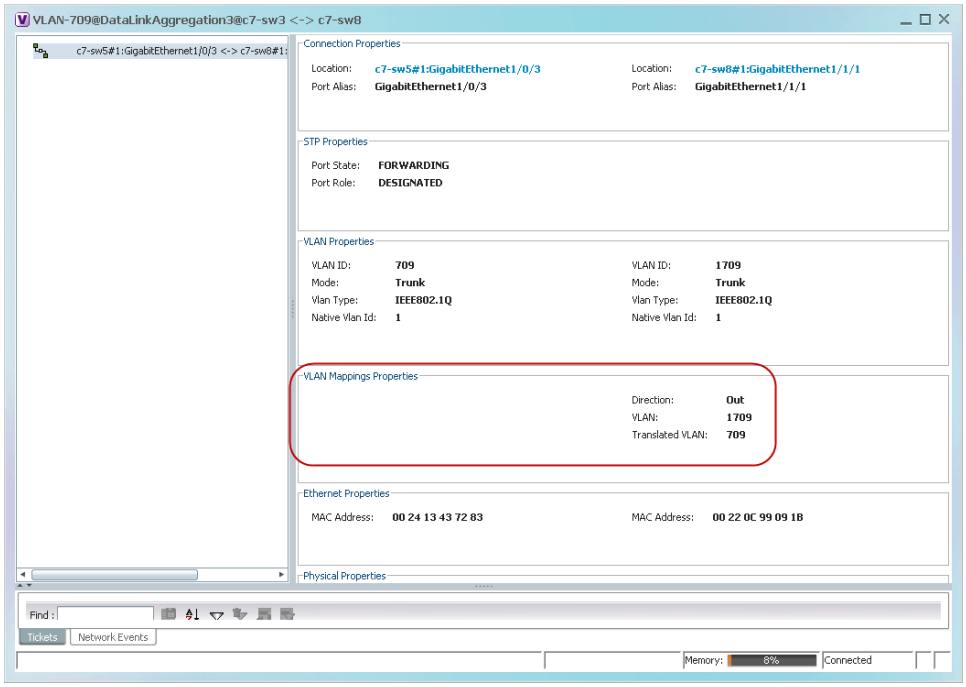


Step 3 To view additional information, right-click a link, and choose **Properties**.

The Link Properties window is displayed as shown in Figure 18-31.

If VLAN tag manipulation is configured on the link, the VLAN Mapping Properties area in the Link Properties window displays the relevant information. For example, in Figure 18-31, the VLAN Mapping Properties area shows that a one-to-one VLAN mapping for VLAN tag 1709 to VLAN tag 709 is configured on GigabitEthernet1/1/1 on c7-sw8 on the egress direction.

Figure 18-31 VLAN Mapping Properties in Link Properties Window



For additional information about viewing network VLAN service link properties, see:

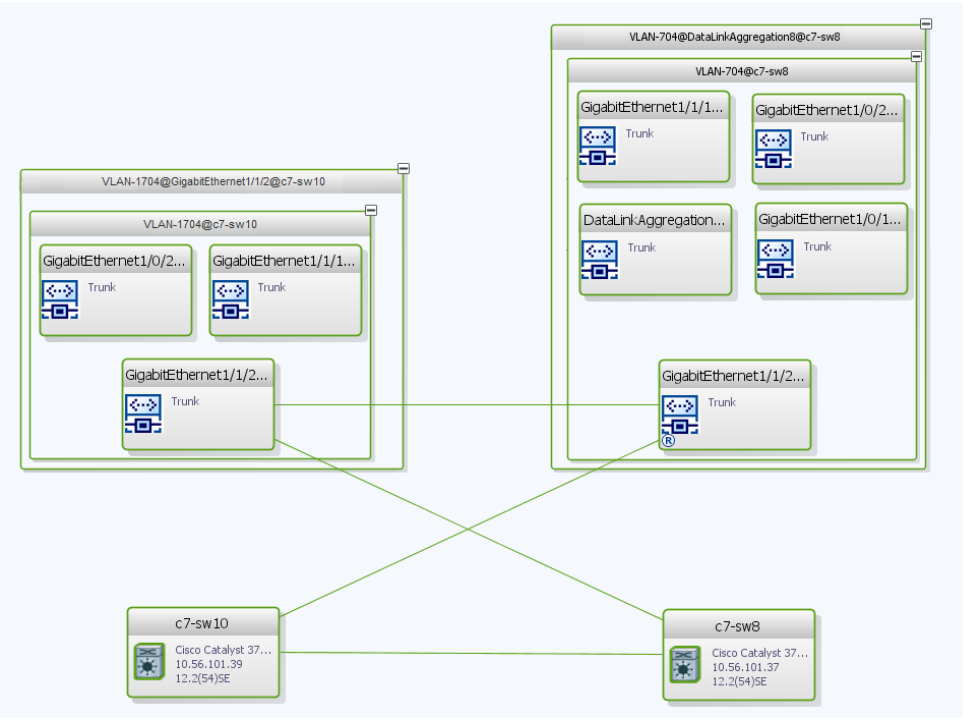
- Viewing REP Properties for VLAN Service Links, page 18-81
- Viewing STP Properties for VLAN Service Links, page 18-84

Viewing VLAN Links Between VLAN Elements and Devices

If a Vision client map contains a VLAN and the network element on which the VLAN is configured, along with EFPs, switching entities, or network VLANs, you might see what appear to be multiple associations between the logical and physical entities. Actually, however, you are seeing other views of the original VLAN link.

For example, assume that you have the following situation, as shown in Figure 18-32 and described in the following paragraphs.

Figure 18-32 VLAN Elements and Devices in the Vision Window



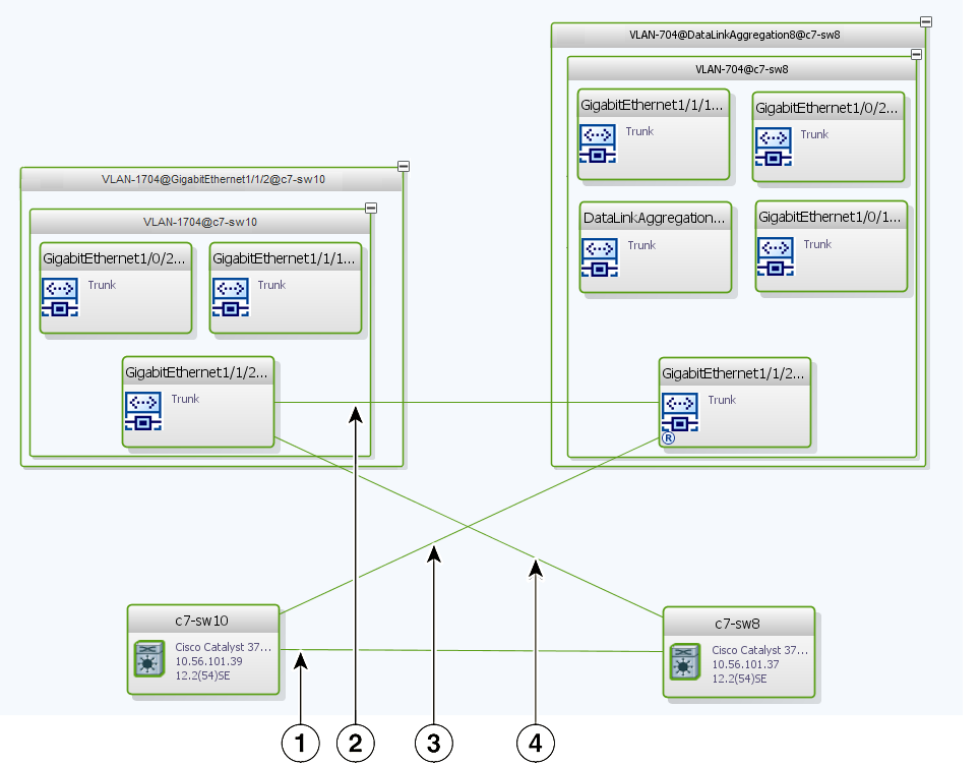
The elements are configured as follows:

- Port GigabitEthernet1/1/2 on element c7-sw10 is connected to port GigabitEthernet1/1/2 on element c7-sw8 by an Ethernet topology link.
- Port GigabitEthernet1/1/2 on element c7-sw10 is a trunk port associated with VLAN-1704 which is configured on element c7-sw10.
- Port GigabitEthernet1/1/2 on element c7-sw8 is a trunk port associated with VLAN-704 which is configured on element c7-sw8.
- Port GigabitEthernet1/1/2 on element c7-sw8 has a VLAN mapping to tunnel VLAN-1704 (C-VLAN) in VLAN-704 (SP-VLAN).

In this example, VLAN discovery identified two network VLANs: VLAN-1704 and VLAN-704. Each of these network VLANs contains a switching entity and an EFP that represent the connected ports, GigabitEthernet1/1/2@c7-sw10 and GigabitEthernet1/1/2@c7-sw8, respectively.

The four links in the map are identified in Figure 18-33 and described in the following table.

Figure 18-33 Links Between VLAN Elements and Devices



1	The Ethernet topological link between port GigabitEthernet1/1/2 on VNE c7-sw10 and GigabitEthernet1/1/2 on VNE c7-sw8.
2	The VLAN link between GigabitEthernet1/1/2@c7-sw10 EFP and GigabitEthernet1/1/2@c7-sw8 EFP.
3	Another view of the VLAN link (link 2), shown as a link between GigabitEthernet1/1/2@c7-sw10 EFP and GigabitEthernet1/1/2@c7-sw8 EFP.
4	Another view of the VLAN link (link 2), shown as a link between GigabitEthernet1/1/2@c7-sw10 EFP and GigabitEthernet1/1/2@c7-sw8 EFP.

The key point is that a link between a VNE and EFP, switching entity, or network VLAN **does not** represent an association between the VNE and the logical element. Such a link is simply another view of the VLAN link.

If the thumbnail view is closed, instead of a link between the VNE and EFP, you will see a link between the VNE and the switching entity or network VLAN.

Displaying VLANs By Applying VLAN Overlays to a Map

You can create an overlay of a specific VLAN on top of the physical network elements displayed in a map view. The overlay highlights the network elements and links that the selected VLAN and its associated VLANs traverse. Network elements and links that are not part of the VLAN are dimmed in the map view.

The VLAN overlay is a snapshot of the network to help you visualize the network elements and links connected to a VLAN. The overlay displays STP and REP link and port information.

If you select a network VLAN that is associated with other VLANs, the associated VLANs are included in the overlay.

The VLAN service overlay allows you to isolate the parts of a network that are being used by a particular service. This information can then be used for troubleshooting. For example, the overlay can highlight configuration or design problems when bottlenecks occur and all site interconnections use the same link.

Adding a VLAN Overlay

To add a VLAN overlay:

Step 1 Display the network map for which you want to create an overlay in the Vision client.

Step 2 In the toolbar, choose **Choose Overlay Type > VLAN**.

Step 3 In the Select VLAN Overlay dialog box, do either of the following:

- Choose a search category, enter a search string, then click **Go** to narrow the selection to a set of overlays or a specific overlay.

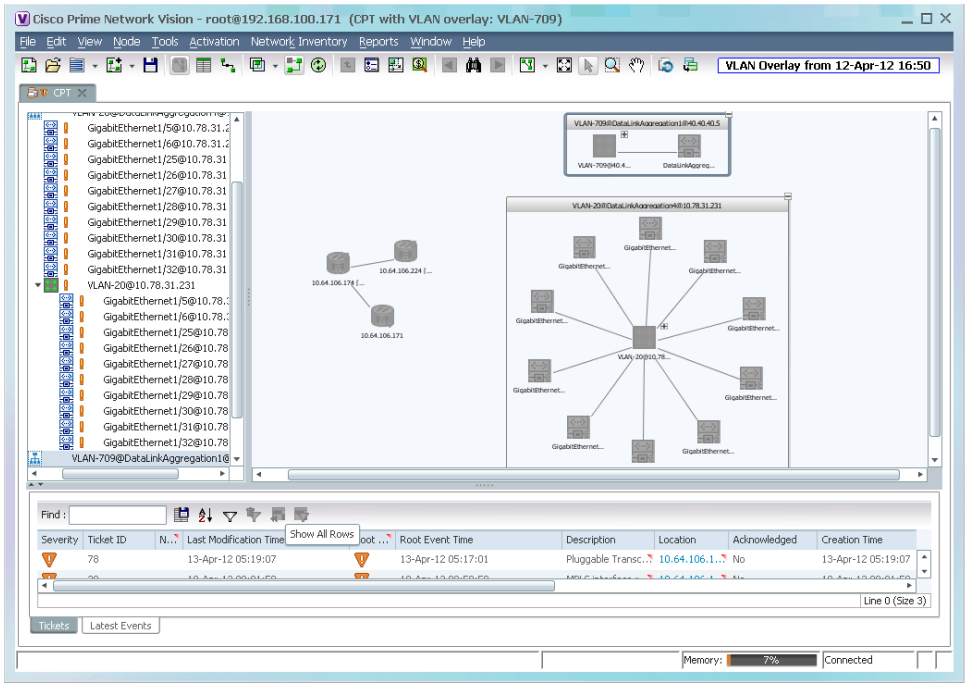
  The search condition is “contains.” Search strings are case-insensitive. For example, if you choose the Name category and enter “net,” the Vision client displays overlays that have “net” in their names. The string “net” can be at the beginning, middle, or end of the name, such as Ethernet.

- Choose **Show All** to view all overlays.

Step 4 Select an overlay, then click **OK**.

The network elements and physical links used by the selected VLAN overlay are highlighted in the network map. All other network elements and links are dimmed. The VLAN name is displayed in the title of the window. See Figure 18-34.

Figure 18-34 VLAN Overlay Example



Note The overlay is a snapshot taken at a specific point in time. As a result, the information in the overlay might become stale. To update the overlay, click **Refresh the Last Selected Overlay** in the toolbar.

The VLAN overlay service also supports multi-chassis devices. If a network element in the overlay is dimmed, then all the hosts of the network element along with the Inter Rack Links (IRL) and the Inter Chassis Links (ICL) used for transportation will also be dimmed. Apart from these, the chassis that holds the configured port will also be dimmed.

Displaying or Hiding VLAN Overlays

After you create a VLAN overlay, you can hide it by clicking **Hide Overlay** in the toolbar. All previously dimmed network elements and links are displayed. To display the overlay, click **Show Overlay**.

Note The Overlay icon toggles between Show Overlay and Hide Overlay. When selected, the VLAN overlay is displayed and the Hide Overlay tool is active. When deselected, the VLAN overlay is hidden and the Show Overlay tool is active.

Removing a VLAN Overlay

To remove a VLAN overlay from a map, choose **Choose Overlay Type > None** in the toolbar. The overlay is removed from the map, and the Show Overlay/Hide Overlay icon is dimmed.

Viewing VLAN Service Link Properties

See the following topics for information on viewing VLAN service link properties:

- Viewing REP Properties for VLAN Service Links, page 18-81
- Viewing STP Properties for VLAN Service Links, page 18-84
- Viewing Associated Network VLAN Service Links and VLAN Mapping Properties, page 18-74

Viewing REP Information in VLAN Domain Views and VLAN Overlays

You can view REP segment and port information in the Vision client in the map view. The icons displayed depend on whether you view the REP information in the VLAN domain view or in a VLAN overlay. Table 18-35 describes the icons and badges used to represent REP segment and port information.

Table 18-35 REP Icons and Badges in VLAN Domain Views and Overlays

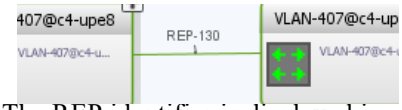
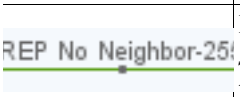
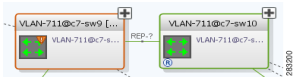
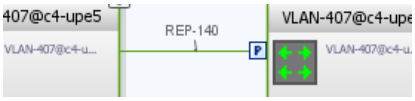
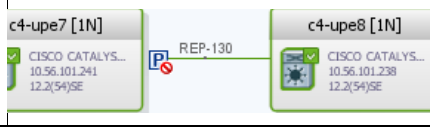
Item	Description	VLAN Domain View	VLAN Overlay
	REP identifier—Uses the format REP-*id* where *id* represents the REP segment identifier.	 The REP identifier is displayed in the domain view if the visual link represents only one link. f the visual link represents more than one link, no REP identifier is displayed.	 The REP identifier is displayed in a VLAN overlay view if all the links represented by the visual link are from the same source to the same destination.
	REP No Neighbor *segment*— Indicates that the specified segment has no neighbor.		
	REP identifier for incorrect configuration—Indicates that the two sides of the link are configured differently or incorrectly.		

Table 18-35 REP Icons and Badges in VLAN Domain Views and Overlays (continued)

Item	Description	VLAN Domain View	VLAN Overlay
	Multiple links with badges icon—Indicates that one or more link is represented by the visual link and at least one of the links contains a badge.	 The multiple links icon is displayed in the domain view if more than one link is represented by the visual link and at least one of the links contains a badge.	 The multiple links icon is displayed in a VLAN overlay view if either of the following is true: • More than one link is represented by the visual link and the links have different sources or destinations. • A badge or REP identifier exists on a sublink.
	REP primary badge—Indicates a REP primary port.		
	Blocking badge—Indicates a REP alternate port.		
	Primary and blocking badge—Indicates a REP primary port that is also blocking.		

Viewing REP Properties for VLAN Service Links

To view REP properties for a VLAN service link, open the Link Properties window in either of the following ways:

- Double-click the VLAN service link.
- Right-click the VLAN service link, and choose **Properties**.

Figure 18-35 shows an example of the Link Properties window with REP information.

Figure 18-35 VLAN Service Link Properties Window with REP Information

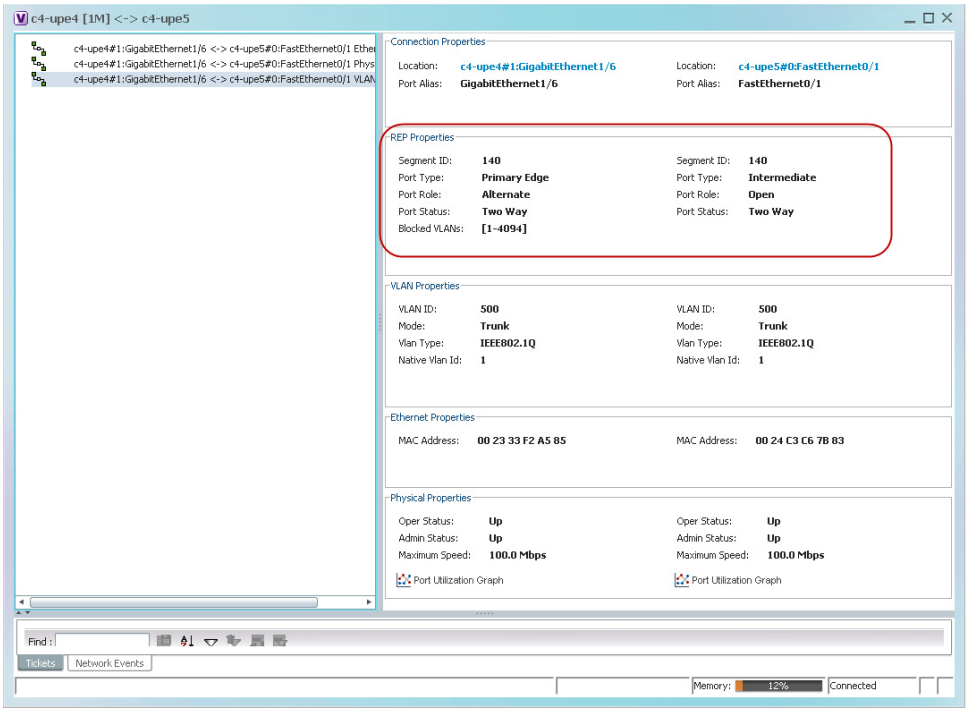


Table 18-36 describes the information that is displayed for REP for each end of the link.

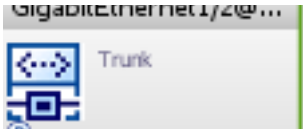
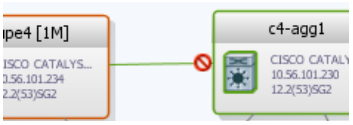
Table 18-36 REP Properties in VLAN Service Link Properties Window

Field	Description
Segment ID	REP segment identifier.
Port Type	Port type: Primary Edge, Secondary Edge, or Intermediate.
Port Role	Role or state of the REP port depending on its link status and whether it is forwarding or blocking traffic: Failed, Alternate, or Open.
Port Status	Operational link state of the REP port: None, Init Down, No Neighbor, One Way, Two Way, Flapping, Wait, or Unknown.

Viewing STP Information in VLAN Domain Views and VLAN Overlays

You can view STP segment and port information in the Vision client in the map view. The icons displayed depend on whether you view the STP information in the VLAN domain view or in a VLAN overlay. Table 18-37 describes the icons and badges used to represent STP link and port information.

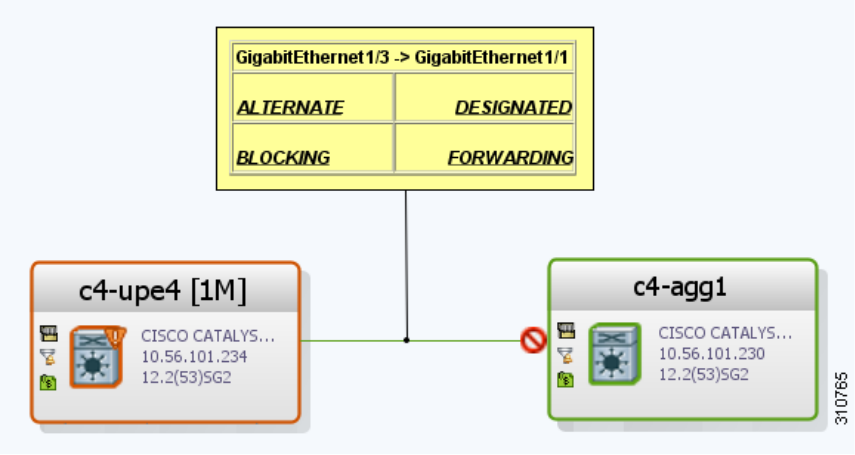
Table 18-37 STP Information in VLAN Domain Views and Overlays

Item	Description	VLAN Domain View	VLAN Overlay
	The STP root bridge, or root of the STP tree, is indicated by an uppercase R.		
	An STP root port is the port at the root of the STP tree. Each switching entity in the network VLAN should have a port designated as the root port. The STP root port is indicated by an uppercase R on the Ethernet flow point that is designated the root port.		
	STP blocks some VLAN ports to ensure a loop-free topology. The blocked port is marked with a red deny badge on the side on which traffic is denied.		

To view additional STP information in a VLAN overlay, right-click an STP link and choose **Show Callouts**. The following STP port information is displayed as shown in Figure 18-36:

- Port name
- Port role
- Port state

Figure 18-36 STP Link Information in a VLAN Overlay



Viewing STP Properties for VLAN Service Links

To view STP properties for a VLAN service link, open the Link Properties window in one of the following ways:

- Double-click the VLAN service link.
- Right-click the VLAN service link, and choose **Properties**.

Figure 18-37 shows an example of the Link Properties window with STP information.

Figure 18-37 STP Properties in VLAN Service Link Properties Window

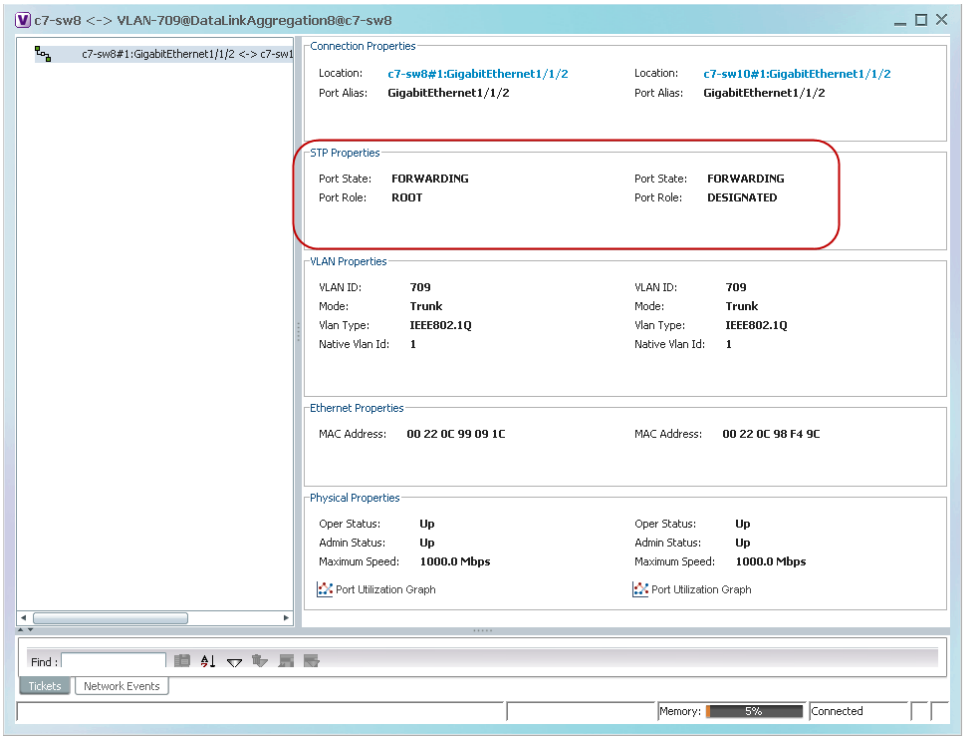


Table 18-38 describes the information that is displayed for STP for the VLAN service link.

Table 18-38 STP Properties in VLAN Service Link Properties Window

Field	Description
Port State	STP port state: Disabled, Blocking, Listening, Learning, or Forwarding,
Port Role	STP port role: Unknown, Backup, Alternative, Designated, Root, or Boundary.

Viewing VLAN Trunk Group Properties

VTP is a Layer 2 multicast messaging protocol that manages the addition, deletion, and renaming of VLANs on a switched network-wide basis.

The Vision client displays VTP information in the logical inventory. VTP information is shown only for Cisco devices that support VTP, and support is provided only for VTP Version 1 and 2. Support for Version 3 is limited to the additional attributes that are supported by the version, such as primary and secondary server. No support is provided for the display of VTP information at the port (trunk) level.

The Vision client shows all VTP modes: Server, Client, Transparent, and Off. For each mode, the Vision client displays the relevant mode information such as VTP domain, VTP mode, VTP version, VLAN trunks, and the trunk encapsulation. The Vision client also displays VTP domain information in a view that includes a list of all switches that are related to these domains, their roles (server, client, and so on), and their VTP properties.

To view VTP properties:

Step 1 In the Vision client, choose **Network Inventory > VTP Domains**.

Step 2 Double-click the VTP domain you want to view.

The VTP Domain Properties window is displayed as shown in Figure 18-38.

Figure 18-38 VTP Domain Properties Window in Logical Inventory

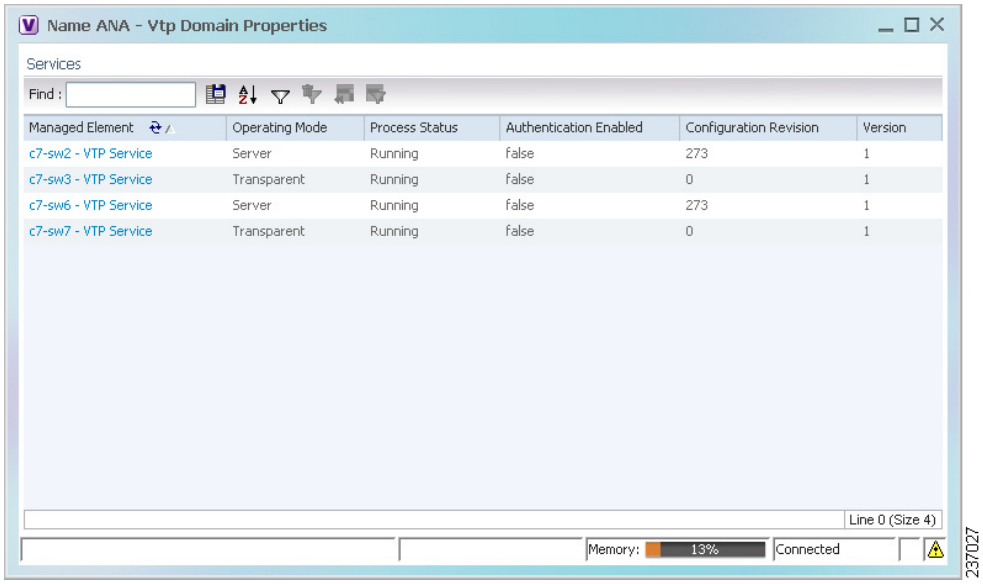


Table 18-39 describes the information that is displayed in the VTP Domain Properties window.

Table 18-39 VTP Domain Properties Window

Field	Description
Managed Element	Managed element name, hyperlinked to VTP in logical inventory.
Operating Mode	VTP operating mode: • Server—Allows VLAN creation, modification, and deletion, and specification of other configuration parameters for the entire VTP domain. Server is the default mode. • Client—Same behavior as VTP server, except VLANs cannot be created, changed, or deleted. • Transparent—The device does not participate in the VTP. The device does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, the device forwards received VTP advertisements out of their trunk ports in VTP Version 2. • Off—The device does not participate in VTP and does not forward VTP advertisements.
Process Status	Status of the VTP process: Running or Disabled.
Authentication Enabled	Whether or not VTP authentication is enabled: True or False. Authentication ensures authentication and integrity of switch-to-switch VTP messages. VTP Version 3 introduces an additional mechanism to authenticate the primary VTP server as the only device allowed to change the VLAN configuration on a network-wide basis.
Configuration Revision	32-bit number that indicates the level of revision for a VTP packet. Each VTP device tracks the VTP configuration revision number that is assigned to it. Most VTP packets contain the VTP configuration revision number of the sender.
Version	VTP version: 1, 2, or 3.

Step 3 To view the VTP properties at the device, double-click the VTP domain.

Table 18-40 describes the VTP information that is displayed in the inventory window content pane.

Table 18-40 VTP Properties in Inventory

Field	Description
Operating Mode	VTP operating mode: Server, Client, Transparent, or Off.
Domain Name	VTP domain name.
Version	VTP version: 1, 2, or 3.
Pruning	Whether or not VTP pruning is enabled: True or False. VTP pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.

Table 18-40 VTP Properties in Inventory (continued)

Field	Description
Configuration Revision	32-bit number that indicates the level of revision for a VTP packet.
Authentication	Whether or not VTP authentication is enabled: True or False.

Step 4 When finished, press **Ctrl** + **F4** to close each VTP properties window.

Viewing VLAN Bridge Properties

You can view VLAN bridges provisioned on a device by displaying the device in the Vision client inventory window and choosing Bridges in logical inventory.

To view VLAN bridge properties:

Step 1 In the Vision client, double-click the device containing the VLAN bridges you want to view.

Step 2 In the **Inventory** window, choose **Logical Inventory > Bridges >** *bridge*.

VLAN bridge properties are displayed as shown in Figure 18-39.

Figure 18-39 VLAN Bridge Properties in Logical Inventory

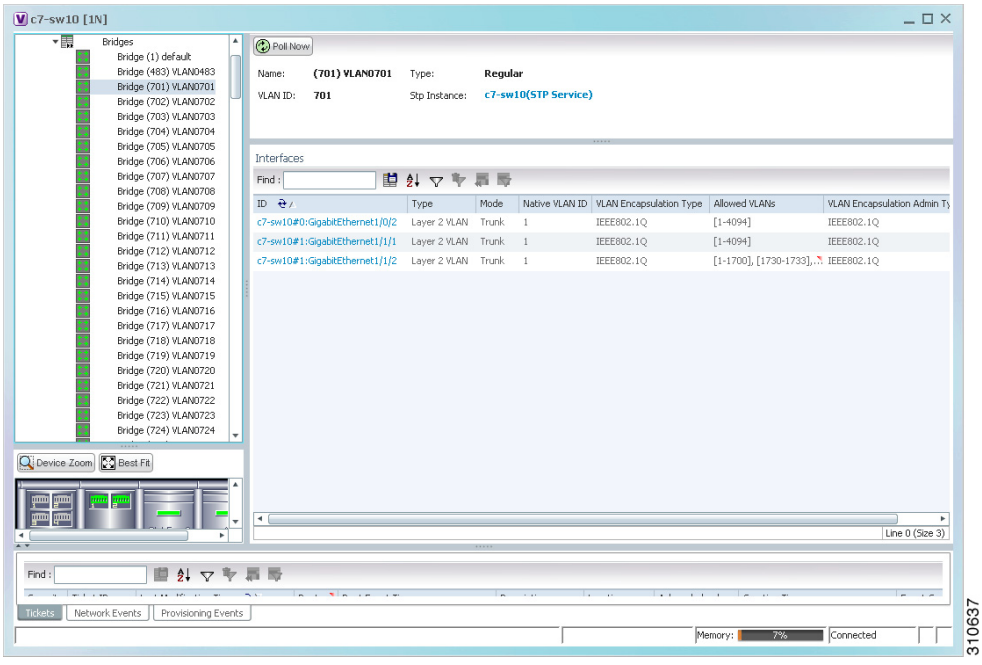


Table 18-41 describes the information that is displayed. Depending on the bridge configuration, any of the tabs might be displayed for the selected bridge.

Table 18-41 VLAN Bridge Properties

Field	Description
Name	VLAN bridge name.
Type	VLAN bridge type.
MAC Address	VLAN bridge MAC address.
VLAN ID	VLAN bridge VLAN identifier.
STP Instance	STP instance information, hyperlinked to the STP entry in logical inventory.
Bridge Table Tab	
MAC Address	Bridge MAC address.
Port	Port associated with the bridge, hyperlinked to the interface in physical inventory.
Interfaces Tab	
ID	VLAN interface identifier, hyperlinked to the interface in physical inventory.
Type	VLAN interface type, such as Layer 2 VLAN.
Mode	VLAN interface configuration mode: • Unknown—The interface is not VLAN aware. • Access—Puts the interface into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes nontrunking. • Dynamic Auto—The interface can convert the link to a trunk link. The interface becomes a trunk if the neighbor interface is set to Trunk or Dynamic Desirable mode. • Dynamic Desirable—The interface actively attempts to convert the link to a trunk link. The interface becomes a trunk if the neighboring interface is set to Trunk, Dynamic Desirable, or Dynamic Auto mode. Dynamic Desirable is the default mode for all Ethernet interfaces. • Trunk—Puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link. The interface becomes a trunk interface even if the neighbor interface is not a trunk interface. • Dot1Q Tunnel—Configures the interface as a tunnel (nontrunking) port to be connected in an asymmetric link with an 802.1Q trunk port. 802.1Q tunneling is used to maintain customer VLAN integrity across a service provider network.
Native VLAN ID	VLAN Identifier (VID) associated with this VLAN. The range of the VLAN ID is 1 to 4067.
VLAN Encapsulation Type	Type of encapsulation configured on the VLAN, such as IEEE 802.1Q.

Table 18-41 VLAN Bridge Properties (continued)

Field	Description
Allowed VLANs	List of the VLANs allowed on this VLAN interface.
VLAN Encapsulation Admin Type	VLAN administration encapsulation type, such as IEEE 802.1Q.
EFPs Tab	
EFP ID	EFP identifier.
Operational State	EFP operational state.
VLAN	VLAN identifier.
Inner VLAN	CE-VLAN identifier.
Translated VLAN	Translated VLAN identifier.
Translated Inner VLAN	Translated CE-VLAN identifier.
Binding Port	Hyperlinked entry to the port in physical inventory.
Description	Brief description of the EFP.
Pseudowires Tab	
ID	Pseudowire identifier, hyperlinked to the VLAN entry in Bridges in logical inventory.
Peer	Identifier of the pseudowire peer, hyperlinked to the entry in the Pseudowire Tunnel Edges table in logical inventory.
Tunnel ID	Tunnel identifier.
Tunnel Status	Status of the tunnel: Up or Down.
Peer Router IP	IP address of the peer router for this pseudowire.
Sub Interfaces Tab	
BER	VLAN bit error rate.
Interface Name	Interface on which the VLAN is configured.
VLAN Type	Type of VLAN, such as Bridge or IEEE 802.1Q.
Operational State	Subinterface operational state.
VLAN ID	VLAN identifier.
Inner VLAN	CE-VLAN identifier.

Step 3 When finished, press **Ctrl** + **F4** to close each VLAN Bridge properties window.

Using Commands to Work With VLANs

The following commands can be launched from the physical inventory by right-clicking an Ethernet slot and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see Permissions for Managing Carrier Ethernet, page B-12). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 18-42 VLAN Commands

Command	Inputs Required and Notes
Create VLAN	VLAN ID, VLAN Context Name, Bind Interface Name, Status
Modify VLAN	VLAN ID, Delete Bind Interface, Context Name, Bind Interface Name, Status
Delete VLAN	VLAN ID

Working with VXLANs

The following topics provide information and properties for working with VXLANs.

Understanding Virtual Extensible LAN (VXLAN) and BGP EVPN Address Family, page 18-90

Viewing VXLAN Properties, page 18-91

Understanding Virtual Extensible LAN (VXLAN) and BGP EVPN Address Family

Virtual Extensible LAN (VXLAN) is an overlay virtual network technology that is built on top of existing network Layer 2 and Layer 3 technologies to support elastic compute architectures.VXLAN uses VXLAN Identifier (VNI) that is similar to a VLAN ID to identify a user. VNI is a 24 bit ID which enables scalability of up to 16 million VNIs. Also, it is interchangeable with VXLAN Segment ID.

VXLAN architecture consists of following devices.

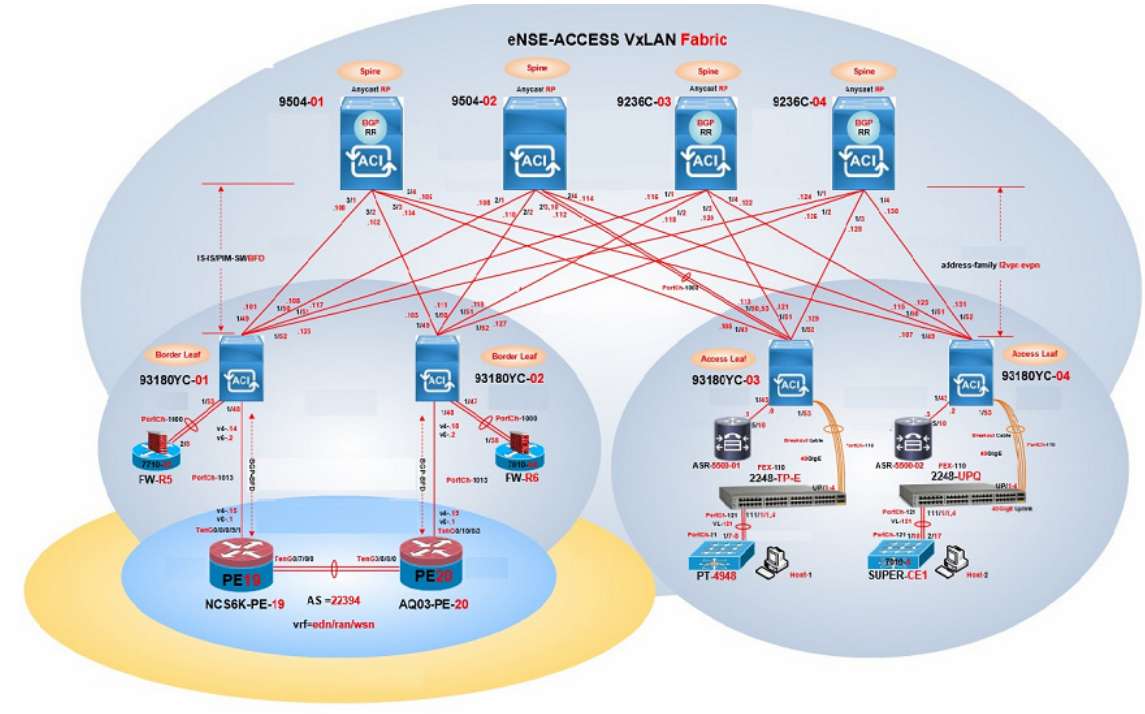
- Spine Devices— Spine devices are responsible for learning infrastructure routes and end-host subnet routes. Leaf devices communicate with their peers through Spine devices. Spine layer is the backbone of the network and is responsible for interconnecting all leaf switches fabric.
- Access Leaf Devices—Consists of access switches that connect to Ethernet devices such as servers (host interfaces)
- Border Leaf Devices—Connects to external network devices or services like router ports.

Note VXLAN is enabled only on Leaf devices and not on Spine devices. BGP is used as an underlay protocol in Spine devices.

Prime Network 5.3 supports VXLAN and BGP EVPN Address Family in inventory and fault. You can find associated VNIs information in logical inventory.

VXLAN Architecture

Figure 18-40 VXLAN Architecture



Viewing VXLAN Properties

To view VXLAN information:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > VXLANs > VXLAN**.

Table 18-43 describes the information that is displayed for VXLAN.

Table 18-43 VXLAN Information in Logical Inventory

Field	Description
Name	Name of the VXLAN.
VNI Details Tab	
VNI	VXLAN identifier used to identify a user.
NVE Interface	The name of the endpoint interface.
Multicast Group	The IP address of the multicast group.
State	The state of the VNI.
Mode	The mode of the VNI (For example, Control Plane or Data Plane)

Table 18-43 VXLAN Information in Logical Inventory (continued)

Field	Description
Layer Type	The type of the layer of the VNI. For example, L2 for a bridge/VLAN and L3 for a VRF.
Associated VLAN	The link to the associated entity, which when clicked will highlight the associated **Bridges** record under the **Bridges node**.
Associated VRF	The link to the associated entity, which when clicked will highlight the Associated **VRF** record under the **VRF node**.
Flags	Displays the flag information pertaining to the VNI.
VNI Neighbors Tab	
NVE Interface	The name of the endpoint interface.
Peer IP	Remote peer IP address.
Peer State	State of the remote peer. For example, Up or Down.
Learn Type	The learn type of the peer (For example, Control or Data Plane).
Peer UP Time	The amount of time the interface has been active.
Router MAC Address	MAC address of the router.

Mapping Associated VNI to Bridges

To view the VXLAN ID associated with a bridge:

1. Double-click the required device in the Vision client.
2. In the **Logical Inventory** window, choose **Logical Inventory** > Context > **Bridges** > **Bridge**.
3. Click the required bridge. The **Associated VNI** field in the content pane displays the VXLAN ID associated with the bridge or VLAN. You can click the link to go to the corresponding VNI row in the VNI Details pane.

Note The **Associated VNI** field is not visible in the content pane if there is no VNI associated with the bridge.

Understanding Unassociated Bridges

Some switching entities might not belong to a flow domain, such as a network VLAN, a VPLS instance, or a network pseudowire. These switching entities are referred to as *unassociated bridges*.

In addition, a switching entity that belongs to a network VLAN is considered an unassociated bridge if it meets both of the following criteria:

- The network VLAN contains a null Ethernet flow domain (EFD).
- The switching entity contains no switch ports.

Unassociated bridge switching entities can hold Ethernet flow points that serve as termination points on different network VLANs. If these switching entities are added to a map with the relevant VLANs, the links are displayed in the Vision client map.

Adding Unassociated Bridges

The Vision client enables you to add unassociated bridges to maps and to view their properties.

To add an unassociated bridge to a map:

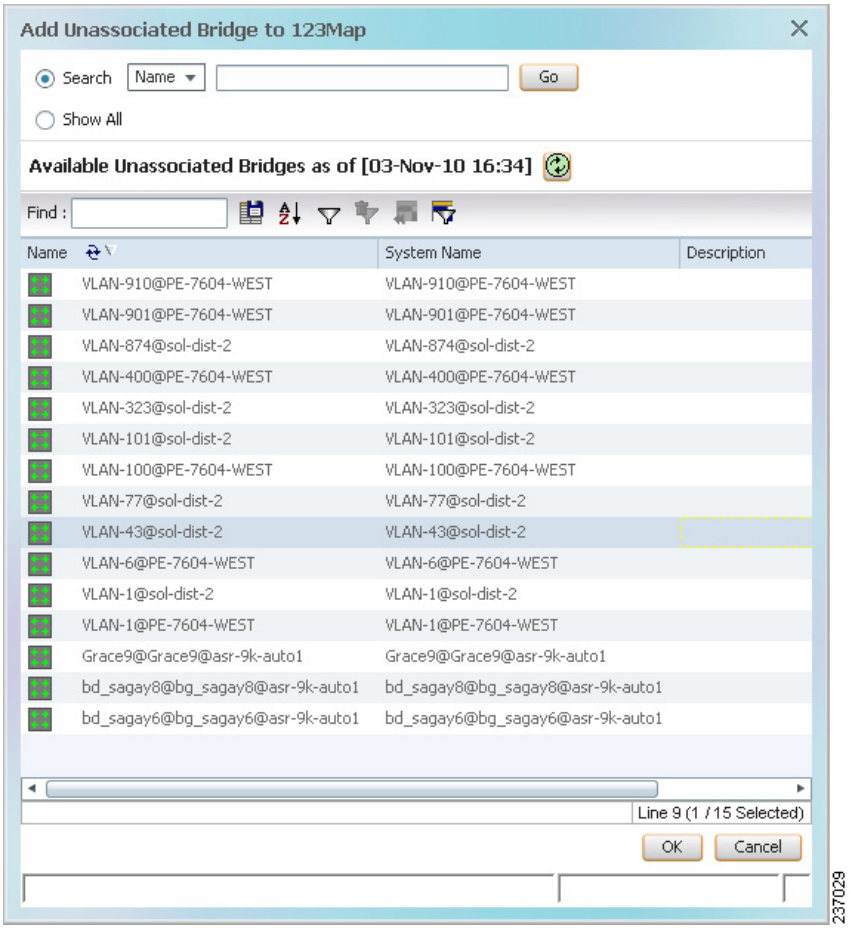
Step 1 In the Vision client, select the required map or domain.

Step 2 Open the Add Unassociated Bridge dialog box in one of the following ways:

- Choose **File Add to Map > Unassociated Bridge**.
- In the toolbar, click **Add to Map** and choose **Unassociated Bridge**.

Figure 18-41 shows an example of the Add Unassociated Bridge dialog box.

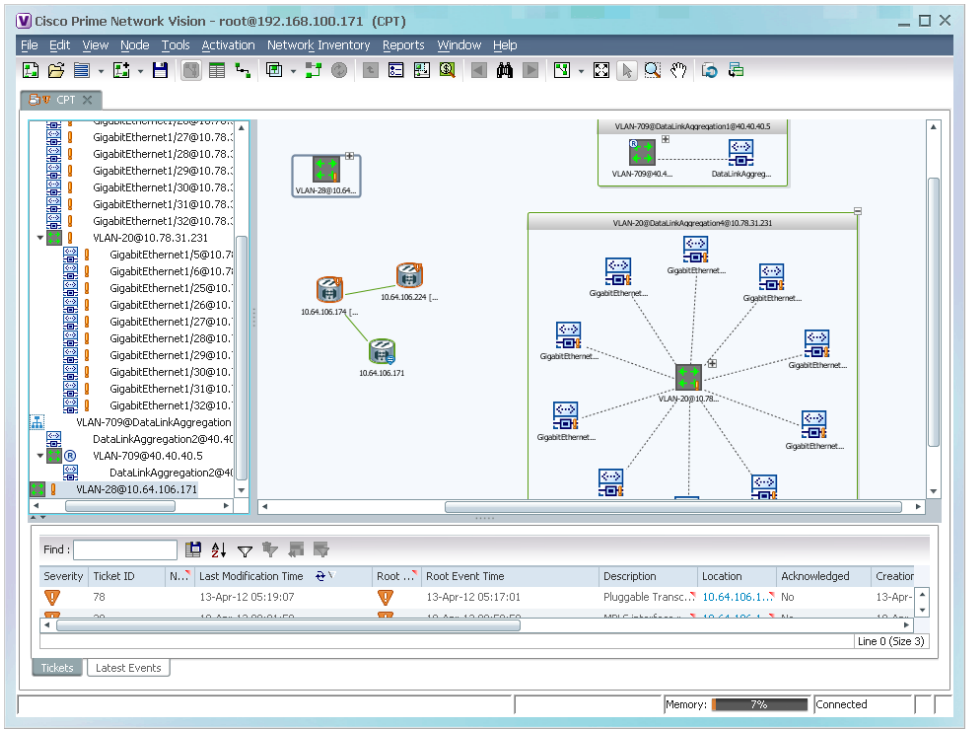
Figure 18-41 Add Unassociated Bridge Dialog Box



Step 3 In the Add Unassigned Bridge to *domain* dialog box, select the required bridge and click **OK**.

The map is refreshed and displays the newly added bridge as shown in Figure 18-42.

Figure 18-42 Unassociated Bridge in the Vision Window



Working with Ethernet Flow Point Cross-Connects

Prime Network automatically discovers Ethernet flow point (EFP) cross-connects, also known as locally switched EFPs. Prime Network also identifies changes in already identified EFP cross-connects, such as cross-connect deletions or changes. Cross-connect changes can occur when one side of the cross-connect is removed or replaced.

Prime Network also associates the VLANs that contain the EFPs that are part of the cross-connects. If the cross-connect contains a range EFP, which represents a range of VLANs, and you add the related VLANs to a map, the Vision client displays the links between them and the cross-connect as well.

The Vision client enables you to add EFP cross-connects to maps and to view their properties in inventory, as described in the following topics:

- Adding EFP Cross-Connects, page 18-94
- Viewing EFP Cross-Connect Properties, page 18-95

Adding EFP Cross-Connects

To add an EFP cross-connect to a map:

Step 1 In the Vision client, select the map to which you wish to add the cross-connect.

Step 2 Open the Add EFP Cross-Connect dialog box in one of the following ways:

- Choose **File Add to Map > Cross Connect**.
- In the toolbar, click **Add to Map** and choose **Cross Connect**.

Step 3 In the Add EFP Cross Connect to *domain* dialog box, select the required EFP cross-connect and click **OK**.

The map is refreshed and displays the newly added EFP cross-connect.

Viewing EFP Cross-Connect Properties

To view EFP cross-connect properties in the Vision client, do either of the following:

- Select the EFP cross-connect with the properties you want to view, and choose **Node > Properties**.
- Double-click the device configured with an EFP cross-connect and, in the inventory window, choose **Logical Inventory > Local Switching > Local Switching Entity**.

The information that is displayed for EFP cross-connects is the same in both the Local Switching Entry Properties window and in the Local Switching Table in logical inventory (as shown in Figure 18-43).

Figure 18-43 Local Switching Table in Logical Inventory

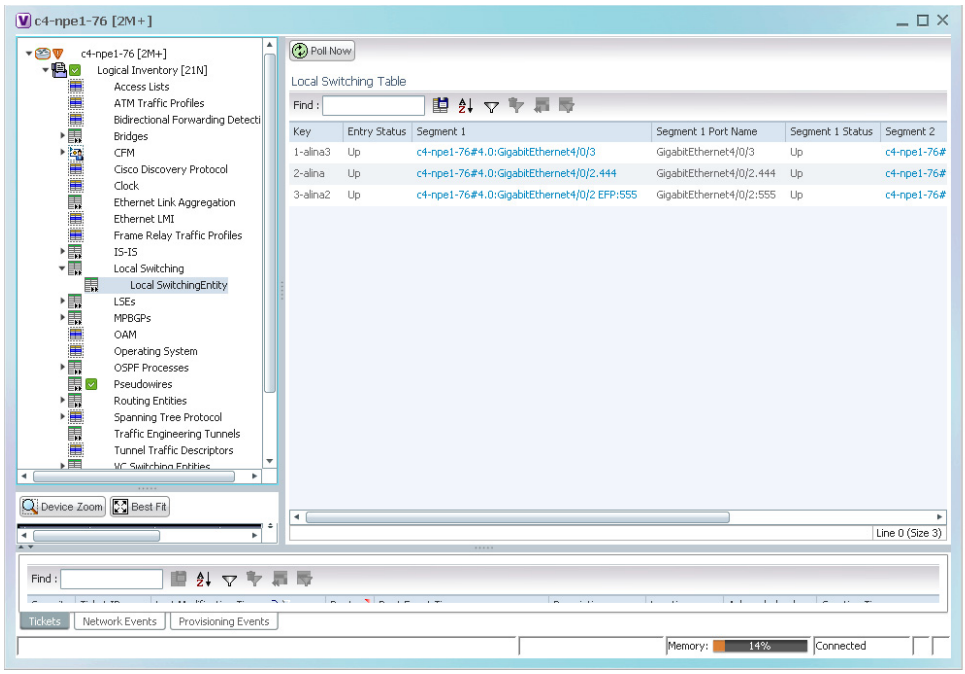


Table 18-44 describes the information displayed for the EFP cross-connects in the Local Switching Table.

Table 18-44 EFP Cross-Connect Properties in Local Switching Table

Field	Description
Key	Entry key for the cross-connect group.
Entry Status	Status of the cross-connect: Down, Unresolved, or Up.

Table 18-44 EFP Cross-Connect Properties in Local Switching Table (continued)

Field	Description
Segment 1	Identifier of the first cross-connect segment, hyperlinked to the relevant entry in physical inventory.
Segment 1 Port Name	Identifier of the first cross-connect segment port.
Segment 1 Status	Status of the first cross-connect segment, such as Admin Up, Admin Down, Oper Down, or Up.
Segment 2	Identifier of the second cross-connect segment, hyperlinked to the relevant entry in physical inventory.
Segment 2 Port Name	Identifier of the second cross-connect segment port.
Segment 2 Status	Status of the second cross-connect segment, such as Admin Up, Admin Down, Oper Down, or Up.

Working with VPLS and H-VPLS Instances

Virtual Private LAN Service (VPLS) is a Layer 2 VPN technology that provides Ethernet-based multipoint-to-multipoint communication over MPLS networks. VPLS allows geographically dispersed sites to share an Ethernet broadcast domain by connecting sites through pseudowires. The network emulates a LAN switch or bridge by connecting customer LAN segments to create a single bridged Ethernet LAN.

Hierarchical VPLS (H-VPLS) partitions the network into several edge domains that are interconnected using an MPLS core. The edge devices learn only of their local N-PE devices and therefore do not need large routing table support. The H-VPLS architecture provides a flexible architectural model that enables Ethernet multipoint and point-to-point Layer 2 VPN services, as well as Ethernet access to Layer 3 VPN services, enabling service providers to offer multiple services across a single high-speed architecture.

Prime Network discovers the following VPLS-related information from the network and constructs VPLS instances:

- VSIs
- Pseudowires
- EFPs
- Switching entities

The Vision client enables you to:

- Add VPLS instances to a map—See Adding VPLS Instances to a Map, page 18-97.
- Apply VPLS overlays—See Applying VPLS Instance Overlays, page 18-98.
- View link details in VPLS overlays—See Viewing Pseudowire Tunnel Links in VPLS Overlays, page 18-99.
- View VPLS-related properties—See the following topics:
  - Viewing VPLS Instance Properties, page 18-101
  - Viewing Virtual Switching Instance Properties, page 18-102

  - Viewing VPLS Core or Access Pseudowire Endpoint Properties, page 18-104
  - Viewing VPLS Access Ethernet Flow Point Properties, page 18-106
- Configure VFI Autodiscovery and Signaling—Configuring VFI Autodiscovery and Signaling, page 18-107

You can delete a VPLS forward from the Vision client if it is displayed with the reconciliation icon.

Adding VPLS Instances to a Map

You can add the VPLS instances that Prime Network discovers to maps as required.

To add a VPLS instance to a map:

Step 1 In the Vision client, select the required map or domain.

Step 2 Open the Add VPLS Instance to *map* dialog box in either of the following ways:

- In the toolbar, choose **Add to Map > VPLS**.
- In the menu bar, choose **File > Add to Map > VPLS**.

Step 3 In the Add VPLS Instance dialog box, do either of the following:

- To search for specific elements:

  a. Choose **Search**.

  b. To narrow the display to a range of VPLS instances or a group of VPLS instances, enter a search string in the search field.

  c. Click **Go**.

  For example, if you enter `VPLS1`, the VPLS instances that have names containing the string VPLS1 are displayed.
- To view all available VPLS instances, choose **Show All** and click **Go**.

The VPLS instances that meet the specified search criteria are displayed in the Add VPLS Instance dialog box in table format. The dialog box also displays the date and time at which the list was generated. To update the list, click **Refresh**.

Note If an element is not included in your scope, it is displayed with the locked device icon.

For information about sorting and filtering the table contents, see Viewing a Table of NEs and Their Properties (List View), page 7-7.

Step 4 In the Add VPLS Instance dialog box, select the instances that you want to add. You can select and add multiple instances by pressing **Ctrl** while selecting individual instances or by pressing **Ctrl +Shift** to select a group of instances.

Step 5 Click **OK**.

The VPLS instance is displayed in the navigation pane and in the content area. In addition, any associated tickets are displayed in the ticket pane.

The VPLS instance information is saved with the map in the Prime Network database.

Applying VPLS Instance Overlays

An VPLS instance overlay allows you to isolate the parts of a network that are being used by a specific VPLS instance.

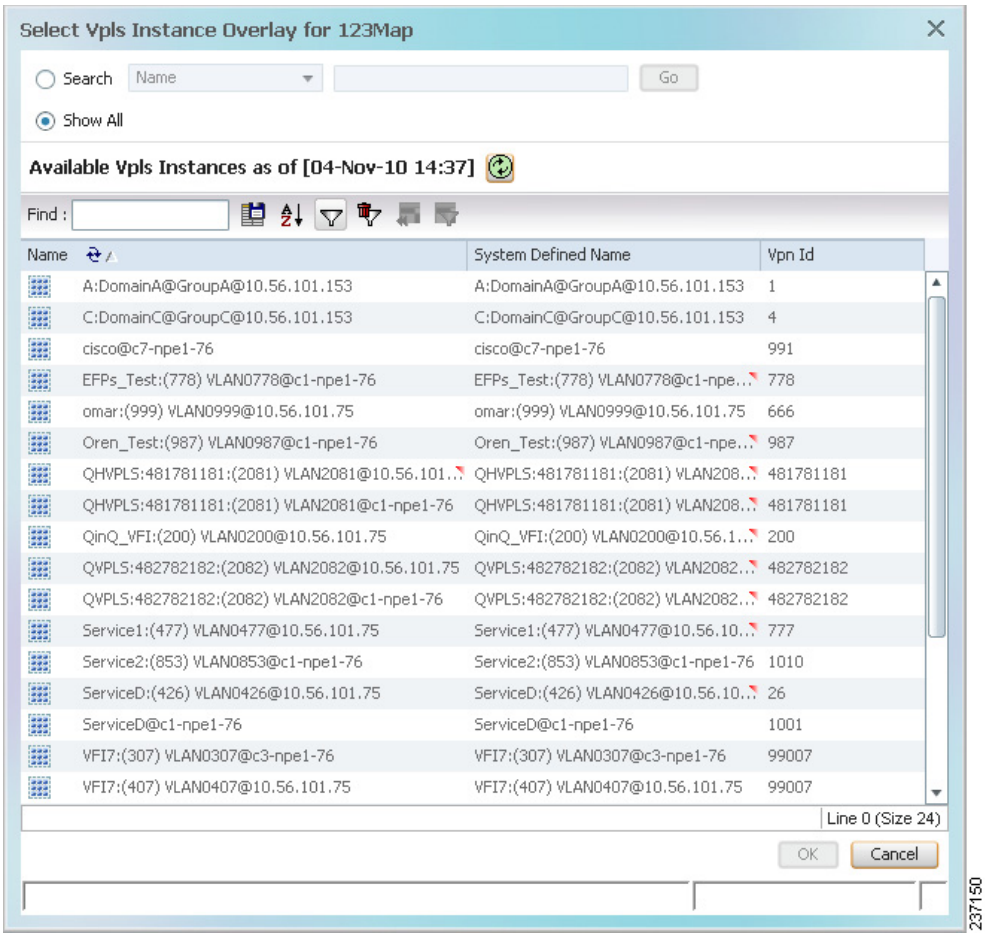
To apply a VPLS instance overlay:

Step 1 In the Vision client, choose the map in which you want to apply an overlay.

Step 2 From the toolbar, choose **Choose Overlay Type > VPLS**.

Figure 18-44 shows an example of the Select VPLS Instance Overlay for *map* dialog box.

Figure 18-44 Select VPLS Instance Overlay Dialog Box

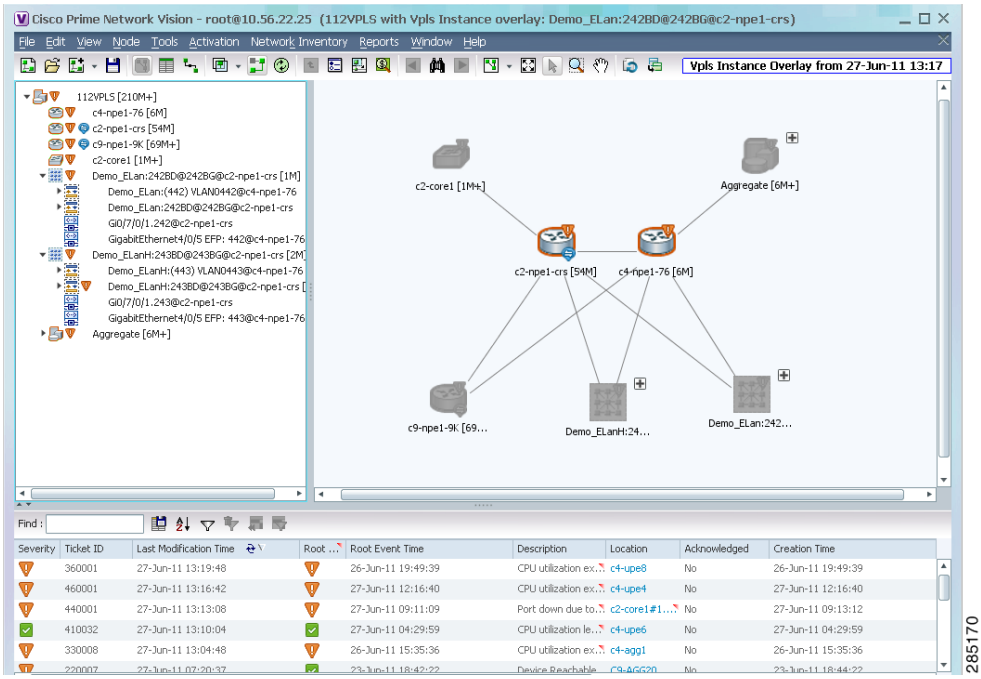


Step 3 Select the required VPLS instance for the overlay.

Step 4 Click **OK**.

The elements being used by the selected VPLS instance are highlighted in the map while the other elements are dimmed, as shown in Figure 18-45.

Figure 18-45 VPLS Instance Overlay in Vision Window



Step 5 To hide and view the overlay, click **Hide Overlay/Show Overlay** in the toolbar. The button toggles depending on whether the overlay is currently displayed or hidden.

Step 6 To remove the overlay, choose **Choose Overlay Type > None**.

Viewing Pseudowire Tunnel Links in VPLS Overlays

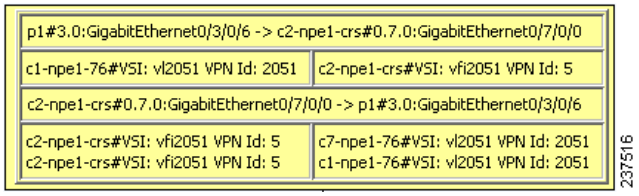
When a VPLS overlay is applied to a map in the Vision client, you can view the details of the pseudowires that are interconnected through selected links.

To view unidirectional or bidirectional pseudowire traffic links when a VPLS overlay is applied to a map:

Step 1 Right-click the required link in the overlay, and choose **Show Callouts**. The link must be visible (not dimmed) in the map.

Link information is displayed as shown in Figure 18-46.

Figure 18-46 Link Callout Window for a VPLS Overlay



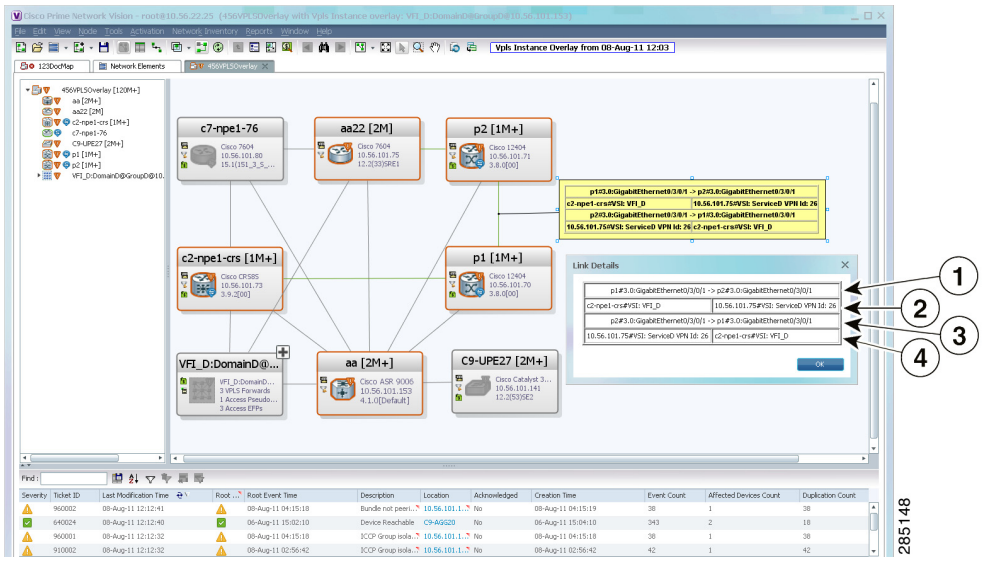
The callout window displays the following information for each link represented by the selected link:

- Link details and direction.
- Details of the sites using the link and the interlinks.

Step 2 To view the pseudowire link details, double-click the yellow callout window.

The details about the link are displayed in the Link Details window as shown in Figure 18-47.

Figure 18-47 Link Details Window for a VPLS Overlay



The Link Details window provides the following information:

1	Link details and direction. In this example, the link is from p1 to p2.
3	Link details and direction. In this example, the link is from p2 to p1.
2 and 4	Details of the pseudowire tunnel traversing this link.

Step 3 Click **OK** to close the Link Details window.

Step 4 To close the link callout window, right-click the selected link, then choose **Hide Callouts**.

Viewing VPLS-Related Properties

The Vision client enables you to view the properties of the following VPLS-related elements:

- VPLS instances—See Viewing VPLS Instance Properties, page 18-101.
- Virtual Switching Instances—Viewing Virtual Switching Instance Properties, page 18-102
- Tunnels—See Viewing VPLS Core or Access Pseudowire Endpoint Properties, page 18-104.
- Port connectors—See Viewing VPLS Access Ethernet Flow Point Properties, page 18-106.

Viewing VPLS Instance Properties

To view the properties of a VPLS instance in the Vision client, open the VPLS Instance Properties window in either of the following ways:

- In the navigation pane or the map pane, right-click the VPLS instance and choose **Properties**.
- In the navigation pane or the map pane, select the VPLS instance and choose **Node > Properties**.

Figure 18-48 shows an example of the VPLS Instance Properties window.

Figure 18-48 VPLS Instance Properties Window

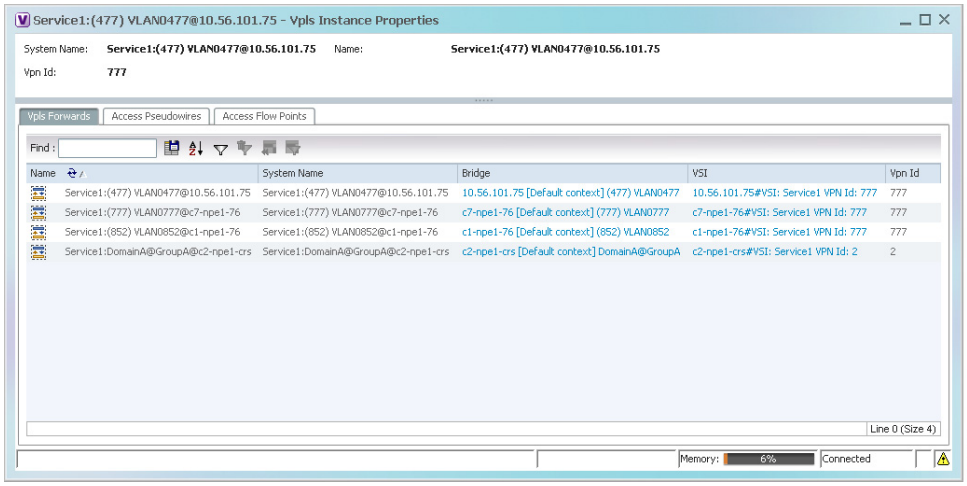


Table 18-45 describes the information that is displayed for VPLS instance properties.

The tabs that appear in the window depend on the VPLS instance and its configuration.

Table 18-45 VPLS Instance Properties

Field	Description
System Name	Name that Prime Network assigns to the VPLS instance.
Name	User-defined name of the VPLS instance. When the VPLS instance is created, the system name and this name are the same. If you change the name of the VPLS instance (right-click, then choose **Rename**), the changed name appears in this field whereas the system name retains the original name.
VPN ID	VPN identifier used in an MPLS network to distinguish between different VPLS traffic.
VPLS Forwards Tab	
Name	User-defined name of the VPLS forward.
System Name	Name that Prime Network assigns to the VPLS forward.
Bridge	Bridge that the VSI is configured to use, hyperlinked to the bridge table in logical inventory.
VSI	VSI hyperlinked to the relevant entry in logical inventory.
VPN ID	VPN identifier for the VSI.

Table 18-45 VPLS Instance Properties (continued)

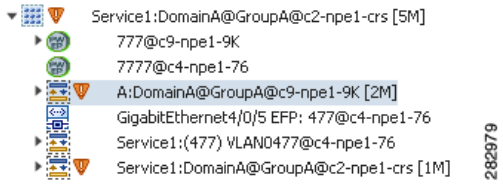
Field	Description
Access Pseudowires Tab	
Name	Pseudowire name.
Port	VSI on which the pseudowire is configured, hyperlinked to the entry in logical inventory.
Local Router IP	Local router IP address on which the pseudowire is configured.
Tunnel ID	Virtual circuit identifier of the pseudowire.
PTP Tunnel	Hyperlinked entry to the pseudowire properties in logical inventory.
Peer Router IP	Peer router IP address on which the pseudowire is configured.
Peer OID	Hyperlinked entry to the pseudowire properties of the peer.
Pseudowire Type	Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, or SAToP.
Pseudowire Edge Binding Type	Pseudowire endpoint association: • 0—Unknown • 1—Connection termination point • 2—Ethernet flow point • 3—Switching entity • 4—Pseudowire switching entity • 5—VPLS forward
Access Flow Points Tab	
Name	Access flow point name. Double-click to view port connector properties.
Port	Interface configured as a flow point, hyperlinked to the interface in physical inventory.

Viewing Virtual Switching Instance Properties

To view VSI properties in the Vision client, open the VSI properties window in either of the following ways:

- Double-click the required device and, in the **Inventory** window, choose **Logical Inventory > VSIs >** *vsi*.
- In the navigation pane, expand the VPLS instance, right-click the required VPLS forward, and choose **Inventory** or **Properties**. (See Figure 18-49.)

Figure 18-49 VPLS Forward in Vision Window Navigation Pane



If you right-click the VPLS forward and choose **Inventory**, the inventory window is displayed. If you right-click the VPLS forward and choose **Properties**, the VSI Properties window is displayed. The information displayed is the same for both options.

VSI properties are displayed as shown in Figure 18-50.

Figure 18-50 VSI Properties in Logical Inventory

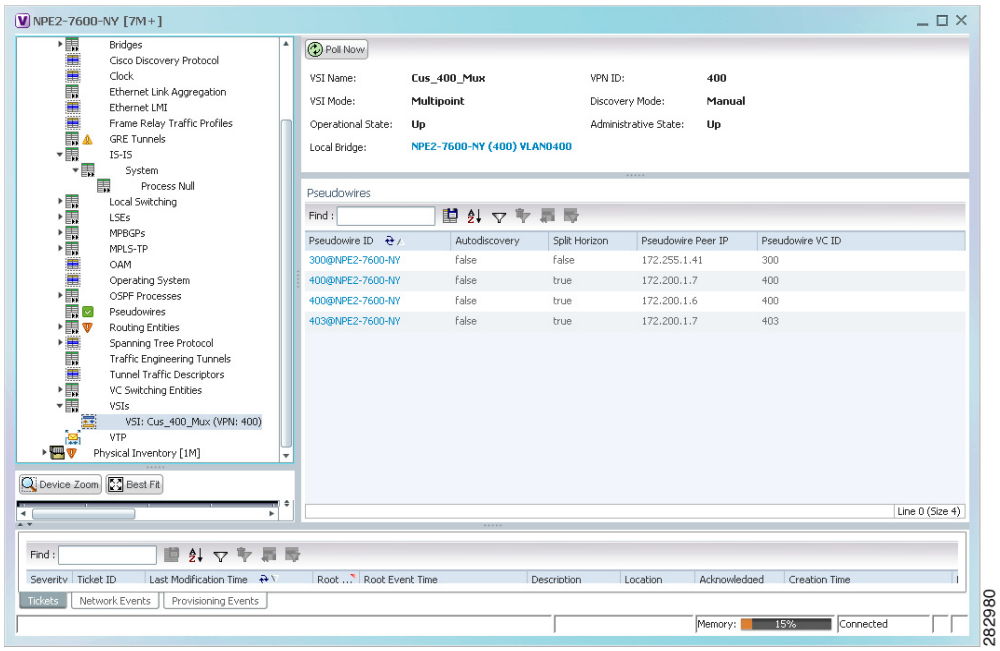


Table 18-46 describes the information that is displayed for the selected VSI.

Table 18-46 VSI Properties in Logical Inventory

Field	Description
VSI Name	VSI name.
VPN ID	VPN identifier used in an MPLS network to distinguish between different VPLS traffic.
VSI Mode	VSI mode: Point-to-Point (default) or Multipoint.
Discovery Mode	VSI discovery mode: Manual, BGP, LDP, RADIUS, DNS, MSS/OSS, or Unknown.
Operational State	VSI operational status: Up or Down.
Administrative State	VSI administrative status: Up or Down.
Local Bridge	Local bridge, hyperlinked to the bridge in logical inventory.
Pseudowires Table	
Pseudowire ID	Pseudowire identifier, hyperlinked to the Tunnel Edges table under Pseudowires in logical inventory.
Autodiscovery	Whether the pseudowire was automatically discovered: True or False.
Split Horizon	SSH pseudowire policy that indicates whether or not packets are forwarded to the MPLS core: True or False.
Pseudowire Peer IP	IP address of the pseudowire peer.
Pseudowire VC ID	Pseudowire virtual circuit identifier.

Viewing VPLS Core or Access Pseudowire Endpoint Properties

Pseudowire endpoints are displayed under VPLS Instance (Access) or VPLS Forward (Core) in the Vision client navigation pane.

To view pseudowire endpoint properties for a VPLS instance, right-click the required pseudowire endpoint in the navigation pane, and choose **Properties**. (See Figure 18-51.)

Figure 18-51 VPLS Pseudowire in Vision Window Navigation Pane

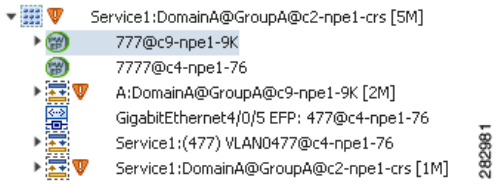


Figure 18-52 shows an example of the Tunnel Properties window that is displayed.

Figure 18-52 VPLS Tunnel Properties Window

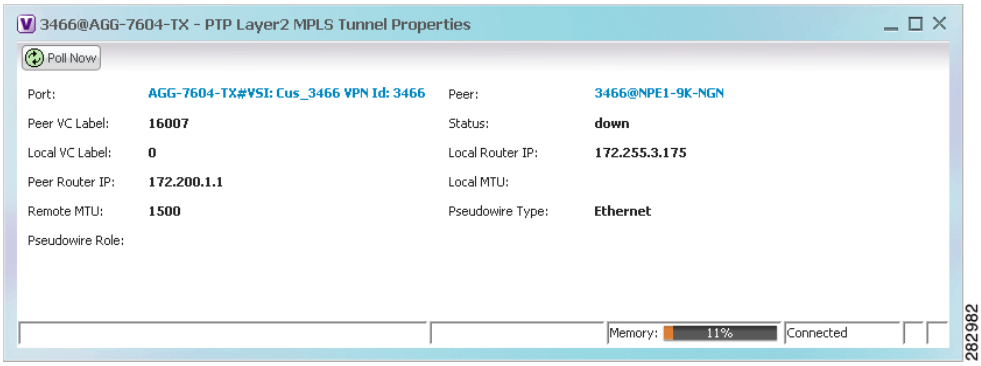


Table 18-47 describes the information that is displayed for pseudowire endpoint properties.

Table 18-47 Tunnel Properties Window

Field	Description
Port	VSI on which the pseudowire is configured, hyperlinked to the VSI in logical inventory.
Peer	Hyperlinked entry to the pseudowire endpoint peer pseudowires in logical inventory.
Peer VC Label	MPLS label that is used by this router to identify or access the tunnel. It is inserted into the MPLS label stack by the peer router.
Tunnel Status	Operational state of the tunnel: Up or Down.
Local VC Label	MPLS label that is used to identify or access the tunnel. It is inserted into the MPLS label stack by the local router.
Local Router IP	IP address of this tunnel edge, which is used as the MPLS router identifier.
Tunnel ID	Identifier that, along with the router IP addresses of the two pseudowire endpoints, identifies the PWE3 tunnel.
Peer Router IP	IP address of the peer tunnel edge, which is used as the MPLS router identifier.
Local MTU	Size, in bytes, of the MTU on the local interface.
Remote MTU	Size, in bytes, of the MTU on the remote interface.
Signaling Protocol	Protocol used by MPLS to build the tunnel, such as LDP or TDP.
Pseudowire Type	Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, or SAToP.

Viewing VPLS Access Ethernet Flow Point Properties

The ports that represent the attachment circuits to VPLS instances are displayed under VPLS instances in the Vision client navigation pane.

To view the properties for the Access Ethernet Flow Points configured for a VPLS instance, right-click the required interface in the navigation pane, and choose **Inventory**. (See Figure 18-53.)

Figure 18-53 VPLS Interface in Vision Window Navigation Pane

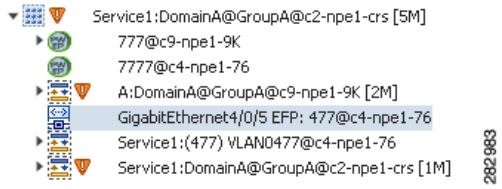
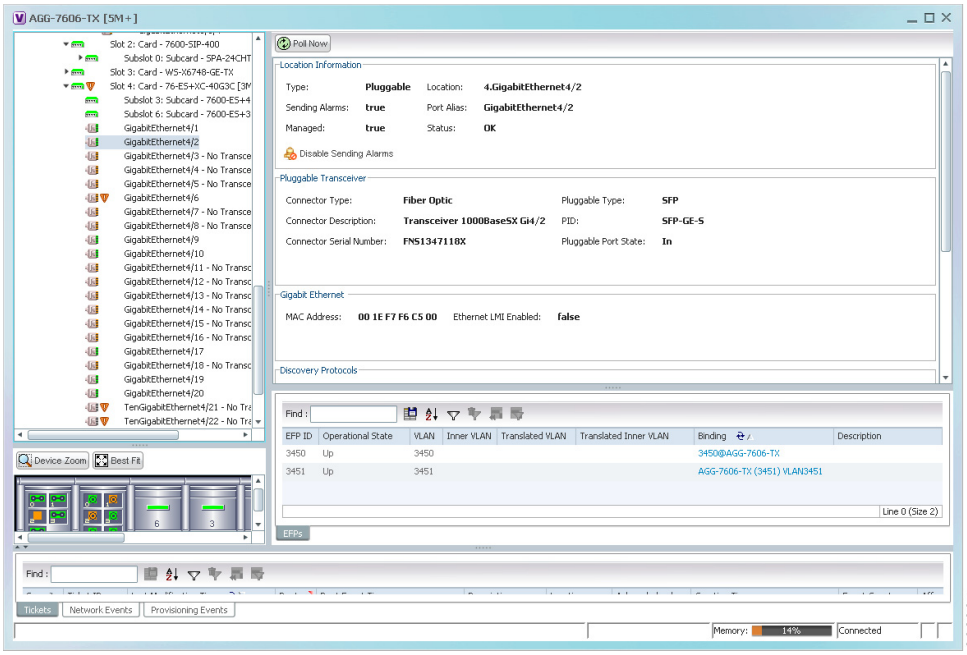


Figure 18-54 shows an example of the information displayed for the interface in physical inventory.

Figure 18-54 EFP Properties in Physical Inventory



The information displayed in this window is the same as that displayed when the interface is selected in physical inventory.

The following information is displayed, depending on the interface and its configuration:

- Location and interface details.
- Technology-related information, such as Ethernet CSMA/CD or ATM IMA properties.
- VLAN configuration details.
- List of the configured subinterfaces on the port. For more information on the Subinterfaces table, see Drilling Down Into a Port's Configuration Details (Including Services and Subinterfaces), page 8-17.

- List of the configured EFPs on the port. For more information on the EFPs table, see Viewing EFP Properties, page 18-51.
- List of VLAN mappings configured on the port. For more information about the VLAN Mappings table, see Viewing VLAN Mappings, page 18-70.

Configuring VFI Autodiscovery and Signaling

The following commands enable you to configure VFI autodiscovery and signalling at the device level or at the VSI Level. To find out if a device supports these commands, see the Cisco Prime Network 5.3 Supported Cisco VNEs.

Command	Navigation	Description
Configure VFI Autodiscovery and Signaling	**Logical Inventory** > *right-click the VSI* > **Commands** > **Configuration** > **Configure VFI Autodiscovery and Signaling**	Use this command to configure Autodiscovery and Signaling at the VFI level.
	Right-click the *ASR 9000 series device* > **Commands** > **Configuration** > **Configure VFI Autodiscovery and Signaling**	Use this command to configure Autodiscovery and Signaling at the device level.

Working with Pseudowires

Prime Network supports the discovery and modeling of Any Transport over MPLS (AToM) and Ethernet over MPLS (EoMPLS) domains that span multisegment pseudowires. After discovery is complete, you can add any of the pseudowires to a map, view their properties in logical inventory, or view their redundancy status. For information on the devices that support pseudowire technology, refer to *Cisco Prime Network 5.3 Supported Cisco VNEs*.

The following topics describe the options available to you for working with pseudowires in Prime Network:

- Adding Pseudowires to a Map, page 18-108
- Viewing Pseudowire Properties, page 18-110
- Displaying Pseudowire Information, page 18-112
- Viewing Pseudowire Redundancy Service Properties, page 18-113
- Applying Pseudowire Overlays, page 18-115
- Monitoring the Pseudowire Headend, page 18-117

Adding Pseudowires to a Map

You can add a pseudowire that Prime Network discovers to maps as required.

To add a pseudowire to a map:

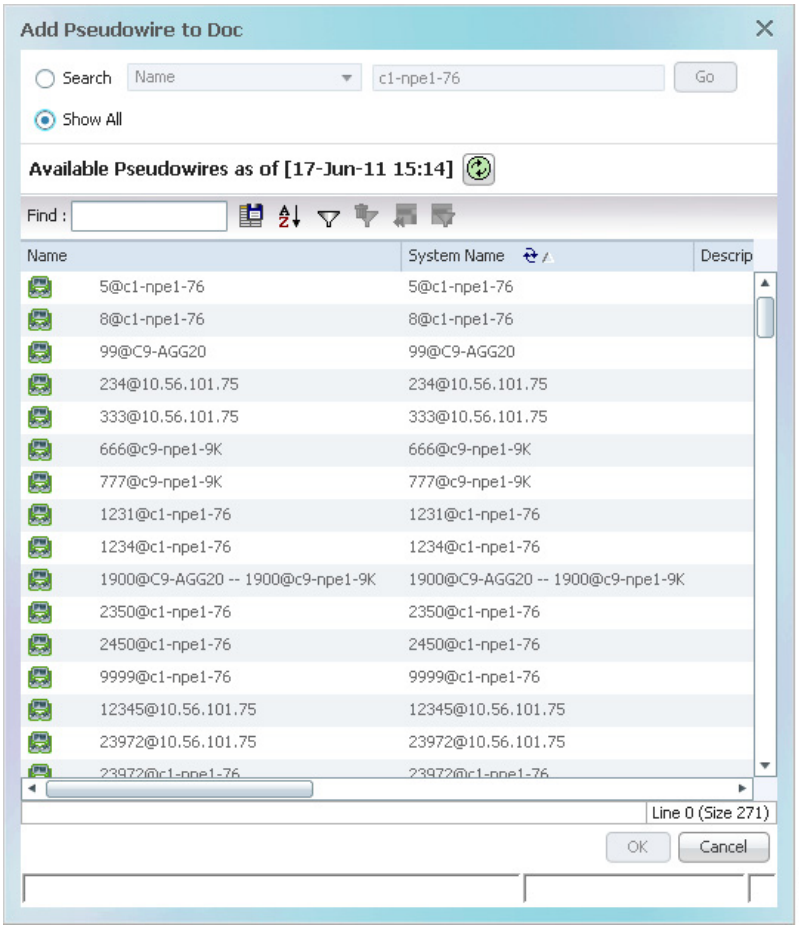
Step 1 In the Vision client, select the required map or domain.

Step 2 Open the Add Pseudowire to *map* dialog box in either of the following ways:

- In the toolbar, choose **Add to Map > Pseudowire**.
- In the menu bar, choose **File > Add to Map > Pseudowire**.

Figure 18-55 shows an example of the Add Pseudowire dialog box.

Figure 18-55 Add Pseudowire Dialog Box



Step 3 In the Add Pseudowire dialog box, do either of the following:

- To search for specific elements:

  a. Choose **Search**.

  b. To narrow the display to a range of pseudowire or a group of pseudowires, enter a search string in the search field.

  c. Click **Go**.

For example, if you enter `pseudo1`, the pseudowires that have names containing the string "pseudo1" are displayed.

- To view all available pseudowires, choose **Show All** and click **Go**.

The pseudowires that meet the specified search criteria are displayed in the Add Pseudowire dialog box in table format. The dialog box also displays the date and time at which the list was generated. To update the list, click **Refresh**.

Note If an element is not included in your scope, it is displayed with the locked device icon.

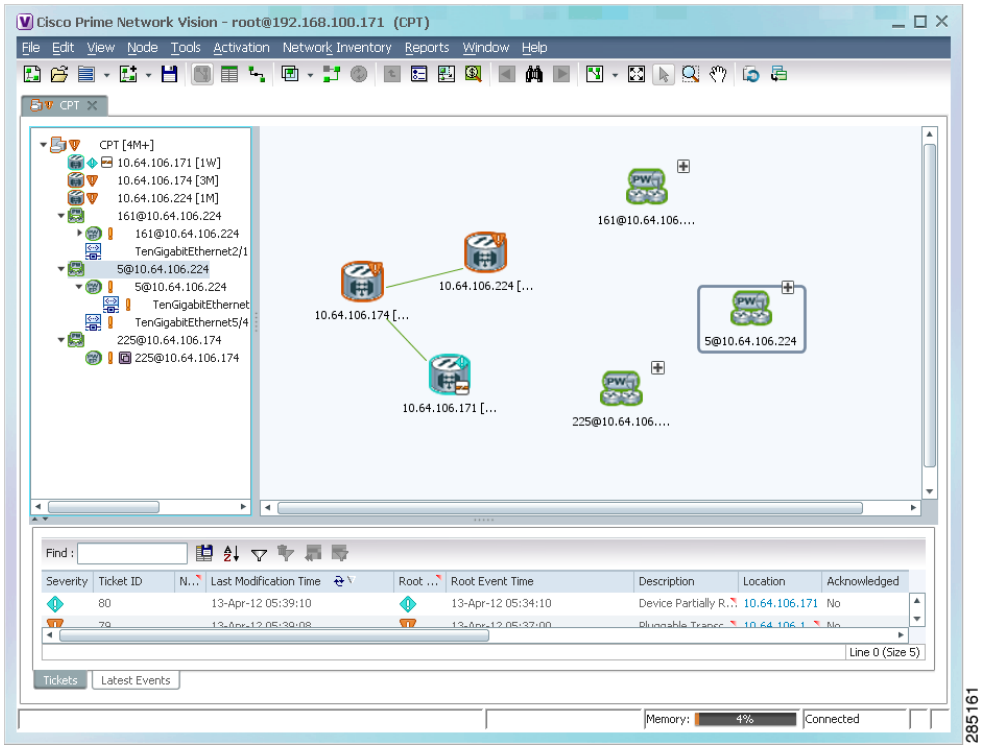
For information about sorting and filtering the table contents, see Viewing a Table of NEs and Their Properties (List View), page 7-7.

Step 4 In the Add Pseudowire dialog box, select the pseudowires that you want to add. You can select and add multiple pseudowires by pressing **Ctrl** while selecting individual pseudowires or by pressing **Ctrl +Shift** to select a group of pseudowires.

Step 5 Click **OK**.

The pseudowire is displayed in the navigation pane and in the content area. In addition, any associated tickets are displayed in the ticket pane. See Figure 18-56.

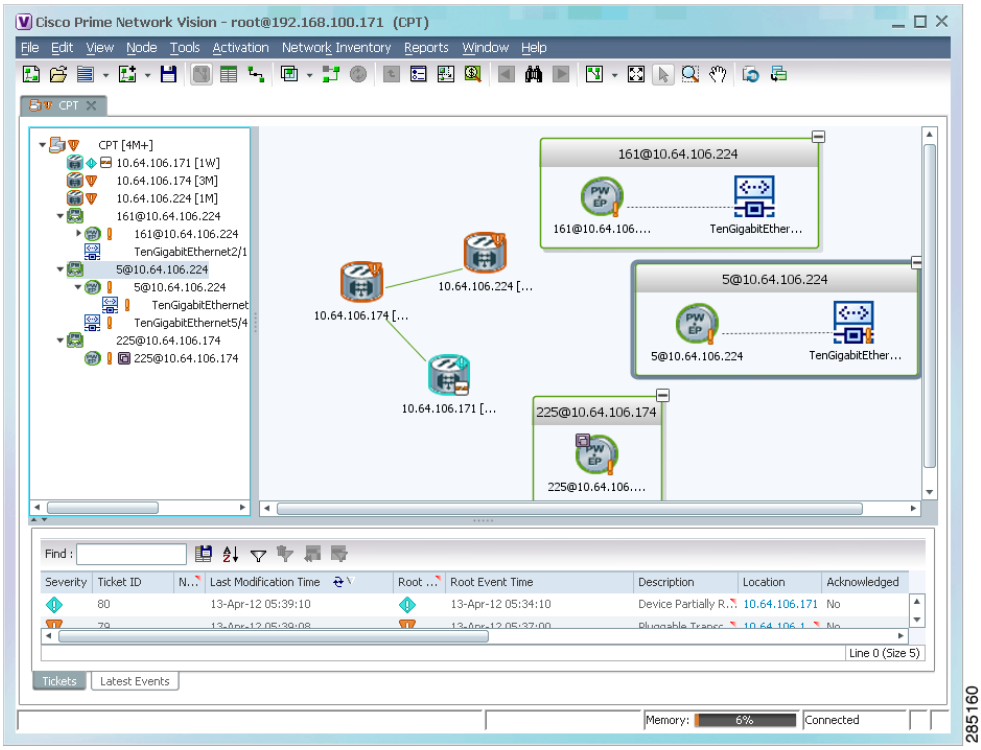
Figure 18-56 Pseudowire in Vision Map



Step 6 Click the pseudowire in the navigation pane or double-click the pseudowire in the map pane to view the pseudowire components, such as pseudowire endpoints, pseudowire switching entities, and terminating interfaces.

Figure 18-57 shows an example of an expanded pseudowire in the Vision client.

Figure 18-57 Pseudowire Components in Vision Maps



The pseudowire information is saved with the map in the Prime Network database.

Pseudowire discovery

As explained earlier, a pseudowire is a point-to-point connection between pairs of provider edge (PE) routers.

In a PW-HE configuration, the network PseudoWire service will include pseudowire edges. One of these edges will be connected to a dedicated ethernet flow point that will represent the pseudowire headend port.

Viewing Pseudowire Properties

To view pseudowire properties:

Step 1 In the Vision client, select the required map or domain.

Step 2 To view pseudowire endpoint properties configured on an element:

a. In the navigation or map pane, right-click the required element and then choose **Inventory**.

b. In the **Inventory** window, choose **Logical Inventory > Pseudowires**.

The Tunnel Edges table is displayed, listing the pseudowire endpoints configured on the selected element. For a description of the information contained in the Pseudowires Tunnel Edges table, see Table 17-29.

Step 3 To view the properties of a pseudowire that you added to a map, do either of the following:

- If the pseudowire icon is of the largest size, click the **Properties** button.
- Right-click the element, and then choose **Properties**.

The Pseudowire Properties window is displayed as shown in Figure 18-58.

Figure 18-58 Pseudowire Properties Window

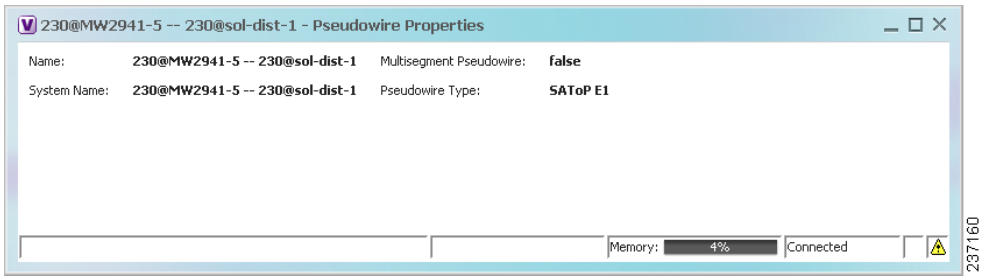


Table 18-48 describes the information presented in the Pseudowire Properties window.

Table 18-48 Pseudowire Properties Window

Field	Description
Name	Name of the pseudowire.
Multisegment Pseudowire	Whether or not the pseudowire is multisegment: True or False.
System Name	Internal or system-generated name of the pseudowire.
Pseudowire Type	Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, or SAToP.

Step 4 To view the properties of a pseudowire endpoint associated with a pseudowire, right-click the required pseudowire endpoint, and then choose **Properties**.

The Tunnel Properties window containing the pseudowire endpoint properties is displayed as shown in Figure 18-52 and described in Table 18-47.

Step 5 To view the properties of a pseudowire switching entity associated with the pseudowire, select the switching entity, and then choose **Node > Inventory**.

The Local Switching table is displayed as shown in Figure 18-43.

Table 18-44 describes the information displayed in the Local Switching table.

Step 6 To view the properties of the pseudowire endpoint that terminates on the subinterface, right-click the required interface, and then choose **Properties**.

Note The selected port must be an Ethernet subinterface for the Contained Current CTPs table to be displayed.

Table 18-49 describes the information displayed in the Contained Current CTPs table.

Table 18-49 Contained Current CTPs Table

Field	Description
Local Interface	The name of the subinterface or port, hyperlinked to the interface in physical inventory.
ID	The tunnel identifier, hyperlinked to Pseudowires Tunnel Edges table in logical inventory.
Peer	The peer tunnel identifier, hyperlinked to the peer pseudowire tunnel in logical inventory.
Tunnel ID	The identifier that, along with the router IP addresses of the two tunnel edges, identifies the tunnel.
Tunnel Status	The operational state of the tunnel: Up or Down.
Local Router IP	The IP address of this tunnel edge, which is used as the router identifier.
Peer Router IP	The IP address of the peer tunnel edge, which is used as the router identifier.
Pseudowire Type	Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, or SAToP.
Local MTU	The size, in bytes, of the MTU on the local interface.
Remote MTU	The size, in bytes, of the MTU on the remote interface.
Local VC Label	The MPLS label that is used by this router to identify or access the tunnel. It is inserted in the MPLS label stack by the local router.
Peer VC Label	The MPLS label that is used by this router to identify or access the tunnel. It is inserted in the MPLS label stack by the peer router.
Signaling Protocol	The protocol used to build the tunnel, such as LDP or TDP.
Preferred Path Tunnel	The path to be used for pseudowire traffic.

Step 7 To view the properties of an Ethernet flow point associated with the pseudowire, right-click the EFP and then choose Properties.

See Viewing EFP Properties, page 18-51 for the information that is displayed for EFPs.

Displaying Pseudowire Information

Use the following procedure to view Virtual Circuit Connectivity Verification (VCCV) and Control Channel (CC) information for a pseudowire endpoint. Your permissions determine whether you can run these commands (see Permissions for Managing Carrier Ethernet, page B-12). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Step 1 In the require map, double-click the required device configured for pseudowire.

Step 2 In the **Inventory** window, choose **Logical Inventory > Pseudowire**.

Step 3 In the Tunnel Edges table, right-click the required interface and choose **Commands > Show > Display Pseudowire**.

Step 4 In the Display Pseudowire dialog box, preview or execute the command. The following information is displayed:

- The element name.
- The command issued.
- The results, including:
  - VCCV: CC Type—The types of CC processing that are supported. The number indicates the position of the bit that was set in the received octet. The available values are:

    - CW [1]—Control Word

    - RA [2]—Router Alert

    - TTL [3]—Time to Live

    - Unkn [x]—Unknown

  - Elapsed time—The elapsed time, in seconds.

Step 5 Click **Close** to close the Display Pseudowire dialog box.

Viewing Pseudowire Redundancy Service Properties

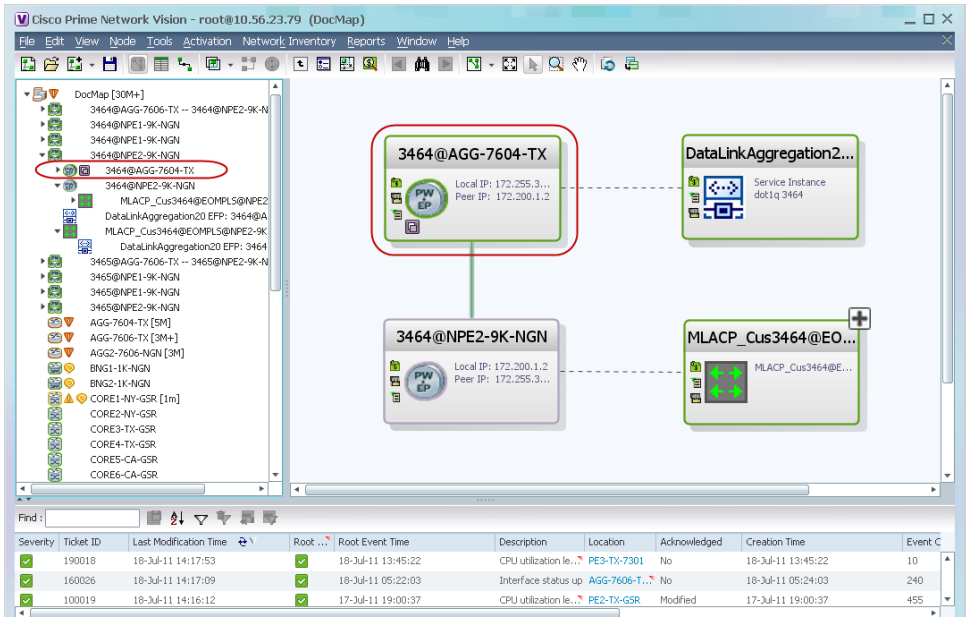
If a pseudowire is configured for redundancy service, a redundancy service badge is applied to the secondary (backup) pseudowire in the navigation and map panes in the Vision client. Additional redundancy service details are provided in the inventory window for the device on which the pseudowire is configured.

To view redundancy service properties for pseudowires:

Step 1 To determine if a pseudowire is configured for redundancy service, expand the required pseudowire in the navigation or map pane.

If the pseudowire is configured for redundancy service, the redundancy service badge appears in the navigation and map panes as shown in Figure 18-59.

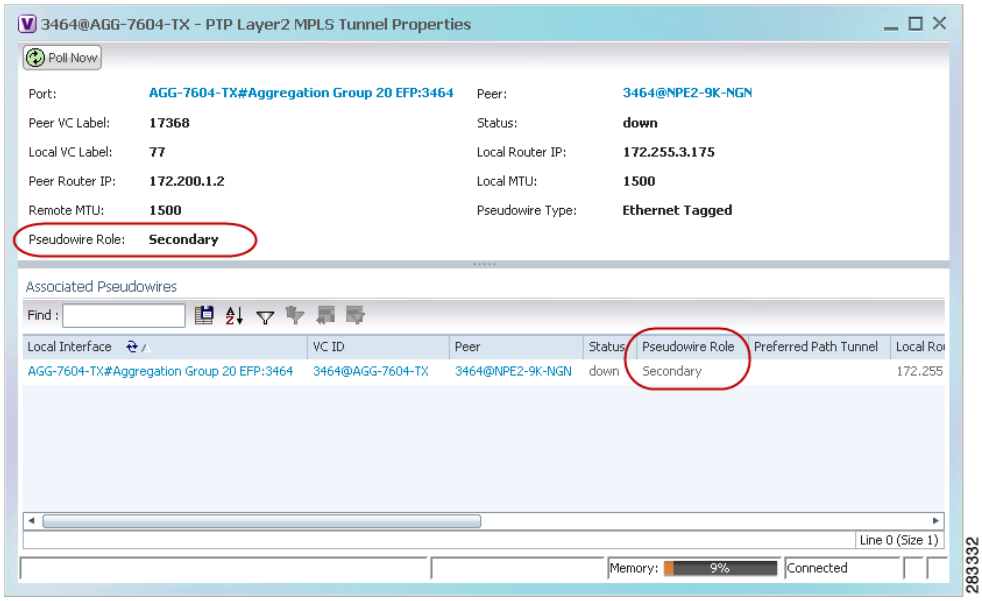
Figure 18-59 Pseudowire Redundancy Service Badge in a Map



Step 2 To view additional details, in the map, double-click the element with the redundancy service badge.

The PTP Layer 2 MPLS Tunnel Properties window is displayed as shown in Figure 18-60 and shows that the selected pseudowire has a Secondary role in a redundancy service.

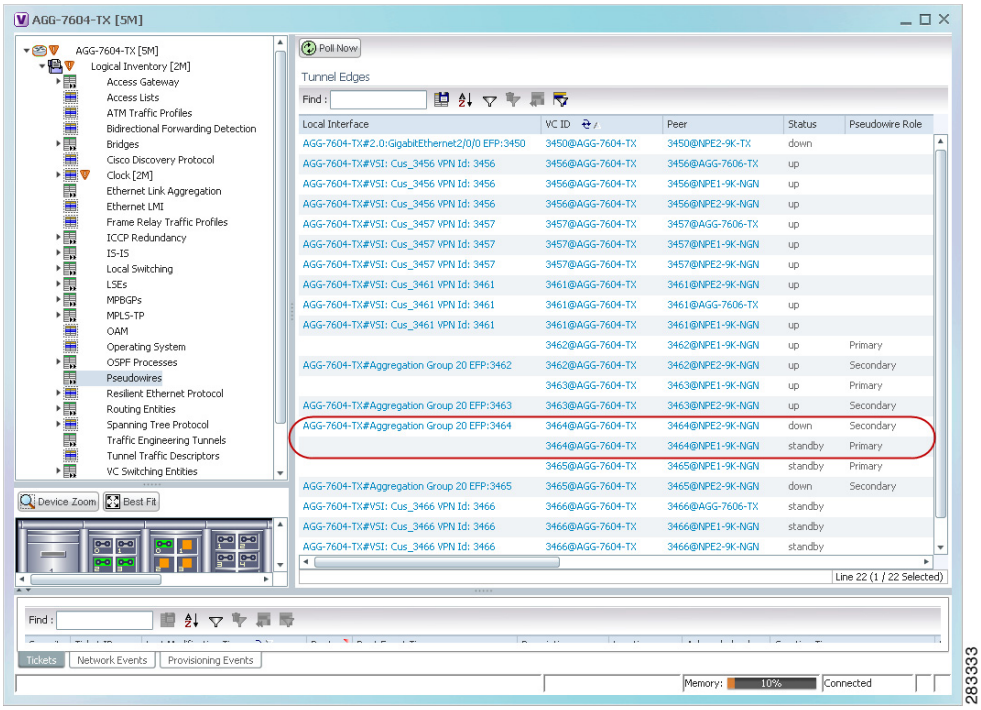
Figure 18-60 Layer 2 MPLS Tunnel Properties for Pseudowire Redundancy Service



Step 3 In the PTP Layer 2 MPLS Tunnel Properties window, click the VC ID hyperlink.

The Tunnel Edges table in logical inventory is displayed, with the local interface selected in the table. (See Figure 18-61.)

Figure 18-61 Pseudowire Redundancy Service in Logical Inventory



The entries indicate that the selected tunnel edge has a Secondary role in the first VC and a Primary role in the second VC.

For more information about the Pseudowires Tunnel Edges table, see Table 17-29.

Applying Pseudowire Overlays

A pseudowire overlay allows you to isolate the parts of a network that are used by a specific pseudowire.

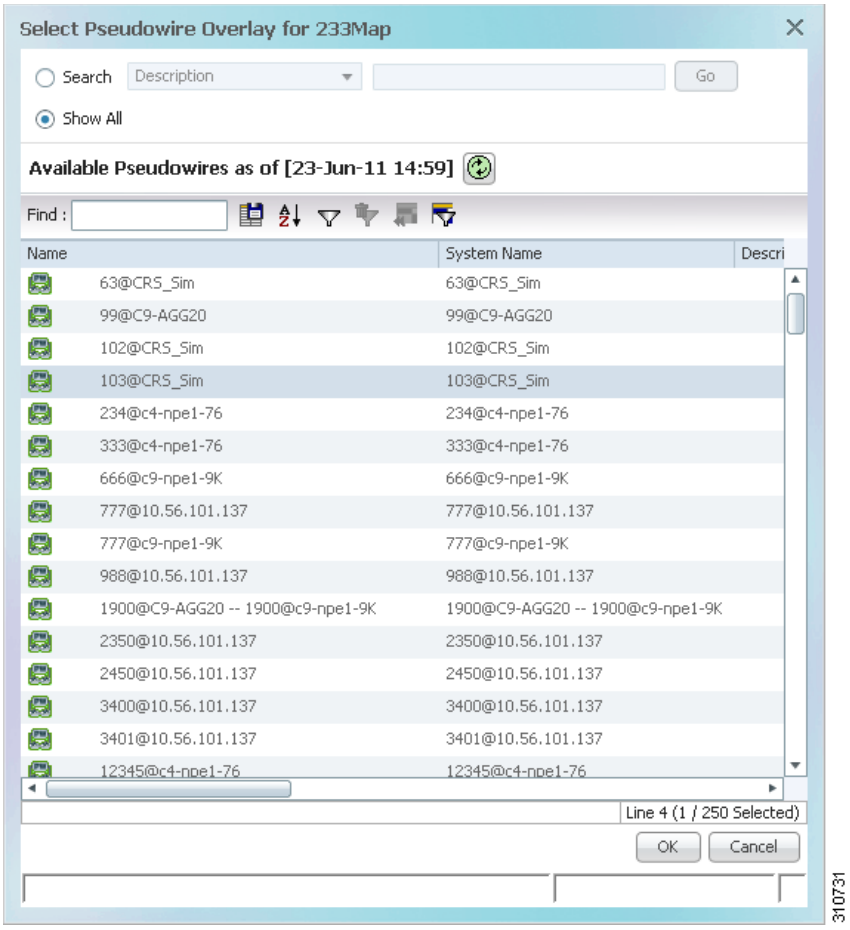
To apply a pseudowire overlay:

Step 1 In the Vision client, choose the map in which you want to apply an overlay.

Step 2 From the toolbar, choose **Choose Overlay Type > Pseudowire**.

Figure 18-62 shows an example of the Select Pseudowire Overlay for *map* dialog box.

Figure 18-62 Select Pseudowire Overlay Dialog Box

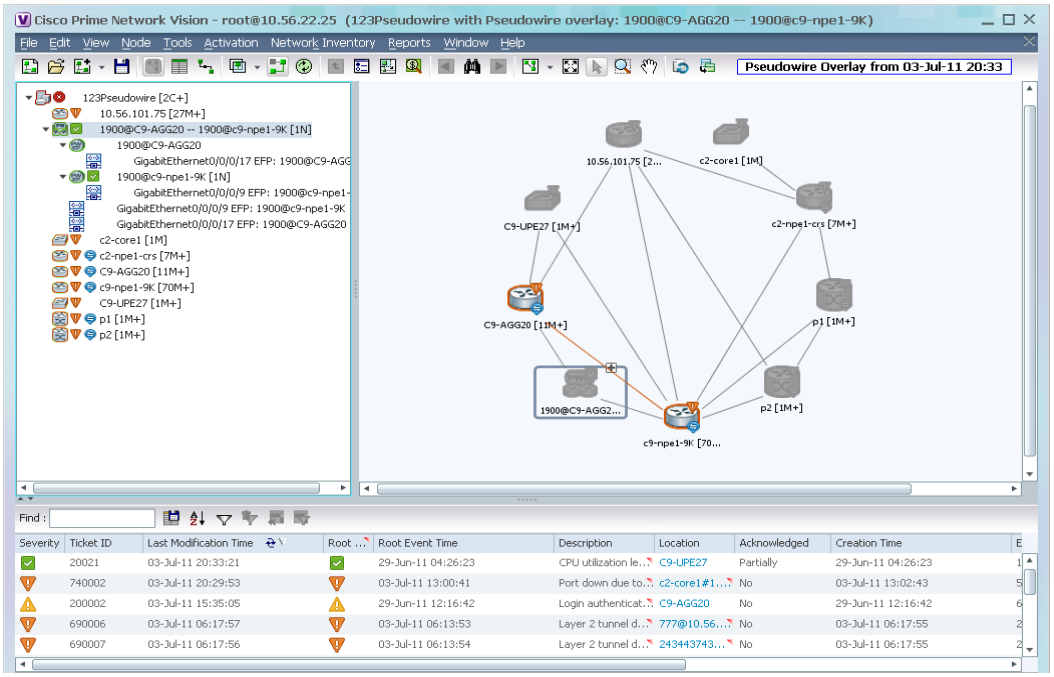


Step 3 Select the required pseudowire for the overlay.

Step 4 Click **OK**.

The elements being used by the selected pseudowire are highlighted in the map while the other elements are dimmed, as shown in Figure 18-63.

Figure 18-63 Pseudowire Overlay in Vision Window



Step 5 To hide and view the overlay, click **Hide Overlay/Show Overlay** in the toolbar. The button toggles depending on whether the overlay is currently displayed or hidden.

Step 6 To remove the overlay, choose **Choose Overlay Type > None**.

Monitoring the Pseudowire Headend

A pseudowire (PW) is an emulation of a point-to-point connection over a packet-switching network (PSN). It operates over a uniform packet-based access/aggregation network. The composite L2 AC and the PW segment together form a point-to-point virtual CE-PE link that functions like a traditional CE-PE link technology.

Figure 18-64 displays a typical pseudowire deployment over core network and Figure 18-65 displays a pseudowire deployment over access network.

Figure 18-64 Pseudowire Deployment Over Core Network

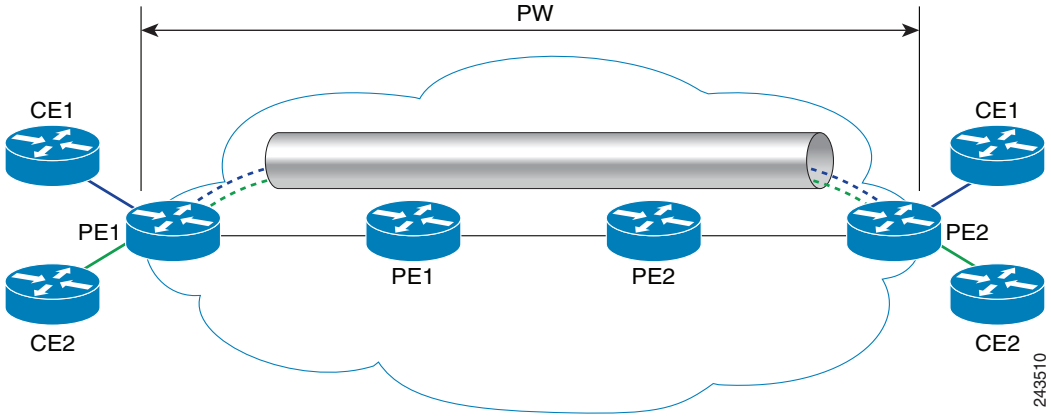
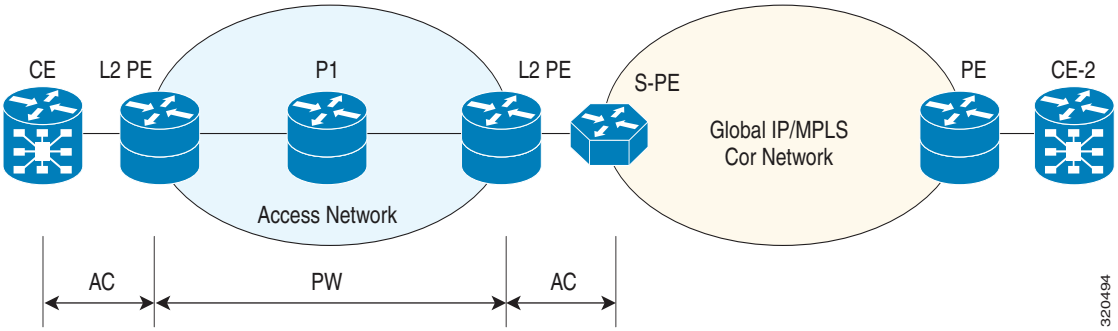


Figure 18-65 Pseudowire Deployment Over Access Network

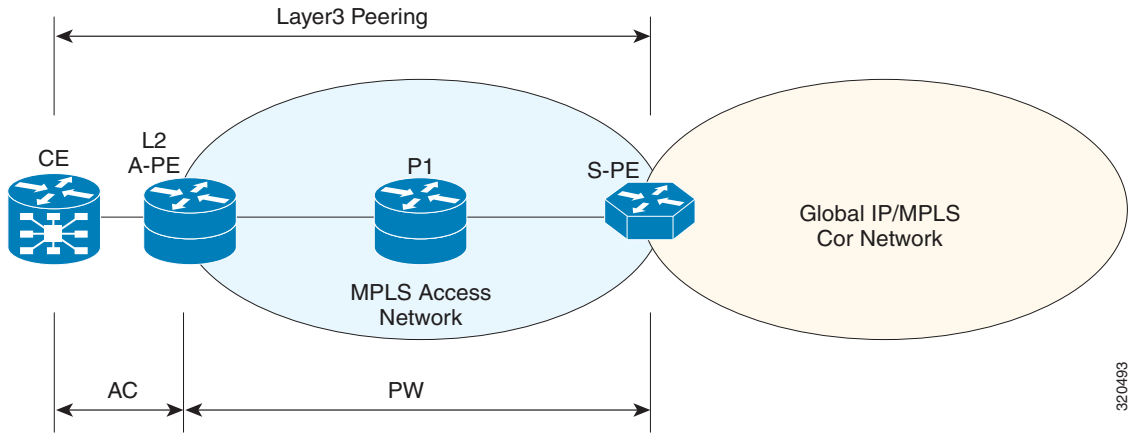


A pseudowire headend (PW-HE) virtual interface originates as a PW on an access node and terminates on a Layer 3 service instance on the service provider router. For example, a PWHE can originate on the Layer 2 PW feeder node and terminate on a VRF instance on the Cisco CRS Router. You can configure all ingress and egress QoS function on the PW-HE interface, including policing, shaping, queuing, and hierarchical policies.

In other words, the PW-HE is a technology that allows termination of access or aggregation pseudowires into an L2 or L3 domain. It allows us to replace a 2-node solution with a 1-node solution. Without a PW-HE, a L2 PE node must terminate a PW and then handoff the data to a S-PE via an Access Circuit.

The following figure displays the PW-HE interface:

Figure 18-66 PW-HE Interface



The PW-HE interface is treated like any existing L3 interface and operates on one of the following nodes:

- Bridged interworking (VC type 5 or 4) node—PW will carry customer Ethernet frames with IP payload. The S-PE device must perform ARP resolution for customer IP addresses learnt over PW-HE, which acts as a broadcast interface.
- IP interworking node (VC type 11)—The PW-HE acts as a point-to-point interface. Hence, there will be two types of PW-HE interface-PW-Ether and PW-IW. These PW's can terminate into a VRF or the IP global table on SP-E.

Viewing the PW-HE configuration

To view the PW-HE configuration:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > PW-HE**. The list of PW-HE interfaces configured in Prime Network are displayed in the content pane.

Step 3 From the **PW-HE** node, choose a PW-HE interface. The PW-HE interface details are displayed in the content pane as shown in Figure 18-67.

Figure 18-67 PW-HE Configuration Details

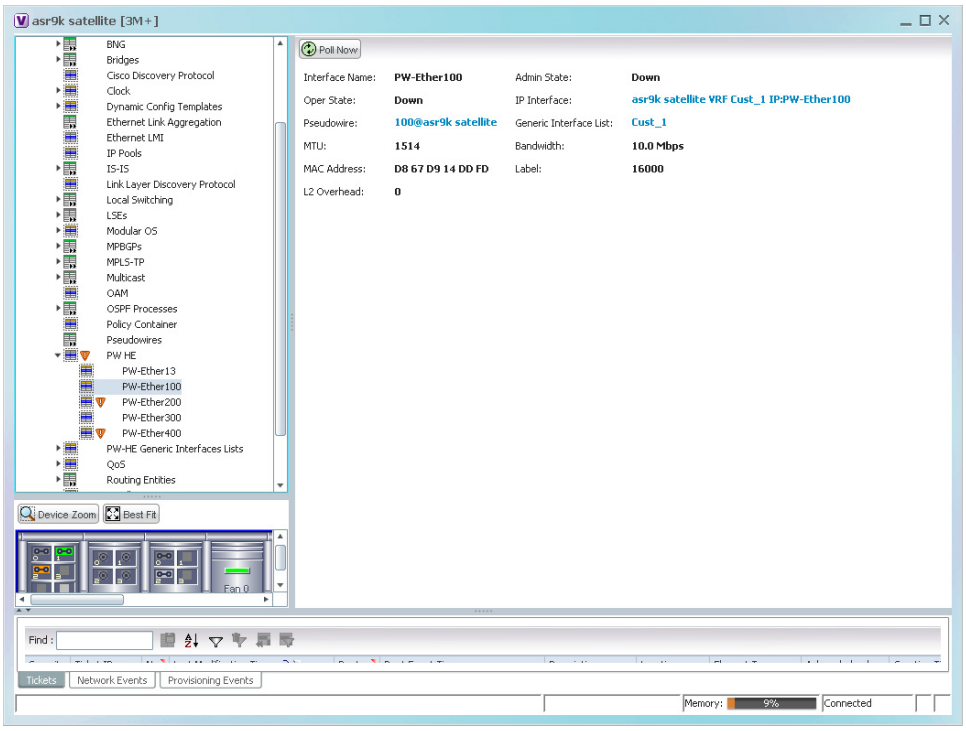


Table 18-50 displays the PW-HE interface details.

Table 18-50 PW-HE Interface Details

Field	Description
Interface Name	The unique name to identify the PW-HE interface.
Admin State	The administrative state of the PW-HE, which can be any one of the following: • Up • Down
Oper State	The operational state of the PW-HE, which can be any one of the following: • Up • Down
IP Interface	The IP interface for the PW-HE, which when clicked will take you either to the associated VRF interface site under the VRF node or the associated IP Interface under the Routing Entity node.
Pseudowire	The pseudowire to which the PW-HE is associated with, which when clicked will take you to the **Pseudowire** node.
Generic Interface List	The generic interface list linked to the PW-HE, which when clicked will take you to the relevant node under the **PW-HE Generic Interfaces Lists** node.
MTU	The maximum number of transmission units (in bytes) for the PW-HE interface.
Bandwidth	The bandwidth (in kbits) for the PW-HE interface.
MAC Address	The MAC address specified for the PW-HE interface, which is generally in the xxx.xxx.xxx format.
Label	The MPLS label for the PW-HE interface.
L2 Overhead	The layer 2 overhead (in bytes) configured on the PW-HE interface, which can be any value between 0 and 64. This field defaults to 0.

You can also view the following configuration details for a PW-HE interface:

- Viewing PW-HE Configured as a Local Interface under Pseudowire, page 18-121
- Viewing PW-HE L2 Sub-Interface Properties, page 18-122
- Viewing PW-HE L3 Sub-interface Properties, page 18-122
- Viewing PW-HE Generic Interface List, page 18-123
- Viewing PW-HE as an Associated Entity for a Routing Entity, page 18-124
- Viewing PW-HE as an Associated Entity for a VRF, page 18-124

Viewing PW-HE Configured as a Local Interface under Pseudowire

To view the local interface details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > Pseudowire**. The list of Pseudowire interfaces configured in Prime Network are displayed in the content pane. For more information on Pseudowire properties, see Viewing Pseudowire Properties, page 18-110.

Viewing PW-HE L2 Sub-Interface Properties

To view the L2 Sub-Interface details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory** > **PW HE** > *PW-Ether interface*. The list of PW-HE interfaces configured in Prime Network are displayed in the content pane.

Step 3 Choose the EFPs tab of an interface to view the details.

Table 18-51 displays the PW-HE L2 Sub-Interface details.

Table 18-51 PW-HE L2 Sub-Interface Details

Field	Description
EFPs tab	
EFP ID	EFP identifier.
Operational State	EFP operational state: Up or Down.
VLAN	VLAN associated with this EFP.
Inner VLAN	CE-VLAN identifier.
Translated VLAN	Translated, or mapped, VLAN identifier.
Translated Inner VLAN	Translated, or mapped, inner VLAN identifier.
Binding	Hyperlinked entry to the specific bridge in logical inventory.
Description	Description for the EFP.
Ingress Policy	The name of the ingress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates.
Egress Policy	The name of the egress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates.
Service Control Policy	Specifies the policy for a port or operation.

Viewing PW-HE L3 Sub-interface Properties

To view the L3 Sub-Interface details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory** > **PW HE** > *PW-Ether interface*. The list of PW-HE interfaces configured in Prime Network are displayed in the content pane.

Step 3 Choose the Sub Interfaces tab of an interface to view the details.

Table 18-52 displays the PW-HE L3 Sub-Interface details.

Table 18-52 PW-HE L3 Sub-Interface Details

Field	Description
Sub Interfaces tab	
Address	EFP identifier.
Mask	The mask of the specific network.
VLAN Type	The VLAN interface type, such as Layer 2 VLAN.
Operational State	EFP operational state: Up or Down.
VLAN ID	VLAN identifier.
Inner VLAN	CE-VLAN identifier.
IP Interface	IP interface, hyperlinked to the VRF properties in the inventory window.
VRF Name	Virtual Routing and Forwarding (VRF) name, if the pool belongs to a VRF.
VC	Virtual connection identifier.
Binding	Hyperlinked entry to the specific bridge in logical inventory.
Description	Description for the EFP.
Ingress Policy	The name of the ingress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates.
Egress Policy	The name of the egress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates.
Service Control Policy	Specifies the policy for a port or operation.

Viewing PW-HE Generic Interface List

To view the PW-HE generic interface list:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > PW-HE Generic Interface List**. The list of generic interfaces configured in Prime Network are displayed in the content pane.

Step 3 From the **PW-HE Generic Interface List** node, choose a generic interface list. The interface details are displayed in the content pane.

Table 18-53 displays the PW-HE Generic Interface List details.

Table 18-53 PW-HE Generic Interface List Details

Field	Description
Generic Interface	The name of the generic interface list.
Interfaces tab	
Interface	The Ethernet Link Aggregation Group (LAG) for the PW-HE service, which when clicked will take you to the **LAG** node.

Viewing PW-HE as an Associated Entity for a Routing Entity

To view the routing entity details for a PW-HE:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > Routing Entities > Routing Entity**. The routing entity details for the PW-HE is displayed in the content pane. For more information on Routing entity details, see Viewing Routing Entities, page 17-32.

Viewing PW-HE as an Associated Entity for a VRF

To view the VRF details for a PW-HE:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > VRF >** *PW-HE node*. The VRF details for the PW-HE is displayed in the content pane. For more information on VRF details, see Viewing VRF Properties, page 17-28.

Working with Ethernet Services

Ethernet services are created when the following business elements are linked to one another:

- Network VLAN and bridge domain are linked through a shared EFP.
- Network VLAN and VPLS instance are linked through either of the following:
  - A shared, standalone EFP.
  - A shared switching entity.
- Network VLAN and network pseudowire (single or multi-segment) are linked through either of the following:
  - A shared, standalone EFP.
  - A shared switching entity.
- VPLS-EoMPLS connected via a shared access pseudowire endpoint.
- Network VLAN and cross-connect are connected by a shared EFP.
- Network VLAN and service link are connected by a shared EFP.

If a VPLS, network pseudowire, cross-connect, or network VLAN object is not connected to another business element, it resides alone in an Ethernet service.

In releases prior to Prime Network 3.8, EVC multiplex was discovered by means of Ethernet flow point associations. Beginning with Prime Network 3.9, multiplex capabilities were enhanced to distinguish multiplexed services based on the Customer VLAN ID; that is, Prime Network 3.9 is Inner Tag-aware.

As a result, in environments in which service providers have customers with multiplexed services, an EVC can distinguish each service and create its own EVC representation.

Prime Network discovers Ethernet services and enables you to add them to maps, apply overlays, and view their properties. See the following topics for more information:

- Adding Virtual Connections to a Map, page 18-125
- Applying Ethernet Service Overlays, page 18-126
- Viewing Ethernet Service Properties, page 18-128

Adding Virtual Connections to a Map

You can add the virtual connections that Prime Network discovers to maps as required.

To add a virtual connection to a map:

Step 1 In the Vision client, select the required map or domain.

Step 2 Open the Add Ethernet Service to *map* dialog box in either of the following ways:

- In the toolbar, choose **Add to Map > Virtual Connection**.
- In the menu bar, choose **File > Add to Map > Virtual Connection**.

Step 3 In the Add Virtual Connection dialog box, do either of the following:

- To search for specific elements:

  a. Choose **Search**, and then choose a search category: EVC Terminating EFPs, Name, or System Name.

  b. To narrow the display to a range of virtual connection or a group of virtual connections, enter a search string in the search field.

  c. Click **Go**.

  For example, if you choose Name and enter `EFP1`, the network elements that have names beginning with EFP1 are displayed.

- To view all available virtual connections, choose **Show All** and click **Go**.

The available elements that meet the specified search criteria are displayed in the Add Virtual Connections dialog box in table format. The dialog box also displays the date and time at which the list was generated. To update the list, click **Refresh**.

Note If an element is not included in your scope, it is displayed with the locked device icon.

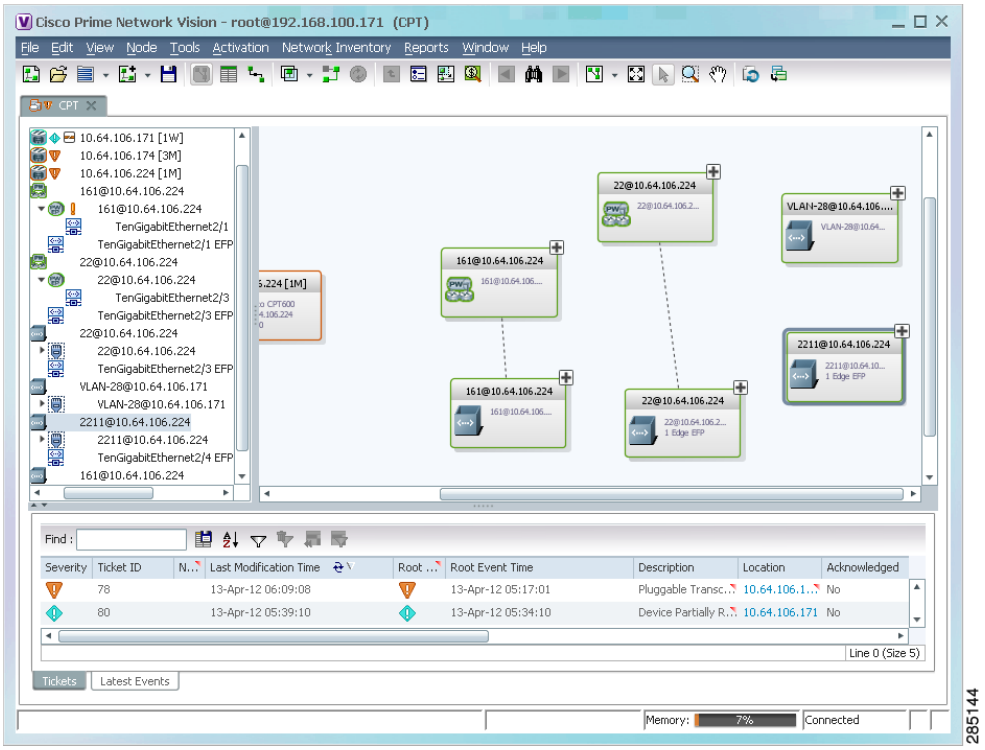
For information about sorting and filtering the table contents, seeViewing a Table of NEs and Their Properties (List View), page 7-7.

Step 4 In the Add Virtual Connections dialog box, select the elements that you want to add. You can select and add multiple elements by pressing **Ctrl** while selecting individual elements or by pressing **Ctrl +Shift** to select a group of elements.

Step 5 Click **OK**.

The virtual connection is displayed in the navigation pane and in the content area. In addition, any associated tickets are displayed in the ticket pane. See Figure 18-68.

Figure 18-68 Ethernet Service in Prime Vision Window



The Ethernet service information is saved with the map in the Prime Network database.

Applying Ethernet Service Overlays

An Ethernet service overlay allows you to isolate the parts of a network that are being used by a specific Ethernet service.

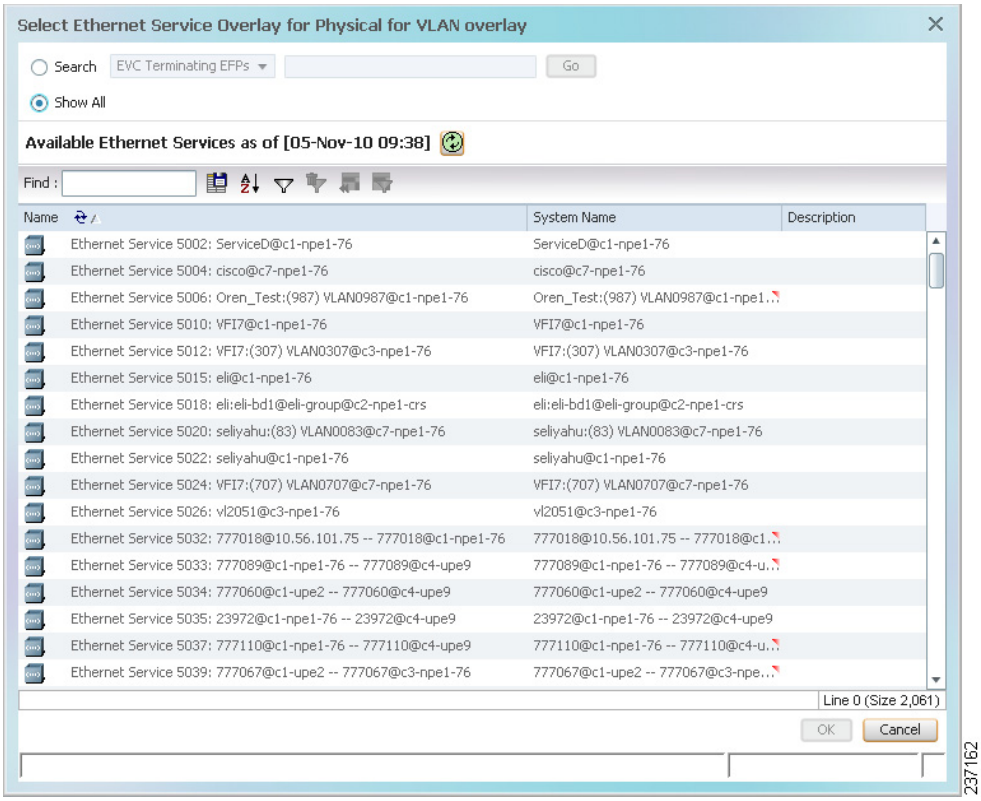
To apply an Ethernet service overlay:

Step 1 In the Vision client, choose the map in which you want to apply an overlay.

Step 2 From the toolbar, choose **Choose Overlay Type > Ethernet Service**.

Figure 18-69 shows an example of the Select Ethernet Service Overlay for *map* dialog box.

Figure 18-69 Select Ethernet Service Overlay Dialog Box

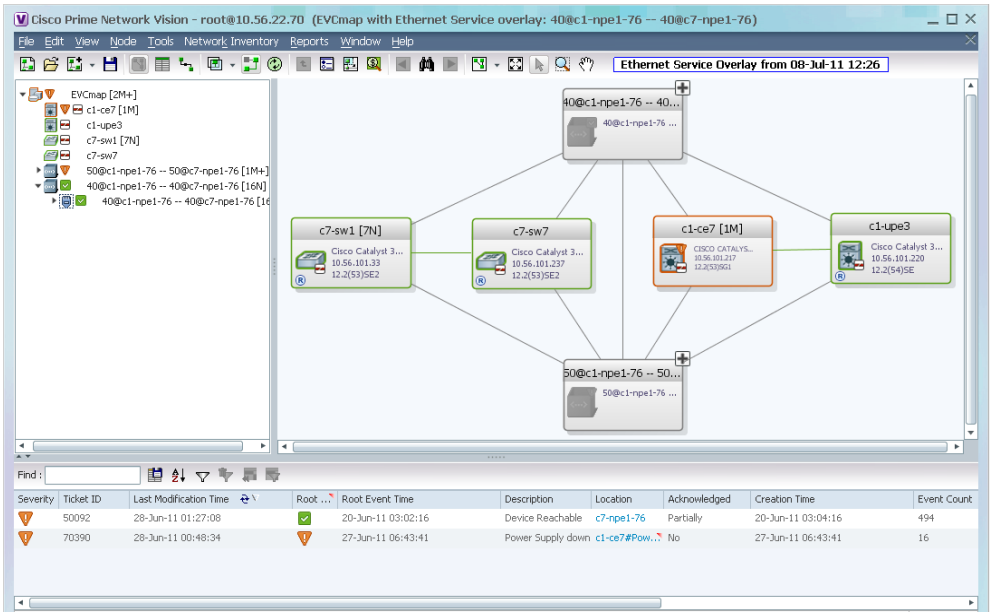


Step 3 Select the required Ethernet Service for the overlay.

Step 4 Click **OK**.

The elements being used by the selected Ethernet service are highlighted in the map while the other elements are dimmed, as shown in Figure 18-70.

Figure 18-70 Ethernet Service Overlay in Vision Window



Step 5 To hide and view the overlay, click **Hide Overlay/Show Overlay** in the toolbar. The button toggles depending on whether the overlay is currently displayed or hidden.

Step 6 To remove the overlay, choose **Choose Overlay Type > None**.

Viewing Ethernet Service Properties

To view Ethernet service properties:

Step 1 In the Vision client, select the map containing the required Ethernet service.

Step 2 In the navigation or map pane, right-click the Ethernet service and choose **Properties**.

Figure 18-71 shows an example of an Ethernet Service Properties window with the EVC Terminating table. Depending on the types of service in the EVC, tabs might be displayed. For example, if the EVC contains two network VLANs and a VPLS, tabs are displayed for the following:

- EVC Terminating table
- Network VLANs
- VPLS

Figure 18-71 Ethernet Service Properties Window

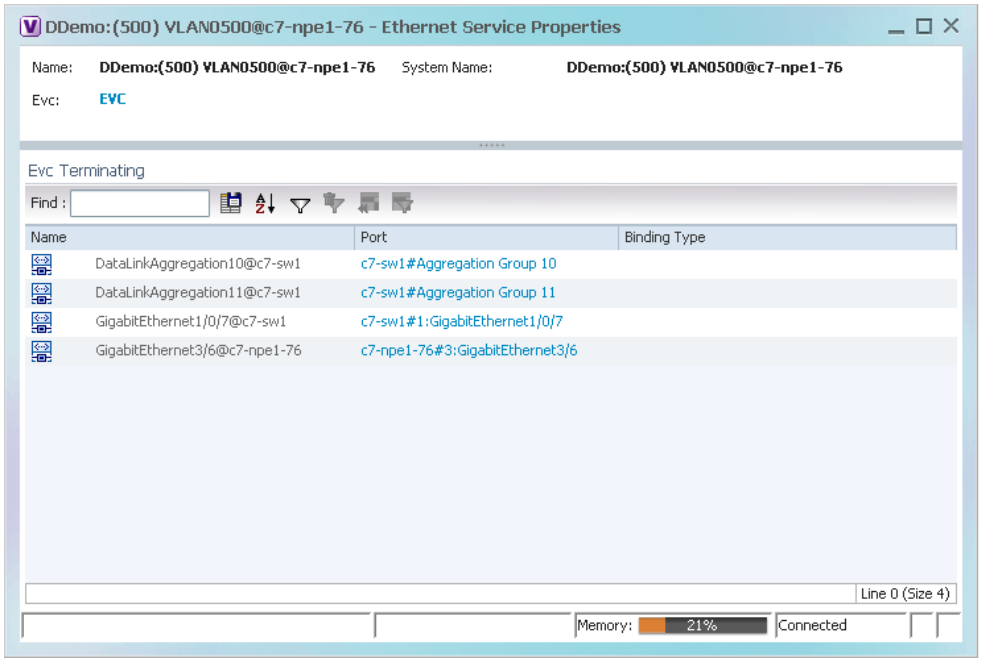


Table 18-54 describes the information that is displayed for an Ethernet service.

Table 18-54 Ethernet Service Properties Window

Field	Description
Name	Ethernet service name.
System Name	Name that Prime Network assigns to the Ethernet service.
EVC	Name of the EVC associated with the Ethernet service, hyperlinked to the EVC Properties window.
EVC Terminating Table	
Name	EVC name, represented by the interface name, EFP, and the EFP name.
Network Element	Hyperlinked entry to the specific interface and EFP in physical inventory.
Port	Hyperlinked entry to the specific interface in physical inventory.

Step 3 To view the EVC Properties window, click the hyperlink in the EVC field.

Figure 18-72 shows an example of the EVC Properties window.

Figure 18-72 EVC Properties Window

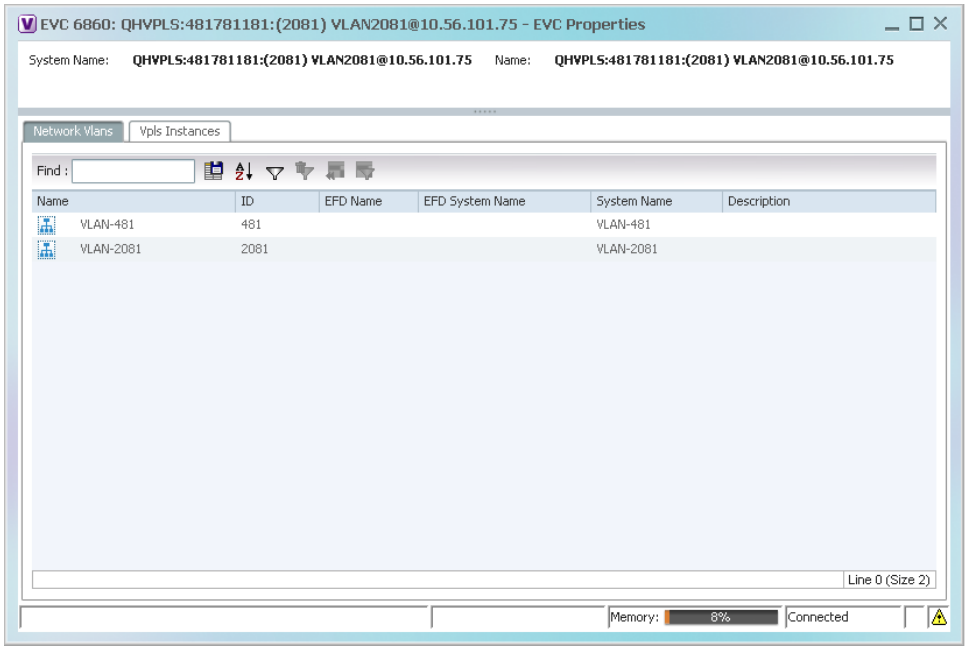


Table 18-55 describes the information that is displayed in the EVC Properties window. The tabs that are displayed depend on the services included in the EVC. For example, if the EVC contains two network VLANs and a VPLS, tabs are displayed for the following:

- EVC Terminating table
- Network VLANs
- VPLS

Table 18-55 EVC Properties Window

Field	Description
System Name	Name of the system on which the EVC is configured.
Name	EVC name.
Cross-Connects Table	
Name	Cross-connect name.
Segment 1	Identifier of the first cross-connect endpoint.
Segment 2	Identifier of the second cross-connect endpoint.
System Name	Cross-connect system name.

Table 18-55 EVC Properties Window (continued)

Field	Description
Network VLANs Tab	
Name	VLAN name.
ID	VLAN identifier.
EFD Name	Name of the Ethernet flow domain.
EFD System Name	Name that Prime Network assigns to the EFD.
System Name	VLAN system name.
Description	Brief description of the VLAN.
Network Pseudowires Tab	
Name	Pseudowire name.
System Name	System on which the pseudowire is configured.
Description	Brief description of the pseudowire.
Pseudowire Type	Type of pseudowire.
Is Multisegment Pseudowire	Whether or not the pseudowire is multisegment: True or False.
VPLS Instances Tab	
Name	VPLS instance name.
System Defined Name	Name that Prime Network assigns to the VPLS instance.
VPN ID	Identifier of associated VPN.

Viewing IP SLA Responder Service Properties

Cisco IOS Service Level Agreements (SLAs) software allows you to analyze IP service levels for IP applications and services by using active traffic monitoring to measure network performance.

The IP SLA responder is a component embedded in the destination Cisco device that allows the system to anticipate and respond to IP SLAs request packets. The responder provides accurate measurements without requiring dedicated probes. The responder uses the Cisco IOS IP SLAs Control Protocol to provide a mechanism through which it can be notified on which port it should listen and respond.

Two-Way Active Measurement Protocol (TWAMP) defines a standard for measuring round-trip network performance between any two devices that support the protocol.

For information on the devices that support IP SLA Responders, refer to *Cisco Prime Network 4.1 Supported VNEs*.

To view IP SLA Responder service properties:

Step 1 In the Vision client, double-click the device configured for IP SLA Responder service.

Step 2 In the **Inventory** window, choose **Logical Inventory > IP SLA Responder**.

IP SLA Responder properties are displayed as shown in Figure 18-73.

Figure 18-73 IP SLA Responder in Logical Inventory

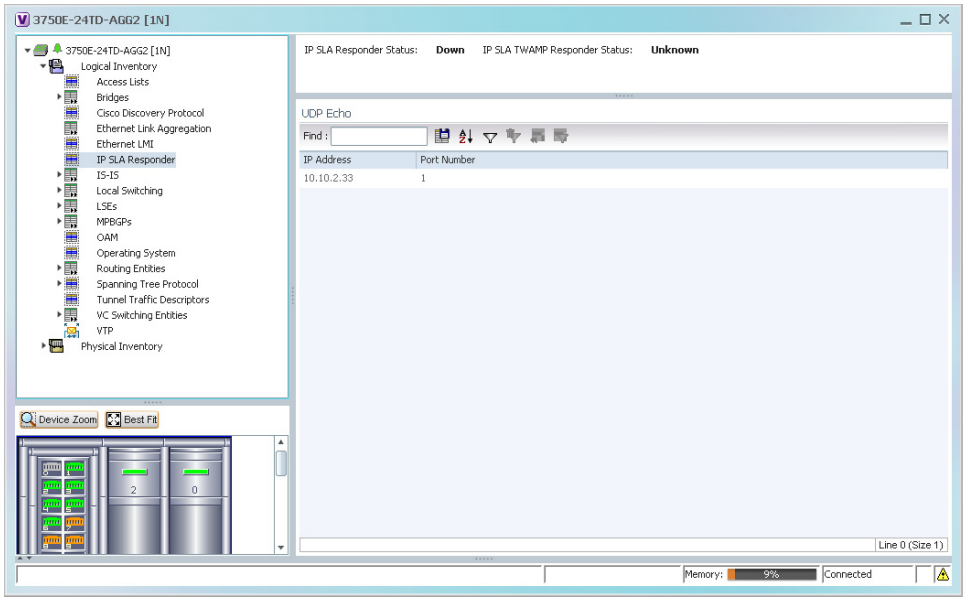


Table 18-56 describes the properties displayed for IP SLA Responder service.

Table 18-56 IP SLA Responder Properties in Logical Inventory

Field	Description
IP SLA Responder Status	Status of the IP SLA Responder: Up or Down.
IP SLA TWAMP Responder Status	Status of the IP SLA TWAMP responder: Up or Down.
UDP Echo Tab	
IP Address	Destination IP address used for the UDP echo operation.
Port Number	Destination port number used for the UDP echo operation.
TCP Connect Tab	
IP Address	Destination IP address used for the TCP connect operation.
Port Number	Destination port number used for the TCP connect operation.

Viewing IS-IS Properties

Intermediate System-to-Intermediate System (IS-IS) protocol is a routing protocol developed by the ISO. It is a link-state protocol where IS routers exchange routing information based on a single metric to determine network topology. It behaves in a manner similar to OSPF in the TCP/IP network.

IS-IS networks contain end systems, intermediate systems, areas, and domains. End systems are user devices. Intermediate systems are routers. Routers are organized into local groups called areas, and areas are grouped into a domain. For configuring IS-IS, see Configuring IS-IS, page 18-159.

To view IS-IS properties:

Step 1 In the Vision client, double-click the device configured for IS-IS.

Step 2 In the **Inventory** window, choose **Logical Inventory > IS-IS > System**.

Figure 18-74 shows an example of the IS-IS window with the Process table in logical inventory.

Figure 18-74 IS-IS Window in Logical Inventory

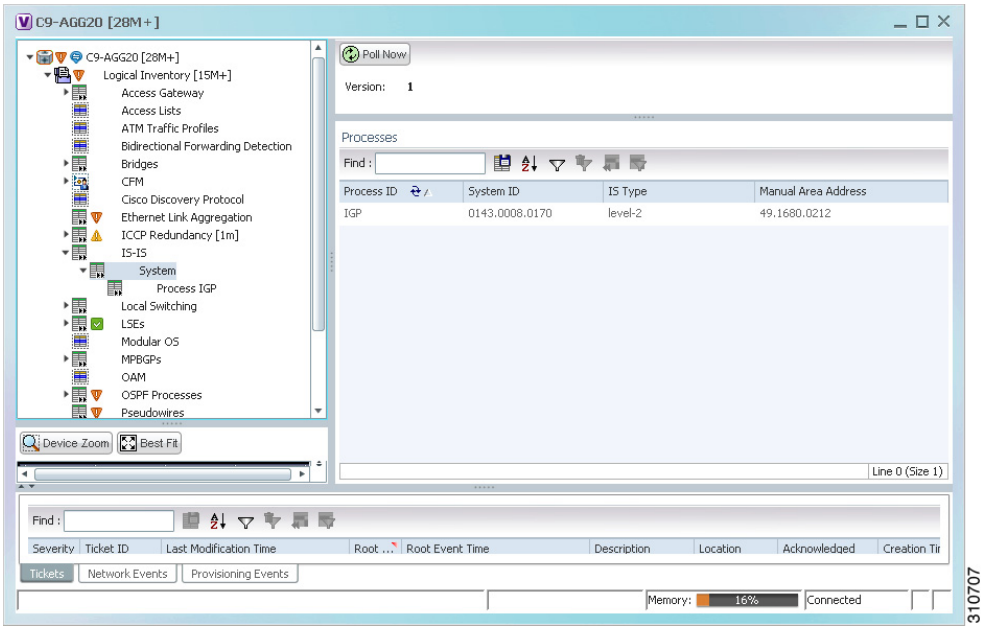


Table 18-57 describes the information that is displayed in this window and the Processes table.

Table 18-57 IS-IS Properties in Logical Inventory - Processes Table

Field	Description
Version	Version of IS-IS that is implemented.
Processes Table	
Process ID	Identifier for the IS-IS process.
System ID	Identifier for this Intermediate System.
IS Type	Level at which the Intermediate System is running: Level 1, Level 2, or Level 1-2.
Manual Area Address	Address assigned to the area.

Step 3 To view IS-IS process information, choose **Logical Inventory > IS-IS > Process** *nnn*.

Figure 18-75 shows an example of the information that is displayed for the IS-IS process.

Figure 18-75 IS-IS Process Properties in Logical Inventory

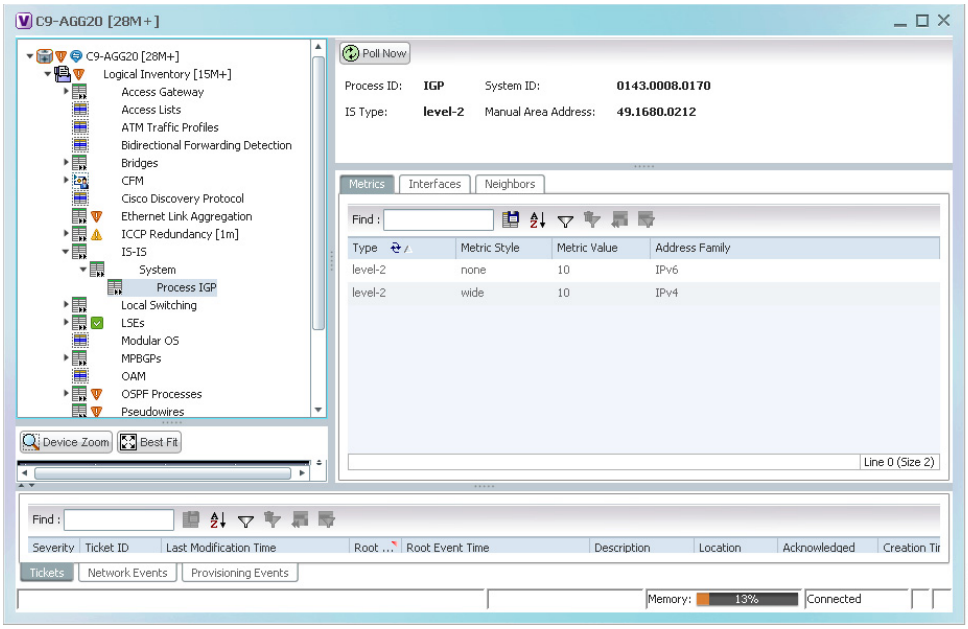


Table 18-58 describes the information that is displayed for the selected IS-IS process.

Table 18-58 IS-IS Process Properties in Logical Inventory

Field	Description
Process	Unique identifier for the IS-IS process.
System ID	Identifier for this Intermediate System.
IS Type	Level at which the Intermediate System process is running: Level 1, Level 2, or Level 1-2.
Manual Area Address	Address assigned to the area.
Metrics Tab	
IS Type	Level at which the Intermediate System is running: Level 1, Level 2, or Level 1-2.
Metric Style	Metric style used: Narrow, Transient, or Wide.
Metric Value	Metric value assigned to the link. This value is used to calculate the path cost via the links to destinations. This value is available for Level 1 or Level 2 routing only. If the metric style is Wide, the value can range from 1 to 16777214. If the metric style is Narrow, the value can range from 1 to 63. The default value for active IS-IS interfaces is 10, and the default value for inactive IS-IS interfaces is 0.
Address Family	IP address type used: IPv4 or IPv6.
Interfaces Tab	
Interface Name	Interface name.
Neighbors Tab	

Table 18-58 IS-IS Process Properties in Logical Inventory (continued)

Field	Description
System ID	Identifier for the neighbor system.
Interface	Neighbor interface name.
IP Address	Neighbor IP address.
Type	IS type for the neighbor: Level 1, Level 2, or Level 1-2.
SNPA	Subnetwork point of attachment (SNPA) for the neighbor.
Hold Time	Holding time, in seconds, for this adjacency. The value is based on received IS-to-IS Hello (IIH) PDUs and the elapsed time since receipt.
State	Administrative status of the neighbor system: Up or Down.
Address Family	IP address type used by the neighbor: IPv4 or IPv6.

Viewing Segment Routing Properties on IS-IS

Prime Network 5.3 supports Segment Routing on IS-IS technology for devices NCS 540, NCS 55xx, and Nexus 9K. However, Segment Routing is supported with IS-IS IPv4 address family only.

The source chooses a path and encodes it in the packet header as an ordered list of segments (an identifier for an instruction - forwarding or service). The rest of the network executes the encoded instructions.

Segment routing does not require any additional protocol.

To view Segment Routing properties:

Step 1 In the Vision client, double-click the device configured for IS-IS.

Step 2 In the **Inventory** window, choose **Logical Inventory > IS-IS System**.

Step 3 To view Segment Routing process information, choose **Logical Inventory > IS-IS System> Process** *nnn*.

The following figure shows an example of the information that is displayed for the IS-IS process with Segment Routing.

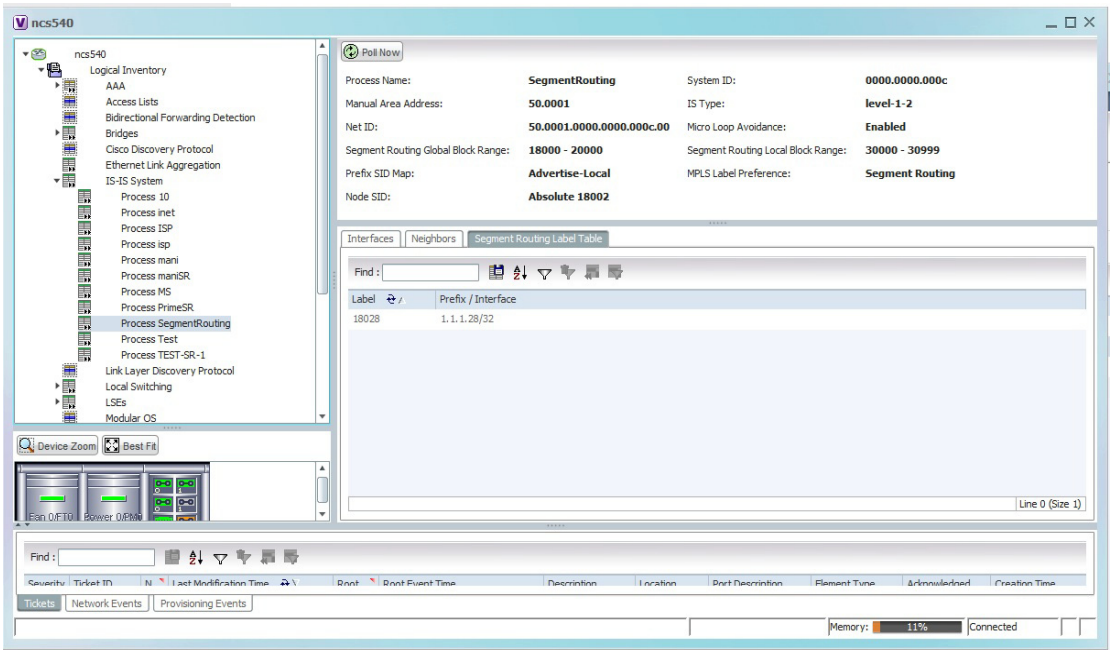


Table 18-59 describes the information that is displayed for the selected IS-IS process.

Table 18-59 Segment Routing Properties on IS-IS in Logical Inventory

Field	Description
IS-IS Process Properties	
Net ID	Address of a Network Service Access Point (NSAP) which identifies an instance of the IS-IS routing protocol running on an IS.
Micro Loop Avoidance	Shows if microloop avoidance is enabled or disabled.
Segment Routing Global Block Range	Shows the Segment Routing global block range.
Segment Routing Local Block Range	Shows the Segment Routing local block range.
Prefix SID Map	Shows about to Advertise-local or receive prefix-SID mappings.
MPLS Label Preference	Shows if Segment Routing labels are preferred over LDP labels.
Node SID	The label representing the node segment.
Interfaces Tab	
SR Algorithm	Flex Algorithm (Shortest Path First) used for Segment Routing: FA:0 SPF FA:1 Strict SPF

Table 18-59 Segment Routing Properties on IS-IS in Logical Inventory

Field	Description
IS-IS Process Properties	
Prefix SID Flags	Denotes the SR Prefix SID flags (R, N, P, E, V, L): R-Flag: Re-advertisement flag. If set, then the prefix to which this Prefix-SID is attached, has been propagated by the router either from another level (i.e., from level-1 to level-2 or the opposite) or from redistribution (e.g., from another protocol). N-Flag: Node-SID flag. If set, then the Prefix-SID refers to the router identified by the prefix. Typically, it is set on Prefix-SIDs attached to a router loopback address. P-Flag: no-PHP flag. If set, then the penultimate hop MUST NOT pop the Prefix-SID before delivering the packet to the node that advertised the Prefix-SID. E-Flag: Explicit-Null Flag. If set, any upstream neighbor of the Prefix-SID originator MUST replace the Prefix-SID with a Prefix-SID having an Explicit-NULL value (0 for IPv4 and 2 for IPv6) before forwarding the packet. V-Flag: Value flag. If set, then the Prefix-SID carries a value instead of an index. By default, the flag is UNSET. L-Flag: Local Flag. If set, then the value/index carried by the Prefix-SID has local significance. By default, the flag is UNSET.
Node Max SID Depth - Label Imposition	Maximum number of SID's that HW/SW are capable of imposing on a given node.
TI-LFA	Shows if Topology-Independent Loop-Free Alternate (TI-LFA) is enabled or not.
Segment Routing Lable Table Tab	
Label	Segment Routing Labels: Absolute value - for NCS540, NCS55xx devices; Index value - for Nexus-9K devices
Prefix/Interface	Loopback interface IP address with mask or associated loopback interface name.

Viewing OSPF Properties

Open Shortest Path First (OSPF) is a link-state routing protocol for IP networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). It uses the Shortest Path First (SPF) algorithm to calculate the best path for a given destination. OSPF is perhaps the most widely used interior gateway protocol (IGP) in large enterprise networks.

The OSPF topology is a multilink topology, i.e. there can be multiple links from the same OSPF process. It is also a single layer and dynamic topology.

Prime Network supports the following versions of OSPF:

- OSPFv2
- OSPFv3

Using the Vision client you can view OSPF properties for:

- OSPF processes, including the process identifier and OSPF version.
- OSPF network interfaces, such as the area identifier, network type, and status.
- OSPF neighbors, including the neighbor identifier, neighbor interface address, and status.

You can view the OSPF topological links for neighbors whose status is Full or Two Way.

To view OSPF properties:

Step 1 In the Vision client, double-click the device configured for OSPF.

Step 2 To view OSPF processes, choose **Logical Inventory > OSPF Processes > OSPF Process (v*n*)** *ID* where **v***n* represents the OSPF version and *ID* is the OSPF process identifier.

For example, in Figure 18-76, the entry in the navigation tree is OSPF Process (v2) 10.

Figure 18-76 OSPF Processes in Logical Inventory

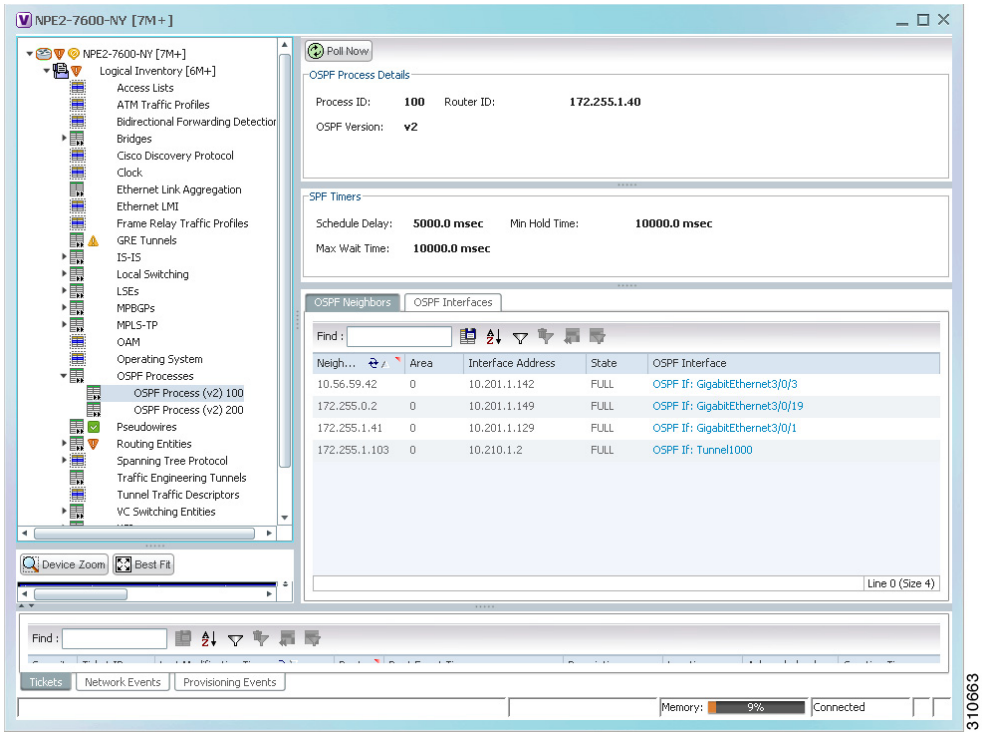


Table 18-60 describes the information that is displayed for OSPF processes.

Table 18-60 OSPF Processes in Logical Inventory

Field	Description
OSPF Process Details	
Process ID	Unique process identifier.
Router ID	Router IP address.
OSPF Version	OSPF version: v1, v2, or v3.
SPF Timers	
Schedule Delay	Number of milliseconds to wait after a change before calculating the shortest path first (SPF).
Min Hold Time	Minimum number of milliseconds to wait between two consecutive SPF calculations.
Max Wait Time	Maximum number of milliseconds to wait between two consecutive SPF calculations.
OSPF Neighbors Table	
Neighbor ID	OSPF neighbor IP address.
Area	OSPF area identifier.
Interface Address	IP Address of the interface on the neighbor configured for OSPF.
State	State of the communication with the neighbor: Down, Attempt, Init, 2-Way, Exstart, Exchange, Loading, and Full.
OSPF Interface	Hyperlinked entry to the OSPF Interface Properties window. The OSPF Interfaces window displays the same information as the OSPF Interfaces Table below.

Figure 18-77 Viewing OSPF Interface

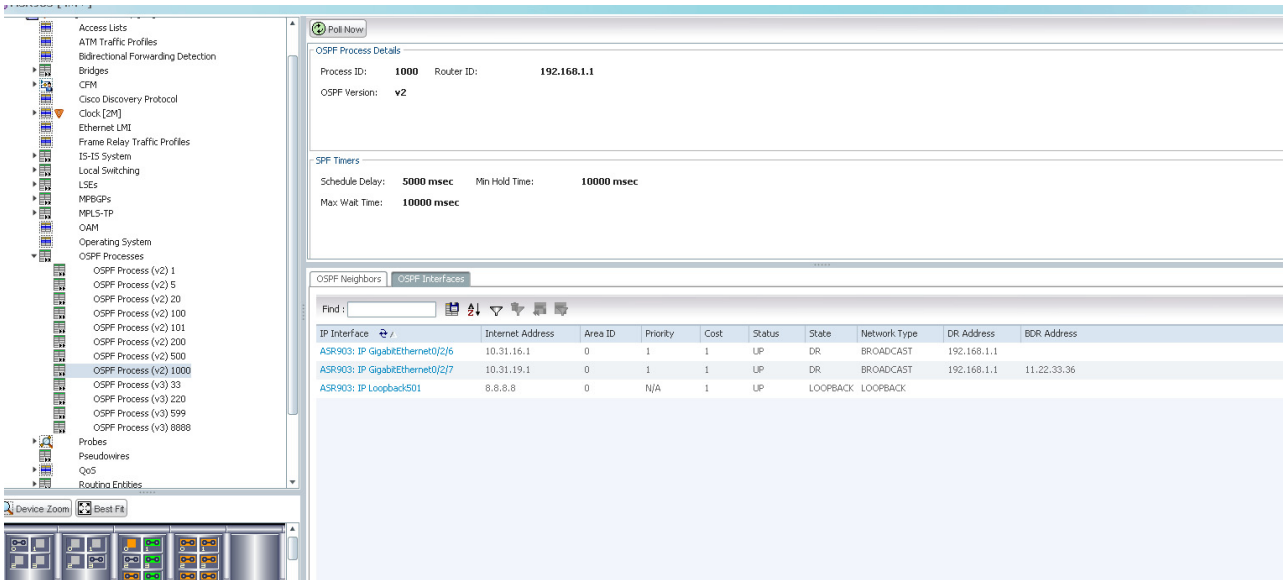


Table 18-61 OSPF Processes in Logical Inventory (continued)

OSPF Interfaces Table	
IP Interface	OSPF interface, hyperlinked to the relevant entry in the routing entity IP Interfaces table in logical inventory. For more information about the IP Interfaces table, see Table 17-8.
Internet Address	OSPF interface IP address.
Area ID	OSPF area identifier.
Priority	Eight-bit unsigned integer that specifies the priority of the interface. Values range from 0 to 255. Of two routers, the one with the higher priority takes precedence.
Cost	Specified cost of sending a packet on the interface, expressed as a metric. Values range from 1 to 65535.
Status	State of the interface: Up or Down.
State	The displayed OSPF state will be either BDR, DR, DR-Other, or LOOPBACK.
Network Type	Type of OSPF network: Broadcast, Nonbroadcast Multiple Access (NBMA), Point-to-Multipoint, Point-to-Point, or Loopback.
DR Address	Designated router IP address.
BDR Address	Backup designated router IP address.

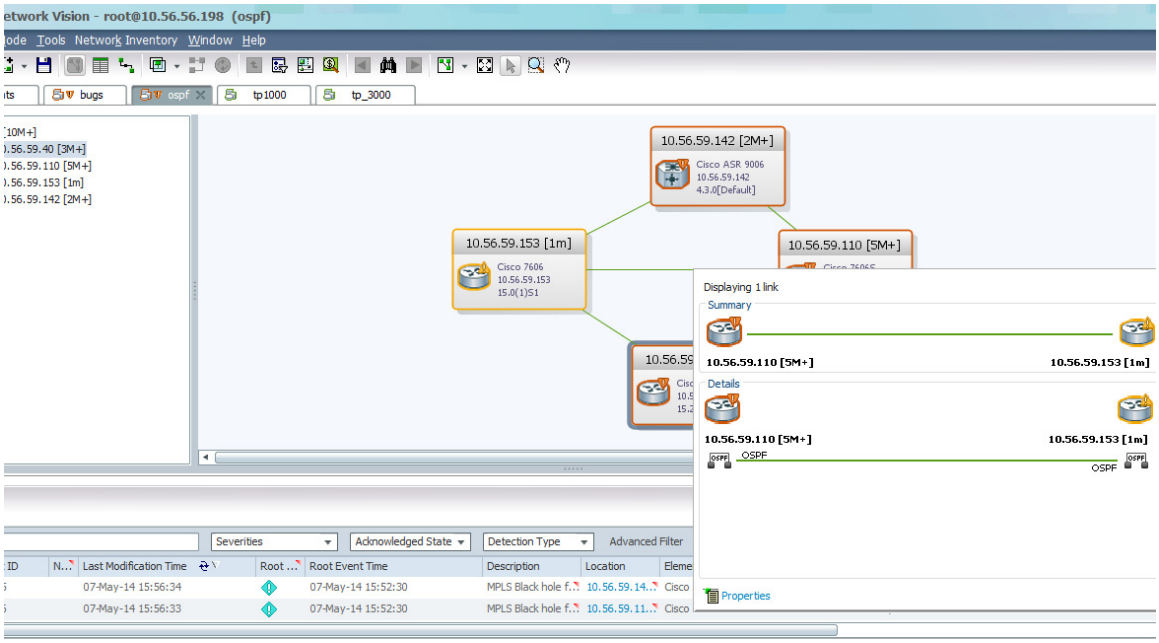
OSPF Topology

In OSPF topology, the links will be formed among the OSPF Process Device Components even though the link signifies the neighborship among them. The OSPF is a multilink topology, thus enabling the creation of multiple links from the same OSPF process. From Prime Network 5.1, the OSPF topology will be added along with the existing support.

The various types of topologies that can be formed under OSPF are

- Single layer topology
- Dynamic topology

The OSPF topological links are shown for the neighbors which has the Neighbor State as either FULL or TWOWAY. For neighbors with TWOWAY state, the OSPF interface's network type should be either BROADCAST or NBMA.



Viewing OSPF Link Properties

To view the OSPF link properties:

Step 1 In the Vision client, right-click on the link between the devices and select **Properties** to view the link properties.

Step 2 In the link properties window, the left pane displays the selected link and the right pane displays the link properties.

Figure 18-78 Viewing OSPF Link Properties

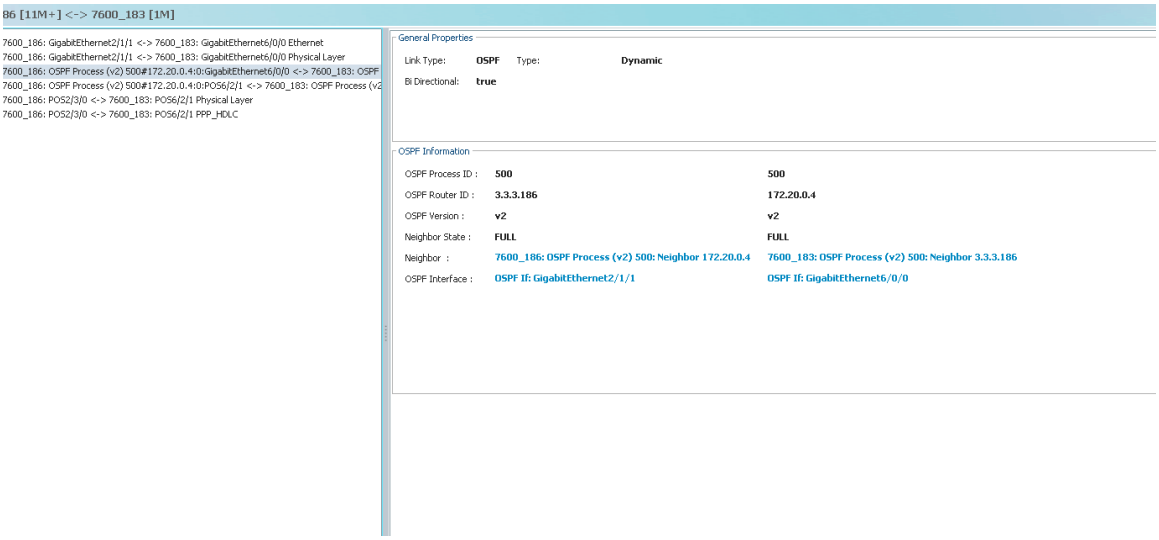


Table 18-62 describes the information that is displayed in link properties window.

Table 18-62 OSPF Link Properties window

Field	Description
Link Type	The link protocol, which is OSPF in this instance.
Type	The type of link, which is **Dynamic**.
Bi Directional	Indicates whether the link is bidirectional.
OSPF Information tab	
OSPF Process ID	The unique code to identify the OSPF process.
OSPF Router ID	The IP address of the OSPF router.
OSPF Version	The OSPF version, which can be v1, v2, or v3.
Neighbor State	The status of the OSPF neighbor, which can be Full and Two-Way.
Neighbor	Provides IP address of the OSPF Neighbor
OSPF Interface	The link to the OSPF interface.

Service Alarms

As part of the topological link support, two new service alarms **OSPF link down** and **OSPF link up** are introduced. These alarms are generated on the OSPF links in cases such as misconfigurations, shutting down of physical interfaces or any other scenario that might break the OSPF neighborship.

Correlation

The **OSPF link down** alarm is a ticketable event. It also can be correlated under the physical link alarms. If OSPF configured interface goes down, the OSPF link also goes down. For e.g, In case of interface shut down, the **OSPF link down** alarm is generated and correlated to the **Link down due to admin** service alarm.

Monitoring the CPT 50 Ring Support

The Cisco Carrier Packet Transport (CPT) Product Family with CPT600, CPT200 and CPT50 Series sets the industry benchmark as a compact carrier-class converged access and aggregation platform for Unified Packet Transport architectures.

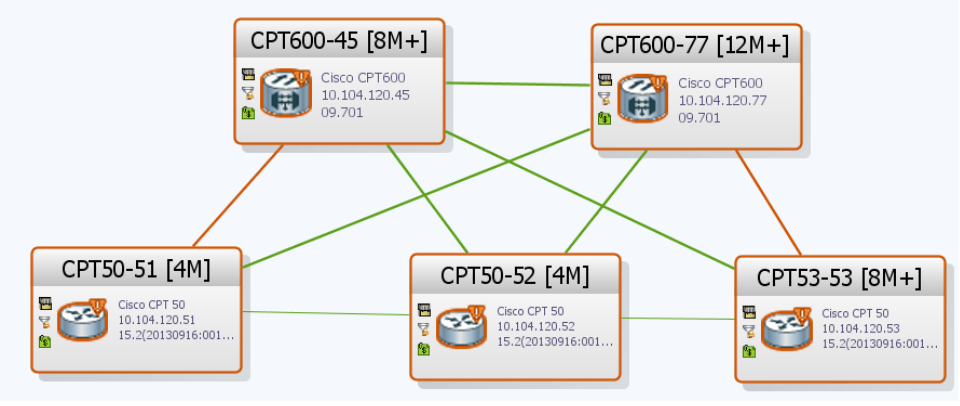
The CPT 50 is a compact and operationally simple, yet highly scalable and flexible platform optimized for delivering TDM like Ethernet Private 5.3 as well as multipoint capabilities for Business, Residential, Mobile Backhaul, Data Center, and Video Services. Its unique satellite architecture is designed to scale, simplify and enhance the operational and deployment aspects of service-delivery networks.

The CPT system also provides the ability to operate CPT 50 in a physical ring homed back to a single CPT 600 or CPT 200 chassis. This feature provides the flexibility of connecting CPT 50 in a closed-ended ring or an open-ended ring. As a result, the failure of a line or uplink card does not impact the traffic in a ring. CPT 50 in a ring works like a route processor and each CPT 50 interacts with Transport Node Controller (TNC) directly.

CPT 50 supports the following types of rings:

- Single Homed—A ring that is subtending from a single CPT-600 or CPT 200. There are two types of single home rings:
  - Open Ended Ring—Connects to the CPT-600 or CPT-200 through one interface only. Hence, there is only one unprotected path available to the traffic on the ring.
  - Closed—Connects to the CPT-600/200 through two interfaces. Hence there is a protected path available for the traffic either through the east or west interface on the ring.
- Dual Homed —A ring whose east port exists on one CPT 200 or CPT 600 (Working Ring Controller) and west port exists on another CPT 200 or CPT 600 (Protected Ring Controller). If WRC fails, this type of ring provides access to all the CPT 50s in the ring by switching the traffic to the other controller.

The following figure depicts the CPT 50 dual homed in Prime Network:



In the above figure, the dual ring home starts in one CPT 600 device and ends in another CPT 600 device. The CPT 600 device from which the dual ring starts is the Working Ring Controller (WRC) and the other CPT 600 device is the Protected Ring Controller (PRC).

Note To view more details about the device, right-click the device and choose **Inventory** to view the inventory details. The Node Role field in the content pane denotes whether the CPT device is WRC or PRC.

Configuring CPT

The following commands can be launched from the inventory by right-clicking the appropriate node and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands. To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Navigation	Description
Configure L2 Control Protocol	**Physical Inventory > Chassis > Backplane >** *slot* > *right-click on the Ethernet card* > **Commands > Configuration**	Use this command to configure the L2 Control Protocol.
Show L2 Control Protocol	**Physical Inventory > Chassis > Backplane >** *slot* > *right-click on the Ethernet card* > **Commands > Show**	Use this command to view details of the L2 Control protocol parameters configured for the selected port.
Add Loopback **Remove Loopback**	**Physical Inventory > Chassis > Backplane >** *slot* > *right-click on the Ethernet card* > **Commands > Configuration**	Use these commands to add and remove a loop-back respectively. **Note** Loop-back refers to the process of routing electronic signals or digital data streams, back to their source with processing or modifying it.
Configure CDP	**Physical Inventory > Chassis > Backplane >** *slot* > *right-click on the Ethernet card* > **Commands > Configuration**	Use this command to configure CDP. **Note** Cisco Discovery Protocol (CDP) is used to obtain protocol addresses of neighboring devices and discover the platform of those devices. It can also be used to show information about the interfaces your router uses.
Configure Ethernet		Use this command to configure Ethernet parameters.

Command	Navigation	Description
Show Ethernet Parameters	**Physical Inventory > Chassis > Backplane >** *slot* > *right-click on the Ethernet card* > **Commands** > **Show**	Use this command to view details of the Ethernet parameters configured for the selected Ethernet port.
Configure Port Parameters	**Physical Inventory > Chassis > Backplane >** *slot* > *right-click on the Ethernet card* > **Commands** > **Configuration**	Use this command to configure port parameters.
Show Port Parameters	**Physical Inventory > Chassis > Backplane >** *slot* > *right-click on the Ethernet card* > **Commands** > **Show**	Use this command to view the port parameters configured for the selected port.

Viewing the G8032 ERPS Configuration

Ethernet Ring Protection Switching is an effort at ITU-T under G.8032 Recommendation to provide sub-50ms protection and recovery switching for Ethernet traffic in a ring topology and at the same time ensuring that there are no loops formed at the Ethernet layer.

Ring Protection Switching Architecture works based on the following fundamentals:

- Principle of Loop Avoidance—Loop avoidance is achieved by guaranteeing that traffic flows on all but one of the ring links at any point of time. The one ring link from which traffic does not flow is called the Ring Protection Link (RPL), which is generally blocked. A designated Ethernet ring node—the RPL owner node—is responsible for blocking traffic at one end of the RPL. In the event of an Ethernet ring failure, the RPL owner node must unblock its end of the RPL and allow the RPL to be used for traffic.
- Utilization of learning, forwarding, and filtering database mechanisms defined in the Ethernet Flow Forwarding Function—Failure of Ethernet ring results in protection switching of traffic, which is controlled by the Ethernet Flow Forwarding Function. An APS protocol is used to coordinate the protection action over the ring, which transmits Ring Automatic Protection Switching (R-APS) messages.

Ethernet rings also supports multi ring/ladder network that consists of conjoined Ethernet rings by one or more interconnection points. The protection switching mechanisms and protocol are also applicable for multi ring/ladder network on adherence of certain principles.

The G8032 technology also supports multiple ERP instances over a ring. An ERP instance is an entity that is responsible for the protection of subset of VLANs carried over the physical ring and it should configure its own R-APS channel, RPL, RPL Owner and RPL Neighbor nodes.

Ring protection switching process also occurs based on the detection of defects on the transport entity on the ring link, and the transport entity can have a failed or non-failed condition. To monitor these defects, Ethernet ring protection may use any one of the following methods:

- Inherent—The fault condition status of each link connection is derived from the status of the underlying server layer trail.

- Sub-layer—Each ring link is monitored using Tandem Connection Monitoring (TCM).
- Test trail—An extra test trail is used to detect defects, which is setup along each ring link.

In Prime Network, the G8032 Ethernet Ring Protection Switching configuration can be viewed in the following nodes:

- Profile—This node displays the G8032 profile details. Each G8032 ring is associated to a profile, which consists of several timers. The timer displays details of the time frame the ring needs to wait before, during and after performing an action to avoid race conditions and unnecessary switching operations. If a ring is not associated to a profile, the default profile is automatically associated to it.
- Ring—This node displays the properties of the ring as well as the properties that are shared across all ERP instances

To view the G8032 Ethernet Ring Protection Switching Profile configuration:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **G8032** > **Profiles**. A list of all the G8032 profiles are displayed in the content pane.

Step 3 In the content pane, right-click on the profile name to view the **G8032 Profile Properties** window.

Table 18-63 describes the information displayed in the G8032 Profile Properties window.

Table 18-63 G8032 Profile Properties

Field	Description
Profile Name	The unique name of the profile associated to the G8032 ring.
WTR Interval	The Wait-to-Restore interval (in minutes) applicable to the G8032 ring. This interval refers to the duration before traffic is restored to the state, when it is found that a failure is no longer occurring. This interval also avoids toggling protection states in case of intermittent defects. This field defaults to 5 minutes.
Guard Interval	The Guard Interval (in milliseconds) that denotes the duration the node waits before performing a node state transition. This is done to block outdated R-APS messages from causing unnecessary node state changes. This field defaults to 500.
Holdoff Timer	The duration (in seconds) applicable for the G8032 ring. The node waits for the specified duration to expire before reporting faults to the ring protection mechanism.
Mode Type	The operating mode applicable for the G8032 ring, which can be any one of the following: • Revertive—In case the condition causing the switch is cleared, the traffic channel is restored to the working transport entity. • Non revertive—In case the condition causing the switch is cleared, the traffic channel continues to use the RPL. This field defaults to **Revertive**.

To view the G8032 Ethernet Ring Protection Switching Ring configuration:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **G8032** > **Ring** > *ring name*. The details of the ring are displayed in the content pane.

Table 18-64 describes the Ring properties.

Table 18-64 G8032 Ring Properties

Field	Description
Ring Name	The name of the ring.
Ring Type	The ring type, which can be any one of the following: • Open—When the ring is terminated by an Ethernet access such as VPLS. • Closed—When the arcs or links in the ring are simple Ethernet links.
Excluded VLAN ID	The range of VLAN ID that are excluded by the ring. In other words, the VLAN ID included in this range are not serviced by the ring and not blocked by the ring switching mechanism.
Untagged in Excluded VLANs	Indicates whether untagged Ethernet traffic is also blocked by the VLAN exclusion list.
Ring Ports Entries tab	
Port Number	The port number associated to the ring.
Local Port	The link to the local physical port that is used for this ring port.
Monitor Interface	The link to the interface that is used as the monitor interface. A monitor interface is used to monitor the ring port and detect ring failures.
Blocked VLAN IDs	The range of VLAN IDs that are blocked by the ring port.
Untagged in Blocked VLANs	Indicates whether untagged traffic is blocked by the ring port.
Unblocked VLAN IDs	The list of VLAN IDs that are not blocked by the ring port.
Untagged in Unblocked VLANs	Indicates whether untagged traffic is unblocked by the ring port.
Ring Instance Entries tab	
Instance	The unique code assigned to the instance.
Node Type	The node type that determines the node's responsibility towards the instance. This can be Normal, Owner, Neighbor, or Next Neighbor.
Node State	The state of the node for a specific instance, which can be any one of the following: Idle, Pending, Protection, Forced Switch, and Manual Switch. This state is configured by the administrator or determined by the APS as part of the G8032 protection protocol.
Port 0 State	The status of the port that is configured as Port 0, which can be N/A, RPL-Link, Faulty, Blocked, Local Forced Switch, or Local Manual Switch.
Port 1 State	The status of the port that is configured as Port 1, which can be N/A, RPL-Link, Faulty, Blocked, Local Forced Switch, or Local Manual Switch.
Instances tab	

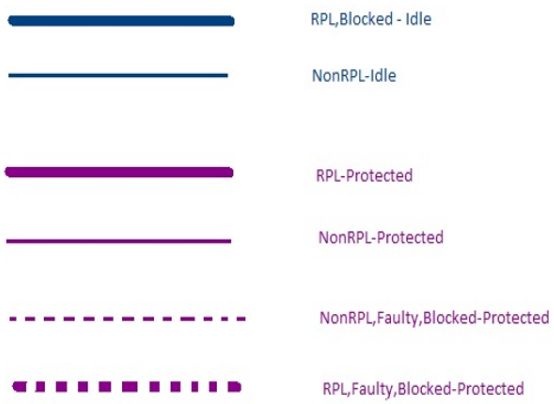
Table 18-64 G8032 Ring Properties

Field	Description
ID	The unique code assigned to the instance.
Instance Description	The description of the instance.
Profile	The link to the ring profile associated to the instance.
Included VLAN IDs	The list of VLAN IDs included or served by this instance, which includes all VLANs associated with the ring instance.
RPL Port Role	The Ring Protection Link (RPL) port in charge of the RPL, which enables it to turn the RPL on or off according to the ring instance functionality. This port can be Port 0 or Port 1.
APS Channel Level	The APS Channel Level for the ring instance, which can be any value between 0 and 7. This value is defined by the Maintenance Entity group Level (MEL) and is used to differentiate various Ethernet problems and to signal them.
Configuration State	The configuration status of the ring instance, which can be Resolved or Unresolved.
Unresolved Reason	The feedback to the configurator that explains the reason for the unresolved configuration state.

Viewing Ring Topology Properties from Topology View

An Ethernet ring consists of multiple Ethernet ring nodes. Each Ethernet ring node is connected to adjacent Ethernet ring nodes using two independent ring links. A ring link prohibits formation of loops that affect the network. The Ethernet ring uses a specific link to protect the entire Ethernet ring. This specific link is called the Ring Protection Link (RPL). A ring link is bound by two adjacent Ethernet ring nodes and a port for a ring link (also known as a ring port). There must be at least two Ethernet ring nodes in an Ethernet ring.

Prime Network uses the following color and pattern conventions to denote the types of links based on their ring type, ring state, and link state:



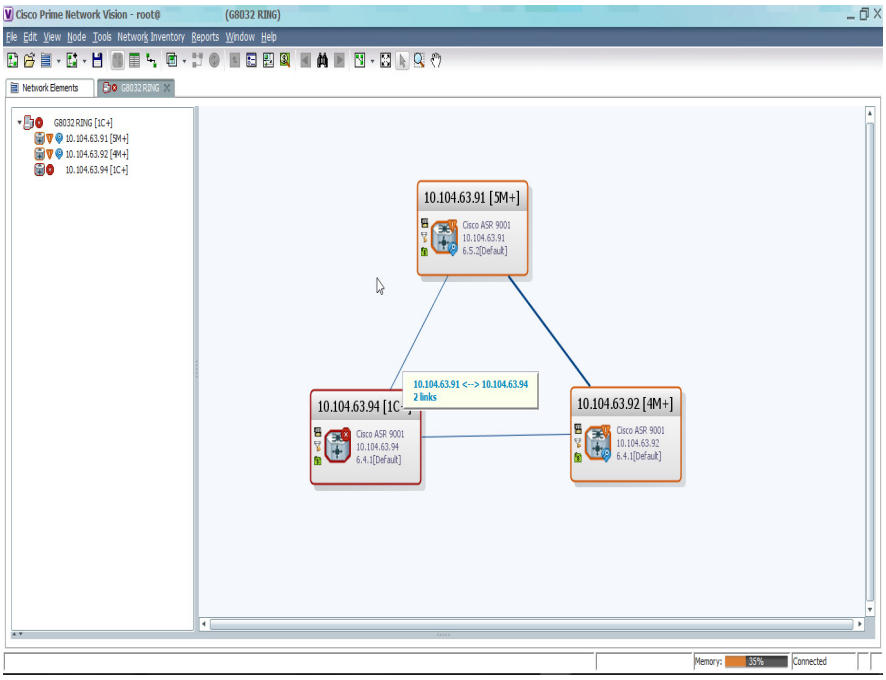
Links are displayed in the map based on the following propagation priority rules:

1. The critical events have first priority and are displayed in the map with corresponding color and pattern of the link (refer Image below) between the devices.
2. If there are no critical events, then faulty events are prioritized.
3. If there are no critical, faulty, or major events, then events with RPL Link color and pattern are prioritized.
4. If there are no RPL links, then the Non RPL link are prioritized.
5. RPL-Protected and Non RPL-Protected are prioritized over RPL,Blocked-Idle and Non RPL-Idle respectively.

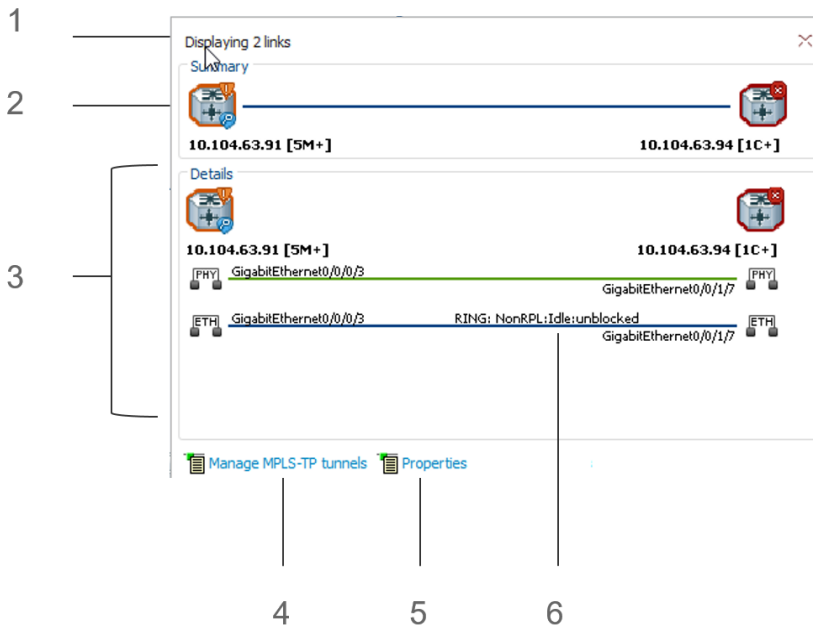
Viewing Ring Link Properties

To view link properties:

Step 1 In the Vision client map view, hover your mouse cursor over the link to display the link tool tip.



Step 2 Click the tooltip. The **Link Quick View** opens.



The Link Quick View provides the following information:

1	Number of links represented by the ring link in the map (in this example, two links).
2	Link endpoints.
3	List of all links represented by the ring link, including the link type, detail, and alarm status (color).
4	Opens the Manage MPLS-TP tunnels commands dialog box.
5	Opens the topological link properties window.
6	Ring information - ring type, ring state, and link state

Note The propagation priority rules of map mentioned above are applicable to Link Quick View too in case of two instances of same interface.

Step 3 Click **Properties** at the bottom of the **Link Quick View**. The **Topological Link Properties** window opens.

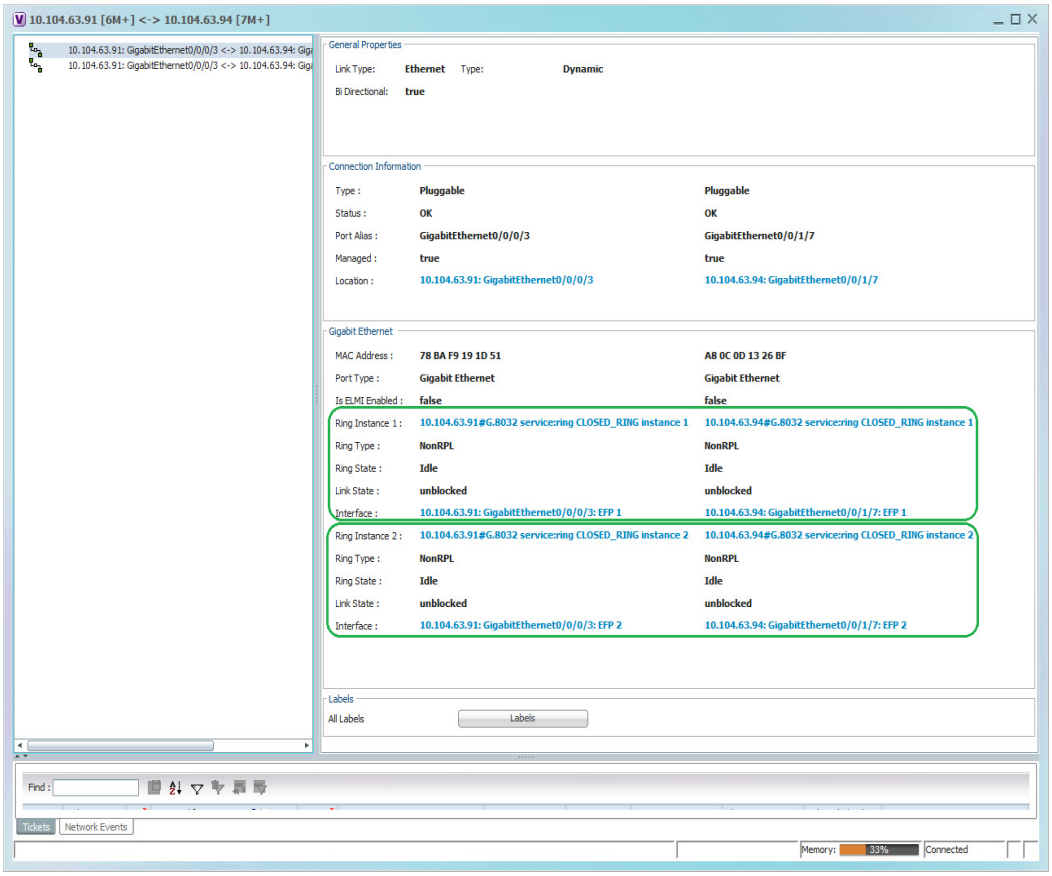


Table 18-65 describes the information that is displayed in the above window for the ring topology instances:

Table 18-65 Ring Instance properties

Field	Description
Gigabit Ethernet	
Ring Instance 1	Link to the Logical Inventory listing of the first ring instance
Ring Type	Type of the ring link of the first ring instance: • RPL • Non RPL
Ring State	State of the ring link of the first ring instance: • Protection • Idle
Link State	State of the link of the first ring instance: • Blocked • Unblocked • Faulty, blocked

Table 18-65 Ring Instance properties

Field	Description
Interface	Link to the Physical Inventory listing of the first ring instance
Ring Instance 2	Link to the Logical Inventory listing of the second ring instance
Ring Type	Type of the ring link of the second ring instance: • RPL • Non RPL
Ring State	State of the ring link of the second ring instance: • Protection • Idle
Link State	State of the link of the second ring instance: • Blocked • Unblocked • Faulty, blocked
Interface	Link to the Physical Inventory listing of the second ring instance

Note If there is only one ring instance in a ring topology, the properties of the second ring instance are not displayed.

Configuring REP and mLACP

The following commands can be launched from the inventory by right-clicking the appropriate node and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see Permissions for Managing Carrier Ethernet, page B-12). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Navigation	Description
REP Command		
Show REP Segment Information	**Commands > Show**	This action performed at the command launch point.
mLACP Commands		
Show Group **Show MPLS LDP** **Show Channel** **Show LACP Internal**	**Commands > Show**	These actions are performed at the command launch point.

Viewing the Remote Loop Free Alternate Configurations

When a link or router in the network fails, there is loss of data during the time it takes for the routers to converge after a topology change. Since it takes hundreds of milliseconds for the router to converge, the application traffic is sensitive to losses especially in the case of interactive multimedia services such as VoIP and pseudowires.

The Loop Free Alternate Fast ReRoute (LFA-FRR) technology helps reduce the packet loss that happens in the event of link or router failure. It reduces the failure reaction time to tens of milliseconds. This is achieved by using a pre-computed alternate next-hop. If the currently selected primary next-hop fails, then the alternate next-hop is used in the event of failure. A network that is configured with the LFA-FRR experiences less traffic loss and micro-looping of packets when compared to a network without LFA-FRR.

The Remote LFA-FRR technology is an extension of LFA that covers all topologies. It can dynamically compute its LFA node and forward traffic around a failed node to a remote LFA that is more than one hop away. After a node dynamically determines an alternate node (which is not directly connected to it), it establishes a directed Label Distribution Protocol (LDP) session to the alternate node. The directed LDP session exchanges labels for the particular forward error correction (FEC). When the network experiences link failure, the node manages to forward the data to the destination by using label stacking.

By configuring Remote LFA-FRR on your network, you can eliminate additional traffic engineering protocols, simplify operations with minimum configuration, prevent hair-pinning that occurs in TE-FRR, and compute node dynamically without manual provision.

In Prime Network, Remote LFA-FRR is configured using IS-IS and OSPF configurations.

To view the OSPF Remote LFA configuration:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **OSPF Processes** > *OSPF Process (version) ID*. The OSPF process details are displayed in the content pane. For more information, see Viewing IS-IS Properties, page 18-132.

Step 3 In the content pane, click the **RLFA Tunnels** tab as shown in Figure 18-79.

Figure 18-79 RLFA Tunnels tab

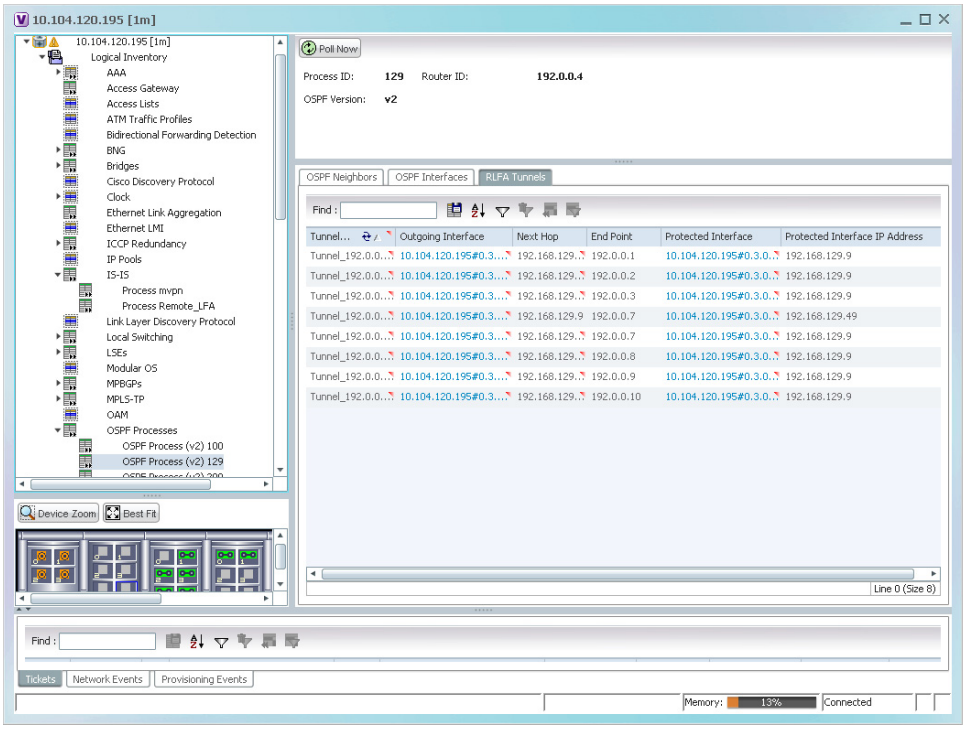


Table 18-66 describes the information that is displayed in the RLFA Tunnels tab.

Table 18-66 OSPF Processes - RLFA Tunnels tab

Field	Description
Tunnel Name	The name of the RLFA tunnel.
Out-Interface	The outgoing interface of the tunnel, which is used to reach the end point. Clicking this link will take you to the relevant entry in the physical inventory node.
Next Hop	The IP address of the next hop in the path.
End Point	The end point of the RLFA tunnel.
Protected Interface	The interface protected by the Remote RLFA tunnel.
Protected Interface IP Address	The IP Address of the interface protected by the Remote RLFA tunnel.

To view the IS-IS Remote LFA configuration:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **IS-IS** > *Process*. The IS-IS process details are displayed in the content pane. For more information, see Viewing IS-IS Properties, page 18-132.

Step 3 In the content pane, click the **RLFA Tunnels** tab. For more information, see Table 18-66.

Tie-Breaking Rules for Remote LFA

A primary path can have multiple LFAs. A routing protocol is used to implement tie-breaking rules. When the primary path fails, then these rules help to eliminate multiple candidate LFAs, select one LFA per primary path, and distribute the traffic over multiple LFAs.

Note The tie-breaking rule has certain conditions and attributes based on which multiple candidate LFAs are eliminated. If a rule eliminates all candidate LFAs, then the rule is omitted.

Configuring OSPF and ISIS with Remote LFA

The following can be launched from the inventory by right-clicking on the appropriate node and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see Permissions for Managing Carrier Ethernet, page B-12). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Navigation	Description
Create OSPF Process	In the Inventory window, right-click on the device > **Commands** > **Configuration** > **OSPF**.	Create a new OSPF process. The new OSPF process created here will be available under the **OSPF Processes** node in the Logical Inventory.
Show OSPF Database		View the OSPF database details.
Create OSPF Network	**Logical Inventory** > **OSPF Processes** > *OSPF Process*. Right-click on the process and choose **Commands > Configuration**.	Create one or more of the following OSPF Networks—Broadcast, Non-broadcast, Point-to-multipoint, and Point-to-point.
Delete OSPF Network		Delete an OSPF Network created using the **Create OSPF Network** command.
Delete OSPF Process		Delete an OSPF process created using the **Create OSPF Process** command.
Modify OSPF Process		Modify details of the OSPF process created using the **Create OSPF Process** command.
Create OSPF Passive Interface		Create a passive interface for an OSPF process.
Delete OSPF Passive Interface		Delete a passive interface for an OSPF process.

Command	Navigation	Description
Show OSPF Neighbor	**Logical Inventory** > **OSPF Processes** > *OSPF process*. Right-click and choose **Commands** > **Show**.	View the OSPF neighbor details. **Note** This command is available only for ASR 9000 devices.
Show OSPF Process	**Logical Inventory** > **OSPF Processes** > *OSPF process*. Right-click and choose **Commands** > **Show**	View the OSPF process details.
Create OSPF on Interface	**Logical Inventory** > **Routing Entities** > **Routing Entity**. In the content pane, right-click the name in the **IP Interfaces** tab and choose **Commands** > **Configuration**.	Create a new IP interface on an existing OSPF process. The new interface details can be viewed under the **OSPF Interfaces** section in the content pane on selection of an OSPF process.
Modify OSPF on Interface	**Logical Inventory** > **OSPF Processes** > *OSPF process.* In the **OSPF Interfaces** section in the content pane, right-click the IP Interface > **Commands** > **Configuration**.	Modify the OSPF interface details for a selected OSPF process. **Note** This command is available only for ASR 9000 devices.
Delete OSPF from Interface		Delete the OSPF interface details for a selected OSPF process. **Note** This command is available only for ASR 9000 devices.
Show OSPF On Interface	**Logical Inventory** > **Routing Entities** > **Routing Entity**. In the content pane, Right-click the name in the **IP Interfaces** tab and choose **Commands** > **Configuration**.	View the OSPF interface details.
Create ISIS Router	**Logical Inventory** > **IS-IS** > **System**. Right-click and choose **Commands** > **Configuration**.	Create a new ISIS process.

Command	Navigation	Description
Create ISIS Address Family	**Logical Inventory** > **IS-IS**. In the content pane, Right-click the process and choose **Commands** > **Configuration**.	Create an Address Family (IPV4 or IPV6)for a selected ISIS process.
Create ISIS Interface		Create an ISIS interface for the selected process.
Delete ISIS Address Family		Delete the Address Family (IPV4 or IPV6) created for the selected ISIS process.
Delete ISIS Router		Delete the ISIS process.
Modify ISIS Address Family		Modify the Address Family (IPV4 or IPV6) details created for the ISIS process.
Modify ISIS Router		Modify the ISIS process details.
Create ISIS Interface Address Family		Create an Address Family for an ISIS interface. **Note** This command is applicable only for ASR 9000.
Modify ISIS Interface Address Family		Modify the Address Family details created for an ISIS interface. **Note** This command is applicable only for ASR 9000 devices.
Delete ISIS Interface Address Family		Delete the Address Family details created for an ISIS interface. **Note** This command is applicable only for ASR 9000 devices.

Using Pseudowire Ping and Show Commands

The following commands can be launched from the inventory by right-clicking the appropriate node and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see Permissions for Managing Carrier Ethernet, page B-12). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Navigation	Description
Ping Pseudowire	**Logical Inventory** > **Pseudowires** > *right-click the interface* > **Commands > Configure >**	Pings the peer router with a tunnel ID from a single or multisegment pseudowire. This command can be used to verify connectivity between any set of PE routers in the pseudowire path. For a multisegment pseudowire this command can be used to verify that all the segments of the multisegment pseudowire are operating. You can use this command to verify connectivity at the following pseudowire points: • From one end of the pseudowire to the other • From one of the pseudowires to a specific segment • The segment between two adjacent PE routers You can choose to ping the peer router by default or provide the IP of the required destination router to ping.
Display Pseudowire	**Logical Inventory** > **Pseudowire >** *right-click the required interface* > **Commands > Show > Display Pseudowire**	Shows the MPLS Layer 2 (L2) transport binding using tunnel identifier. MPLS L2 transport binding allows you to identify the VC label binding information. This command can be used to display information about the pseudowire switching point.

Configuring IS-IS

In order to enable IS-IS for IP on a Cisco router and have it exchange routing information with other IS-IS enabled routers, you must perform these two tasks:

- Enable the IS-IS process and assign area
- Enable IS-IS for IP routing on an interface

You can configure the router to act as a Level 1 (intra-area) router, as Level 1-2 (both a Level 1 router and a Level 2 router), or as Level 2 (an inter-area router only).

The following IS-IS commands can be launched from the inventory by right-clicking on the appropriate node and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see Permissions for Managing Carrier Ethernet, page B-12). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Navigation	Description
Create ISIS Router	**ISIS** > *right-click System* > **Commands** > **Configuration**	Creates an IS-IS routing process and specify the area for each instance of the IS-IS routing process. An appropriate Network Entity Title (NET) must be configured to specify the area address for the IS-IS area and system ID of the router.Up to eight processes are configurable. A maximum of five IS-IS instances on a system are supported.
Modify ISIS Router **Delete ISIS Router**	**ISIS > System >** *right-click Process ID in content pane* **> Commands > Configuration**	Modifies or deletes an existing IS-IS routing configuration for the specified routing process.
Create ISIS Interface	**ISIS > System >** *right-click Process ID in content pane* **> Commands > Configuration**	Creates or modifies an IS-IS routing process and assign it to a specific interface, rather than to a network.
Modify ISIS Interface **Delete ISIS Interface**	**ISIS >** *expand* **System >** *select a Process* **>** *select* **Interfaces** *tab* **>** *right-click the Interface Name* **> Commands > Configuration**	
Create ISIS Address Family **Modify ISIS Address Family** **Delete ISIS Address Family**	**ISIS > System >** *right-click Process ID in content pane* **> Commands > Configuration**	Configure or modify IS-IS routing to use standard IP Version 4 (IPv4) and IP Version 6 (IPv6) address prefixes.

Managing Ethernet Networks Using Operations, Administration, and Maintenance Tools

Prime Network supports three, interrelated OAM components, including:

- Connectivity Fault Management—Connectivity Fault Management (CFM) is an end-to-end per-service-instance (per VLAN) Ethernet layer OAM protocol that includes connectivity monitoring, fault verification, and fault isolation. CFM allows you to manage individual customer service instances. Ethernet Virtual Connections (EVCs) are the services that are sold to customers and are designated by service VLAN tags. CFM operates on a per-service-VLAN (or per-EVC) basis. It lets you know when an EVC fails and provides tools to isolate the failure. See Viewing Connectivity Fault Management Properties, page 19-2 and Configuring CFM, page 19-16.
- Ethernet Local Management Interface—Ethernet Local Management Interface (Ethernet LMI) operates between the customer edge (CE) and the user-facing provider edge (U-PE) devices. Ethernet LMI allows you to automatically provision CEs based on EVCs and bandwidth profiles. See Viewing Ethernet LMI Properties, page 19-8 and Configuring E-LMI, page 19-18.
- Link OAM—Link OAM allows you to monitor and troubleshoot a single Ethernet link. It is an optional sublayer implemented in the Data Link Layer between the Logical Link Control (LLC) and MAC sublayers of the Open Systems Interconnect (OSI) model. You can monitor a link for critical events and, if needed, put a remote device into loopback mode for link testing. Link OAM also discovers unidirectional links, which are created when one transmission direction fails. See Viewing Link OAM Properties, page 19-11 and Configuring L-OAM, page 19-18.

The following topics describe how you can use the Vision client to monitor Ethernet operations, administration, and maintenance (OAM) tools. If you cannot perform an operation that is described in these topics, you may not have sufficient permissions; see Permissions for Using Ethernet OAM Tools, page B-17.

Viewing Connectivity Fault Management Properties

CFM allows you to discover and verify end-to-end, Carrier Ethernet PE-to-PE or CE-to-CE paths through bridges and LANs.

CFM consists of maintenance domains. Maintenance domains are administrative regions used to manage and administer specific network segments. Maintenance domains are organized in a hierarchy. The administrator assigns a maintenance level to the domain from 0 (lowest level) to 7 (highest level); the maintenance level determines the domain's position within the CFM hierarchy.

CFM maintenance domain boundaries are indicated by maintenance points. A maintenance point is an interface point that participates within a CFM maintenance domain. Maintenance point types include:

- Maintenance Endpoints—Maintenance endpoints (MEPs) are active CFM elements residing at the edge of a domain. MEPs can be inward or outward facing. They periodically transmit continuity check messages and expect to periodically receive similar messages from other MEPs within a domain. If requested, MEPs can also transmit traceroute and loopback messages. MEPs are responsible for keeping CFM messages within the boundaries of a maintenance domain.
- Maintenance Intermediate Points—Maintenance intermediate points (MIPs) are passive elements that catalog information received from MEPs and other MIPs. MIPs only respond to specific CFM messages such as traceroute and loopback, and they forward those messages within the maintenance domain.

Note The Vision client does not display information for CFM maintenance endpoints or maintenance intermediate points for Cisco Viking devices if errors exist in their configurations. An error in the configuration is indicated by an exclamation point (!) in the CLI output.

For example, if you enter the command **`show ethernet cfm local maintenance-points`**, a configuration error is indicated as follows:

```
cfm_d100/2        cfm_s100        Te0/2/0/3.110        Up MEP 2100 eb:7a:53!
```

CFM uses standard Ethernet frames. CFM frames are distinguishable by EtherType and for multicast messages, by MAC address. CFM frames are sourced, terminated, processed, and relayed by bridges. Routers support only limited CFM functions.

Bridges that cannot interpret CFM messages forward them as normal data frames. All CFM messages are confined to a maintenance domain and to an S-VLAN (PE-VLAN or Provider-VLAN). CFM supports three types of messages:

- Continuity check—Multicast heartbeat messages exchanged periodically among MEPs. They allow MEPs to discover other MEPs within a domain and allow maintenance intermediate points (MIPs) to discover MEPs. Continuity check messages (CCMs) are confined to a domain and S-VLAN.
- Loopback—Unicast frames that a MEP transmits, at the request of an administrator, to verify connectivity to a particular maintenance point. A reply to a loopback message indicates whether a destination is reachable but does not allow hop-by-hop discovery of the path. A loopback message is similar in concept to an Internet Control Message Protocol (ICMP) Echo (ping) message.
- Traceroute—Multicast frames that a MEP transmits, at the request of an administrator, to track the path (hop-by-hop) to a destination MEP. They allow the transmitting node to discover vital connectivity data about the path, and allow the discovery of all MIPs along the path that belong to

the same maintenance domain. For each visible MIP, traceroute messages indicate ingress action, relay action, and egress action. Traceroute messages are similar in concept to User Datagram Protocol (UDP) traceroute messages.

From the Logical Inventory tree, you can troubleshoot MEPs using CFM ping, traceroute, MEP status, and MEP cross-check status. These commands, and all CFM commands, are described in Configuring CFM, page 19-16.

Prime Network associates alarms with the corresponding MEP or global CFM logical inventory objects. Prime Network correlates MEP down, MEP up, MEP missing, ETH-AIS, and ETH-RDI events with root cause alarms and corresponding tickets that exist along the path between the MEP on the reporting network element and the network element hosting the remote MEP.

To view CFM properties:

Step 1 In the Vision client, double-click the required device for CFM.

Step 2 In the **Inventory** window, choose **Logical Inventory > CFM**.

Figure 19-1 shows an example of CFM in logical inventory.

Figure 19-1 CFM in Logical Inventory

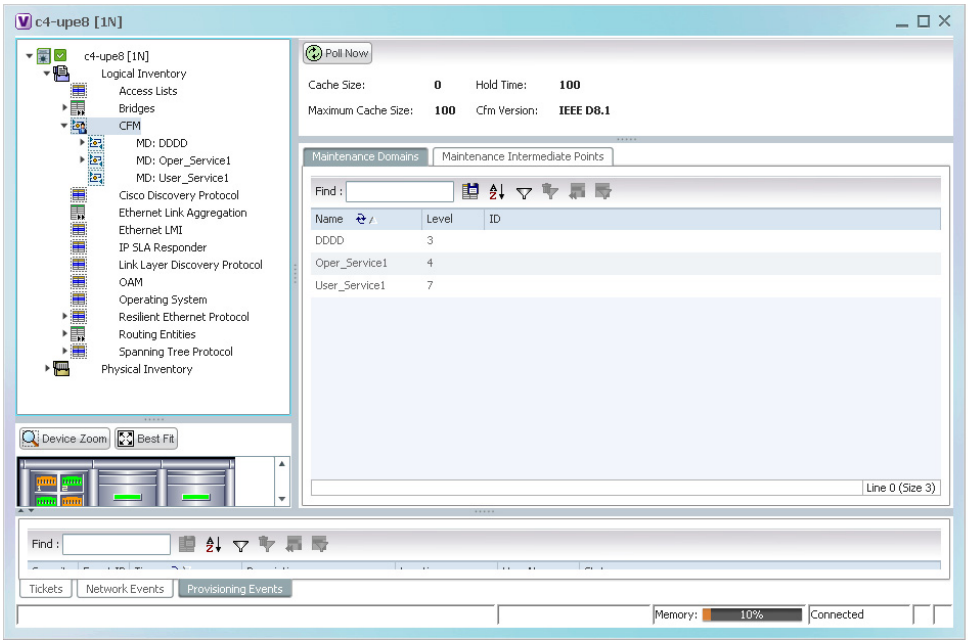


Table 19-1 describes the information displayed for CFM.

Table 19-1 CFM Properties

Field	Description
Cache Size	CFM traceroute cache size in number of 5.3.
Hold Time	Configured hold time (in minutes) that is used to indicate to the receiver the validity of traceroute and loopback messages transmitted by the device. The default value is 2.5 times the transmit interval.
Maximum Cache Size	Maximum CFM traceroute cache size in number of 5.3.

Table 19-1 CFM Properties (continued)

Field	Description
CFM Version	CFM version, such as IEEE D8.1.
Maintenance Domains Table	
Name	Domain name.
Level	Unique level the domain is managed on. Values range from 0 to 7.
ID	Optional domain identifier.

Step 3 Click the Maintenance Intermediate Points tab to view MIP information. See Figure 19-2.

Figure 19-2 CFM Maintenance Intermediate Points Tab

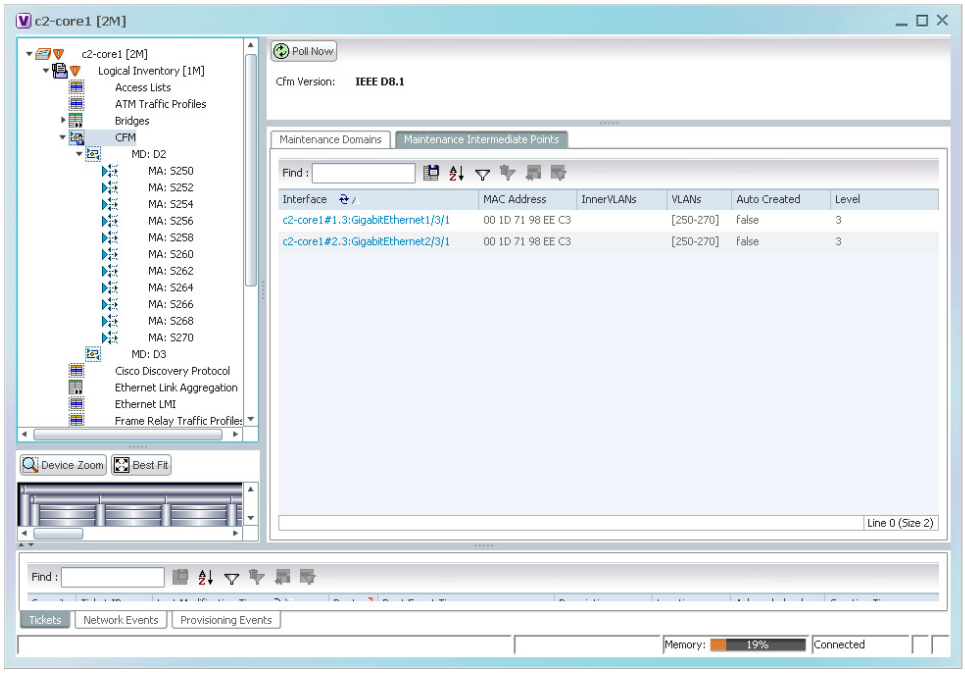


Table 19-2 describes the information that is displayed in the Maintenance Intermediate Points tab.

Table 19-2 CFM Maintenance Intermediate Point Properties

Field	Description
Interface	Interface configured as a MIP, hyperlinked to its entry in physical inventory.
MAC Address	MAC address of the interface.
Inner VLANs	Inner VLAN identifiers.
VLANs	VLANs associated with the interface.
Auto Created	Whether or not the MIP was automatically created: True or False.
Level	Unique level the domain is managed on. Values range from 0 to 7.

Step 4 To view the details of a specific maintenance domain, do one of the following:

- Choose **Logical Inventory > CFM >** *domain*.
- Double-click the required entry in the Maintenance Domains table.

Figure 19-3 shows an example of the information displayed for the maintenance domain.

Figure 19-3 CFM Maintenance Domain Properties

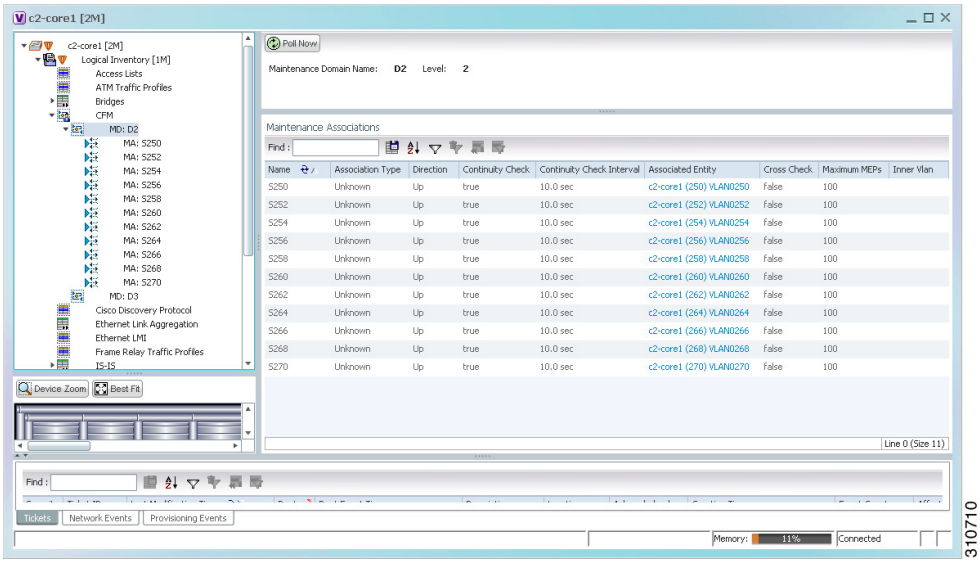


Table 19-3 describes the information that is displayed for CFM maintenance domains.

Table 19-3 CFM Maintenance Domain Properties

Field	Description
Maintenance Domain Name	Name of the domain.
Level	Level at which the domain is managed: 0-7.
ID	Optional maintenance domain identifier.
Maintenance Associations Table	
Name	Name of the maintenance association.
Association Type	Maintenance association type.
Direction	Direction of the maintenance association: Up or Down.
Continuity Check	Whether or not the continuity check is enabled: True or False.
Continuity Check Interval	Interval (in seconds) for checking continuity.
Associated Entity	Bridge, port, or pseudowire that the maintenance association uses for CFM. Click the hyperlinked entry to view the item in inventory.
Cross Check	Whether or not cross checking is enabled: True or False.
Maximum MEPs	Maximum number of maintenance endpoints (MEPs) that can be configured on the maintenance association.
Inner VLAN	Inner VLAN identifier.

Step 5 To view the properties for a maintenance association's endpoints, do one of the following:

- Choose **Logical Inventory > CFM >** *domain* **>** *association*.
- In the Maintenance Associations table, double-click the required association.

Figure 19-4 shows the information displayed for the maintenance association endpoints.

Figure 19-4 CFM Maintenance Association - Endpoint Properties

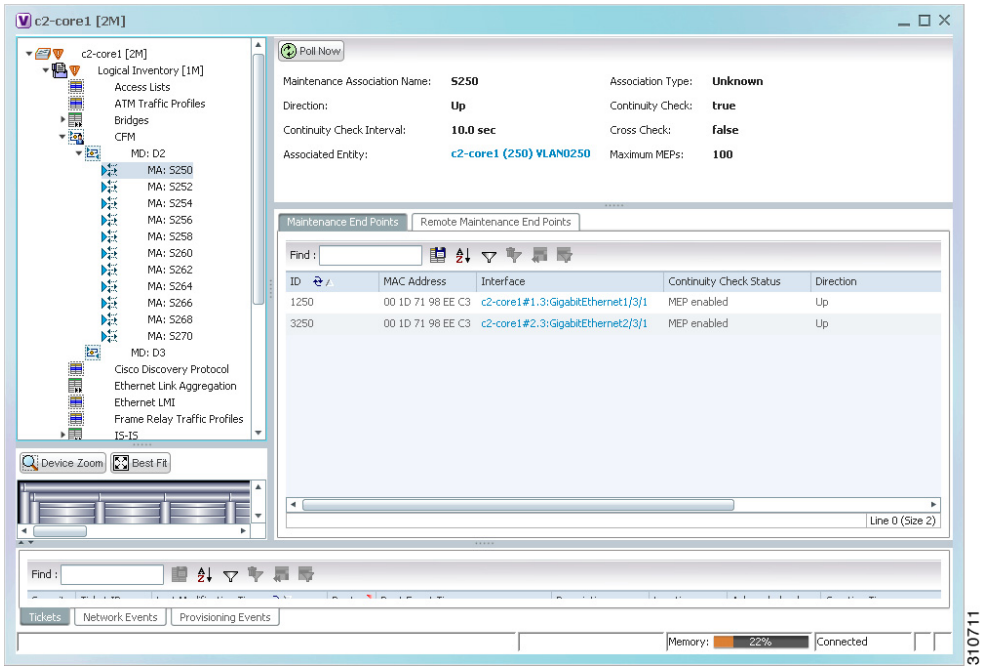


Table 19-4 describes the information that is displayed for CFM maintenance associations and MIPs.

Table 19-4 CFM Maintenance Association Properties

Field	Description
Maintenance Association Name	Name of the maintenance association.
Association Type	Maintenance association type, such as Bridge Domain.
Direction	Direction of the maintenance association: Up or Down.
Continuity Check	Whether or not the continuity check is enabled: True or False.
Continuity Check Interval	Interval (in seconds) for checking continuity.
Cross Check	Whether or not cross checking is enabled: True or False.
Associated Entity	Bridge that the maintenance association uses for CFM. Click the hyperlinked entry to view the bridge in logical inventory.
Maximum MEPs	Maximum number of MEPs that can be configured on the maintenance association.
Inner VLANs	Inner VLAN identifiers.
Maintenance End Points Table	
ID	Local identifier for the MEP.

Table 19-4 CFM Maintenance Association Properties (continued)

Field	Description
MAC Address	MAC address that identifies the MEP.
Interface	Interface on which the MEP is configured, hyperlinked to the respective EFP, VSI or interface in inventory.
Continuity Check Status	CFM continuity check status: MEP Active, MEP Inactive, MEP Enabled, MEP Disabled, or Unknown.
Direction	Direction of traffic on which the MEP is defined: Up, Down, or Unknown.

Step 6 Click the **Remote Maintenance End Points** tab to view the information displayed for remote MEPs. See Figure 19-5.

Figure 19-5 Remote Maintenance End Points Table

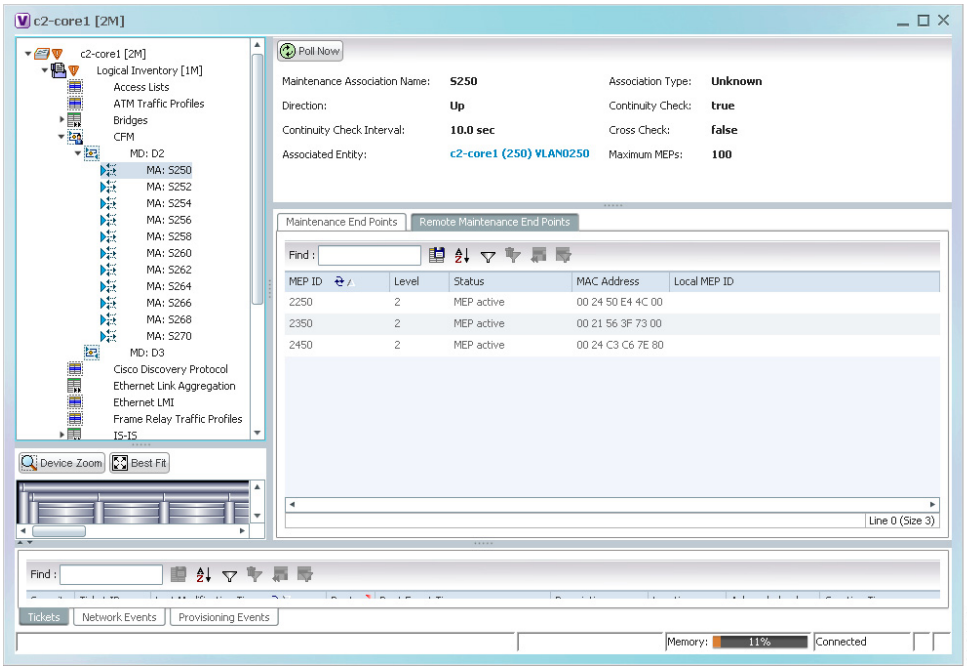


Table 19-5 describes the information presented for remote MEPs.

Table 19-5 CFM Remote Maintenance End Points Table

Field	Description
MEP ID	Remote MEP identifier.
Level	Level at which the remote MEP is managed: 0-7.
Status	Status of the remote MEP, such as MEP Active.
MAC Address	MAC address of the remote MEP.
Local MEP ID	Numeric identifier assigned to the local MEP. Values range from 1 to 8191. **Note** If the remote MEP is in Up mode, the remote MEP is not associated to the local MEP. As a result, the Local MEP ID column is empty.

Viewing Ethernet LMI Properties

Ethernet Local Management Interface (E-LMI) is a protocol that operates between the customer edge (CE) network element and the provider edge (PE) network element. Ethernet LMI is a protocol between the CE network element and the provider edge (PE) network element. It runs only on the PE-CE UNI link and notifies the CE of connectivity status and configuration parameters of Ethernet services available on the CE port. Ethernet LMI interoperates with an OAM protocol, such as CFM, that runs within the provider network to collect OAM status. CFM runs at the provider maintenance level. Ethernet LMI relies on the OAM Ethernet Infrastructure (EI) to work with CFM for end-to-end status of EVCs across CFM domains. E-LMI commands are described in Configuring E-LMI, page 19-18.

The IOS OAM manager stream interaction between OAM protocols, and handles the interaction between CFM and E-LMI. Ethernet LMI interaction with the OAM manager is unidirectional, running only from the OAM manager to E-LMI on the U-PE side of the switch. Information is exchanged either as a result of a request from E- LMI or triggered by the OAM manager when it receives notification of a change from the OAM protocol. Information that is relayed includes the EVC name and availability status, remote UNI name and status, and remote UNI counts.

To view Ethernet LMI properties:

Step 1 In the Vision client, double-click the device configured for Ethernet LMI.

Step 2 In the **Inventory** window, choose **Logical Inventory > Ethernet LMI**.

Figure 19-6 shows an example of Ethernet LMI properties in logical inventory.

Figure 19-6 Ethernet LMI in Logical Inventory

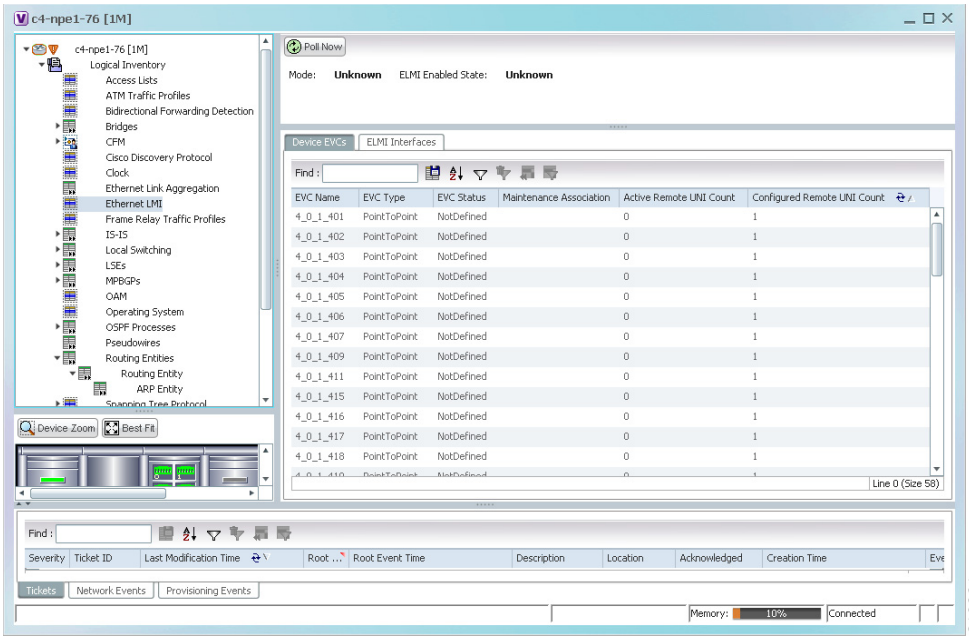


Table 19-6 describes the information displayed for Ethernet LMI.

Table 19-6 Ethernet LMI Properties in Logical Inventory

Field	Description
Globally Enabled	Whether or not Ethernet LMI is enabled globally: True or False.
Mode	Ethernet LMI mode: CE or PE.
Device EVCs Tab	
EVC Name	Name of the EVC.
EVC Type	Type of EVC: Point-to-point or Multipoint.
EVC Status	EVC status: Active, Inactive, Not Defined, or Partially Active.
Maintenance Association	Hyperlinked entry to the maintenance association in CFM in logical inventory. For more information about maintenance associations, see Table 19-4.
Active Remote UNI Count	Number of active remote UNIs.
Configured Remote UNI Count	Number of configured remote UNIs.
ELMI Interfaces Tab	
Interface Name	Hyperlinked entry to the interface in physical inventory. For more information, see Step 4 in this procedure.
T391	Frequency at which the customer equipment sends status inquiries. The range is 5-30 seconds, with a default of 10 seconds.
T392	Frequency at which the metro Ethernet network verifies that status enquiries have been received. The range is 5-30 seconds, with a default of 15 seconds. A value of 0 (zero) indicates the timer is disabled.

Table 19-6 Ethernet LMI Properties in Logical Inventory (continued)

Field	Description
N391	Frequency at which the customer equipment polls the status of the UNI and all EVCs. The range is 1-65000 seconds, with a default of 360 seconds.
N393	Error count for the metro Ethernet network. The range is 1-10, with a default of 4.

Step 3 To view device EVC properties, double-click an EVC name in the Device EVCs tab.

The Device EVC Properties window is displayed as shown in Figure 19-7.

Figure 19-7 Device EVC Properties Window

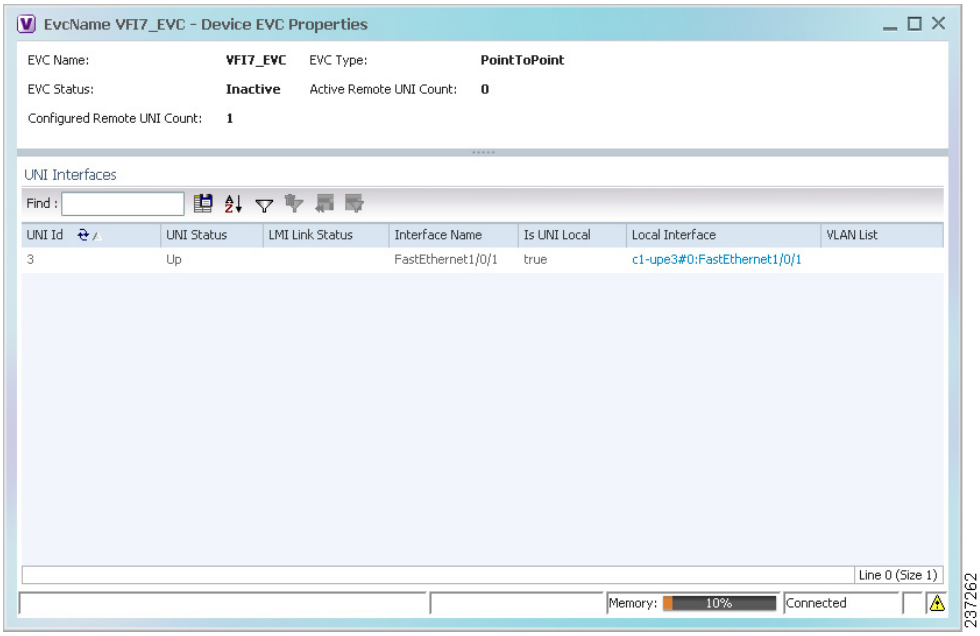


Table 19-7 describes the information displayed in the Device EVC Properties window.

Table 19-7 Device EVC Properties in Logical Inventory

Field	Description
EVC Name	Name of the EVC.
EVC Type	Type of EVC: Point-to-point or Multipoint.
EVC Status	EVC status: Active, Inactive, Not Defined, or Partially Active.
Maintenance Association	Hyperlinked entry to the maintenance association in CFM in logical inventory. For more information about maintenance associations, see Table 19-4.
Active Remote UNI Count	Number of active remote UNIs.
Configured Remote UNI Count	Number of configured remote UNIs.

Table 19-7 Device EVC Properties in Logical Inventory (continued)

Field	Description
UNI Interfaces Table	
UNI Id	UNI identifier.
UNI Status	Status of the UNI: Up or Down.
LMI Link Status	Status of the LMI link: Up or Down.
Interface Name	Interface on which UNI is configured.
Is UNI Local	Whether or not UNI is local: True or False.
Local Interface	Hyperlinked entry to the interface in physical inventory.
VLAN List	Name of the VLAN associated with the UNI interface.

Step 4 To view properties for an Ethernet LMI interface in physical interface, click the required interface name in the ELMI Interfaces table.

Table 19-8 describes the information displayed in the UNI Properties area in physical inventory.

Table 19-8 Ethernet LMI UNI Properties in Physical Inventory

Field	Description
Service Multiplexing Enabled	Whether or not the interface is configured for UNI multiplexing: True or False.
Bundling Enabled	Whether or not the interface is configured for UNI bundling: True or False.
UNI Id	UNI identifier.
Bundling Type	Type of bundling applied: All-to-One or None. This field appears only when a bundling type is set.

Viewing Link OAM Properties

Link OAM is an optional sublayer implemented in the OSI Data Link Layer between the Logical Link Control and MAC sublayers. Link (802.3AH) OAM (L-OAM) can be implemented on any full-duplex point-to-point or emulated point-to-point Ethernet link.

The frames (OAM Protocol Data Units [OAMPDUs]) cannot propagate beyond a single hop within an Ethernet network and have modest bandwidth requirements (frame transmission rate is limited to a maximum of 10 frames per second).

Link OAM processes include:

- Discovery—Discovery is the first Link OAM process. During discovery, Link OAM identifies the devices at each end of the link and learns their OAM capabilities.
- Link monitoring—Link OAM link monitoring includes:
  - Monitoring links and issuing notifications when error thresholds are exceeded or faults occur.

  - Collecting statistics on the number of frame errors (or percent of frames that have errors) and the number of coding symbol errors.
- Remote MIB Variable Retrieval—Provides 802.3ah MIB polling and response.
- Remote Failure indication—Informs peers when a received path goes down. Because link connectivity faults caused by slowly deteriorating quality are difficult to detect, Link OAM communicates such failure conditions to its peer using OAMPDU flags. The failure conditions that can be communicated are a loss of signal in one direction on the link, an unrecoverable error (such as a power failure), or some other critical event.
- Remote Loopback—Puts the peer device in (near-end) intrusive loopback mode using the OAMPDU loopback control. Statistics can be collected during the link testing. In loopback mode, every frame received is transmitted back unchanged on the same port (except for OAMPDUs, which are needed to maintain the OAM session). Loopback mode helps ensure the quality of links during installation or troubleshooting. Loopback mode can be configured so that the service provider device can put the customer device into loopback mode, but the customer device cannot put the service provider device in loopback mode.

Prime Network supports topology discovery based on Link OAM information and enables you to view Link OAM properties. You can also configure L-OAM using the commands described in Configuring L-OAM, page 19-18.

For information on CFM and Ethernet LMI, see Viewing Connectivity Fault Management Properties, page 19-2 and Viewing Ethernet LMI Properties, page 19-8.

To view Link OAM properties:

Step 1 In the Vision client, double-click the device configured for Link OAM.

Step 2 In the **Inventory** window, choose **Logical Inventory > OAM**.

Figure 19-8 shows an example of Link OAM properties in logical inventory.

Figure 19-8 Link OAM Properties in Logical Inventory

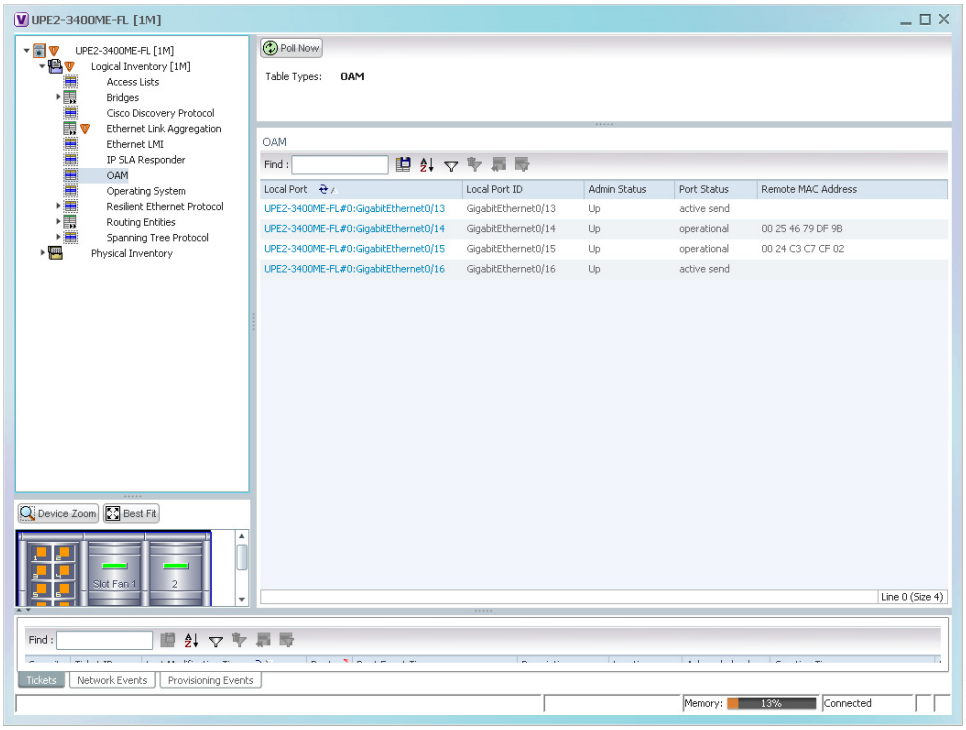


Table 19-9 describes the information displayed for Link OAM.

Table 19-9 Link OAM Properties in Logical Inventory

Field	Description
Table Types	Type of table. In this case, it is OAM.
OAM Table	
Local Port	Name of the OAM-supported interface, hyperlinked to the location in physical inventory.
Local Port ID	Local port identifier, such as FastEthernet1/0/9.
Admin Status	Administrative status of the interface.
Port Status	Status of the port.
Remote MAC Address	Remote client MAC address.

Step 3 To view detailed information about an entry in the table, double-click the required entry.

The Link OAM Data Properties window is displayed as shown in Figure 19-9.

Figure 19-9 Link OAM Data Properties Window

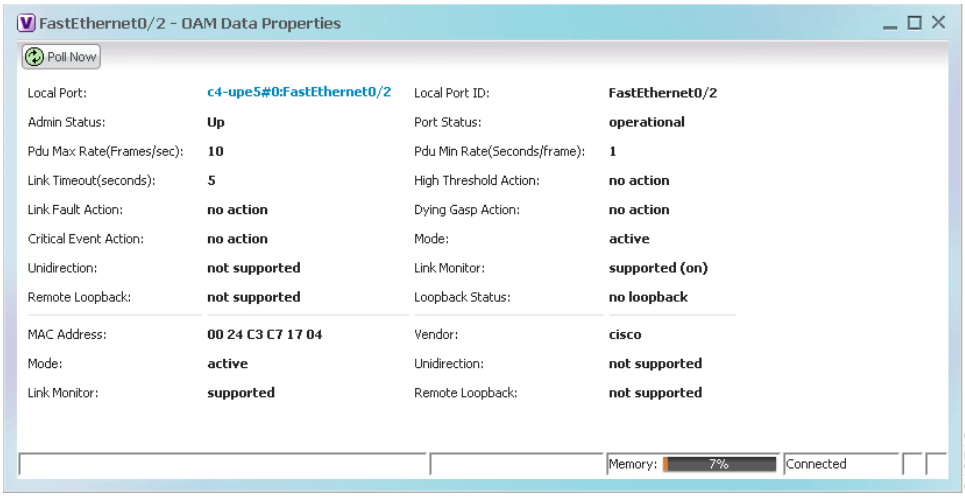


Table 19-10 describes the information that is displayed in the Link OAM Data Properties window.

Table 19-10 Link OAM Data Properties Window

Field	Description
Local Interface	
Local Port	Name of the OAM-supported interface, hyperlinked to the location in physical inventory.
Local Port ID	Local port identifier.
Admin Status	Administrative status of the interface: Up or Down.
Port Status	Status of the port, such as Operational.
PDU Max Rate (Frames/sec)	Maximum transmission rate measured by the number of OAM PDUs per second; for example, 10 packets per second.
PDU Min Rate (Seconds/frame)	Minimum transmission rated measured by the number of seconds required for one OAM PDU; for example, 1 packet per 2 seconds.
Link Timeout	Number of seconds of inactivity on a link before the link is dropped.
High Threshold Action	Action that occurs when the high threshold for an error is exceeded.
Link Fault Action	Action that occurs when the signal is lost.

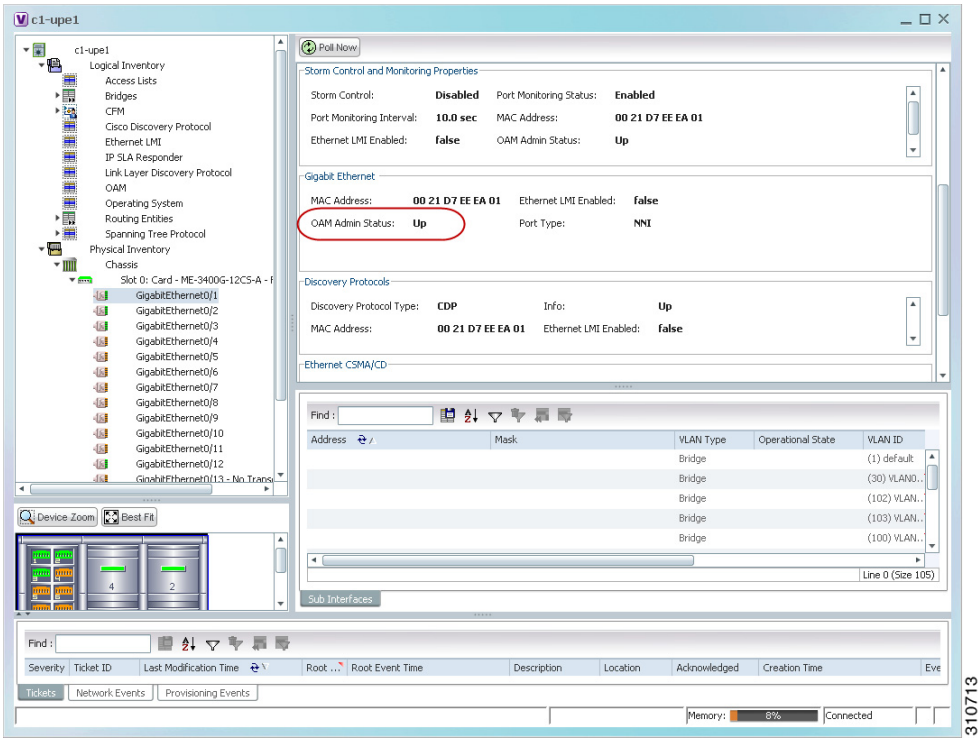
Table 19-10 Link OAM Data Properties Window (continued)

Field	Description
Dying Gasp Action	Action that occurs when an unrecoverable condition is encountered.
Critical Event Action	Action that occurs when an unspecified vendor-specific critical event occurs.
Mode	Mode of the interface: Active or Passive.
Unidirection	Status of unidirectional Ethernet on the local interface: Supported or Not supported.
Link Monitor	Status of link monitoring on the local interface: Supported or Not supported.
Remote Loopback	Status of remote loopback on the local interface: Supported or Not supported.
Loopback Status	Status of loopback on the local interface: Supported or No loopback.
Remote Client	
MAC Address	MAC address for the remote client.
Vendor	Vendor of the remote client.
Mode	Mode of the remote client: Active or Passive.
Unidirection	Status of unidirectional Ethernet on the remote client interface: Supported or Not supported.
Link Monitor	Status of link monitoring on the remote client interface: Supported or Not supported.
Remote Loopback	Status of loopback on the remote client interface: Supported or Not supported.

Step 4 To view Link OAM status in physical inventory, choose **Physical Inventory** > *chassis* > *slot* > *interface*.

The Link OAM administrative status is displayed as shown in Figure 19-10.

Figure 19-10 Link OAM Administrative Status in Physical Inventory



Configuring CFM

The following CFM-related commands can be launched from the inventory by right-clicking a CFM node and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see Permissions for Using Ethernet OAM Tools, page B-17). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Description
Maintenance Domain > Configure CFM Maintenance Domain	A maintenance domain is a management space for the purpose of managing and administering a network. A single entity owns and operates a domain and is defined by the set of ports internal to it and at its boundary. Each maintenance domain can contain any number of maintenance associations. Each maintenance association identifies a service that can be uniquely identified within the maintenance domain. The CFM protocol runs within a particular maintenance association. Using this command, assign a unique maintenance level to each domain and a maintenance endpoint archived hold time. Maintenance level defines the hierarchical relationship among domains and MEP Archive Hold time acts as a demarcation point on an interface that participates in CFM.
Global Parameters > Configure CFM Global Parameters	Enable CFM globally for a network element. Using this command you can configure the device to transmit traceroute and loopback messages with a hold-time value that indicates the validity of the messages.
Enable > Cisco > Continuity Check > Configure CFM Continuity Check **Enable > Cisco > Continuity Check > Enable CFM Continuity Check**	Enable continuity check parameters on the specified domain, service[1], bridge group, and bridge domain names.
MIP > Configure CFM MIP	The Configure CFM MIP command configures an operator-level maintenance intermediate point (MIP) for the domain-level ID. If the port on which a MIP is configured is blocked by Spanning-Tree Protocol (STP), the MIP cannot receive CFM messages or relay them toward the relay function side. The MIP can, however, receive and respond to CFM messages from the wire. A MIP has only one level associated with it, and the command-line interface (CLI) does not allow you to configure a MIP for a domain that does not exist.
Service ID > Configure CFM Service ID	Use the Configure CFM Service ID command to configure the CFM service ID.

Command	Description
MEP > Configure CFM MEP	Use this command to configure maintenance endpoints (MEPs), which have the following characteristics: • Per-maintenance domain (level) and service (S-VLAN or EVC) • At the edge of a domain, define the boundary • Within the bounds of a maintenance domain, confine CFM messages • When configured to do so, proactively transmit CFM continuity check messages (CCMs) • At the request of an administrator, transmit traceroute and loopback messages
Enable > Cisco > SNMP Server Traps > Enable CFM SNMP Server Traps	Enables Ethernet CFM continuity check traps and Ethernet CFM cross-check traps

1. Applicable for Cisco ASR 9000 series that run on Cisco IOS XR software.

Configuring E-LMI

The following E-LMI commands can be launched from the inventory by right-clicking an E-LMI node and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see Permissions for Using Ethernet OAM Tools, page B-17). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Description
Enable > Global E-LMI	Enable Ethernet LMI globally.
Enable On Interface	If E-LMI is disabled globally, you can use this command to enable E-LMI on specific interfaces.
Configure MultiPoint To MultiPoint or Point To Point EVC	UNI count indicates the range of the Unified network interface(UNI) is 2 to 1024; the default is 2. If you enter a value of 2, you have the option to select point-to-multipoint service. If you configure a value of 3 or greater, the service is point-to-multipoint.
Configure UNI in an Interface	
Configure Service Instance Vlan Id on Interface	Specify the service interface ID (Per-interface Ethernet service instance identifier that does not map to a VLAN).

Configuring L-OAM

The following Link-OAM commands can be launched from the inventory by right-clicking and L-OAM node and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see Permissions for Using Ethernet OAM Tools, page B-17). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Description
Assign Template on Interface	Assign template name
Configure MultiPoint To MultiPoint or Point To Point EVC	Configure OAM (L-OAM) on any full-duplex point-to-point or emulated point-to-point Ethernet link.
Enable OAM on Interface **Disable OAM on Interface**	Enable or disable OAM on the specified interface.
Enable E-LMI On Interface	Interface name (if E-LMI is disabled globally, you can use this command to enable E-LMI on specific interfaces)
Configure OAM Parameter on Interface	Configure OAM parameters, like maximum and minimum transmission rate of OAM PDU , OAM client mode and remote loopback ability on an interface.
Start Remote Loopback	Specify the local interface name on which the remote loopback should be started.
Stop Remote Loopback	Specify the local interface name on which the remote loopback should be stopped.

Monitoring Carrier Grade NAT Configurations

Carrier Grade NAT is a large-scale Network Address Translation (NAT) that provides translation of millions of private IPv4 addresses to public IPv4 addresses. These translations support subscribers and content providers with a bandwidth throughput of at least 10 Gbps full-duplex.

Carrier Grade NAT addresses the IPv4 address completion problem. It employs Network Address and Port Translation (NAPT) to aggregate many private IPv4 addresses into fewer public IPv4 addresses. For example, a single public IPv4 address with a pool of 32,000 port numbers supports 320 individual private IP subscribers, assuming that each subscriber requires 100 ports. Carrier Grade NAT also offers a way to implement a graceful transition to IPv6 addresses.

To route internal public addresses to external public addresses, a VPN Routing and Forwarding (VRF) instance is created. Interfaces are created for the VRF at the subscriber-side (private) and the Internet-side (public). The VRF enables static or dynamic routing of protocols on the interfaces.

Prime Network supports the following instances for Carrier Grade NAT:

- Stateful Address Translation- NAT44 Stateful
- Stateless Address Translation- NAT 64 Stateless (X-LAT)
- IPv6 rapid deployment (6rd)

Each Carrier Grade NAT instance has several attributes listed under them, such as preferred location, address pools, associated interfaces, and statistics. The attributes are grouped under related categories. The categories and attributes are listed below:

Note IPv4 Network Address Translation (NAT44) is not supported for devices running Cisco IOS XR software version 4.1.

For information on the devices that support Carrier Grade NAT, refer to *Cisco Prime Network 5.0 Supported VNEs*.

The following topics describe how to use the Vision client to view Carrier Grade NAT properties. If you cannot perform an operation that is described in these topics, you may not have sufficient permissions; see Permissions for Managing Carrier Grade NAT, page B-16.

Viewing Carrier Grade NAT Properties in Logical Inventory

To view Carrier Grade NAT properties in logical inventory:

Step 1 In the Vision client, double-click the Cisco CRS device configured for Carrier Grade NAT.

Step 2 In the **Inventory** window, click **Logical Inventory > Carrier Grade NAT**.

The Carrier Grade NAT properties are displayed in logical inventory as shown in Figure 20-1.

Figure 20-1 Carrier Grade NAT in Logical Inventory

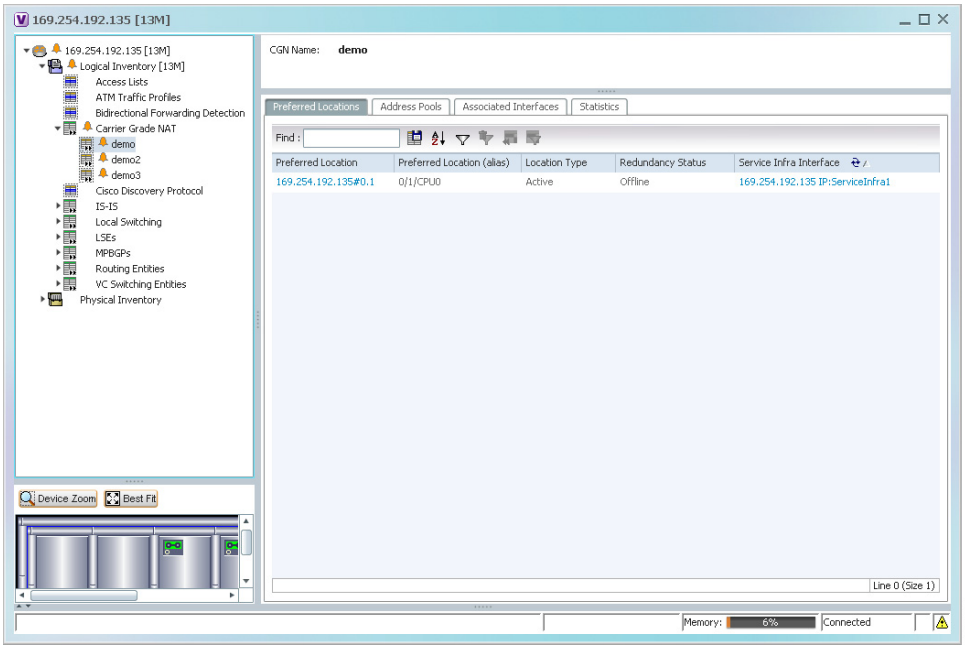


Table 20-1 describes the Carrier Grade NAT properties that are displayed.

Table 20-1 Carrier Grade NAT Properties in Logical Inventory

Field	Description
CGN Name	Name of the Carrier Grade NAT service.
Preferred Location Tab	
Preferred Location	Hyperlinked entry to the card in physical inventory.
Preferred Location (alias)	Location of module in clear text.
Location Type	Configured type of location: Active or Standby.
Redundancy Status	Redundancy state: Online or Offline. If the field is empty, it means the data was not collected from the device.
Service Infra Interface	Hyperlinked entry to the routing entity in logical inventory. For more information about routing entities in logical inventory, see Viewing Routing Entities, page 17-32.
Address Pools Tab	
Inside VRF	Hyperlinked entry to the inside VRF in logical inventory. For more information about VRF properties in logical inventory, see Viewing VRF Properties, page 17-28.
Address Family	Type of IP address in this pool: IPv4 or IPv6.
Outside VRF	Hyperlinked entry to the outside VRF in logical inventory. For more information about VRF properties in logical inventory, see Viewing VRF Properties, page 17-28.
Address Pool	Range of IP addresses that can be used for the service instance. If an end address is not specified, the entire range of 255 addresses is used for the address pool.
Associated Interfaces Tab	
Interface	Hyperlinked entry to the associated entry in logical inventory: • For SVI service interfaces, hyperlinked entry to the routing entity in logical inventory. • For SVI service applications, hyperlinked entry to the VRF entity in logical inventory.
Service Types Tab	
Service Type Name	Name of the Carrier Grade NAT service.
Service Type	Type of Carrier Grade NAT service: 6RD, XLAT, or NAT44.
Statistics Tab	
Statistics Name	Name of the statistic. For statistic names and descriptions, see Table 20-2.
Statistics Value	Value of the statistic.

You can also display pool utilization by right-clicking a VNE and choosing **Commands > Show > Pool Utilization.**

Table 20-2 Carrier Grade NAT Statistics in Logical Inventory

Statistic Name	Description
Inside to outside drops port limit exceeded	Number of packets dropped because the port limit has been exceeded. The value is calculated from the time Carrier Grade NAT was configured and running on the card.
Inside to outside drops resource depletion	Number of packets that are dropped because no ports are available. The value is calculated from the time Carrier Grade NAT was configured and running on the card.
Inside to outside drops limit system reached	Number of packets that are dropped because the system limit has been exceeded. The value is calculated from the time Carrier Grade NAT was configured and running on the card.
Inside to outside forward rate	Number of packets forwarded from the inside to the outside in the last one second.
Outside to inside forward rate	Number of packets forwarded from the outside to the inside in the last one second.
Translations create rate	Number of translation entries created in the last one second.
Translations delete rate	Number of translation entries deleted in the last one second.

Viewing Carrier Grade NAT Properties in Physical Inventory

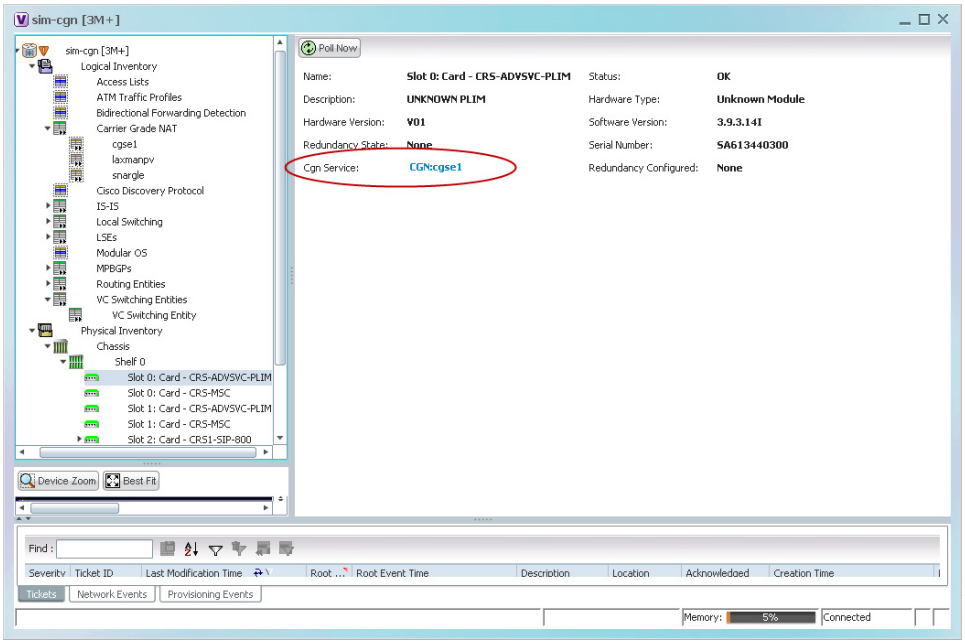
To view Carrier Grade NAT properties in physical inventory (in this example, a Cisco CRS device):

Step 1 In the Vision client, double-click the Cisco CRS device.

Step 2 To view Carrier Grade NAT properties configured on a specific interface, click **Physical Inventory > *chassis*** > *shelf* > *slot* > *card* > *interface*. See Drilling Down Into a Port's Configuration Details (Including Services and Subinterfaces), page 8-17 for a description of the information displayed in the Subinterfaces table.

Step 3 To view Carrier Grade NAT properties configured on a Cisco CRS-CGSE-PLIM card, click **Physical Inventory** > *chassis* > *shelf* > *slot* > *PLIM-card*. Figure 20-2 shows an example of Carrier Grade NAT properties in physical inventory.

Figure 20-2 Carrier Grade NAT Properties in Physical Inventory



The field CGN Service is displayed, and the entry is hyperlinked to the associated Carrier Grade NAT service in logical inventory.

Configuring a CG NAT Service

The following CG NAT commands can be launched from the inventory by right-clicking the appropriate node and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see Permissions for Managing Carrier Grade NAT, page B-16). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command and Navigation	Description
Configure > Add Static Port Forwarding	Configures CG NAT service instance for static port forwarding.
Configure > Add NAT 64 Forwarding	Configures CG NAT service instance for NAT 64.
Configure > Add 6rd Forwarding	Configures CG NAT service instance for 6rd.
Delete > Static Port Forwarding	Removes CG NAT instance.
Show > Pool Utilization	Displays the CGN instance name, inside VRF name, start and end address

Monitoring Quality of Service

Quality of Services (QoS) is the technique of prioritizing traffic flows and specifying preferences for forwarding packets with higher priority. It prioritizes traffic flow for different applications, users, or data flows and ensures certain level of performance to a data flow. This service plays an important part when the network capacity is insufficient, especially for real time streaming multimedia applications such as VoIP, online games, and IP-TV.
In Prime Network, you can view all the services configured for the selected network element in the QoS node under logical inventory.

The QoS Node under logical inventory is made up of two sub-nodes—the Policy Container and the Class of Service container. Both these sub-nodes are explained in greater detail in the following sections.

Viewing the Service Policy and Policy Group Profiles

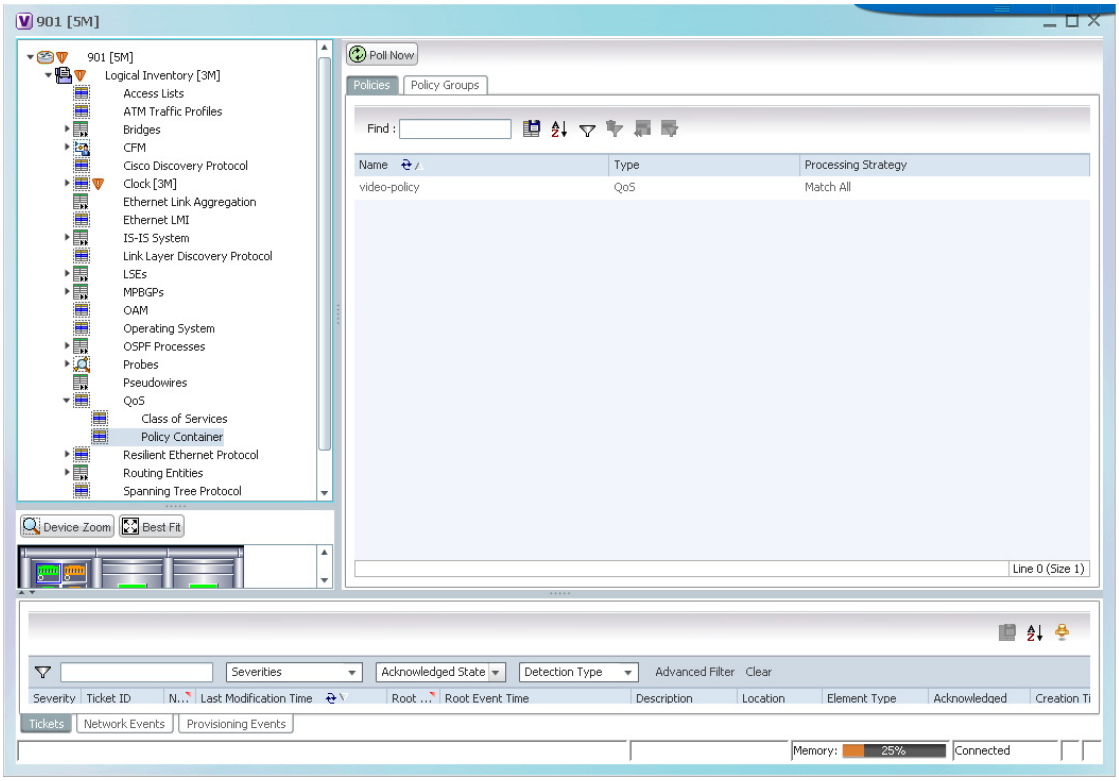
The Policy Container node in the logical inventory lists all the available service groups and service policies that are associated with service templates, BBA groups, and subscriber access points.

To view the service policy and policy group profiles:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory**> **QoS**> **Policy Container**. The Policies tab is displayed by default in content pane, which lists the existing policies are displayed as shown in Figure 21-1.

Figure 21-1 Policy Container



Step 3 Right-click the policy and choose **Properties**. The Service Policy Properties window is displayed. Table 21-1 describes the fields that are displayed in the Service Policy Properties window.

Table 21-1 Service Policy Properties

Field Name	Description
Name	The name of the policy.
Type	The type of policy, which defaults to QoS.
Processing Strategy	The strategy in applying the policy, which defaults to Match All.
Policy Rules & Actions tab	
Name	The name of the policy rule.
Match Condition	The class of service associated to the policy. Clicking this link will take you to the relevant service under the Class of Service node in the logical inventory.
Action Execution Strategy	The policy execution strategy, which can be any of the following: • Execute All • Execute Until Success • Execute Until Failure
Applied Interfaces tab	

Table 21-1 Service Policy Properties (continued)

Field Name	Description
Interface Name	The name of the interface on which the service policy is applied.
Entity Association	The logical or physical port to which the policy is associated to. Clicking this link will display the relevant ethernet/gigabit ethernet port. Verify the Ingress Policy or Egress Policy applicable to the port.
Action Lists tab	
Sequence Number	The sequence number of the action list.
Action Type	The action taken on the entity. For example, Activate, Deactivate, Authenticate and Authorize.
Affected Entity Type	The entity type affected due to the selected action list. For example, service-policy, traffic shaping.
Affected Entity	The entity that gets affected due to the selected action.
Entity Association	The link to the entity affected due to the action. Clicking on this link will take you to the relevant entity. For example, if the associated entity is a policy, then clicking this link will take you to the relevant policy under the Policy Container node.

Step 4 Close the **Service Policy Properties** window.

Step 5 In the content pane, click the **Policy Group** tab. A list of existing groups are displayed.

Step 6 Right-click the policy group and choose **Properties**.

Table 21-2 describes the fields in the Policy Group tab.

Table 21-2 Policy Group Properties

Field Name	Description
Name	The name of the policy group.
Type	The type of policy group, which can be any one of the following: • Accounting • Control • PBR • Performance Traffic • QoS • Traffic • Redirect This field defaults to Control.
Processing Strategy	The strategy in applying the policy, which defaults to Match All.
Policies	
Name	The name of the service policy map.
Type	The type of policy map.
Processing Strategy	The strategy in applying the policies on the incoming traffic.

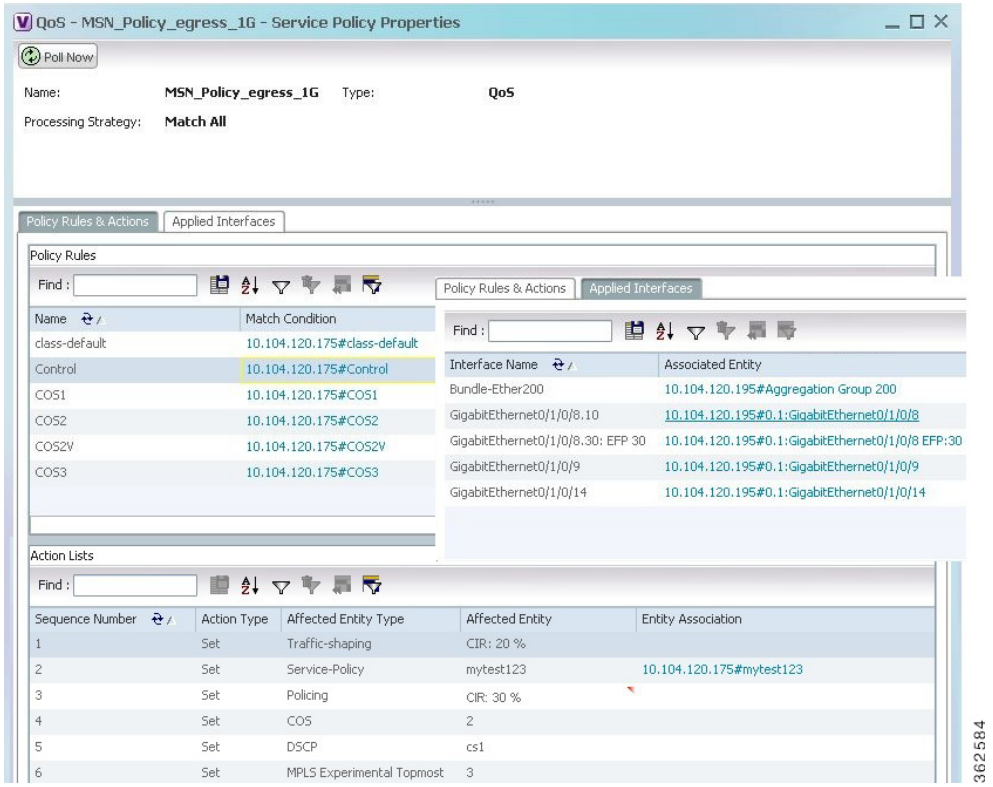
Table 21-2 Policy Group Properties (continued)

Field Name	Description
Applied Interfaces tab	
Interface Name	The name of the interface on which the service policy is applied.
Entity Association	The logical or physical port to which the policy is associated to. Clicking this link will display the relevant logical or physical port. Verify the Ingress Policy or Egress Policy applicable to the port.

Step 7 In the **Policies** tab, Right-click the policy from the list and choose **Properties**. The Service Policy Properties dialog box is displayed. See Table 21-1 for more details.

Figure 21-2 shows the association between the policy and interface.

Figure 21-2 Policy and Interface Association



Viewing the Class of Services Profile

To view the QoS profile:

Step 1 Right-click on the device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **QoS** > **Class of Services**. A list of existing policies are displayed in the content pane.

Step 3 Right-click a service in the list and choose **Properties**. The Class of Services Properties dialog box is displayed. You can click on the tabs to view more details.

Table 21-3 describes the fields that are displayed in the Class of Services Properties dialog box.

Table 21-3 Class of Services Properties

Field Name	Description
Name	The name of the class of service.
Type	The type of the class of service, which can be any one of the following: • Control • QoS • Traffic This field defaults to QoS.
Matching Strategy	The matching condition for the service, which can be any one of the following: • Match All • Match Any • Match None This field defaults to Match All.
Match Criteria Lists	
Index	The sequential number for the match criterion.
Match Type	The type that is used to match lists. For example, Access Group, Discard-class, DSCP, MPLS, QoS-group.
Match Condition	The match condition for the class of service, which can be any one of the following: • available/not available • class • greater-than/not greater-than • greater-than-or-equal/not greater-than-or-equal • less-than/not less-than • less-than-or-equal/not less-than-or-equal
Match Value	The value associated with the match type.
Associated Entity	The entity specified in the Match Value field. Click this hyperlink to view the related record.

Viewing Ingress and Egress Speed Details

Traffic shaping technique is used to match device and link speeds, thereby controlling packet loss, variable delay, and link saturation, which can cause jitter and delay. Traffic shaping must be applied to all outgoing traffic on a physical interface or on a VLAN. Traffic shaping is implemented when packets are ready to be transmitted on an interface. Traffic shaping is applied on the subinterfaces of the layer 2 and layer 3 when QoS policy is applied.

To view the ingress and egress details when QoS policy is applied on the subinterfaces:

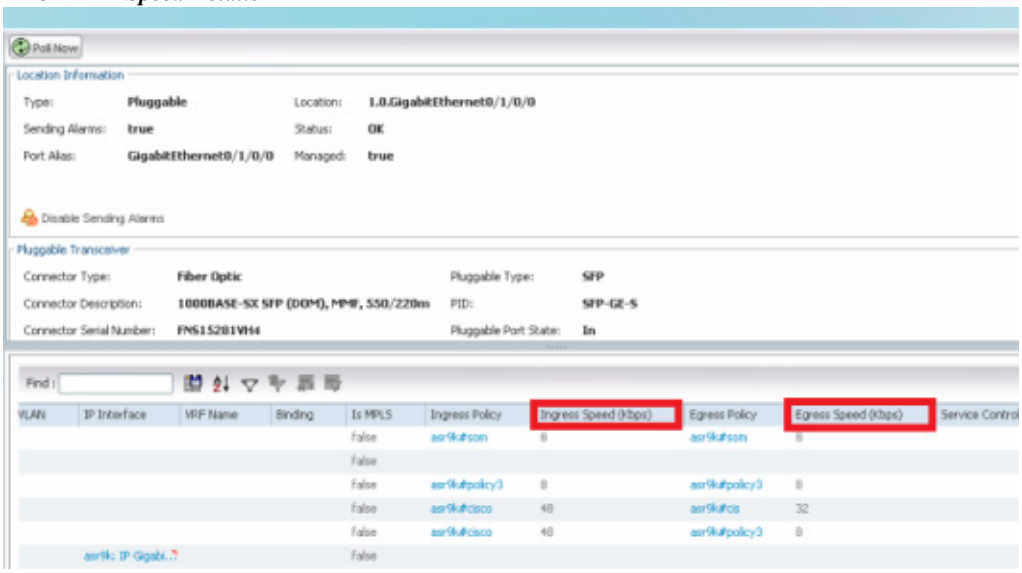
Step 1 In the **Inventory** window, choose **Physical Inventory**.

Step 2 Select an interface in layer 2 or layer 3.

Step 3 Select a subinterface for which you want to view the ingress and egress speed details.

Step 4 Click the **EFP** tab or **Sub Interface** tab to view the speed details of the subinterface mapped on layer 2 or layer 3 respectively. Figure 21-2 shows the speed details on a subinterface.

Figure 21-3 Speed Details



The following table provides information about the fields that are not self-explanatory.

Table 21-4 describes the fields that are not self-explanatory

Table 21-4 Traffic Shaping Details

Field Name	Description
Egress Policy	The name of the egress policy.
Egress Speed	The traffic shaping of the outgoing packets in an interface.
Ingress Policy	The name of the ingress policy.
Ingress Speed	The traffic shaping of the incoming packets in an interface.

Note Ingress policy, egress policy, ingress speed, and egress speed are supported in Cisco ASR 9000 devices but ingress policy and ingress speed are not supported in Cisco ASR 903 device and egress policy and egress speed are not supported in Cisco ASR 901 device

qos

qos.html

Managing IP Service Level Agreement (IP SLA) Configurations

In Prime Network, devices that are configured using Y.1731 (an ITU-T recommendation that provides mechanisms for service-level OAM functionality in Ethernet networks) are detected, scanned for configurations, and monitored. A device configured using Y.1731 has probes, which are root objects or containers that hold single or multiple instances of Service Level Agreement (SLA) probes configured by the user. To see which devices support Y.1731, refer to *Cisco Prime Network 5.2 Supported VNEs*.

Y.1731 Performance Management Mechanisms

The OAM functions for performance monitoring according to Y.1731 allow measurement of the following performance parameters.

- Frame Loss Ratio—Expressed as a percentage. This ratio is defined as the number of frames not delivered divided by the total number of frames during a time interval.
- Frame Delay—A one-way delay for a frame, where one-way frame delay is defined as the time elapsed since the start of transmission of the first bit of the frame by a source node until the reception of the last bit of the same frame by the destination node.
- Frame Delay Variation—The measure of the variations in the frame delay between a pair of service frames. The service frames belong to the same CoS (Class of Service) instance on a point-to-point Ethernet (ETH) connection or multipoint ETH connectivity.
- Throughput—The average rate of successful traffic delivery over a communication channel. Typically used under test conditions, such as out-of service tests, when there is no traffic for the tested Ethernet connection.

The following topics provide an overview of the Y.1731 technology and describe how to view and monitor Y.1731 configurations in the Vision client. If you cannot perform an operation that is described in these topics, you may not have sufficient permissions; see Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1.

Viewing Y.1731 Probe Properties

To view Y.1731 probes and their properties for a device:

Step 1 Right-click on the device and choose **Inventory**.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **Probes** > **Y1731 Probes**. A list of Y.1731 probes is displayed in the Y.1731 Probes content pane as shown in Figure 22-1.

Figure 22-1 Y.1731 Probes Content Pane

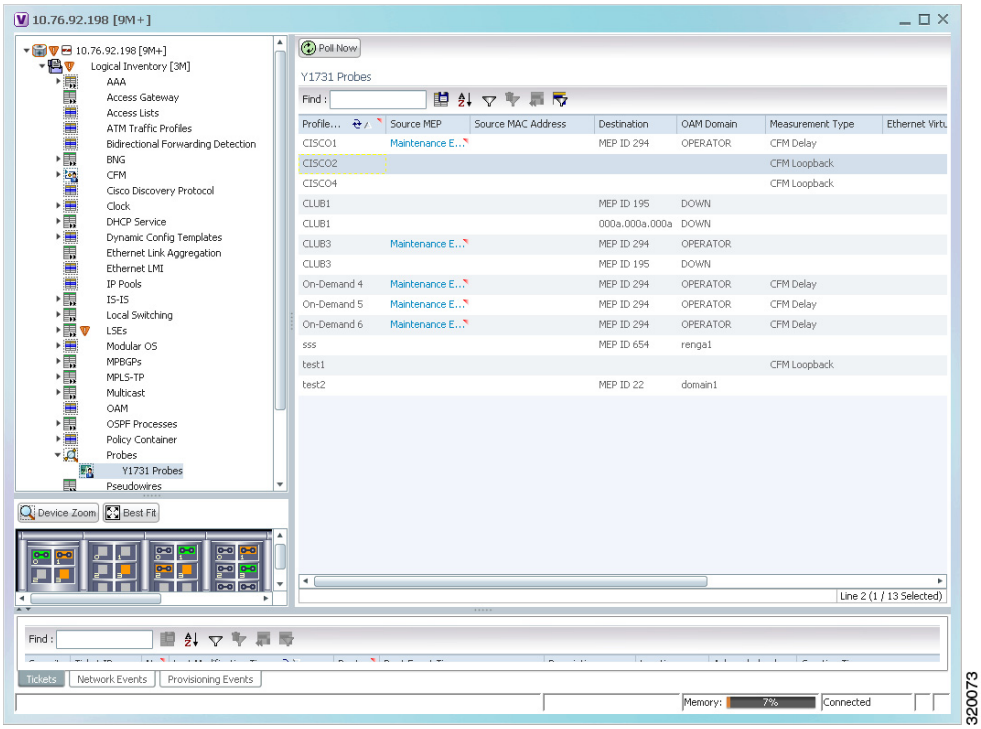


Table 22-1 describes the fields that are displayed in the content pane.

Table 22-1 Y.1731 Content Pane

Field Name	Description
Profile Name	The name of the profile created for performance monitoring of the SLA configuration.
Source MEP	The maintenance endpoint (MEP) interface ID where the probe is getting initiated.
Source MAC Address	The source interface MAC address where the probe is getting initiated.
Destination	The interface ID or MAC address, which will help the probe to reach its destination.
OAM Domain	The name of the OAM domain.
Measurement Type	The type of performance operation, which could be cfm-delay-measurement or cfm-loopback.
Ethernet Virtual Connection	The name or identifier of the ethernet virtual connection, which connects two User-Network Interfaces (UNI). This is applicable only for the Cisco CPT devices.
Packet Size	The size of the service packet. This includes padding size when required.

Table 22-1 Y.1731 Content Pane (continued)

Field Name	Description
Packets Per Burst	The number of packets transmitted per burst.
Burst Period	The time taken to send the packets from the source to their destination. This period is usually specified in terms of seconds or milliseconds.

Step 3 Right-click a probe and choose **Properties** to view its properties. The following additional information is displayed in the Probe Properties window for certain devices, such as Cisco CPT devices.

Table 22-2 Probe Properties Window

Field Name	Description
Delay Measurement Configurations	
Statistics Type	The statistics type, which is Round Trip Delay or Round Trip Jitter.
Aggregate Bin Count	The aggregate count of bins to store the counter values of the result of each performance parameter. **Note** The counter value refers to the counter of number of results that fall within a particular range specified for each performance attribute.
Aggregate Bin Boundaries	The bin boundary for the bins. For some devices, such as Cisco CPT devices, the bin boundary is specified as comma separated intervals; for other devices, such as the Cisco ASR 9000, it is an integer. Bin boundaries are specified in terms of milliseconds.
Bucket Size	The number of buckets required to store the performance attribute results gathered during a specified period. By default, a separate bucket is created for each probe, which will contain the results relating to measurements made by the probe.
Aggregation Period	The period of time (in seconds) during which the aggregation takes place on the performance data.
Aggregate Burst Cycles	The total number of burst cycles on which the aggregation has to happen.
Loss Measurement Configurations	
Statistics Type	The statistics type, which is Round Trip Delay or Round Trip Jitter.
Aggregate Bin Count	The aggregate count of bins to store the counter values of the result of each performance parameter. **Note** The counter value refers to the counter of number of results that fall within a particular range specified for each performance attribute.

Table 22-2 Probe Properties Window (continued)

Field Name	Description
Aggregate Bin Boundaries	The bin boundary for the bins. For some devices, such as Cisco CPT devices, the bin boundary is specified as comma separated intervals; for other devices, such as the Cisco ASR 9000, it is an integer. Bin boundaries are specified in terms of milliseconds.
Bucket Size	The number of buckets required to store the performance attribute results gathered during a specified period. By default, a separate bucket is created for each probe, which will contain the results relating to measurements made by the probe.
Aggregation Period	The period of time during which the aggregation must take place on the loss data.
Aggregate Burst Cycles	The total number of burst cycles on which the aggregation must take place.
Availability Algorithm	The type of algorithm to be used to measure proportion of time when there was a prolonged high loss, which can be any one of the following:
Consecutive Frames	The number of consecutive frames that must be used to calculate frame loss. **Note** Frame loss is calculated by comparing loss measurement data of the specified number of consecutive frames.
Consecutive Frames For Loss Ratio	The number of consecutive frames that is used to calculate loss ratio. **Note** The Frame Loss Ratio is calculated as a ratio between the number of packets sent and the number of packets lost, which is then expressed in terms of percentage.

Configuring Y.1731 Probes

The following IP SLA-related commands can be launched from the inventory by right-clicking the appropriate node and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Navigation	Description
Configure Probe EndPoint Association	*Right-click Y1731 Probes node* > **Commands** > **Configuration** > **Configure Probe EndPoint Association**	Use this command to configure endpoint association for a probe.
Create Profile	*Expand the node Probes* > *Right-click Y1731 Probes node* > **Commands** > **Configuration** > **Create Profile**	Use this command to configure a new profile for the probe.
Create On Demand Probe Configuration	*Expand the node Probes* > *Right-click Y1731 Probes node* > **Commands** > **Configuration** > **Create On Demand Probe Configuration**	Use this command to create an on demand probe configuration.
Deassociate Profile	*Right-click Y1731 Probes node* > **Commands** > **Configuration** > **Deassociate Profile**	Use this command to deassociate a profile from a probe.
Delete Profile	*Right-click Y1731 Probes node* > **Commands** > **Configuration**	Use this command to delete a profile.
Show SLA Operations Detail	*Expand the node Probes* > *Right-click Y1731 Probes node* > **Commands** > **Show** > **Show SLA Operations Detail**	When service providers sell connectivity services to a subscriber, a Service Level Agreement (SLA) is reached between the buyer and seller of the service. The SLA defines the attributes offered by a provider and serves as a legal obligation on the service provider. As the level of performance required by subscribers increases, service providers need to monitor the performance parameters being offered. Use this command to view the SLA operation details.
Show SLA Profiles	*Expand the node Probes* > *Right-click Y1731 Probes node* > **Commands** > **Show** > **Show SLA Profiles**	Use this command to view a list of the SLA profiles.
Configure IP SLA parameters	*Right-click Y1731 Probes node* > **Commands** > **Configuration**	Use this command to configure an IP SLA parameter for the probe.

Command	Navigation	Description
Delete IP SLA parameters	*Right-click an ASR9K* > **Commands** > **Configuration** > **IPSLA** >**Delete IP SLA**	Use this command to delete the IP SLA parameters for a probe.
Show IP SLA	*Right-click an ASR9K* device > **Commands** > **Configuration** > **IPSLA** >**Show IP SLA**	Use this command to view the IP SLA schedule details.

Monitoring IP and MPLS Multicast Configurations

IP Multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients and homes. Applications that take advantage of multicast include video conferences, corporate communications, distance learning, and distribution of software, stock quotes, and news.

IP Multicast delivers source traffic to multiple receivers without adding any additional burden on the source or the receivers while using the least network bandwidth of any competing technology. Multicast packets are replicated in the network by Cisco routers enabled with Protocol Independent Multicast (PIM), Multicast Label Distribution Protocol (MLDP) and other supporting multicast protocols resulting in the most efficient delivery of data to multiple receivers possible.

Multicast is based on the concept of a group. An arbitrary group of receivers expresses an interest in receiving a particular data stream. This group does not have any physical or geographical boundaries—the hosts can be located anywhere on the Internet. Hosts that are interested in receiving data flowing to a particular group must join the group using Internet Group Management Protocol (IGMP). Hosts must be a member of the group to receive the data stream.

For information on the devices that support IP and multicast, refer to *Cisco Prime Network 5.2 Supported VNEs*.

These topics provide an overview of the IP Multicast technology and describe how to view IP and multicast configurations using the Vision client. If you cannot perform an operation that is described in these topics, you may not have sufficient permissions; see Permissions for Managing IP and MPLS Multicast, page B-20.

- Viewing Multicast Nodes, page 23-2
- Viewing Multicast Protocols, page 23-3
- Viewing the Address Family (IPv6) Profile, page 23-4

Prime Network also provides multicast support for:

- MPLS services. See Multicast Label Switching (mLADP), page 17-44.
- Routing entities. If you have configured multicast route information for a VRF, the Vision client displays a separate tab for the related VRF wherein you can view the multicast routing information. See Viewing Routing Entities, page 17-32and Viewing VRF Properties, page 17-28.

Viewing Multicast Nodes

To view the Multicast node:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **Multicast**. The Route Policies and Multicast Global Interfaces tabs are displayed in the content pane as show in Figure 23-1. You can click on the tabs to view more details.

Figure 23-1 Multicast Content Pane

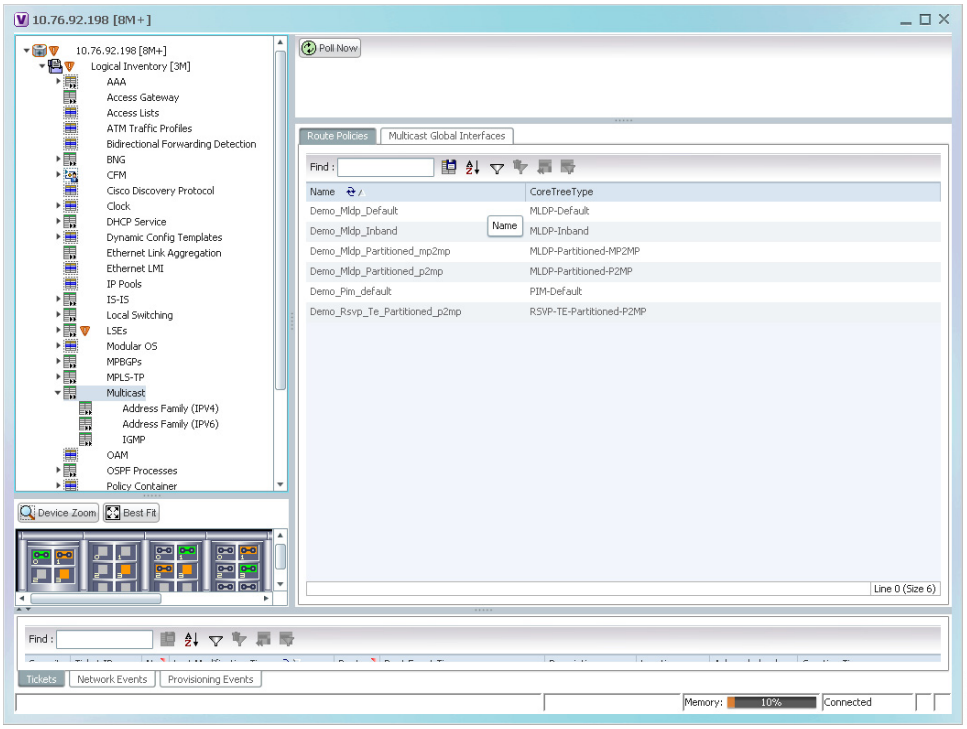


Table 23-1 describes the fields that are displayed in the Route Policies tab.

Table 23-1 Route Policies Tab

Field Name	Description
Name	The name of the multicast route policy.
Core Tree Type	The type of the Multicast Distribution Tree (MDT) core tree configured in the route policy. Values are: • MLDP-Default • MLDP-Inband • MLDP-Partitioned-MP2MP • MLDP-Partitioned-P2MP • PIM-Default • RSVP-TE-Partitioned-P2MP
Multicast Global Interfaces Tab	
Interface Name	The name of the multicast enabled logical or physical interface.
Associated Entity	The link to the associated routing entity, which when clicked will highlight the associated **Default routing entity** record under the **Routing Entity** node.

Viewing Multicast Protocols

The following Multicast protocols are available in Prime Network:

- Address Family (IPv4)—See Viewing the Address Family (IPv4) Profile, page 23-3.
- Address Family (IPv6)—See Viewing the Address Family (IPv6) Profile, page 23-4.
- IGMP—Viewing the IGMP Profile, page 23-5.
- PIM—Viewing the PIM Profile, page 23-7.

Viewing the Address Family (IPv4) Profile

To view the Address Family (IPv4) profile:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **Multicast** > **Address Family (IPV4)**. The profile details are displayed in the content pane.

Table 23-2 describes the fields that are displayed in the **Address Family (IPV4)** profile**.**

Table 23-2 Address Family (IPV4) Profile

Field Name	Description
MDT Source Interface	The source interface to set the multicast VPN data. **Note** This interface can identify the root of the MDT in the service provider network. This interface and its corresponding address is used to update all Multicast VPN (MVPN) peers through multiprotocol Border Gateway Protocol (BGP).
MDT Static	The interface used for transporting MDT data.
Interface All	Indicates whether the multicast routing and protocols are enabled on the interfaces. **Note** You must enable the interfaces using the Interface command in the multicast-routing configuration mode.
NSF Status	Indicates whether the non-stop forwarding capability is enabled for all the relevant components. **Note** If this feature is enabled, then multicast forwarding will not stop on failure of the control plane multicast routing components.
Address Family	The address family, which in this instance is IPV4.
MDT MLDP	Indicates whether the Multicast Distribution Tree (MDT) Multipoint Extensions to Label Distribution Protocol (MLDP) in-band signalling is enabled.

Viewing the Address Family (IPv6) Profile

To view the Address Family (IPv6) profile:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **Multicast** > **Address Family (IPV6)**. The profile details are displayed in the content pane.

Table 23-3 describes the fields that are displayed in the **Address Family (IPV6)** profile**.**

Table 23-3 Address Family (IPV6) profile

Field Name	Description
Interface All	Indicates whether the multicast routing and protocols are enabled on the interface. **Note** You must enable the interfaces using the Interface command in the multicast-routing configuration mode.
NSF Status	Indicates whether the non-stop forwarding capability is enabled for all the relevant components. **Note** If this feature is enabled, then multicast forwarding will not stop if the control plane multicast routing components fail.
Address Family	The address family, which in this instance is IPV6.
MDT MLDP	Indicates whether the Multicast Distribution Tree (MDT) Multipoint Extensions to Label Distribution Protocol (MLDP) in-band signalling is enabled.
MDT Static	The interface used for transporting MDT data.
MDT Source Interface	The source interface to set the multicast VPN data. **Note** This interface can identify the root of the MDT in the service provider network. This interface and its corresponding address is used to update all Multicast VPN (MVPN) peers through multiprotocol Border Gateway Protocol (BGP).

Viewing the IGMP Profile

The IGMP runs between hosts and their immediately neighboring multicast routers. The mechanisms of the protocol allow a host to inform its local router that it wishes to receive transmissions addressed to a specific multicast group. Also, routers periodically query the LAN to determine if known group members are still active. If there is more than one router on the LAN performing IP multicasting, one of the routers is elected querier and assumes the responsibility of querying the LAN for group members. Based on the group membership information learned from the IGMP, a router is able to determine which (if any) multicast traffic needs to be forwarded to each of its leaf sub networks. Multicast routers use this information, in conjunction with a multicast routing protocol, to support IP multicasting across the Internet.

There are three versions of IGMP:

- **IGMP Version 1**
- **IGMP Version 2**
- **IGMP Version 3**

To view the IGMP profile:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **Multicast** > **IGMP**. The IGMP details are displayed in the content pane. You can click on the tabs to view more details.

Table 23-4 describes the fields that are displayed in the **IGMP** profile**.**

Table 23-4 IGMP Profile Details

Field Name	Description
NSF Status	The non-stop forwarding status, which can be **Normal** or **Non-Stop Forwarding Activated**. **Note** The Non-Stop Forwarding Activated status implies that recovery of an IGMP failure is in progress.
Interfaces Tab	
Interface Name	The name of the interface.
Associated Entity	The link to the associated entity, which when clicked will highlight the associated **Default routing entity** record under the **Routing Entity** node.
Interface Address	The internet address of the interface.
VRF	The VRF to which the interface belongs. This is a link, which when clicked will take you to the relevant record under the **VRF** node.
IGMP Status	Indicates whether IGMP is enabled or disabled on the interface.
IGMP Version	The IGMP version installed on the interface.
Groups Tab	
Group Address	The address of the multicast group.
Interface Name	The name of the interface used to reach the group.
Associated Entity	The associated entity for the IGMP profile. Click this link to view the related record under the Subscriber Access Point node.
VRF	The VPN Routing and Forwarding (VRF) to which the interface belongs. This is a link, which when clicked will take you to the relevant record under the VRF node.
Up Time	The period from when the multicast group is available. This information is displayed in terms of hours, minutes, and seconds.
Expires	The duration after which the multicast group will be removed from the IGMP groups table. This information is displayed in terms of hours, minutes, and seconds.
Last Reporter	The most recent host that has reported being a member of the multicast group.

Table 23-4 IGMP Profile Details (continued)

Field Name	Description
Group Ranges Tab	
Group Range	The multicast group range in CDIR format, which is basically the Multicast Group IP address followed by the CDIR prefix.
Protocol	The PIM protocol that is used by the IGMP group range.

Viewing the PIM Profile

PIM is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet. It is termed protocol-independent because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other traditional routing protocols such as the Routing Information Protocol, Open Shortest Path First, Border Gateway Protocol and Multicast Source Discovery Protocol. There are four variants of PIM:

- PIM Sparse Mode (PIM-SM)
- PIM Dense Mode (PIM-DM)
- Bidirectional PIM
- PIM source-specific multicast (PIM-SSM)

Although PIM is called a multicast routing protocol, it actually uses the unicast routing table to perform the Reverse Path Forwarding (RPF) check function instead of building up a completely unrelated multicast routing table. PIM does not send and receive multicast routing updates between routers like other routing protocols.

To view the PIM profile:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **Multicast** > **PIM**. The profile details are displayed in the content pane. You can click on the tabs to view more details.

Table 23-5 describes the fields that are displayed in the **PIM** profile**.**

Table 23-5 PIM Profile Details

Field Name	Description
NSF Status	The non-stop forwarding status, which can be **Normal** or **Non-Stop Forwarding Activated**. **Note** The Non-Stop Forwarding Activated status implies that recovery of an IGMP failure is in progress.
Interfaces Tab	
Interface Name	The name or ID of the interface on which PIM is enabled.
Associated Entity	The link to the associated entity, which when clicked will highlight the associated **Default routing entity** record under the **Routing Entity** node.

Table 23-5 PIM Profile Details (continued)

Field Name	Description
IP Address	The IP address of the interface.
VRF	The name of the VRF associated to the interface. This is a link, which when clicked will take you to the relevant record under the **VRF** node.
PIM Status	Indicates whether the PIM is enabled (ON) or disabled (OFF) on the interface.
Hello Interval	The frequency at which PIM hello messages are sent over the PIM enabled interfaces. These messages are sent at regular intervals by routers on all the PIM enabled interfaces. The router sends these messages to advertise their existence as a PIM router on the subnet.
Designated Router	The IP address of the designated router on the LAN. **Note** Serial do not have a designated router. Hence, the IP address is displayed as 0.0.0.0. If the interface on the router is the designated router, then the words "This system" is displayed. If not, then the IP address of the external neighbor is displayed.
Designated Router Priority	The priority of the designated router, which is advertised by the neighbor in the hello messages. This value in this field will range from 0 to 4294967295.
Rendezvous Points Tab	
RP Address	The address of the interface serving as a rendezvous point for the group range or list. A Rendezvous Point (RP) is a router in a multicast network domain that acts as a shared root for a multicast shared tree. Any number of routers can be configured to work as RPs and they can be configured to cover different group ranges. For correct operation, every multicast router within a Protocol Independent Multicast (PIM) domain must be able to map a particular multicast group address to the same RP.
Mode	The PIM protocol mode for which the router is advertised as a rendezvous point. The mode can be **PIM-SM** or **bidirectional PIM**.
Scope	The number of candidate announcement messages sent out from the rendezvous point.
Priority	The value of the candidate rendezvous point priority.
Uptime	The amount of time from when the rendezvous point is available.
Group List	The IP access list number or name of the group prefixes that are advertised in association with the rendezvous point address.
RP Type	The type of rendezvous point, which can be **BSR** or **Auto RP**. **Note** The **Bootstrap Router** (BSR) is a mechanism for a router to learn RP information. It ensures that all routers in the PIM domain have the same RP cache as the BSR. **Auto-RP** is a mechanism to automate distribution of RP information in a multicast network. The Auto-RP mechanism operates using two basic components, the candidate RPs and the RP mapping agents.

Table 23-5 PIM Profile Details (continued)

Field Name	Description
Topology Tab	
Source Address	The IP address of the source of the multicast entry. In case the IP address is not available, a "*" or 0.0.0.0 is displayed here.
Group Address	The multicast group address or prefix for which the entry is associated with.
PIM Mode	The PIM mode of the topology entry, which can be Sparse, Source Specific, Dense, or Bidirectional.
Tree Type	The MDT tree type for the route entry, which can be **Shortest Path Tree** or Rendezvous Point Tree.
Uptime	The amount of time from which the topology is available. This value is displayed in terms of seconds.
RP Address	The Rendezvous Point address. This value is displayed only if the PIM Mode is SM or Bidirectional.
Join Prune Status	Indicates whether a join or prune message is sent to the RPF neighbor for the route.
RPF	The IP address and interface ID, along with the MoFFR information, of the Reverse Path Forwarding for the topology.
Flags	The comma separated flag information for this topology.
Neighbors Tab	
Neighbor IP Address	The IP address of the neighbor.
Interface Name	The interface name on which the neighbor can be reached.
Associated Entity	The link to the associated entity, which when clicked will highlight the associated **Default routing entity** record under the **Routing Entity** node.
VRF	The name of the VRF.
Flags	The flags that provide information about various states of the neighbor.
Designated Router Priority	The priority of the PIM interface for DR election. The default value is 1.
UpTime	The amount of time from which the interface is available.

Managing Session Border Controllers (SBCs)

This chapter identifies and describes the properties for Session Border Controllers (SBCs) that appear in the Vision client logical inventory. It also describes commands you can run to manage SBCs.

Session Border Controllers (SBCs) control and manage real-time multimedia traffic flows between IP network borders, handling signaling, and media. SBCs perform native IP interconnection functions required for real-time communications such as admission control, firewall traversal, accounting, signaling interworking, and quality-of-service (QoS) management. This includes:

- Protocol and media interworking
- Session routing
- Hosted Network Address Translation (NAT) and firewall traversal
- Security and AAA
- Intra- and inter-VPN interconnections and optimization
- Media transcoding with an external media server

The Prime Network platform provides fault management, configuration, and performance monitoring for SBC services. Prime Network SBC commands allow you to configure SBC components.

An SBC consists of combined DBE and SBE functionality:

- Data Border Element (DBE)—Responsible for media-related functions.
- Signaling Border Element (SBE)—Responsible for call signaling-related functions.

In addition, the SBC can operate in the following deployment models:

- Distributed Model (DM)—Contains only the SBE or DBE, resulting in a distributed SBC.
- Unified Model (UM)—Contains both the SBE and DBE, thereby implementing the SBE and DBE as a single device.

Note The existing Cisco SBC platforms support only DBE.

The following topics describe the SBC properties that are displayed in the Vision client logical inventory. If you cannot perform an operation that is described in these topics, you may not have sufficient permissions; see Permissions for Managing SBCs, page B-20.

- Configuring SBC Components, page 24-13

Viewing SBC Properties in Logical Inventory

To view SBC properties in the Vision client logical inventory, right-click the element configured for SBC, then choose **Inventory > Logical Inventory > Session Border Controller**.

The SBC properties are displayed as shown in Figure 24-1.

Figure 24-1 SBC Properties in Logical Inventory

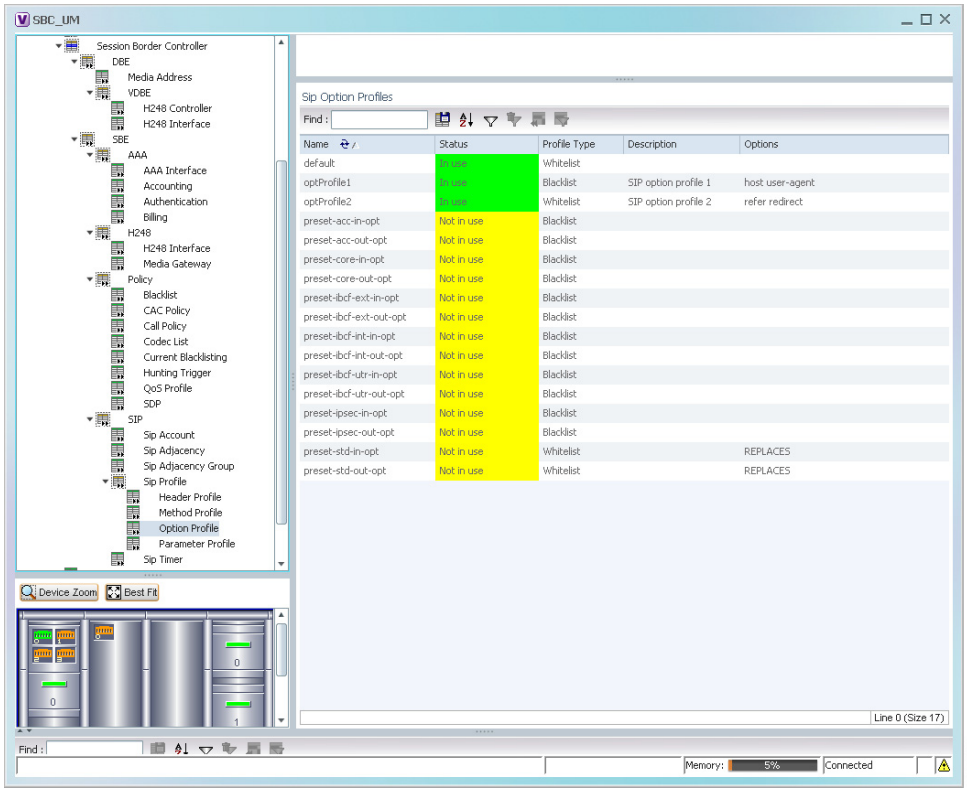


Table 24-1 describes the general SBC properties displayed in logical inventory.

Table 24-1 SBC Properties

Field	Description
Process	Process name, such as Session Border Controller.
Process Status	Status of the process, such as Running.
Application Version	SBC version number.
Mode	Mode in which the SBC is operating: • Unified • Distributed DBE
SBC Service Name	Name of the service.

Viewing SBC DBE Properties

The DBE controls media packet access to the network, provides differentiated services and QoS for different media streams, and prevents service theft.

To view SBC DBE properties, choose **Logical Inventory > Session Border Controller > DBE**.

Table 24-2 describes the DBE properties that appear in logical inventory.

Table 24-2 SBC DBE Properties

Field	Description
Process	Process name, such as DBE.
Process Status	Status of the process, such as Running.
Name	Name assigned to the DBE.
Type	Type of DBE, either DBE or virtual DBE (vDBE).
DBE Location Id	Unique identifier configured on each vDBE within a UM DBE.

Viewing Media Address Properties

A DBE uses a pool of sequential IPv4 media addresses as local media addresses.

To view SBC media address properties, choose **Logical Inventory > Session Border Controller > DBE > Media Address**.

Table 24-3 describes the SBC media address properties that are displayed in logical inventory.

Table 24-3 Media Address Properties

Field	Description
Address Range	IP addresses defined for the pool.
Port Range Lower	Lower end of the port range for the interface. If no range is specified, all possible Voice over IP (VoIP) port numbers are valid.
Port Range Upper	Upper end of the port range for the interface.
VRF Name	VRF that the interface is assigned to.
Service Class	Class of service (CoS) for each port range, such as fax, signaling, voice, or any.

Viewing VDBE H.248 Properties

To view VDBE H.248 properties, choose **Logical Inventory > Session Border Controller > DBE > VDBE**.

Table 24-4 describes the VDBE H.248 properties that are displayed in logical inventory.

Table 24-4 VDBE H.248 Properties

Branch	Description
H248 Controller	H.248 controller used by the DBE. The Media Gateway Configuration (MGC) table displays the following information: • Index—The number of the H.248 controller. The profile is used to interoperate with the SBE. • Remote IP—The remote IP address for the H.248 controller. • Remote Port—The remote port for the H.248 controller. • Transport—The transport for communications with the remote device.
H248 Interface	The SBC H248 Control Interface table displays the following information: • IP Address: – In DM mode, the local IP address of the DBE used to connect to the SBE. – In UM mode, the local IP address used to connect to the media gateway. • Port—The port for the H.248 controller interface. • Transport—The transport the H.248 controller interface uses. • Association—The relationship between the SBE and the media gateway.

Viewing SBC SBE Properties

The SBE controls the access of VoIP signaling messages to the network core and manipulates the contents of these messages. It does this by acting as a SIP B2BUA or H.323 gateway.

To view SBC SBE properties, choose **Logical Inventory > Session Border Controller > SBE**.

Table 24-5 describes the information displayed in logical inventory for an SBE.

Table 24-5 SBC SBE Properties

Field	Description
Process	Name of the process, such as SBE.
Process Status	Status of the process, such as Running or Idle.
Name	Name assigned to this SBE.
Call Redirect Limit	Maximum number of times a call is redirected before the call is declared failed. The range is 0 to 100 with a default of 2.
On Hold Timeout	Amount of time, in milliseconds, that the SBE waits after receiving a media timeout notification from the DBE for an on-hold call before tearing down the call.

Viewing AAA Properties

For devices that support local and remote billing, the SBC can send billing records to a AAA server using the RADIUS protocol.

To view AAA properties, choose **Logical Inventory > Session Border Controller > SBE > AAA**.

Table 24-6 describes the AAA properties that appear in logical inventory for the SBC SBE.

Table 24-6 AAA Properties

Branch	Description
AAA Interface	The SBE AAA Interface table displays the following information: • AAA Address—The local AAA interface address. • Network ID—A unique identifier for the SBE.
Accounting	The Accounting Radius Client table displays the following information: • Name—The name of the accounting client. • Client Type—The type of client, either Accounting or Authentication.
Authentication	The Authentication Radius Client table displays the following information: • Name—The name of the authentication client. • Client Type—The type of client, either Accounting or Authentication.
Billing	The SBE Billing table displays the following information related to billing: • LDR Check Time—The time of day (local time) to run the long duration record check. • Local Billing Address—The local IP address for SBE billing. This IP address can be different from the local AAA IP address and is the IP address written in the bill records. • Admin Status—The configuration status, available with the **running-config** command. • Operational Status—The running status, available from the CLI. This entry indicates whether or not the billing interface is up. The status is derived from the interworking of the SBC and the AAA server.

Viewing H.248 Properties

The H.248 interface is used for signaling between an SBE and a DBE in distributed mode and between an SBE and a transcoding media gateway. The SBE or SBC acts as an H.248 MGC, and the transcoding device acts as an H.248 media gateway. The connection between the MGC and the media gateway is an H.248 link.

To view H.248 properties, choose **Logical Inventory > Session Border Controller > H248**.

Table 24-7 describes the H.248 properties that appear in logical inventory for the SBC SBE.

Table 24-7 H.248 Properties

Branch	Description
H248 Interface	The SBC H248 Control Interface table displays the following information: • IP Address: – In DM mode, the IP address used to connect the DBE and the MGC. – In UM mode, the IP address used to connect the SBC and the media gateway. • Port—The port for the H.248 controller interface. • Transport—The transport the H.248 controller interface uses. • Association—The relationship between the SBE and the media gateway.
Media Gateway	The Media Gateway table displays the following information: • IP Address—The IP address of the media gateway. • Codec List—A comma-separated list of the codecs supported.

Viewing Policy Properties

An SBC policy is a set of rules that define how the SBC treats different kinds of VoIP events. An SBC policy allows control of the VoIP signaling and media that pass through the SBC at an application level.

A *policy set* is a group of policies that can be active on the SBC at any one time. If a policy set is active, the SBC uses the rules defined within it to apply policy to events. Multiple policies can be set on a single SBC.

To view policy properties, choose **Logical Inventory > Session Border Controller > Policy**.

Table 24-8 describes the policy properties that appear in logical inventory for the SBC SBE.

Table 24-8 Policy Properties

Branch	Description
Blacklist	The Blacklists table contains the following information: • Name—The blacklist name. • Type—The type of source that this blacklist applies to, such as critical or normal.
CAC Policy	A Call Admission Control (CAC) policy is used to define admission control. The SBE CAC Policy Set table contains the following information: • Policy Set Number—An identifying number the SBE has assigned to the policy set. • First Table—A CAC policy table. • Status—Whether the policy is active or inactive. If the policy is active, the SBC applies the defined rules to events. • First CAC Scope—The scale that the CAC applies for, such as source adjacency or destination adjacency. This is the first CAC table used for CAC policy match. • Description—A brief description of the policy set.
Call Policy	A call policy set is used for number analysis and routing. The SBE Call Policy Set table contains the following information: • Policy Set Number—An identifying number the SBE has assigned to the policy set. • Status—Whether the policy is active or inactive. If the policy is active, the SBC applies the defined rules to events. • First Call Table—The first call table used for call policy match. • Description—A brief description of the policy set.
Codec List	The SBE Codec List table contains the following information: • Name—The name of the codec list. • Codecs—The codecs contained in each list.

Table 24-8 Policy Properties (continued)

Branch	Description
Current Blacklisting	The Current Blacklistings table contains the following information: • Type—The type of source this blacklist applies to. Blacklists are used to block certain VoIP services that meet specified conditions. • Event Type—The type of event this blacklist applies to, such as CORRUPT_MESSAGE. • Is All Source Addresses—Whether the blacklist applies to all source IP addresses: – True—Ignore any IP address in the Source Address field. – False—Use the IP address in the Source Address field. • Source Address—The IP address that this blacklist applies to. • Source Port Number—The port number that this blacklist applies to. • Source Port Type—The type of port this blacklist applies to. *All* is a valid entry. • Time Remaining—The amount of time, in hours, minutes, or seconds, before the blacklist is removed.
Hunting Trigger	The hunting trigger enables the SBC to search for other routes or destination adjacencies if an existing route fails. The Global Hunting Trigger List table contains the following information: • Hunting Mode—Indicates the protocol to use to search for routes, such as Session Initiation Protocol (SIP). • Hunting Triggers—The SIP responses, such as 468 or 503, that indicate the SBC is to search for an alternate route or destination adjacency. SIP responses are defined in RFC3261.

Table 24-8 Policy Properties (continued)

Branch	Description
QoS Profile	QoS profiles can be used by CAC policies and are used exclusively for marking IP packets. The QoS Profile table contains the following information: • Name—The name of the QoS profile. • Class of Service—The type of call this profile applies to, such as voice, video, signaling, or fax. • Marking Type—The type of marking to be applied to the IP packet. Options include Passthrough, Differentiated Service Code Point (DSCP), and IP Precedence/ToS. • IP Precedence—If the marking type is IP Precedence, the specified precedence, either 0 or 1. • ToS—If the marking type is ToS, the ToS value. • DSCP—If the marking type is DSCP, the DSCP value.
SDP	The Session Description Protocol (SDP) content pane contains the following tabs, each with their respective table: • SBE SDP Policy Table: – Instance Name—The name of the policy table. – SBE SDP Match Table—The name of the SDP match table. • SBE SDP Match Table: – Instance Name—The name of the SDP match table. – Match Strings—The match criteria. – Table Type—The type of table, either Blacklist or Whitelist.

Viewing SIP Properties

To view SIP properties, choose **Logical Inventory > Session Border Controller > SIP**.

Table 24-9 describes the SIP entries that appear in logical inventory for the SBC SBE.

Table 24-9 SIP Properties

Branch	Description
SIP Account	The SBE Account table contains the following information: • Name—The name of the account associated with the adjacencies. • Adjacencies—The identified adjacencies.
SIP Adjacency	An adjacency represents a signaling relationship with a remote call agent. One adjacency is defined per external call agent. Each adjacency belongs within an account. Each incoming call is matched to an adjacency, and each outgoing call is routed out over a second adjacency. The SBC SIP Adjacencies table contains the following information: • Name—The adjacency name. • Status—The status of the adjacency, either Attached or Detached. • Signaling Address—The local IP address and port (optional) for communications. • Signaling Peer—The remote IP address and port (optional) for communications. • Description—A brief description of the adjacency.
SIP Adjacency Group	The Adjacencies Groups table contains the following information: • Name—The name of the SIP adjacency group. • Adjacencies—The adjacencies that belong to the group.
SIP Profile	The SBC can be configured with whitelist and blacklists profiles on SIP messages. The following types of SIP profiles are available: • Header profile—A profile based on SIP header information. • Method profile—A profile based on SIP method strings. • Option profile—A profile based on SIP option strings. • Parameter profile—A profile based on SIP parameters.
SIP Profile > Header Profile	The SIP Header Profiles table contains the following information: • Name—The name of the SIP header profile. • Status—Whether or not the profile is in use. • Profile Type—The type of profile: – Whitelist—Accepts SIP requests that match the profile. – Blacklist—Rejects SIP requests that match the profile. • Description—A brief description of the profile.

Table 24-9 SIP Properties (continued)

Branch	Description
SIP Profile > Method Profile	The SIP Method Profiles table contains the following information: • Name—The name of the SIP method profile. • Status—Whether or not the profile is in use. • Profile Type—The type of profile: – Whitelist—Accepts SIP requests that match the profile. – Blacklist—Rejects SIP requests that match the profile. • Description—A brief description of the profile. • Is Passthrough—Whether or not passthrough is enabled: – True—Permits message bodies to be passed through for nonvital methods that match this profile. – False—Strips the message body out of any nonvital SIP messages that match this profile.
SIP Profile > Option Profile	The SIP Option Profiles table contains the following information: • Name—The name of the SIP option profile. • Status—Whether or not the profile is in use. • Profile Type—The type of profile: – Whitelist—Accepts SIP requests that match the profile. – Blacklist—Rejects SIP requests that match the profile. • Description—A brief description of the profile. • Options—The SIP option strings that define this profile, such as host user-agent, refer redirect, or replaces.

Table 24-9 SIP Properties (continued)

Branch	Description
SIP Profile > Parameter Profile	The SIP Parameter Profiles table contains the following information: • Name—The name of the SIP parameter profile. • Status—Whether or not the profile is in use. • Description—A brief description of the profile.
SIP Timer	The SBE SIP Timer table contains the following information: • TCP Connect Timeout—The time, in milliseconds, that the SBC waits for a SIP TCP connection to a remote peer to complete before failing that connection. The default is 1000 milliseconds. • TCP Idle Timeout—The minimum time, in milliseconds, that a TCP socket does not process any traffic before it closes the connection. The default is 120000 milliseconds (2 minutes). • TLS Idle Timeout—The minimum time, in milliseconds, that a Transport Layer Security (TLS) socket does not process traffic before it closes the connection. • Invite Timeout—The time, in seconds, that the SBC waits for a final response to an outbound SIP invite request. The default is 180 seconds. If no response is received during that time, an internal request timeout response is generated and returned to the caller. • UDP First Retransmit Interval—The time, in milliseconds, that the SBC waits for a UDP response or ACK before sending the first retransmission of a signal. The default value is 500 milliseconds. • UDP Max Retransmit Interval—The maximum time interval, in milliseconds, for an SBC to retransmit a signal. The maximum retransmission interval is 4000 milliseconds (4 seconds). • UDP Response Linger Period—The time, in milliseconds, for which the SBC retains negative UDP responses to invite requests. The default value is 32000 milliseconds (32 seconds).

Viewing SBC Statistics

The following SBC statistics commands can be launched from the inventory by right-clicking the appropriate node and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Navigation	Description
Current 15 Min Statistics	**Show > PM >**	Based on the command selected, the device's statistics are displayed.
Current 5 Min Statistics		
Current Day Statistics		
Current Hour Statistics		
H.248 Statistics		
Previous 15 Minutes Statistics		
Previous 5 Minutes Statistics		
Previous Day Statistics		
Previous Hour Statistics		
CPS Data		
Media Statistics	**Show >**	
Components		

Configuring SBC Components

The following SBC component commands can be launched from the inventory by right-clicking the appropriate node and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Navigation	Description
SIP Adjancencies		
Add SIP Adjacency	*Right-click the SBC node* > **Commands > Add > SIP Adjacency**	Add an SIP adjacency or update an existing SIP adjacency.
Update SIP Adjacency **Delete SIP Adjacency**	In the **SIP Adjacencies** window, *right-click the adjacency instance* > **Commands > Update /Delete > SIP Adjacency**	
Add SIP Adjacency Outbound AuthRealm **Update SIP Adjacency Outbound AuthRealm** **Delete SIP Adjacency Outbound AuthRealm**	In the **SIP Adjacencies** window, *right-click the SIP adjacency instance* > **Commands > Add /Update/Delete > SIP Adjacency Outbound AuthRealm**	Use this command to add a SIP adjacency outbound authentication realm.

Command	Navigation	Description
SIP Header Profiles		
Add SIP Header Profile	*Right-click the SBE node* > **Commands > Add > SIP Header Profile**	Add or change an SIP header profile.
Update SIP Header Profile **Delete SIP Header Profile**	In the **SIP Header Profiles** window*, right-click the profile* > **Commands > Update/Delete > SIP Header Profile**	
Add SIP Header Profile Header	In the **SIP Header Profiles** window, *right-click the SIP header profile instance* > **Commands > Add > SIP Header Profile Header**	Add more headers (up to 3) to an existing SIP header profile (after the existing SIP header profile is discovered).
Delete SIP Header Profile Header	In the header profile properties window, *right-click the header you want to remove and choose* > **Commands > Delete > IP Header Profile Header**	Delete a header from a header profile.
Add SIP Header Profile Entry	*Right-click the SBE node* > **Commands** > **Add** > **SIP Header Profile Entry**	Add an entry to an existing SIP header profile header.
Update SIP Header Profile Entry **Delete SIP Header Profile Entry**	*Right-click an entry in the SIP Header Profile Header Properties window* > **Commands** > **Update/Delete** > **SIP Header Profile Entry**	Update or delete an existing SIP Header Profile entry in the **SIP Header Profile Header Properties** window.
Add SIP Header Profile Condition	Expand the SBE node, SIP node, and SIP Profile node, and click the Header Profile node > *Double-click a header profile to open the SIP Header Profile Properties window* > *Double-click a header* > *Right-click an entry* > **Commands** > **Add** > **SIP Header Profile Condition**	Add a condition to a SIP header profile header.
SIP Option Profiles		
Add SIP Option Profile	*Right-click the SBE node* > **Commands** > **Add** > **SIP Option Profile**	Configure SIP option profile parameters such as option profile type (whitelist or blacklist), profile options, and so on.
Update SIP Option Profile **Delete SIP Option Profile**	*Right-click a profile in the SIP Option Profile window* > **Commands** > **Update/Delete** > **SIP Option Profile**	

Command	Navigation	Description
Add SIP Parameter Profile	*Right-click the SBE node* > **Commands** > **Add** > **SIP Parameter Profile**	Configure SIP parameter profile.
Delete SIP Parameter Profile	*Click the Parameter Profile node, right-click the profile* > **Commands** > **Delete** > **SIP Parameter Profile**	
Add SIP Parameter Profile Parameter	Expand the SBE node, SIP node, SIP Profile node > *Click the Parameter Profile* >R*ight-click the profile instance* > **Commands** > **Add** > **SIP Parameter Profile Parameter**	Add, update, or delete parameter in SIP parameter profiles. Specify the parameter name to be updated and the name of the profile in which you want to add or update the parameter.
Update SIP Parameter Profile Parameter **Delete SIP Parameter Profile Parameter**	*Double-click the profile that contains the parameter* > R*ight-click the parameter* > **Commands** > **Update/Delete** > **SIP Parameter Profile Parameter**	
Blacklists		
Add Blacklist	*Right-click the SBE node* > **Commands** > **Add** > **Blacklist**	Add or delete blacklist in the SBC node. Specify the IP address, port type, and the port number to be blacklisted.
Delete Blacklist	In the **Configured Blacklist Properties** window, *right-click the blacklist* > **Commands** > **Delete** > **Blacklist**	
Add Blacklist Reason	*Right-click the blacklist instance* > **Commands** > **Add** > **Blacklist Reason**	Add, modify, or delete a blacklist reason for the blacklisted node in SBC.
Update Blacklist Reason **Delete Blacklist Reason**	In the **Configured Blacklist Properties** window*, right-click a blacklist reason* > **Commands** > **Update/Delete** > **Blacklist Reason**	
Call Admission Control (CAC) Policies		
Add CAC Policy Set	*Right-click the SBE node* > **Commands** > **Add** > **CAC Policy Set**	Add, modify, or delete a CAC Policy Set
Update CAC Policy Set **Delete CAC Policy Set**	In the **CAC Policy Set** window, *right-click the policy set instance* > **Commands** > **Update/Delete** > **CAC Policy Set**	

Command	Navigation	Description
Add CAC Policy Table	In the **CAC Policy Set** window, *right-click the CAC policy instanc*e > **Commands** > **Add** > **CAC Policy Table**	Add or modify a CAC policy table in an existing CAC policy set.
Update CAC Policy Table **Delete CAC Policy Table**	*Right-click a policy table in the CAC Policy Set Properties window* > **Commands** > **Update/Delete** > **CAC Policy Table**	
Add CAC Rule Entry	*Right-click a policy table* > **Commands** > **Add** > **CAC Rule Entry**	Add or modify a CAC rule entry in an existing CAC policy table.
Update CAC Rule Entry **Delete CAC Rule Entry**	*Right-click an entry in the CAC Rule Entry ta*b > **Commands** > **Update/Delete** > **CAC Rule Entry**	
Add Call Policy Set	*Right-click the SBE node* > **Commands** > **Add** > **Call Policy Set**	Add, modify, or delete a Call Policy Set. **Note** When you add a new call policy set, you can add three call policy tables. You can add more tables after the call policy set you created is discovered.
Update Call Policy Set **Delete Call Policy Set**	*Right-click a policy set in the Call Policy Set window* > **Commands** > **Update** > **Call Policy Set**	
Add Call Policy Table	In the **Call Policy Set** window, *right-click the policy se*t > **Commands** > **Add** > **Call Policy Table**	Add, modify, or delete call policy tables
Update Call Policy Table **Delete Call Policy Table**	*Double-click a policy set, then right-click a policy table* > **Commands** > **Update** > **Call Policy Table**	
Add Call Rule Entry	*Right-click a policy table* > **Commands** > **Add** > **Call Rule Entry**	Add, modify, or delete an entry from an existing call policy table.
Update Call Rule Entry **Delete Call Rule Entry**	*Double-click a policy table, then right-click an entry* > **Commands** > **Update/Delete** > **all Rule Entry**	
Codec Lists		
Add Codec List	*Right-click the SBE node* > **Commands** > **Add** > **Codec List**	Add, or delete a Codec List
Delete Codec List	In the **Codec List** window, *right-click a list instance* > **Commands** > **Delete** > **Codec List**	

Command	Navigation	Description
Add Codec List Entry	In the **Codec List** window, *right-click the codec list instance* > **Commands** > **Add** > **Codec List Entry**	Add, modify, or delete an entry in a codec list.
Update Codec List Entry **Delete Codec List Entry**	*Double-click the codec list, then right-click the codec* > **Commands** > **Update /Delete**> **Codec List Entry**	
Media Addresses		
Add Media Address	*Right-click the SBE node* > **Commands** > **Add** > **Media Address**	Add a media address or media Address DBE with parameters indicating that media address is managed by the Data Border Element (DBE) or Media Gateway Configuration (MGC).
Add Media Address Dbe	*Right-click the DBE node* > **Commands** > **Add** > **Media Address Dbe**	
Delete Media Address	Expand the DBE node and click the Media Address node >*Right-click the media address* > **Commands** > **Delete** > **Media Address**	Delete an existing media address from the DBE node.
QoS Profiles		
Add QoS Profile	*Right-click the SBE node* > **Commands** > **Add** > **QoS Profile**	Configure QoS profile on a SBE node
Update QoS Profile **Delete QoS Profile**	*Right-click the profile in the QoS Profile window* > **Commands** > **Update** > **QoS Profile**	

Monitoring BNG Configurations

Broadband Network Gateway (BNG) provides capabilities that help to improve the service provider's ability to manage the subscriber's services, and simplify overall network operations. BNG is a functionality that comprises subscriber management at a logical aggregation point in the network, which manages the subscriber’s user experience through identification, address assignment, authentication, authorization, accounting, and various other features such as security, Quality of Service (QoS), and subscriber forwarding.

BNG represents the subscriber as a session, which is a logical point to enable services for a given subscriber. A subscriber is usually identified with the protocol that provides the IP address of the subscriber for address assignment. For example, a subscriber that uses the Point-to-Point Protocol (PPP) to connect to the network, receives its IP address through the PPP IP Control Protocol (IPCP) negotiation, and is represented as a PPP session. A subscriber that uses Ethernet to connect to the network receives its IP address through Dynamic Host Control Protocol (DHCP) and is represented as an IP session.

The purpose of deploying BNG at the provider edge is to better manage and enrich the subscriber experience.

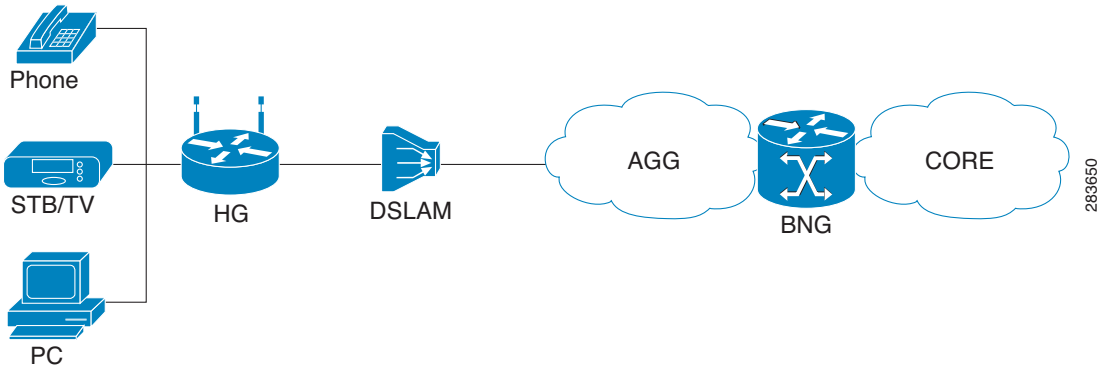
BNG separates subscriber access functions from provider services and yields these benefits:

- Comprehensive session management and billing functions are supported by means of communication with an authentication, authorization, and accounting (AAA) server that is separate from the BNG.
- Subscribers can obtain services based on their subscriber ID or a combination of their subscriber ID and access line.

The network topology for BNG can be explained using the following models:

- BNG Retail Model—The subscriber connects to the network over a digital subscriber line (DSL) circuit into a DSL access multiplexor (DSLAM), which aggregates a number of subscribers. The DSLAMs are connected to an aggregation network, which grooms the subscriber traffic and switches it to BNG. A sample of the retail model is shown in Figure 25-1.

Figure 25-1 BNG Retail Model



- BNG Wholesale Model—The subscriber's traffic is handed off by the carrier (who still owns the infrastructure) to one of the several Internet Service Providers (ISP). There are different ways to make this handoff, Layer 2 Tunneling Protocol (L2TP) or Layer 3 virtual private networking (VPN) being two such methods.

The BNG Retail model is used for deployment in Prime Network.

Prime Network provides BNG support for Cisco Aggregation Service Router (ASR) 9000 series network elements.

These topics provide an overview of the Broadband Network Gateway (BNG) technology and describe how to monitor and view BNG configurations using the Vision client. If you cannot perform an operation that is described in these topics, you may not have sufficient permissions; see Permissions for Managing BNG, page B-22.

Working with BNG Configurations

This topic contains the following sections:

Viewing Broadband Access (BBA) Groups

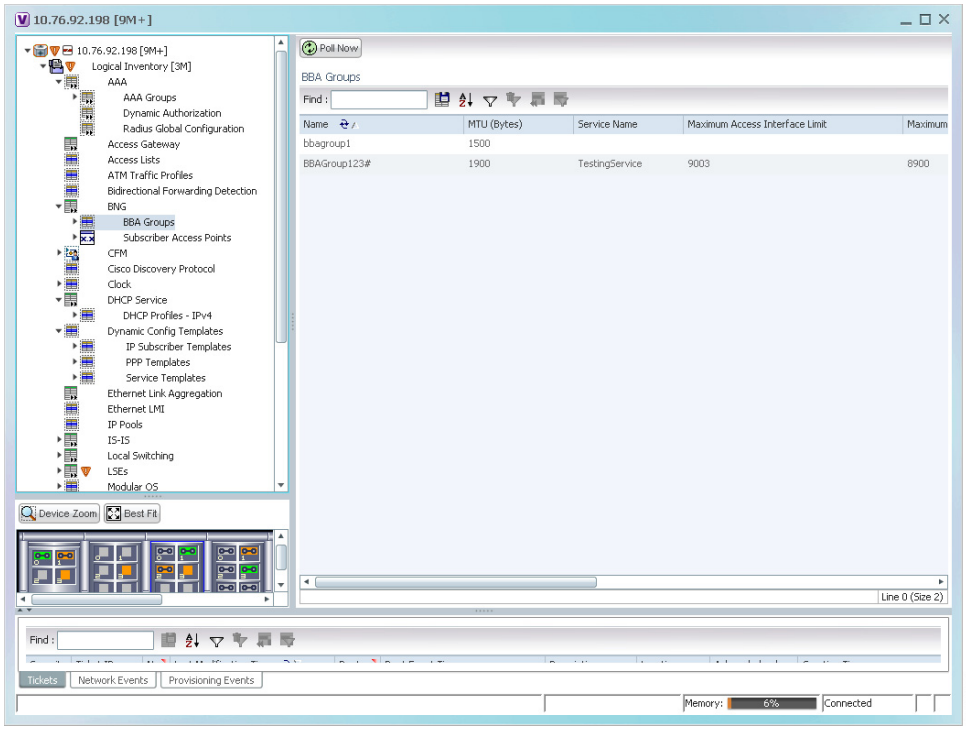
BBA groups refer to the configuration settings applicable to a subscriber session that are accessing the network through an access interface. The same group can be applied to multiple access interfaces. For example, the maximum session limit for an access interface.

To view the BBA group profile:

Step 1 Right-click on the device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **BNG** > **BBA Groups**. A list of BBA groups is displayed in the content pane as shown in Figure 25-2.

Figure 25-2 BBA Groups Content Pane



Step 3 Right-click a group from the list and choose **Properties**. The BBA Group Properties dialog box is displayed.

Table 25-1 describes the fields that are displayed in the BBA Group Properties dialog box.

Table 25-1 BBA Group Properties

Field Name	Description
Name	The name of the BBA Group.
MTU (Bytes)	The default maximum payload, which can be any value between 500 and 2000.
Service Name	The name of the service configured under the specified BBA group.
Maximum Access Interface Limit	The maximum limit of PPP over Ethernet (PPPoE) sessions on the access interface.
Maximum Circuit ID Limit	The maximum limit of PPPoE sessions for the circuit ID.
Maximum Session Limit	The maximum session limit per card. A warning is displayed if the session exceeds the limit specified here.
Maximum MAC Address Access Limit	The maximum limit for MAC address access. A warning is displayed if the access exceeds the limit specified here.
Maximum Payload Limit	The maximum payload limit.
Service Selection	Indicates the status of advertising of unrequested services names. By default, this service is enabled.
Applied Interfaces	
Interface Name	The name of the interface applied to the BBA Group.
Entity Association	The link to the applied interface. Click this hyperlink to view the relevant node under the Subscriber Access Point node.

Viewing Subscriber Access Points

Subscriber access points refer to the access interfaces that are named based on the parent interface. For example, bundle-ether 2.100.pppoe312. The subscribers on bundles (or bundle-VLANs) interfaces allow redundancy and are managed on the route processor (RP). However, the subscribers over physical interfaces are created and managed on the line card (LC) and are not redundant.

To view the subscriber access points profile:

Step 1 Right-click on the device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **BNG** > **Subscriber Access Points**. A list of access points is displayed in the content pane.

Step 3 Right-click the access point from the list and choose **Properties**. The Subscriber Access Point Properties dialog box is displayed.

Table 25-2 describes the fields that are displayed in the Subscriber Access Point Properties dialog box.

Table 25-2 Subscriber Access Point Properties

Field Name	Description
Access Point	The name of the access point.
Associated Entity	The link to the associated entity. Click this hyperlink to view the associated Data Link Aggregation record under the Ethernet Link Aggregation node.
Access Type	The access type for the subscriber access point, which can be any one of the following: • PPPOE_AND_IP • PPPOE • IP
Ingress Service Policy	The service policy for the access point, which when clicked will display the relevant policy under the Policy Container node.
Ingress QoS Policy	The Quality of Service policy for the inbound traffic, which when clicked will display the relevant policy under the Policy Container node.
Egress QoS Policy	The Quality of Service policy for the outbound traffic of the access point, which when clicked will display the relevant policy under the Policy Container node.
BBA Group	The BBA group to which the access point is associated. Click this hyperlink to view the relevant group under the BBA group node.
DHCP Profile	The DHCP profile to which the access point is associated. Click this hyperlink to view the relevant profile under the DHCP node.
IP Address	The destination address for User Datagram Protocol (UDP) broadcasts.
VRF	The Virtual Routing and Forwarding (VRF) in which the access points operates.

Diagnosing Subscriber Access Points

The following commands can be launched from the inventory by right-clicking the **BNG > Subscriber Access Points** node and selecting the **Commands > Diagnose** option**.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 25-3 Diagnose Subscriber Access Points

Diagnose Command	Input parameters
Show DHCP Binding	Binding Type
Show IP Subscriber Management Trace	• Trace Event Type • Trace Count

Table 25-3 Diagnose Subscriber Access Points (continued)

Diagnose Command	Input parameters
Show PPoE Trace	• Trace Filter Type • Trace Count
Show Subscriber Dynamic Template Trace All	• Trace Filter Type • Trace Event Type • Trace Count
Show Subscriber Manager Disconnect History	Disconnect History Filter Type
Show Subscriber Manager Session History	• Session Type • ID Value
Show Subscriber Manager Trace	• Trace Filter Type • Trace Event Type • Trace Count
Show Subscriber Session Details by Filter	• Session Filter Type • Filter Value • Filter State

Viewing Dynamic Host Configuration Protocol (DHCP) Service Profile

DHCP is used to automate host configuration by assigning IP addresses, delegating prefixes (in IPv6), and providing extensive configuration information to network computers.

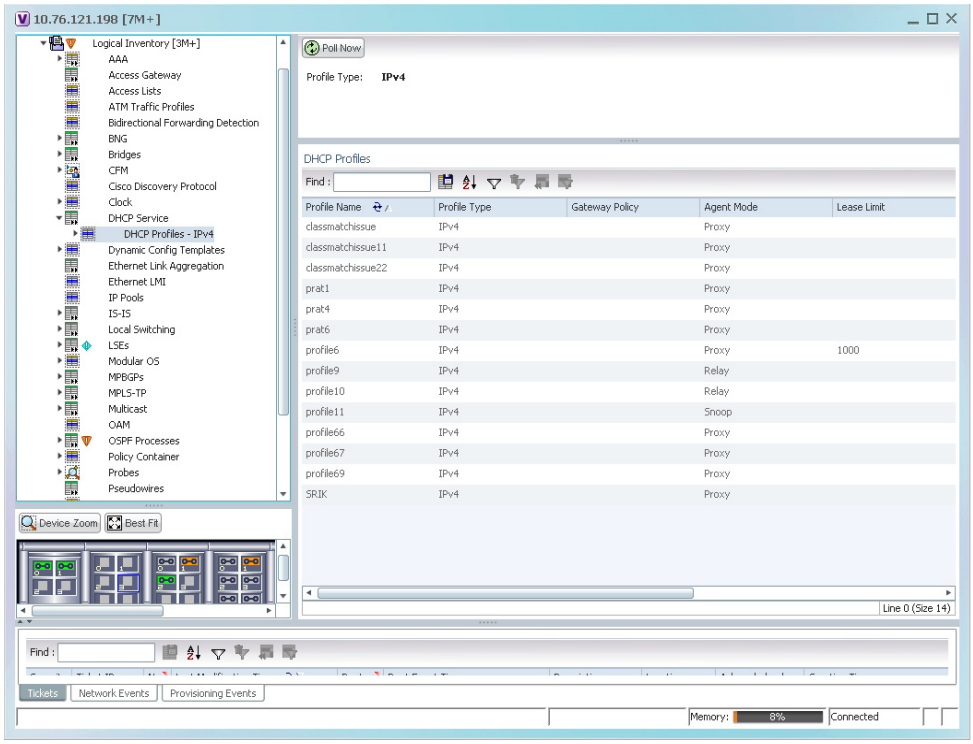
DHCP has the capability to allocate IP addresses only for a specified period of time, which is known as the lease period. If a client device wants to retain the IP addresses for a period longer than the lease period, then the client must renew the lease before it expires. A client can renew the lease depending on the configuration time sent from the server. A REQUEST message is unicast by the client using the server's IP address. On receiving the REQUEST message, the server responds with an acknowledgment, and the client's lease is extended by the lease time configured in the acknowledgment message.

To view the DHCP service profile:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory > DHCP Service > DHCP Profiles - IPv4**. A list of DHCP profiles are displayed in the content pane as shown in Figure 25-3.

Figure 25-3 DHCP Profiles



Step 3 Right-click a service from the list and choose **Properties**. The DHCP Profile Properties dialog box is displayed.

Table 25-4 describes the fields that are displayed in the DHCP Profile Properties dialog box.

Table 25-4 DHCP Profile Properties

Field Name	Description
Profile Name	The name of the DHCP profile.
Profile Type	The network protocol that the profile belongs to. The profile type can be IPV4 or IPV6.
Agent Mode	The DHCP agent mode, which can be Relay, Snoop or Proxy.
Lease Limit	The lease limit for the profile.
Lease Limit Type	The lease limit type.
Relay Information Check	Indicates whether the relay information check is enabled or disabled.
Relay Information Policy	The relay information policy.
DHCP Agent Information Options	
Option	The relay agent information options key parameter.
Value	The value of the relay agent information options.
Applied Interfaces	
Interface Name	The name of the interface applied to the DHCP Group.
Entity Association	The link to the applied interface. Click this hyperlink to view the relevant node under the Subscriber Access Point node.
DHCP Servers	
Profile Class	The profile class.
Server Address	The IP address of the profile, which is used to relay packets.
VRF	The VRF of the DHCP profile. Click this hyperlink to view the relevant node under the VRFs node.
Gateway Address	The IP address of the gateway.
Match Option	The match option of the DHCP profile.
Match Option Value	The value of the match option.
Match Option Mask	The match option mask.

Viewing Dynamic Config Templates

A dynamic template is used to group configuration items, which are later applied to a group of subscribers. This template is globally configured through the command line interface (CLI). However, the template does not get applied to a subscriber interface as soon as it is configured. It must be activated using a control policy. Similarly, you must deactivate the template using a control policy to remove its association with the subscriber interface.

Ideally, you can activate more than one dynamic template on the same subscriber interface, for the same event or different events. The same dynamic-template can be activated on multiple subscriber interfaces through the same control policy.

Prime Network supports the following types of dynamic templates:

- IP subscriber templates
- PPP templates
- Service templates

To view the configuration templates:

Step 1 Right-click on the device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **Dynamic Config Templates > IP Subscriber Templates** or **PPP template** or **Service template**. A list of templates is displayed in the content pane.

Step 3 Select a template from the list, right-click and choose **Properties** to view its details.

Table 25-5 describes the fields that are displayed in the corresponding dialog box.

Table 25-5 Template Properties

Field Name	Description
Name	The name of the subscriber template.
Template Type	The template type, which can be **IP Subscriber, PPP** or **Service** based on the selected template.
Ingress Policy	The name of the ingress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates.
Associated Ingress Policy	The associated ingress policy. Click this hyperlink to view the relevant node under the Policy Container node. This field is applicable only for IP subscriber templates.
Egress Policy	The name of the egress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates.
Associated Egress Policy	The associated egress policy. Click this hyperlink to view the relevant node under the Policy Container node. This field is applicable only for IP Subscriber and Service templates.
Ingress Access-List	The name of the ingress access-list associated with the subscriber template. This field is applicable only for IP subscriber templates.
Associated Ingress-ACL Entity	The associated ingress access list. Click this hyperlink to view the related list in the Access List node. This field is applicable only for IP subscriber templates.
Egress Access-List	The name of the egress access-list associated with the subscriber template. This field is applicable only for IP subscriber templates.
Associated Egress-ACL Entity	The associated egress access list. Click this hyperlink to view the related list in the Access List node. This field is applicable only for IP subscriber templates.
Mtu	The maximum transmission unit for IPv4.
Idle Timeout	The idle timeout for the subscriber template in seconds. This field is applicable only for IP Subscriber and Service templates.

Table 25-5 Template Properties (continued)

Field Name	Description
Keep Alive Enabled	Indicates whether the Keep alive feature is enabled. This field is applicable only for PPP templates.
Keep Alive Interval	The keep alive interval time in terms of seconds. This field is applicable only for PPP templates.
Maximum Bad Authentication Request	The maximum number of authentication failures, which can be any value between 0 and 10. This field is applicable only for PPP templates.
Maximum Unacknowledged Request	The maximum number of unacknowledged configured requests, which can be any value between 4 and 20. This field is applicable only for PPP templates.
Maximum Negative Acknowledgement	The maximum number of consecutive configuration negative acknowledgements, which can be any value between 2 and 10. This field is applicable only for PPP templates.

Viewing the Settings for a PPP Template

In addition to the above details, you can also view the following settings for a PPP template:

- IPCP Settings
- LCP Settings
- Authentication Settings
- PPP Timeout Settings

To view the settings:

Step 1 Right-click on the device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **Dynamic Config Templates > PPP template**. A list of templates is displayed in the content pane.

Step 3 Select a template from the list, right-click and choose **Properties** to view its details. You can click on the tab to view more details. The IPCP tab is displayed by default.

Table 25-6 describes the fields that are displayed in the corresponding dialog box.

Table 25-6 PPP Template Settings

Field Name	Description
DNS Server	The IPCP negotiation primary and secondary DNS IP address.
WINS Server	The IPCP negotiation primary and secondary WINS IP address.
IPAddress PoolName	The IPCP negotiation name of the peer-address pool.
Associated IP Pool Entity	The associated IP pool entity for the template.
ReNegotiation Enabled	Indicates whether the attempts by the peer to renegotiate IPCP is enabled.

Table 25-6 PPP Template Settings (continued)

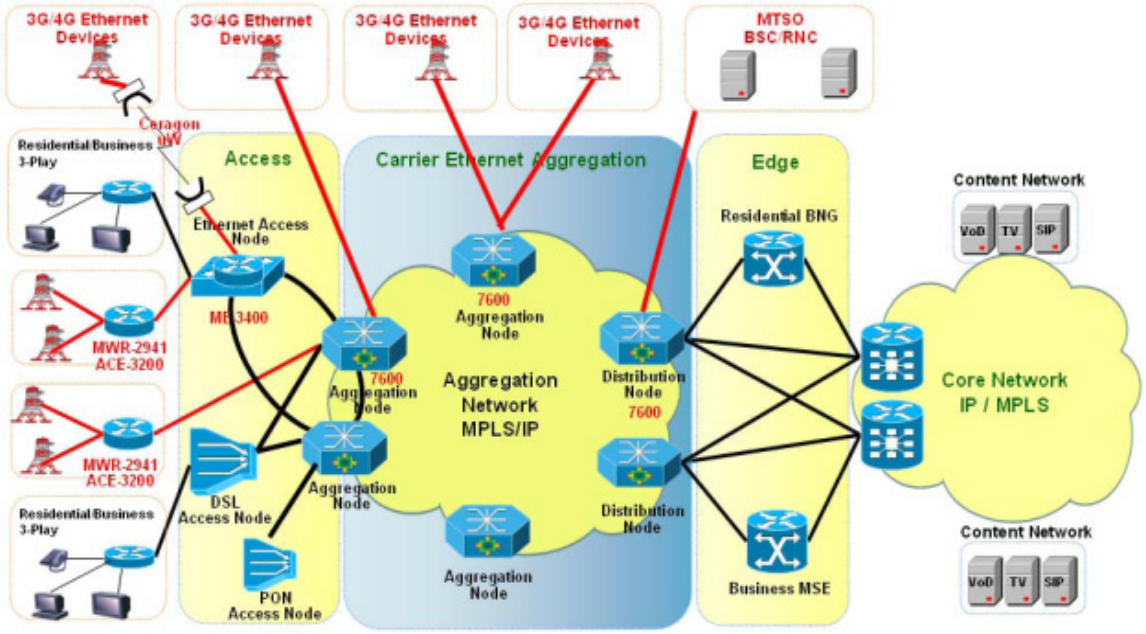
Field Name	Description
LCP Settings tab	
Delay	The time period (in seconds or milliseconds) to delay before starting active LCP negotiations.
ReNegotiation Enabled	Indicates whether the attempts by the peer to renegotiate LCP is enabled.
Authentication Settings tab	
Authentication Type	The PPP link authentication method, which can be any one of the following: • chap • ms-chap • pap
Chap Host Name	The Challenge Handshake Authentication Protocol (CHAP) host name.
MS Chap Host Name	The mobile station CHAP host name.
PPP Timeout Settings	
Absolute Session Timeout	The absolute timeout for a PPP session.
Maximum Authentication Response WaitTime	The maximum time (in seconds) to wait for an authentication response during a PPP negotiation.
Maximum Authentication Retry	The maximum time (in seconds) to wait for a response during a PPP negotiation.

CHAPTER 26

Managing Mobile Transport Over Pseudowire (MToP) Networks

Cisco's Mobile Transport over Pseudowire (MToP) solution builds an MPLS cloud between the distribution nodes (between access and aggregation), and the aggregation nodes on the network edge. The MPLS network is also extended over the point-to-point links from the distribution nodes either via Ethernet, serial, microwave, or a Layer 2 access network. Figure 26-1 provides an example of a Prime Network MToP solution.

Figure 26-1 MToP Network



The following topics describe the Mobile Transport over Packet (MToP) services and properties you can view in the Vision client. If you cannot perform an operation that is described in these topics, you may not have sufficient permissions; see Permissions for Managing MToP, page B-20.

Viewing SAToP Pseudowire Type in Logical Inventory

Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP) enables the encapsulation of TDM bit-streams (T1, E1, T3, or E3) as pseudowires over PSNs. As a structure-agnostic protocol, SAToP disregards any structure that might be imposed on the signals and TDM framing is not allowed.

To view the SAToP pseudowire type in logical inventory:

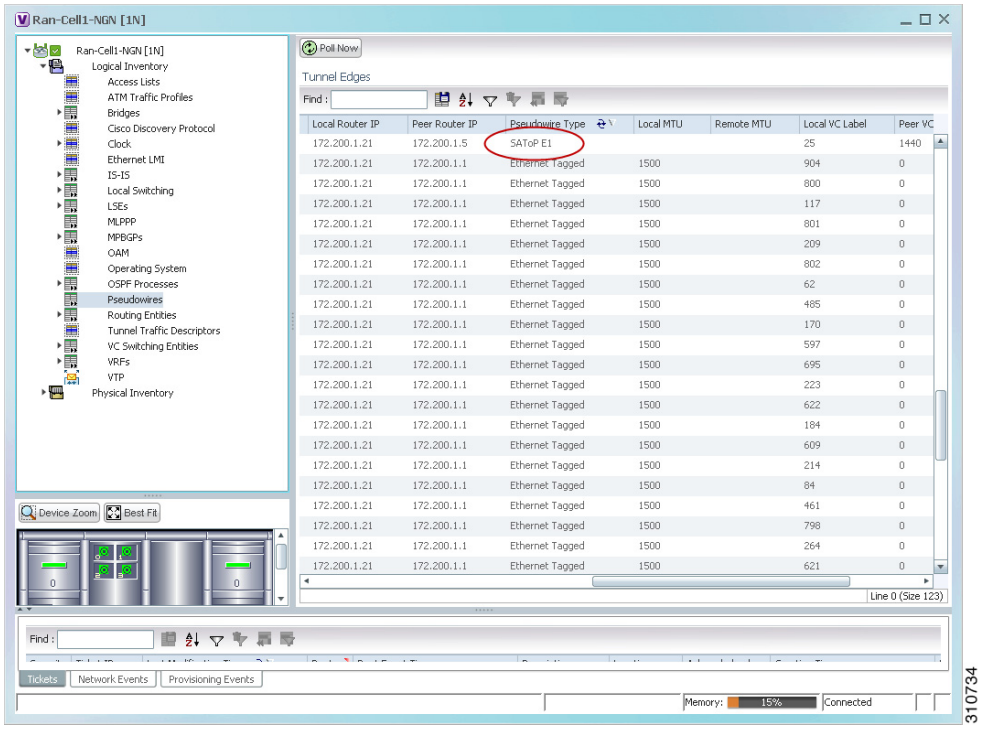
Step 1 In the Vision client, right-click the device on which SAToP is configured, then choose **Inventory**.

Step 2 In the **Inventory** window, choose **Logical Inventory > Pseudowires**.

Step 3 In the Tunnel Edges table, select the required entry and scroll horizontally until you see the Pseudowire Type column. See Figure 26-2.

Note You can also view this information by right-clicking the entry in the table and choosing **Properties**.

Figure 26-2 SAToP Pseudowire Type in Logical Inventory



Step 4 To view the physical inventory for the port, click the hypertext port link.

Viewing CESoPSN Pseudowire Type in Logical Inventory

Circuit Emulation Services over PSN (CESoPSN) is a method for encapsulating structured (NxDS0) TDM signals as pseudowires over packet-switching networks, complementary to SAToP. By emulating NxDS0 circuits, CESoPSN:

- Saves PSN bandwidth.
- Supports DS0-level grooming and distributed cross-connect applications.

To view TDM properties for Circuit Emulation (CEM) groups in the Vision client:

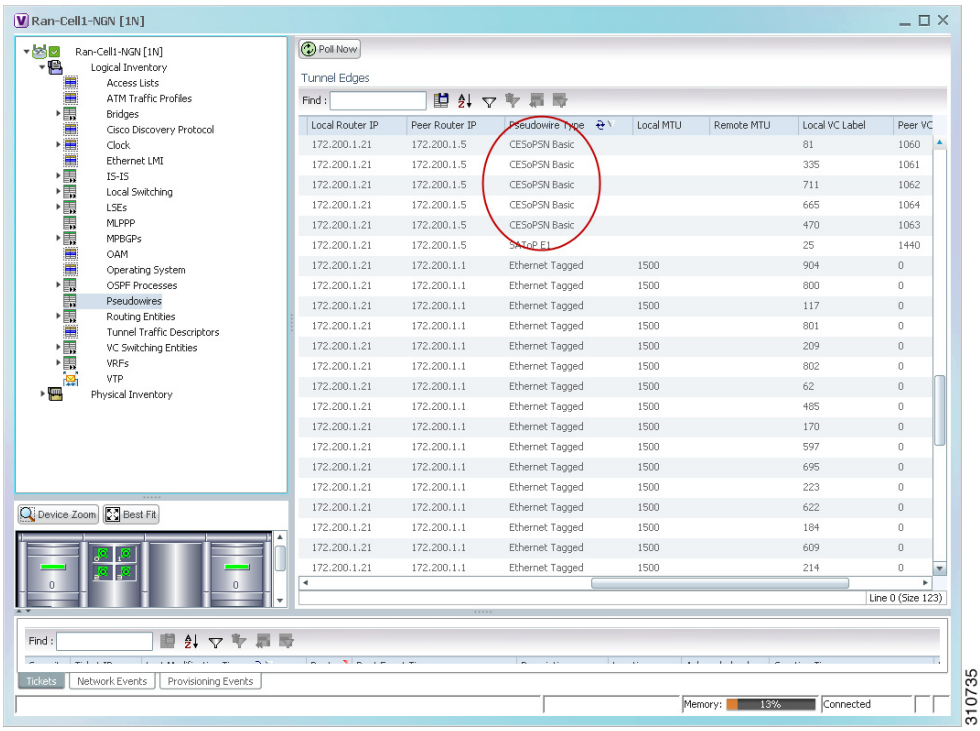
Step 1 In the Vision client, right-click the device on which CESoPSN is configured, then choose **Inventory**.

Step 2 In the **Inventory** window, choose **Logical Inventory > Pseudowires**.

Step 3 In the Tunnel Edges table, select the required entry and scroll horizontally until you see the Pseudowire Type column. See Figure 26-3.

Note You can also view this information by right-clicking the entry in the table and choosing **Properties**.

Figure 26-3 CESoPSN Pseudowire Type in Logical Inventory



Step 4 To view the physical inventory for the port, click the hypertext port link.

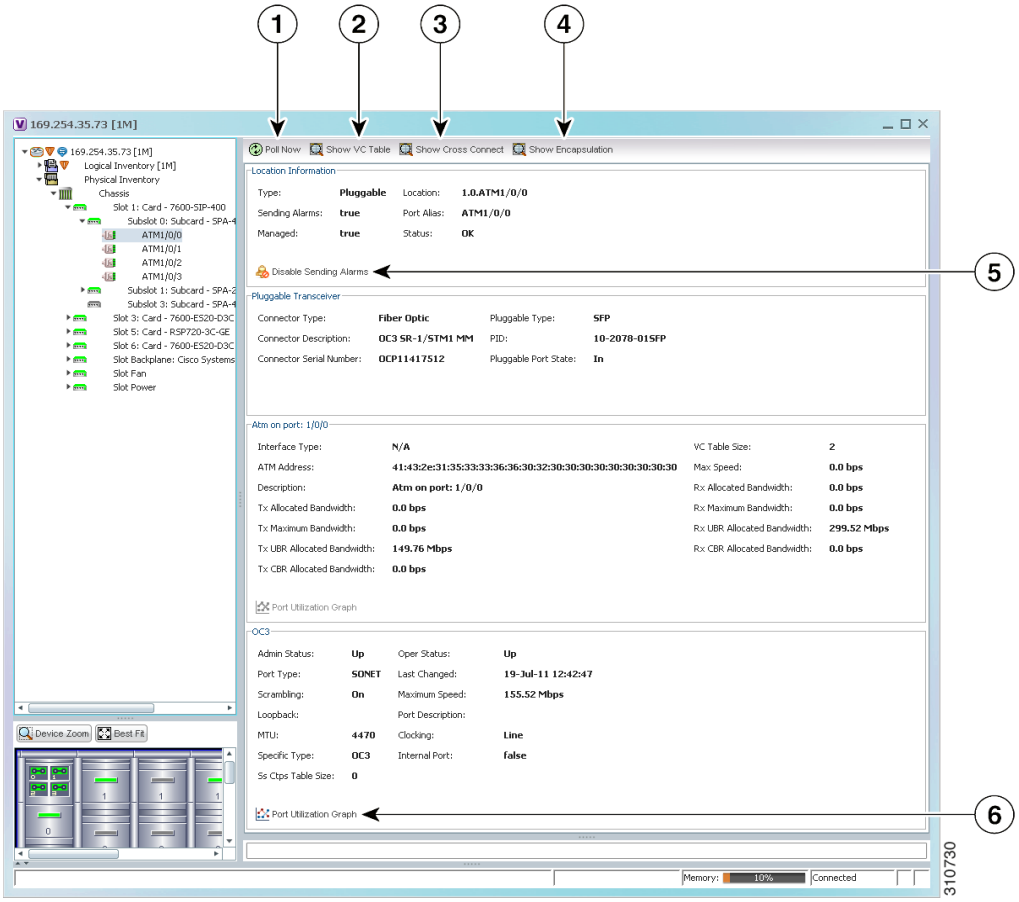
Viewing Virtual Connection Properties

The following topics describe how to view properties related to virtual connections:

- Viewing ATM Virtual Connection Cross-Connects, page 26-6
- Viewing ATM VPI and VCI Properties, page 26-10
- Viewing Encapsulation Information, page 26-11

Buttons for viewing these properties are available at the top of the physical inventory window for the selected interface, as shown in Figure 26-4.

Figure 26-4 ATM-Related Properties Available in Physical Inventory



1	Poll Now button	Polls the VNE for updated status.
2	Show VC Table button	Displays virtual circuit (VC) information for the selected port.. For more information, see Viewing ATM VPI and VCI Properties, page 26-10.
3	Show Cross Connect button	Displays cross-connect information for incoming and outgoing ports. For more information, see Viewing ATM Virtual Connection Cross-Connects, page 26-6.

4	Show Encapsulation button	Displays encapsulation information for incoming and outgoing traffic for the selected item. For more information, see Viewing Encapsulation Information, page 26-11.
5	Disable/Enable Sending Alarms button	Enables you to manage the alarms on a port. For more information, see Viewing Port Status and Properties and Checking Port Utilization, page 8-15.
6	Port Utilization Graph button	Displays the selected port traffic statistics: Rx/Tx Rate and Rx/Tx Rate History. For more information, see Checking a Port's Utilization, page 8-19.
—	Show DLCI Table button (not displayed)	Displays data-link connection identifier (DCLI) information for the selected port.

Viewing ATM Virtual Connection Cross-Connects

ATM networks are based on virtual connections over a high-bandwidth medium. By using cross-connects to interconnect virtual path or virtual channel links, it is possible to build an end-to-end virtual connection.

An ATM cross-connect can be mapped at either of the following levels:

- Virtual path—Cross-connecting two virtual paths maps one Virtual Path Identifier (VPI) on one port to another VPI on the same port or a different port.
- Virtual channel—Cross-connecting at the virtual channel level maps a Virtual Channel Identifier (VCI) of one virtual channel to another VCI on the same virtual path or a different virtual path.

Cross-connect tables translate the VPI and VCI connection identifiers in incoming ATM cells to the VPI and VCI combinations in outgoing ATM cells. For information about viewing VPI and VCI properties, see Viewing ATM VPI and VCI Properties, page 26-10.

To view ATM virtual connection cross-connects:

Step 1 In the Vision client, right-click the required device, then choose **Inventory**.

Step 2 Open the VC Cross Connect table in either of the following ways:

- In the **Inventory** window, choose **Logical Inventory > VC Switching Entities > VC Switching Entity**. The Cross-Connect Table is displayed in the content pane as shown in Figure 26-5.
- In the **Inventory** window:

  a. Choose **Physical Inventory > Chassis >** *Slot* **>** *Subslot* **>** *Port*.

  b. Click the **Show Cross Connect** button.

  The VC Cross Connections window is displayed and contains the same information as the Cross-Connect Table in logical inventory.

Step 3 Select an entry and scroll horizontally until you see the required information.

Figure 26-5 ATM Virtual Connection Cross-Connect Properties

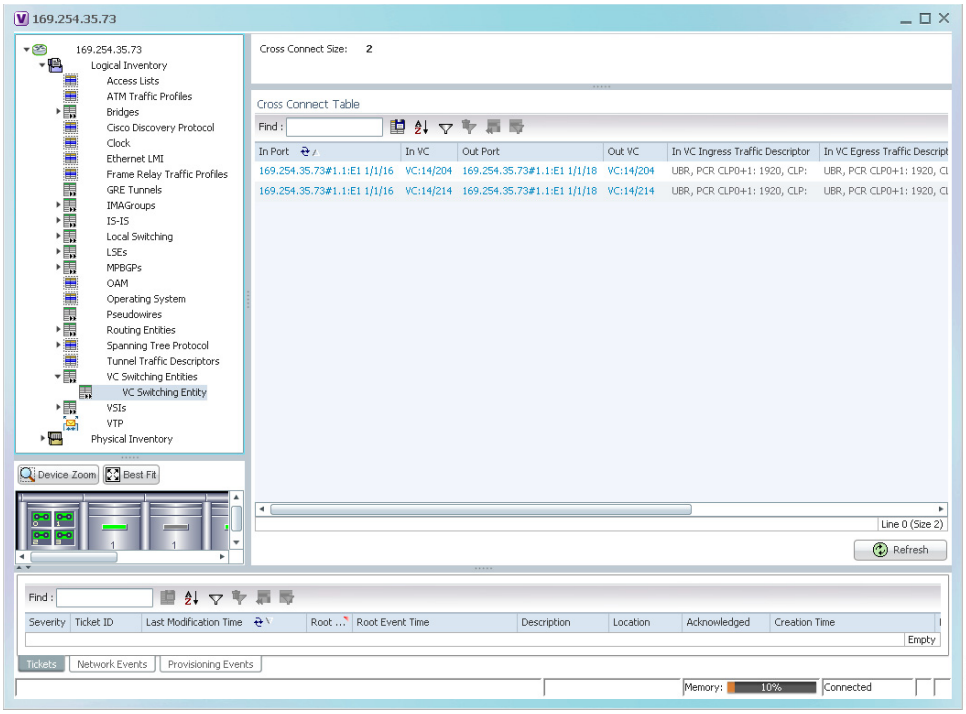


Table 26-1 identifies the properties that are displayed for ATM VC cross-connects.

Table 26-1 ATM Virtual Connection Cross-Connect Properties

Field	Description
In Port	Incoming port for the cross-connect.
In VC	Incoming virtual connection for the cross-connect. You can view additional details about the virtual connection in the following ways: • Click the hyperlinked entry to view the VC table. • Right-click the entry, then choose **Properties** to view information about the incoming and outgoing VCIs, VPI, service category, and traffic descriptors.
Out Port	Outgoing port for the cross-connect.
Out VC	Outgoing virtual connection for the cross-connect. You can view additional details about the virtual connection in the following ways: • Click the hyperlinked entry to view the VC table. • Right-click the entry, then choose **Properties** to view information about the incoming and outgoing VCIs, VPI, service category, and traffic descriptors.
In VC Ingress Traffic Descriptor	ATM traffic parameters and service categories for the incoming traffic on the incoming VC cross-connect. For information on VC traffic descriptors, see Table 26-2.
In VC Egress Traffic Descriptor	ATM traffic parameters and service categories for the outgoing traffic on the incoming VC cross-connect. For information on VC traffic descriptors, see Table 26-2.
Out VC Egress Traffic Descriptor	ATM traffic parameters and service categories for the outgoing traffic on the outgoing VC cross-connect. For information on VC traffic descriptors, see Table 26-2.
Out VC Ingress Traffic Descriptor	ATM traffic parameters and service categories for the incoming traffic on the outgoing VC cross-connect. For information on VC traffic descriptors, see Table 26-2.

Table 26-2 Virtual Connection Traffic Descriptors

Value	Description
ABR	Available bit rate (ABR) supports nonreal-time applications that tolerate high cell delay, and can adapt cell rates according to changing network resource availability to prevent cell loss.
CBR	Constant bit rate (CBR) supports real-time applications that request a static amount of bandwidth that is continuously available for the duration of the connection.
CDVT	Cell Delay Variation Tolerance (CDVT) specifies an acceptable deviation in cell times for a PVC that is transmitting above the PCR. For a given cell interarrival time expected by the ATM switch, CDVT allows for some variance in the transmission rate.
CLP	Cell loss priority (CLP) indicates the likelihood of a cell being dropped to ease network congestion.
MBS	Maximum Burst Size (MBS) specifies the number of cells that the edge device can transmit up to the PCR for a limited period of time without penalty for violation of the traffic contract.
MCR	Minimum Cell Rate (MCR) specifies the cell rate (cells per second) at which the edge device is always allowed to transmit.
PCR	Peak Cell Rate (PCR) specifies the cell rate (cells per second) that the edge device cannot exceed.
PDR CLP0+1: 1536	Packet delivery ratio (PDR) for all cells (both CLP1 and CLP0 cells) on the circuit.
SCR	Sustainable Cell Rate (SCR) specifies the upper boundary for the average rate at which the edge device can transmit cells without loss.
UBR	Unspecified Bit Rate (UBR) supports nonreal-time applications that tolerate both high cell delay and cell loss on the network.
UBR+	Unspecified bit rate plus (UBR+) supports nonreal-time applications that tolerate both high cell delay and cell loss on the network, but request a minimum guaranteed cell rate.
nrt-VBR	Nonreal-time variable bit rate (nrt-VBR) supports nonreal-time applications with bursty transmission characteristics that tolerate high cell delay, but require low cell loss.
rt-VBR	rt-VBR—Real-time variable bit rate (rt-VBR) supports real-time applications that have bursty transmission characteristics.

Viewing ATM VPI and VCI Properties

If you know the interface or link configured for virtual connection cross-connects, you can view ATM VPI and VCI properties from the physical inventory window or from the link properties window.

To view ATM VPI and VCI properties, open the VC Table window in either of the following ways:

- To open the VC Table window from physical inventory:
  a. In the map view, double-click the element configured for virtual connection cross-connects.
  b. In the **Inventory** window, choose **Physical Inventory > Chassis >** *Slot* **>** *Subslot* **>** *Port*.
  c. Click **Show VC Table**.
- To view the VC Table window from the link properties window:
  a. In the map or links view, right-click the required ATM link and choose **Properties**.
  b. In the link properties window, click **Calculate VCs**.
  c. After the screen refreshes, click either **Show Configured** or **Show Misconfigured** to view the virtual connection cross-connects.

The VC Table window is displayed, as shown in Figure 26-6.

Figure 26-6 VC Table

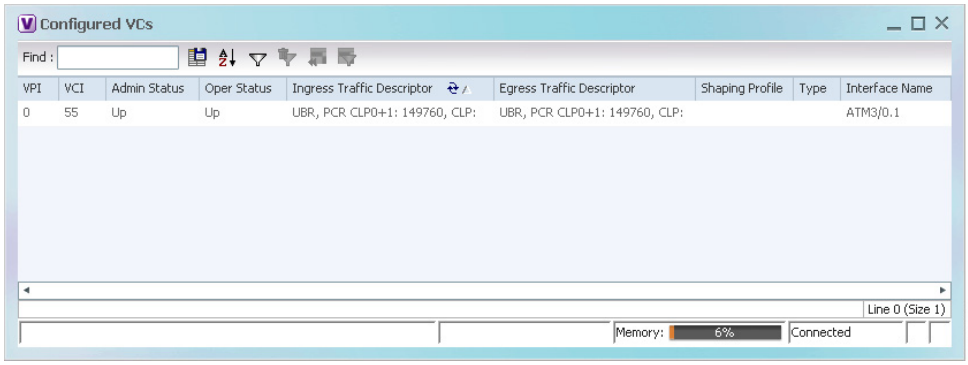


Table 26-3 describes the information displayed in the VC Table window.

Table 26-3 VC Table Properties

Field	Description
VPI	Virtual Path Identifier for the selected port.
VCI	Virtual Channel Identifier for the selected port.
Admin Status	Administrative state of the connection: Up, Down, or Unknown.
Oper Status	Operational state of the connection: Up, Down, or Unknown.
Ingress Traffic Descriptor	Traffic parameters and service categories for the incoming traffic. For information on VC traffic descriptors, see Table 26-2.
Egress Traffic Descriptor	Traffic parameters and service categories for the outgoing traffic. For information on VC traffic descriptors, see Table 26-2.
Shaping Profile	Traffic shape profile used for the virtual connection.
Type	ATM traffic descriptor type for the virtual connection.
Interface Name	Interface name, such as ATM1/1/16.

Viewing Encapsulation Information

To view virtual connection encapsulation information:

Step 1 In the Vision client, double-click the element configured for virtual connection encapsulation.

Step 2 In the **Inventory** window, choose **Physical Inventory > Chassis >** *Slot* **>** *Subslot* **>** *Port*.

Step 3 Click the **Show Encapsulation** button.

The VC Encapsulation window is displayed as shown in Figure 26-7.

Figure 26-7 VC Encapsulation Properties

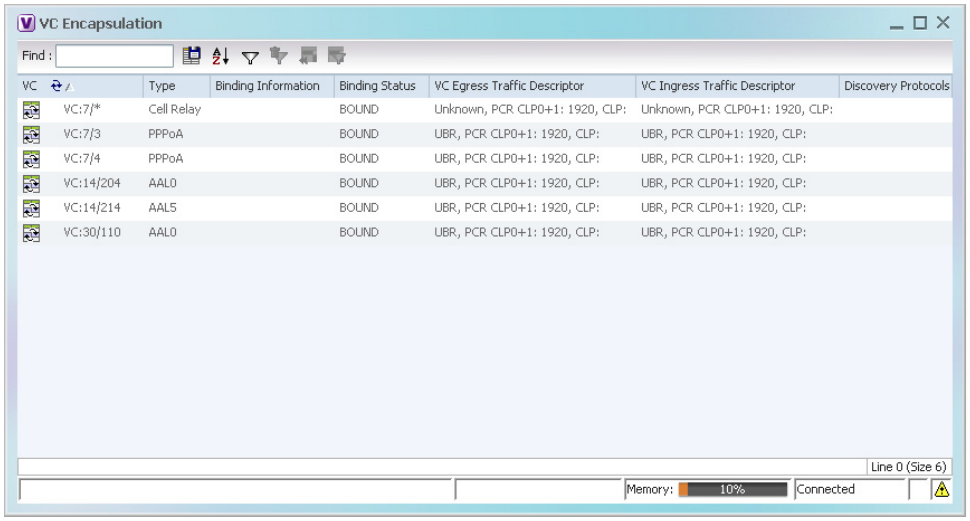


Table 26-4 describes the information displayed in the VC Encapsulation window.

Table 26-4 VC Encapsulation Properties

Field	Description
VC	Virtual connection identifier, such as VC:7/4.
Type	Type of encapsulation, such as Point-to-Point Protocol (PPP) over ATM (PPPoA) or ATM adaption layer Type 5 (AAL5).
Binding Information	Information tied to the virtual connection, such as a username.
Binding Status	Binding state: Bound or Unbound.
VC Egress Traffic Descriptor	Traffic parameters and service categories for the outgoing traffic. For information on VC traffic descriptors, see Table 26-2.
VC Ingress Traffic Descriptor	Traffic parameters and service categories for the incoming traffic. For information on VC traffic descriptors, see Table 26-2.
Discovery Protocols	Discovery protocol used for the VC.

Viewing IMA Group Properties

To view IMA group properties:

Step 1 In the Vision client, double-click the required device.

Step 2 In the **Inventory** window, choose **Logical Inventory > IMA Groups >** *group*. IMA group properties and the IMA Members table are displayed in the content pane as shown in Figure 26-8.

Figure 26-8 IMA Group Properties

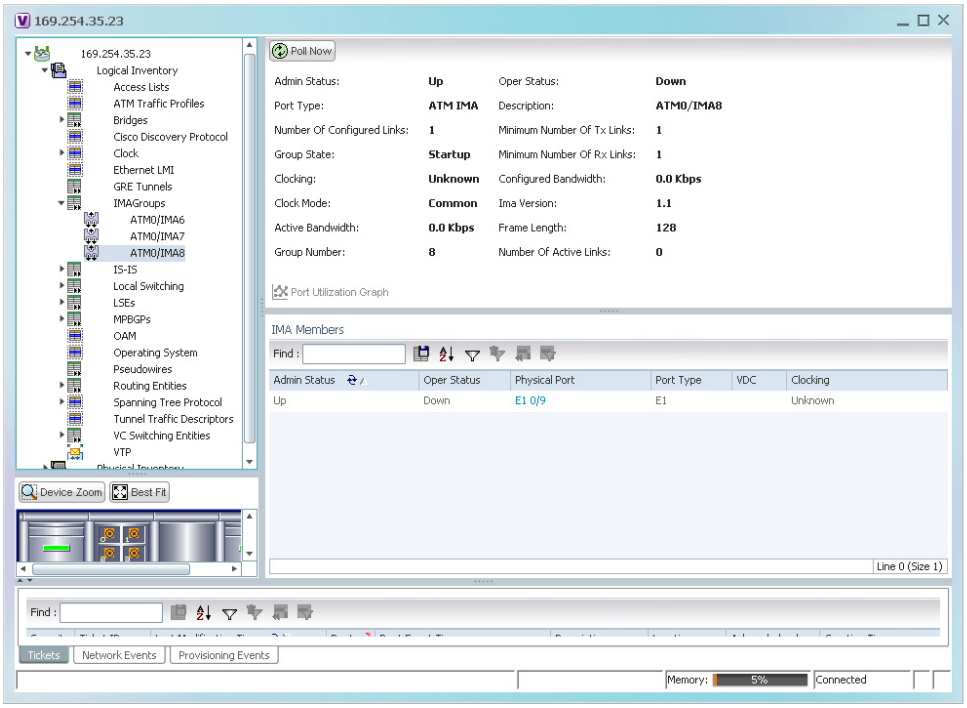


Table 26-5 describes the information displayed for the IMA group.

Table 26-5 IMA Group Properties

Field	Description
Active Bandwidth	Active bandwidth of the IMA group.
Admin Status	Administrative status of the IMA group.
Clock Mode	Clock mode the IMA group is using: • Common—Common transmit clocking (CTC). • Independent—Independent transmit clocking (ITC).
Configured Bandwidth	Total bandwidth of the IMA group, which is the sum of all individual links in the group.
Description	IMA group interface name.

Table 26-5 IMA Group Properties (continued)

Field	Description
Frame Length	Length of the IMA group transmit frames, in the number of cells: 32, 64, 128, or 256. A small frame length causes more overhead but loses less data if a problem occurs. We recommend a frame length of 128 cells.
Group Number	IMA group number.
Group State	IMA group status, in the order of usual appearance: • Startup—The near end is waiting to receive indication that the far end is in Startup. The IMA group moves to the Startup-Ack state when it can communicate with the far end and has recorded IMA identifier, group symmetry, and other IMA group parameters. • Startup ACK—Both sides of the link are enabled. • Config Aborted—The far end has unacceptable configuration parameters, such as an unsupported IMA frame size, an incompatible group symmetry, or an unsupported IMA version. • Insufficient Links—The near end has accepted the far end group parameters, but the far end does not have sufficient links to move into the Operational state. • Operational—The group is not inhibited and has sufficient links in both directions. The IMA interface can receive ATM layer cells and pass them from the IMA sublayer to the ATM layer. • Blocked—The group is blocked, even though sufficient links are active in both directions.
IMA Version	IMA version configured, either 1.0 or 1.1.
Minimum Number of Rx Links	Minimum number of Rx links needed for the IMA group to be operational.
Minimum Number of Tx Links	Minimum number of Tx links needed for the IMA group to be operational.
Number of Active Links	Number of DS1 (E1 or T1) links that are active in the group.
Number of Configured Links	Number of DS1 (E1 or T1) links that are configured in the IMA group.
Oper Status	Operational state of the IMA group interface: • Dormant—The interface is dormant. • Down—The interface is down. • Not Present—An interface component is missing. • Testing—The interface is in test mode. • Unknown—The interface has an unknown operational status. • Up—The interface is up.
Port Type	Type of port, such as ATM IMA.

Table 26-6 describes the information displayed in the IMA Members table.

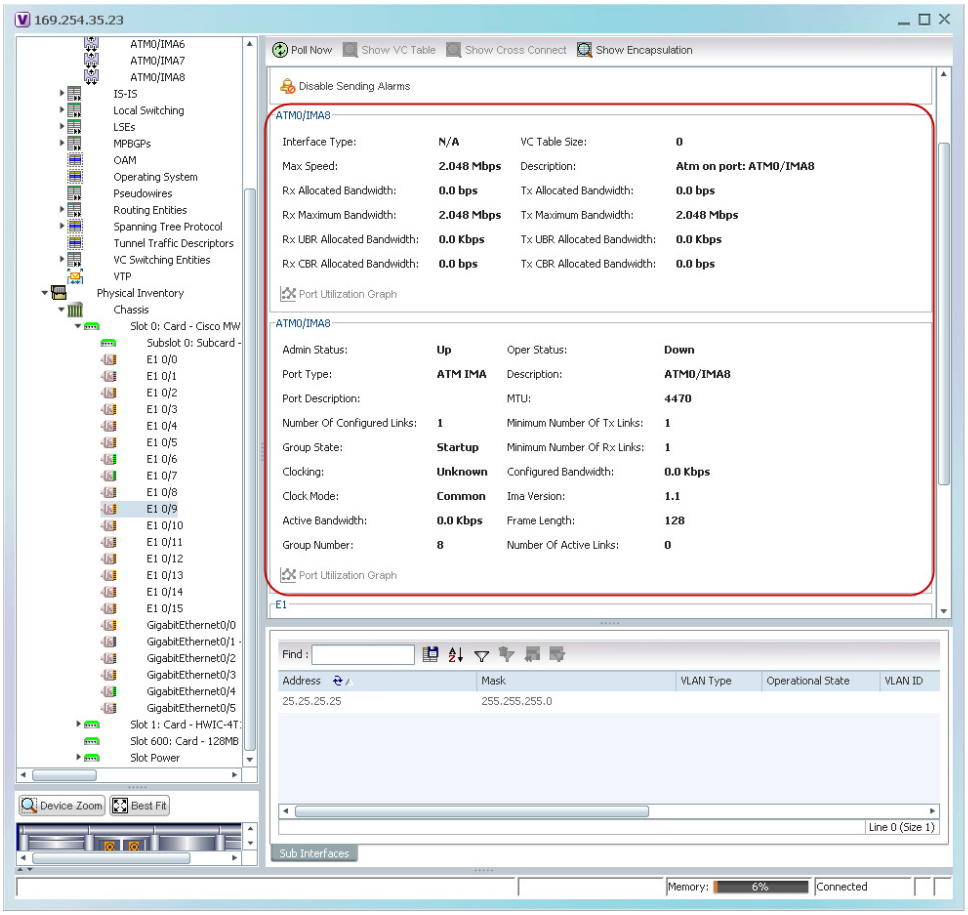
Table 26-6 IMA Members Table

Column	Description
Admin Status	Administrative status of the IMA member.
Channelization	Channelization that occurs through the path, such as STS1-> VTG-> VT15. Information is displayed in this field only if the T1 or E1 path was channelized. If the line was not channelized, this field is not displayed. For example, if the IMA group is configured on a T1 or E1 card, this field is not displayed.
Clocking	Source of the clocking mechanism: Internal or Line.
Description	Type of channelization, such as Synchronous Transport Signal 1 (STS-1) or Synchronous Transport Module level 1 (STM-1).
Oper Status	Operational state of the IMA member:
Physical Port	Hyperlinked entry to the port in physical inventory.
Port Type	Type of port, such as E1 or T1.

Step 3 In the IMA Members table, click a hyperlinked port entry to view the port properties in physical inventory. See Figure 26-9.

The information that is displayed for the port in physical inventory depends on the type of connection, such as SONET or ATM.

Figure 26-9 ATM IMA Port in Physical Inventory



Viewing TDM Properties

TDM is a mechanism for combining two or more slower-speed data streams into a single high-speed communication channel. In this model, data from multiple sources is divided into segments that are transmitted in a defined sequence. Each incoming data stream is allocated a timeslot of a fixed length, and the data from each stream is transmitted in turn. For example, data from data stream 1 is transmitted during timeslot 1, data from data stream 2 is transmitted during timeslot 2, and so on. After each incoming stream has transmitted data, the cycle begins again with data stream 1. The transmission order is maintained so that the input streams can be reassembled at the destination.

MToP encapsulates TDM streams for delivery over packet-switching networks (PSNs) using the following methods:

- SAToP—A method for encapsulating TDM bit-streams (T1, E1, T3, or E3) as pseudowires over PSNs.
- CESoPSN—A method for encapsulating structured (NxDS0) TDM signals as pseudowires over PSNs.

For T1 or E1 entries, the TDM properties presented in Table 26-7 are displayed in physical inventory in addition to the existing T1 or E1 properties.

Table 26-7 TDM-Specific Properties for DS1 (T1 or E1) in Physical Interfaces

Field	Description
International Bit	Whether or not the international bit is used by the controller: • 0—The international bit is not used. • 1—The international bit is used. This property applies only to E1.
National Bits	Whether or not the national reserve bits (sa4, sa5, sa6, sa7, and sa8) are used by the controller: • 0—The national reserve bits are not used. • 1—The national reserve bits are used. This property applies only to E1.
Line Code	Line encoding method for the DS1 link: • For E1, the options are Alternate Mark Inversion (AMI) and high-density bipolar of order 3 (HDB3). • For T1, the options are AMI and bipolar with 8 zero substitution (B8ZS).
Cable Length	For T1 ports in short-haul mode, the length of the cable in feet.

Viewing Channelization Properties

Prime Network supports the channelization of SONET/SDH and T3 5.3. When a line is channelized, it is logically divided into smaller bandwidth channels called paths. These paths (referred to as high order paths or HOPs) can, in turn, contain low order paths, or LOPs. The sum of the bandwidth on all paths cannot exceed the line bandwidth.

For SONET show and configuration commands, see Configuring SONET, page 26-53.

The following topics describe how to view channelization properties for SONET/SDH and T3 5.3:

- Viewing SONET/SDH Channelization Properties, page 26-18
- Viewing T3 DS1 and DS3 Channelization Properties, page 26-21

Viewing SONET/SDH Channelization Properties

SONET and SDH use the same concepts for channelization, but the terminology differs. Table 26-8 describes the equivalent terms for SONET and SDH channelization. The information displayed in the Vision client reflects whether SONET or SDH is configured on the interface.

Table 26-8 SONET and SDH Channelization Terminology

Concept	SONET Term	SDH Term
Frame	Synchronous Transport Signal level N (STS-N)	Synchronous Transport Module level N (STM-N)
HOP channel	STS-1	Administrative Unit (AU-*n*)
Lower-order channels	Virtual Tributary (VT)	Tributary Unit Group (TUG)
LOP payloads	DS1, DS3, or E1	

To view SONET/SDH channelization properties:

Step 1 In the Vision client, right-click the required device, then choose **Inventory**.

Step 2 Choose **Physical Inventory > Chassis >** *slot* **>** *subslot* **>** *SONET/SDH-interface*. The properties for SONET/SDH and OC-3 are displayed in the content pane. See Figure 26-10.

Figure 26-10 SONET/SDH Interface in Physical Inventory

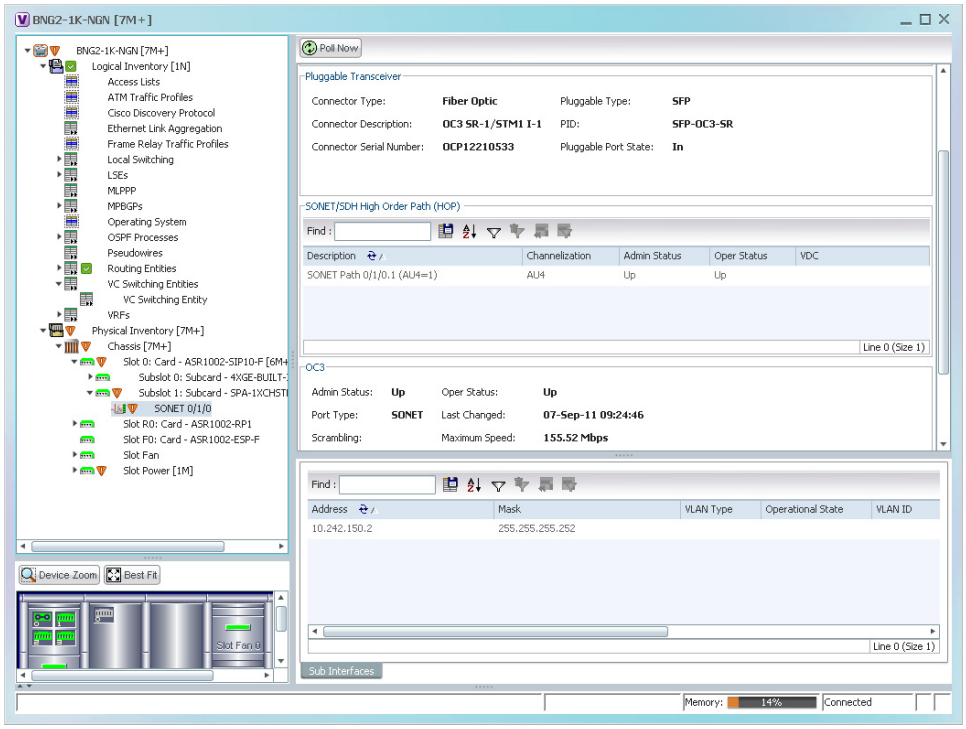


Table 26-9 describes the information that is displayed for SONET/SDH and OC3 in the content pane.

Table 26-9 SONET/SDH and OC3 Properties

Field	Description
SONET/SDH High Order Path (HOP) Area	
Description	SONET/SDH path description including the interface and high order path. Double-click an entry to view additional details about the path.
Channelization	Type of channelization, such as STS-1 or STM-1.
Admin Status	Administrative status of the HOP.
Oper Status	Operational status of the HOP.
OC3 Area	
Admin Status	Administrative status of the OC-3 line.
Oper Status	Operational status of the OC-3 line.
Port Type	Type of port.
Last Changed	Date and time of the last status change of the line.
Scrambling	Any scrambling that has been applied to the SONET payload.
Maximum Speed	Maximum bandwidth for the line.
Loopback	Loopback setting configured on the line.
Port Description	Description of the port defined by the user.
Clocking	Clocking configured on the line.
Specific Type	Specific type of line; in this case, OC3.
Internal Port	Whether or not the line includes an internal port: True or False.
Ss Ctps Table Size	Size of the SONET/SDH Connection Termination Point (CTP) table.

Step 3 To view additional information about a channelized path, double-click the required entry in the Description column. The SONET/SDH High Order Path Properties window is displayed as shown in Figure 26-11.

Figure 26-11 SONET/SDH High Order Path Properties Window

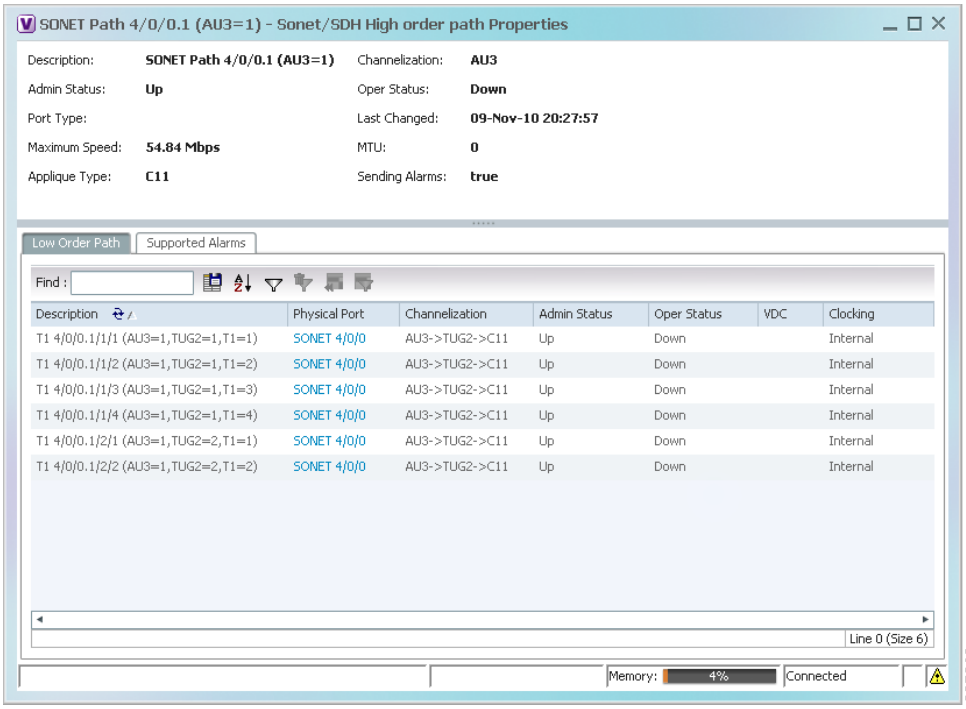


Table 26-10 describes the information displayed in SONET/SDH High Order Path Properties window.

Table 26-10 SONET/SDH High Order Path Properties

Field	Description
Description	SONET/SDH path description including the interface and high order path. Double-click an entry to view additional details about the path.
Channelization	Type of channelization, such as Synchronous Transport Signal 1 (STS-1) or Synchronous Transport Module level 1 (STM-1).
Admin Status	Administrative status of the HOP.
Oper Status	Operational status of the HOP.
Port Type	Type of port.
Last Changed	Date and time of the last status change of the path.
Maximum Speed	Maximum bandwidth for the line.
MTU	MTU for the path.
Applique Type	Sub-STS-1 facility applied to this path. In this example, the facility applied is Virtual Tributary 1.5 (VT1.5).
Sending Alarms	Whether or not the path is sending alarms: True or False.
Low Order Path Tab	
Description	Description of the low order path down to the T1 level, including the channel types (such as STS-1, VTG, or VT) and channel allocated.
Physical Port	Hyperlinked entry to the port in physical inventory.

Table 26-10 SONET/SDH High Order Path Properties (continued)

Field	Description
Channelization	Channelization that occurs through the path, such as STS1-> VTG-> VT15.
Admin Status	Administrative status of the path.
Oper Status	Operational status of the path.
Clocking	Source of the clocking mechanism: Internal or Line.
Supported Alarms Tab	
Name	Supported alarm.
Enable	Whether the alarm is enabled or disabled.

Viewing T3 DS1 and DS3 Channelization Properties

To view T3 DS1 and DS3 channelization properties:

Step 1 In the Vision client, right-click the required device, then choose **Inventory**.

Step 2 Choose **Physical Inventory > Chassis >** *slot* **>** *subslot* **>** *T3-interface*.

Figure 26-12 shows DS1 channelization properties for T3 in physical inventory.

Figure 26-12 T3 DS1 Channelization Properties in Physical Inventory

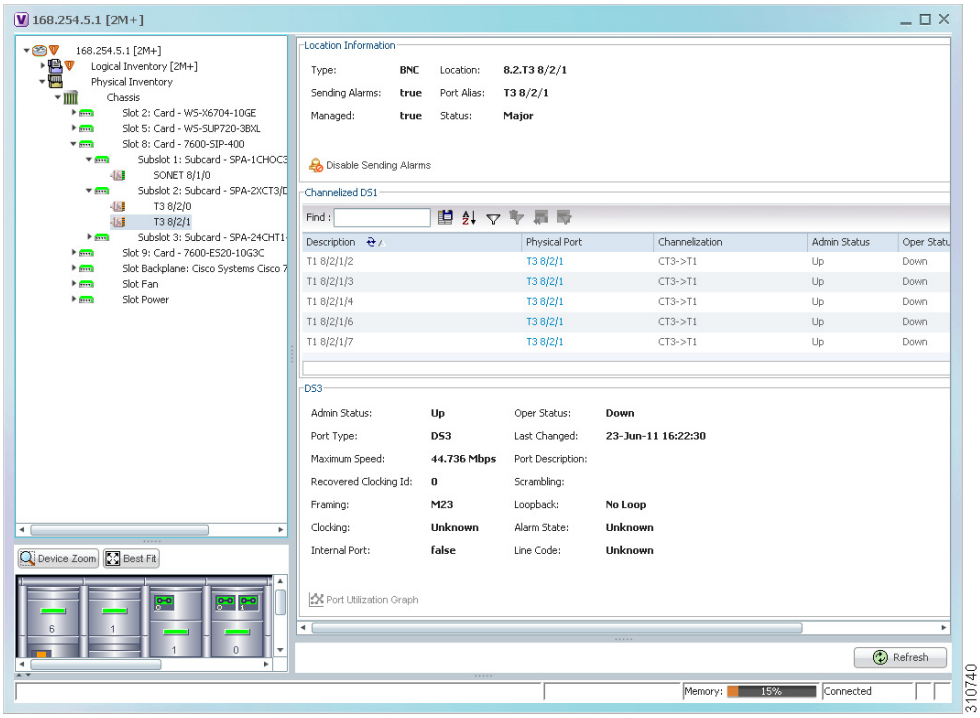


Table 26-11 describes the information that is displayed for Channelized DS1 and DS3 in the content pane.

Table 26-11 Channelized DS1 and DS3 Properties

Field	Description
Channelized DS1 Table	
Description	Path description including the physical interface and the channel number. Double-click an entry to view additional details about the path.
Physical Port	Physical port for the channelized line.
Channelization	Type of channelization, such as channelized T3 (CT3) to T1.
Admin Status	Administrative status of the channelized line.
Oper Status	Operational status of the channelized line.
VDC	For devices with multiple virtual contexts, the context associated with the channelized line.
Clocking	Clocking configured on the line: Internal or Line.

Table 26-11 Channelized DS1 and DS3 Properties (continued)

Field	Description
DS3 Area	
Admin Status	Administrative status of the DS3 line.
Oper Status	Operational status of the DS3 line.
Port Type	Type of port.
Last Changed	Date and time of the last status change of the line.
Maximum Speed	Maximum bandwidth for the line.
Port Description	Description of the port configured on the interface.
Recovered Clocking ID	Recovered clock identifier, if known.
Scrambling	Any scrambling that has been applied to the SONET payload.
Framing	Type of framing applied to the line.
Loopback	Loopback setting configured on the line.
Clocking	Clocking configured on the line: Internal or Line.
Alarm State	Alarm state of the DS3 line: • Clear—The alarm state is clear. • AIS—Alarm Indication Signal (AIS). • LOS—Loss of signal (LOS) alarm. • AIS_LOS—AIS loss of signal alarm. • LOF—Loss of frame (LOF) alarm. • AIS_LOF—AIS loss of frame alarm. • LOS_LOF—Loss of signal and loss of frame alarm. • AIS_LOS_LOF—AIS loss of signal and loss of frame alarm. • Unknown—Unknown alarm.
Internal Port	Whether or not the line includes an internal port: True or False.
Line Code	Line coding applied to the line.

Step 3 To view additional information about a DS1channelized path, double-click the required entry in the Channelized DS1 table. Figure 26-13 shows the information that is displayed in the Channelized DS1 PDH Properties window.

Figure 26-13 Channelized DS1 PDH Properties Window

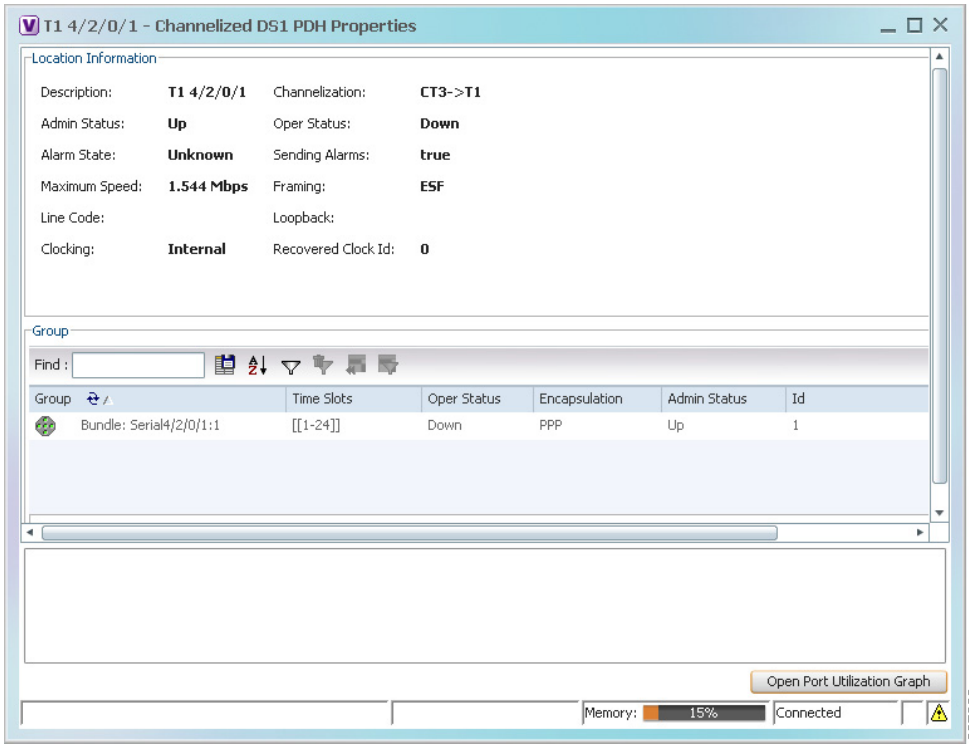


Table 26-12 describes the information that is displayed in the Channelized DS1 PDH Properties window.

Table 26-12 Channelized DS1 PDH Properties Window

Field	Description
Location Area	
Description	Path description including the physical interface and the channel number.
Channelization	Type of channelization used on the line, such as CT3-> T1.
Admin Status	Administrative status of the channelized line.
Oper Status	Operational status of the channelized line.
Alarm State	Alarm state of the DS1 line: • Clear—The alarm state is clear. • AIS—Alarm Indication Signal (AIS). • LOS—Loss of signal (LOS) alarm. • AIS_LOS—AIS loss of signal alarm. • LOF—Loss of frame (LOF) alarm. • AIS_LOF—AIS loss of frame alarm. • LOS_LOF—Loss of signal and loss of frame alarm. • AIS_LOS_LOF—AIS loss of signal and loss of frame alarm. • Unknown—Unknown alarm.

Table 26-12 Channelized DS1 PDH Properties Window (continued)

Field	Description
Sending Alarms	Whether or not the line is sending alarms: True or False.
Maximum Speed	Maximum bandwidth for the line.
Framing	Type of framing applied to the line.
Line Code	Line coding applied to the line.
Loopback	Loopback setting configured on the line.
Clocking	Clocking configured on the line: Internal or Line.
Recovered Clock ID	Recovered clock identifier, if known.
Group Table	
This table appears only if a DS0 bundle is configured on a channelized DS1 line. The properties that are displayed pertain to the DS0 bundle.	
Group	Name of the DS0 bundle.
Time Slots	Range of timeslots (DS0 channels) allotted to the group.
Oper Status	Operational status of the group.
Encapsulation	Type of encapsulation used, such as High-Level Data Link Control (HDLC).
Admin Status	Administrative status of the group.
ID	DS0 bundle identifier.

Viewing MLPPP Properties

Multilink PPP (MLPPP) is a protocol that connects multiple links between two systems as needed to provide bandwidth when needed. MLPPP packets are fragmented, and the fragments are sent at the same time over multiple point-to-point links to the same remote address. MLPPP provides bandwidth on demand and reduces transmission latency across WAN links.

To view MLPPP properties:

Step 1 In the Vision client, right-click the required device, then choose **Inventory**.

Step 2 In the **Inventory** window, choose **Logical Inventory > MLPPP**. See Figure 26-14.

Figure 26-14 MLPPP Properties in Logical Inventory

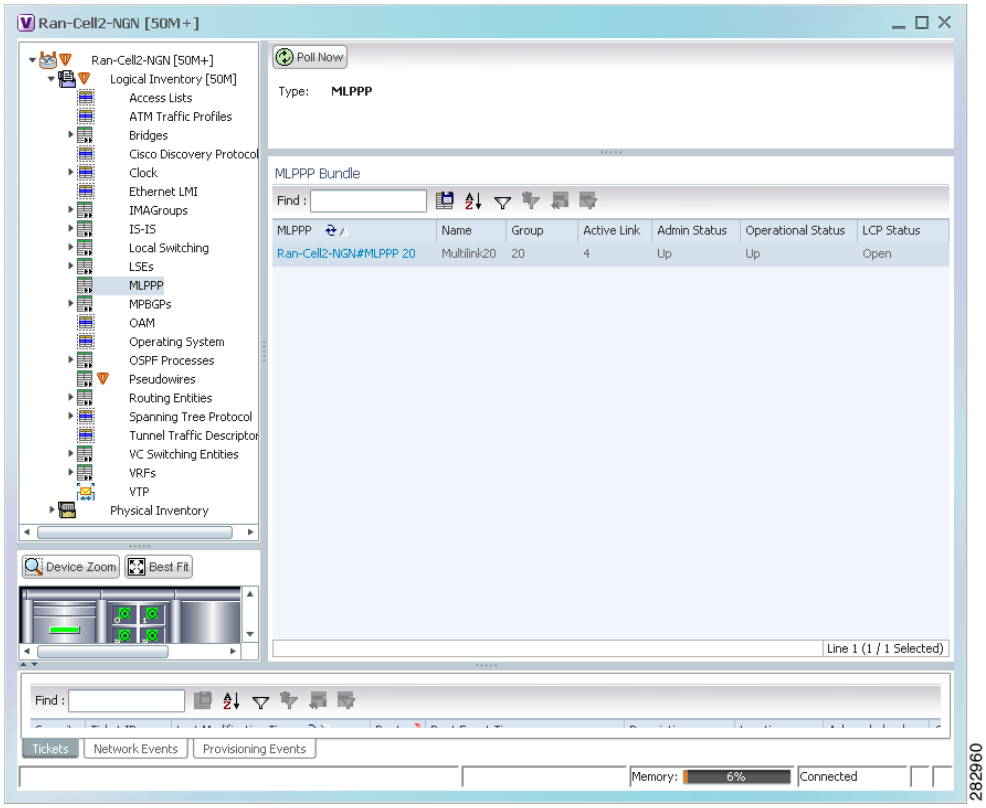


Table 26-13 describes the information that is displayed for MLPPP.

Table 26-13 MLPPP Properties

Field	Description
Type	Type of properties; in this case, MLPPP.
MLPPP Bundle Table	
MLPPP	MLPPP bundle name, hyperlinked to the MLPPP Properties window.
Name	MLPPP interface name.
Group	MLPPP group to which the bundle belongs.
Active Link	Number of active interfaces participating in MLPPP.
Admin Status	Administrative status of the MLPPP bundle: Up or Down.
Operational Status	Administrative status of the MLPPP bundle: Up or Down.
LCP Status	Link Control Protocol (LCP) status of the MLPPP bundle: Closed, Open, Started, or Unknown.

Step 3 To view properties for individual MLPPP bundles, double-click the hyperlinked entry in the MLPPP Bundle table.

Table 26-14 describes the information that is displayed in the MLPPP Properties window.

Table 26-14 MLPPP Bundle and Member Properties

Field	Description
MLPPP	MLPPP bundle name, hyperlinked to MLPPP in logical inventory.
Name	MLPPP interface name.
Group	Group to which the MLPPP bundle belongs.
Active Link	Number of active interfaces participating in MLPPP.
Admin Status	Administrative status of the MLPPP bundle: Up or Down.
Operational Status	Operational status of the MLPPP bundle: Up or Down.
LCP Status	Link Control Protocol (LCP) status of the MLPPP bundle: Closed, Open, Started, or Unknown.
Minimum Configured Link	Minimum number of configured links for an MLPPP bundle.
Maximum Configured Link	Maximum number of configured links for an MLPPP bundle.
Bandwidth	Bandwidth allocated to the MLPPP bundle.
MTU	Size of the Maximum Transmission Unit (MTU), from 1 to 2147483647 bytes.
Keepalive	Status of the keepalive function: Set, Not Set, or Unknown.
Keepalive Time	If keepalive is enabled, the amount of time, in seconds, to wait before sending a keepalive message.
Interleave Enabled	Whether or not interleaving of small fragments is enabled.

Table 26-14 MLPPP Bundle and Member Properties (continued)

Field	Description
Fragment Disable	Whether fragmentation is enabled or disabled: True or False.
Fragment Delay	Maximum size, in units of time, for packet fragments on an MLPPP bundle. Values range from 1 to 999.
Fragment Maximum	Maximum number of MLPPP bundle fragments.
Keepalive Retry	Number of times that the device sends keepalive packets without response before closing the MLPPP bundle protocol. Values range from 2 to 254.
Load Threshold	Minimum load threshold for the MLPPP bundle. If the traffic load falls below the threshold, the link is removed.

Table 26-14 MLPPP Bundle and Member Properties (continued)

Field	Description
MLPPP Members Table	
ID	MLPPP bundle member identifier, hyperlinked to the interface in physical inventory.
Type	No value is displayed in this field.
Binding Information	Binding information to which the interface is associated. The value is null.
Binding Status	No value is displayed in this field.
Discovery Protocols	Discovery protocol used on the interface.

Step 4 To view the interface properties in physical inventory, double-click the required entry in the ID column.

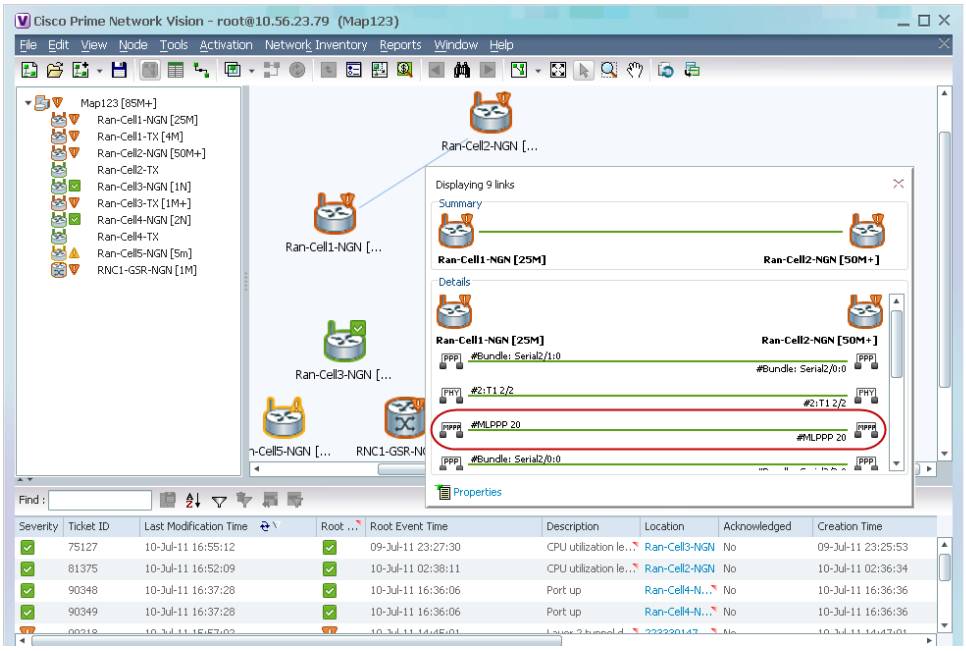
Viewing MLPPP Link Properties

An MLPPP link is a link that connects two MLPPP devices.

To view MLPPP link properties:

Step 1 In the Vision client map view, select a link connected to two MLPPP devices and open the link quick view window as shown in Figure 26-15.

Figure 26-15 MLPPP Link in Link Quick View



Step 2 In the link quick view window, click **Properties**.

Step 3 In the link properties window, select the MLPPP link. The link properties are displayed as shown in Figure 26-16.

Figure 26-16 MLPPP Link Properties

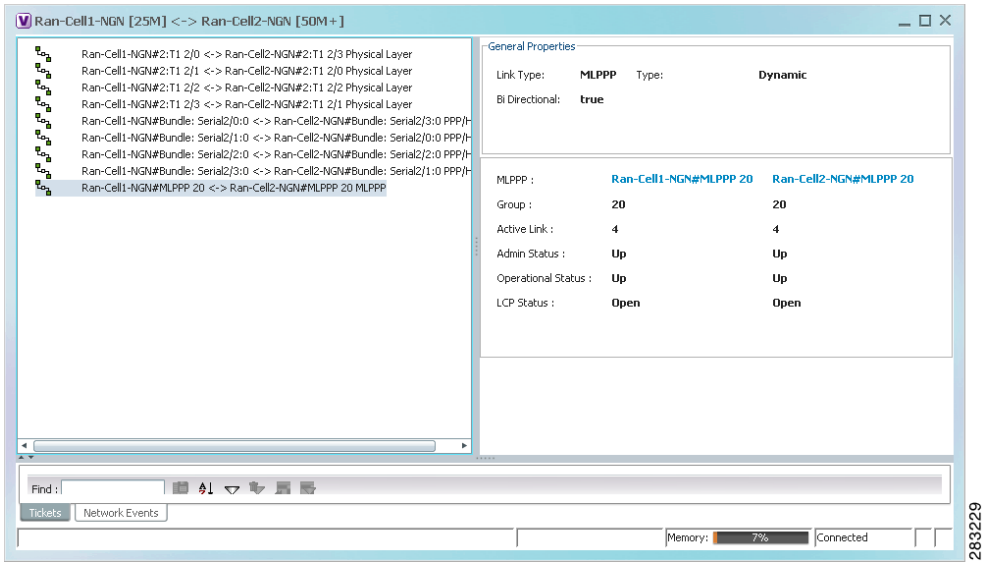


Table 26-15 describes the information that is displayed for the MLPPP link.

Table 26-15 MLPPP Link Properties

Field	Description
General Properties	
Link Type	Link protocol. In this case, MLPPP.
Type	Type of link: Dynamic or Static.
Bi Directional	Whether the link is bidirectional: True or False.
MLPPP Properties	Properties are displayed for both ends of the MLPPP link.
MLPPP	Interface configured for MLPPP, hyperlinked to the entry in physical inventory.
Group	MLPPP group to which the interface belongs.
Active Link	Number of active interfaces participating in the MLPPP link for each device.
Admin Status	Administrative status of the interface: Up or Down.
Operational Status	Operational status of the interface: Up or Down.
LCP Status	LCP status of the MLPPP interface: Closed, Open, Started, or Unknown.

Viewing MPLS Pseudowire Over GRE Properties

Generic routing encapsulation (GRE) is a tunneling protocol, originated by Cisco Systems and standardized in RFC 2784. GRE encapsulates a variety of network layer packets inside IP tunneling packets, creating a virtual point-to-point link to devices at remote points over an IP network. GRE encapsulates the entire original packet with a standard IP header and GRE header before the IPsec process. GRE can carry multicast and broadcast traffic, making it possible to configure a routing protocol for virtual GRE tunnels.

In RAN backhaul networks, GRE is used to transport cell site traffic across IP networks (nonMPLS). In addition, GRE tunnels can be used to transport TDM traffic (TDMoMPLSoGRE) as part of the connectivity in the following sample scenarios:

- Among cell site-facing Cisco 7600 routers and base station controller (BSC) site-facing Cisco 7600 routers.
- Between a Cisco Mobile Wireless Router (MWR) device and a BSC site-facing Cisco 7600 router.

Using GRE tunnels to transport Any Traffic over MPLS (AToM) enables mobile service providers to deploy AToM pseudowires in a network where MPLS availability is discontinuous; for example, in networks where the pseudowire endpoints are located in MPLS edge routers with a plain IP core network, or where two separate MPLS networks are connected by a transit network with plain IP forwarding.

To view the properties for MPLS pseudowire over GRE:

Step 1 In the Vision client, right-click the required device, then choose **Inventory**.

Step 2 In the **Inventory** window, choose **Logical Inventory > Pseudowires**. The Tunnel Edges table is displayed in the content pane as shown in Figure 26-17.

Step 3 Select the required entry and scroll horizontally until you see the required information.

Figure 26-17 MPLS Pseudowire Tunnels over GRE Properties

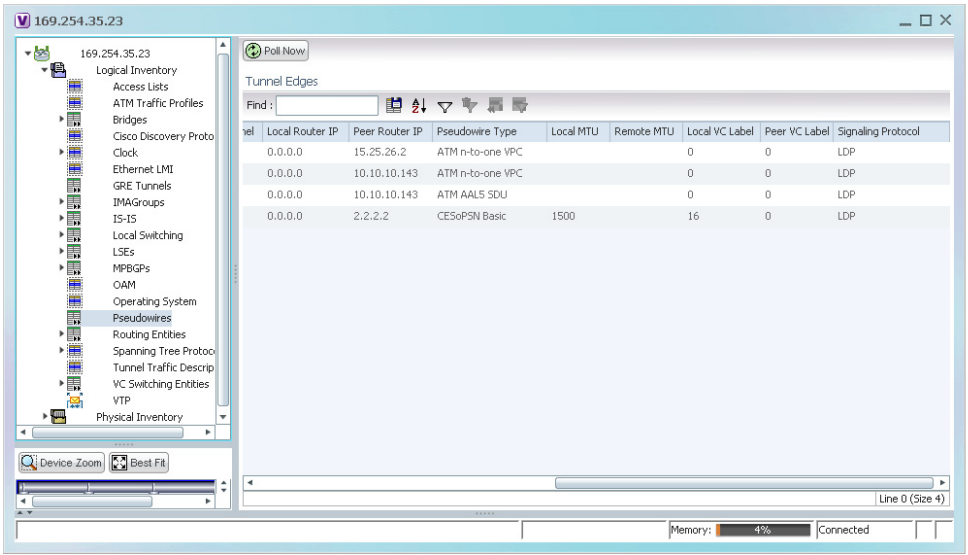


Table 26-16 describes the information included in the Tunnel Edges table specifically for MPLS pseudowire tunnels over GRE.

Table 26-16 MPLS Pseudowire over GRE Properties

Field	Description
Pseudowire Type	Type of pseudowire relevant to MToP: • ATM AAL5 SDU—ATM with ATM Adaptation Layer 5 (AAL5) service data units. • ATM n-to-one VCC—ATM with n-to-one virtual channel connection (VCC). • ATM n-to-one VPC—ATM with n-to-one virtual path connection (VPC). • CESoPSN Basic—CESoPSN basic services with CAS. • SAToP E1—SAToP on an E1 interface.
Local MTU	Size, in bytes, of the MTU on the local interface.
Remote MTU	Size, in bytes, of the MTU on the remote interface.
Preferred Path Tunnel	Path to be used for MPLS pseudowire traffic. Click the hyperlinked entry to view the tunnel details in logical inventory.

Step 4 To view GRE Tunnel properties, choose **Logical Inventory > GRE Tunnels**.

Figure 26-18 shows the Tunnel Edges table that is displayed for GRE tunnels.

Figure 26-18 GRE Tunnel Properties in Logical Inventory

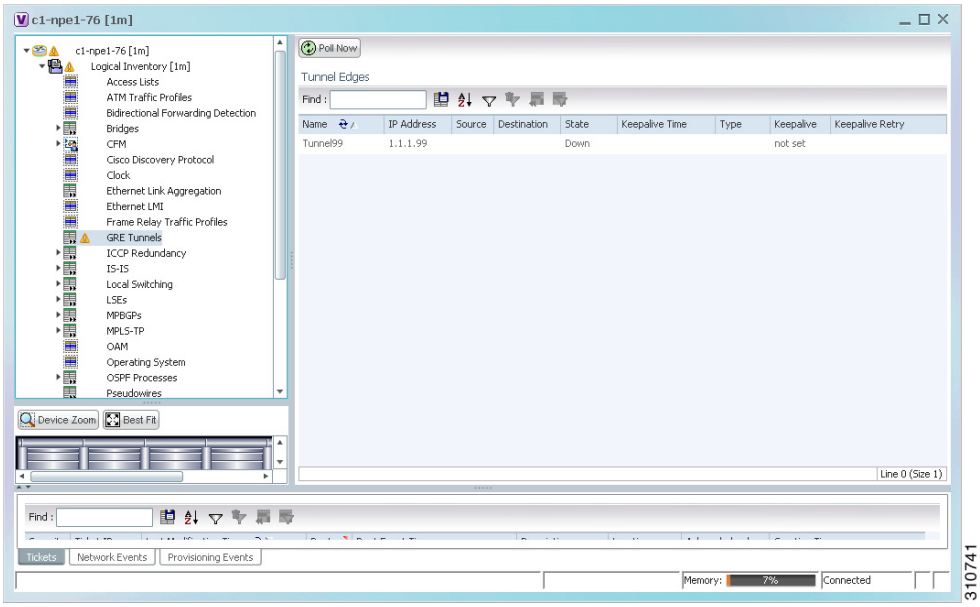


Table 26-17 describes the information that is displayed for GRE tunnels in logical inventory.

Table 26-17 GRE Tunnel Properties in Logical Inventory

Field	Description
Name	Tunnel name.
IP Address	Tunnel IP address.
Source	IP address local to the device.
Destination	IP address of the remote router.
State	State of the tunnel: Up or Down.
Keepalive Time	If keepalive is enabled, the amount of time, in seconds, to wait before sending a keepalive message.
Type	Tunnel type.
Keepalive	Status of the keepalive function: Set, Not Set, or Unknown.
Keepalive Retry	Number times that the device continues to send keepalive packets without response before bringing the tunnel interface protocol down. Values range from 2 to 254, with a default of 3.

Network Clock Service Overview

Network clock service refers to the means by which a clock signal is generated or derived and distributed through a network and its individual nodes for the purpose of ensuring synchronized network operation. Network clocking is particularly important for mobile service providers to ensure proper transport of cellular traffic from cell sites to Base Station Control (BSC) sites.

Note In Prime Network, *clock service* refers to *network clock service*.

The following topics describe how to use the Vision client to monitor clock service:

- Monitoring Clock Service, page 26-34
- Monitoring PTP Service, page 26-35
- Viewing Pseudowire Clock Recovery Properties, page 26-41
- Viewing SyncE Properties, page 26-45
- Applying a Network Clock Service Overlay, page 26-48
- Viewing CEM and Virtual CEM Properties, page 26-49

Monitoring Clock Service

To monitor clock service:

Step 1 In the Vision client, right-click the required device, then choose **Inventory**.

Step 2 In the **Inventory** window, choose **Logical Inventory > Clock**. Clock service information is displayed in the content pane as shown in Figure 26-19.

Figure 26-19 Clock Service Properties

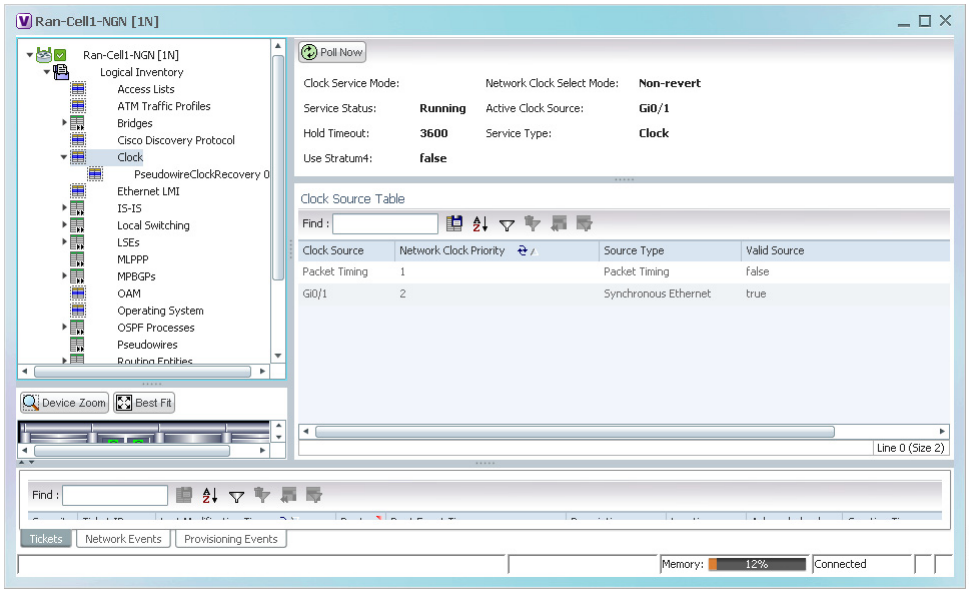


Table 26-18 describes the information displayed for clocking service.

Table 26-18 Clock Service Properties

Field	Description
Clock Service Mode	This field is not populated.
Network Clock Select Mode	Action to take if the master device fails: • Non-revert—Do not use the master device again after it recovers from the failure. • Revert—Use the master device again after it recovers and functions correctly for a specified amount of time. • Unknown—The network clock selection mode is unknown.
Service Status	Status of the system service: • Initializing—The service is starting up. • Down—The service is down. • Reset—The service has been reset. • Running—The service is running. • Other—A status other than those listed.

Table 26-18 Clock Service Properties (continued)

Field	Description
Active Clock Source	Current active clock source used by the device.
Hold Timeout	How long the device waits before reevaluating the network clock entry. Values can be from 0-86400 seconds, Not Set, or infinite.
Service Type	Type of system service, such as Clock or Cisco Discovery Protocol.
Use Stratum4	Quality of the clock source: • True—Use Stratum 4, the lowest level of clocking quality. • False—(Default) Use Stratum 3, a higher level of clocking quality than Stratum 4.
Clock Source Table	This table is displayed only if there are active clock sources.
Clock Source	Current active clock source used by the device.
Network Clock Priority	Priority of the clock source with 1 being the highest priority.
Source Type	Method by which clocking information is provided: • BITS—Timing is supplied by a Building Integrated Timing Supply (BITS) port clock. • E1/T1—Clocking is provided via an E1 or T1 interface. • Packet-Timing—Clocking is provided over a packet-based network. • Synchronous Ethernet—Clocking is provided by Synchronous Ethernet. • Others—Clocking is provided by a source other than the above.
Valid Source	Validity of the clock source: • True—The clock source is valid and operational. • False—The clock source is not valid or is not operational.

Monitoring PTP Service

In networks that employ TDM, periodic synchronization of device clocks is required to ensure that the receiving device knows which channel is which for accurate reassembly of the data stream. The Precision Time Protocol (PTP) standard:

- Specifies a clock synchronization protocol that enables this synchronization.
- Applies to distributed systems that consist of one or more nodes communicating over a network.

Defined by IEEE 1588-2008, PTP Version 2 (PTPv2) allows device synchronization at the nanosecond level.

PTP uses the concept of master and slave devices to achieve precise clock synchronization. Using PTP, the master device periodically starts a message exchange with the slave devices. After noting the times at which the messages are sent and received, each slave device calculates the difference between its system time and the system time of the master device. The slave device then adjusts its clock so that it is synchronized with the master device. When the master device initiates the next message exchange, the

slave device again calculates the difference and adjusts its clock. This repetitive synchronization ensures that device clocks are coordinated and that data stream reassembly is accurate. For configuring PTP, see Configuring SONET, page 26-53.

To monitor PTP service:

Step 1 In the Vision client, right-click the required device, then choose **Inventory**.

Step 2 In the **Inventory** window, choose **Logical Inventory > Clock > PTP Service**. The PTP service properties are displayed in the content pane as shown in Figure 26-20.

Figure 26-20 PTP Service Properties

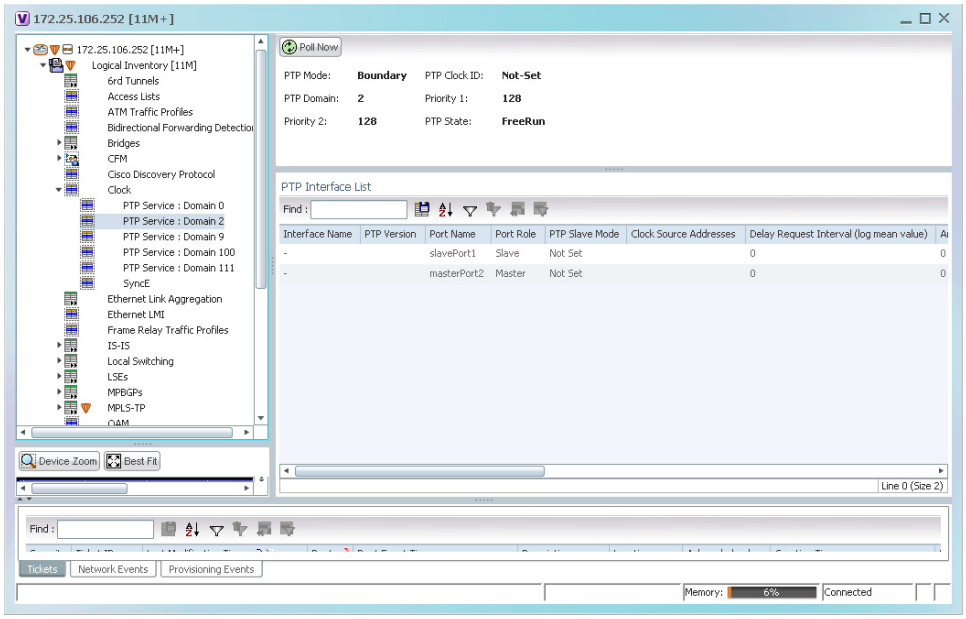


Table 26-19 describes the properties that are displayed for PTP service.

Table 26-19 PTP Service Properties

Field	Description
PTP Mode	Mode of PTP operation: • Boundary—Boundary clock mode. • E2E Transparent—End-to-end transparent clock mode. • Ordinary—Ordinary clock mode. • P2P Transparent—Peer-to-peer transparent clock mode. • Unknown—The clock mode is unknown. **Note** Cisco MWR-2941 routers support Ordinary mode only.
PTP Clock ID	Clock identifier derived from the device interface.
PTP Domain	Number of the domain used for PTP traffic. A single network can contain multiple separate domains.
Priority 1	First value checked for clock selection. The clock with the lowest priority takes precedence.
Priority 2	If two or more clocks have the same value in the Priority 1 field, the value in this field is used for clock selection.
Port State	Clock state according to the PTP engine: • Freerun—The slave clock is not locked to a master clock. • Holdover—The slave device is locked to a master device, but communication with the master is lost or the timestamps in the PTP packet are incorrect. • Acquiring—The slave device is receiving packets from a master and is trying to acquire a clock. • Freq locked—The slave device is locked to the master device with respect to frequency, but is not aligned with respect to phase. • Phase aligned—The slave device is locked to the master device with respect to both frequency and phase. PTP clock status syslog support—As part of the syslog support, Prime Network started supporting PTP clock status syslog besides the PTP inventory information. While receiving the syslog, Prime Network queries the device, and receives the PTP state information and updates in the respective PTP service. The service alarm supported for the PTP status information is PTP port clock state change alarm. Theses service alarms and the syslogs are correlated under the PTP service as clock service. For more information on PTP clock status update service alarm, refer Cisco Prime Network Supported Service Alarms.
PTP Interface List Table	
Interface Name	Interface identifier.
PTP Version	Version of PTP used. The default value is 2, indicating PTPv2.
Port Name	Name of the PTP port clock.
Port Role	PTP role of the clock: Master or Slave.

Table 26-19 PTP Service Properties (continued)

Field	Description
PTP Slave Mode	For an interface defined as a slave device, the mode used for PTP clocking: • Not Set—The slave mode is not used. • Multicast—The interface uses multicast mode for PTP clocking. • Unicast—The interface uses unicast mode for PTP clocking. • Unicast with Negotiation—The interface uses unicast mode with negotiation for PTP clocking.
Clock Source Addresses	IP addresses of the clock source.
Delay Request Interval (log mean value)	When the interface is in PTP master mode, the interval specified to member devices for delay request messages. The intervals use base 2 values, as follows: • 4—1 packet every 16 seconds. • 3—1 packet every 8 seconds. • 2—1 packet every 4 seconds. • 1—1 packet every 2 seconds. • 0—1 packet every second. • -1—1 packet every 1/2 second, or 2 packets per second. • -2—1 packet every 1/4 second, or 4 packets per second. • -3—1 packet every 1/8 second, or 8 packets per second. • -4—1 packet every 1/16 seconds, or 16 packets per second. • -5—1 packet every 1/32 seconds, or 32 packets per second. • -6—1 packet every 1/64 seconds, or 64 packets per second.
Announce Interval (log mean value)	Interval value for PTP announcement packets: • 4—1 packet every 16 seconds. • 3—1 packet every 8 seconds. • 2—1 packet every 4 seconds. • 1—1 packet every 2 seconds. • 0—1 packet every second. • -1—1 packet every 1/2 second, or 2 packets per second. • -2—1 packet every 1/4 second, or 4 packets per second. • -3—1 packet every 1/8 second, or 8 packets per second. • -4—1 packet every 1/16 seconds, or 16 packets per second. • -5—1 packet every 1/32 seconds, or 32 packets per second. • -6—1 packet every 1/64 seconds, or 64 packets per second.
Announce Timeout	Number of PTP announcement intervals before the session times out. Values are 2-10.

Table 26-19 PTP Service Properties (continued)

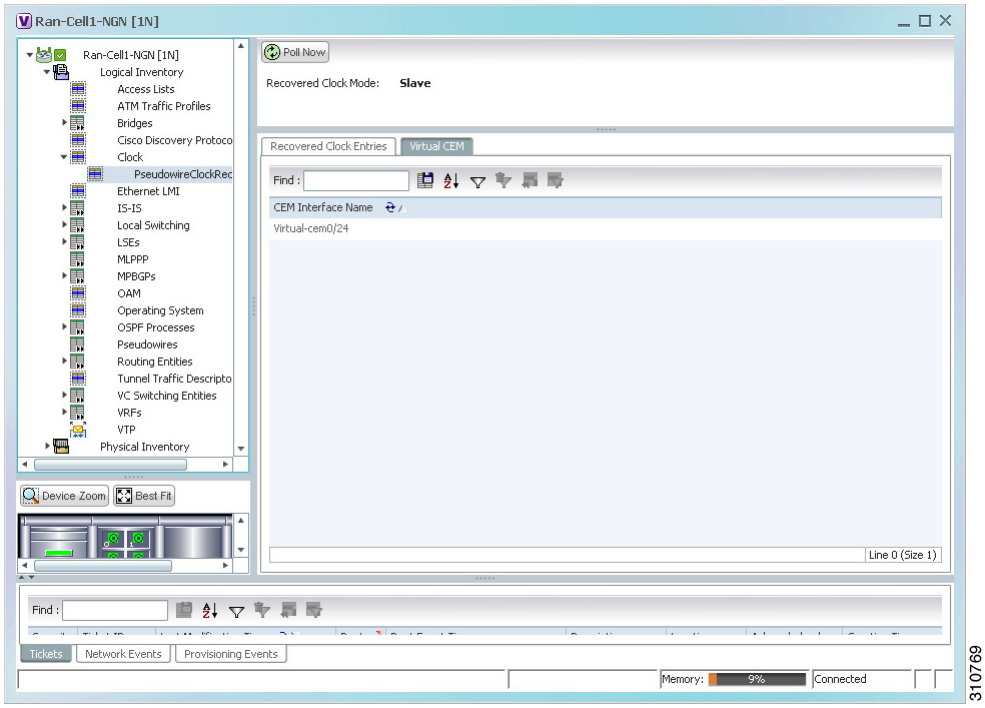
Field	Description
Sync Interval (log mean value)	Interval for sending PTP synchronization messages: • 4—1 packet every 16 seconds. • 3—1 packet every 8 seconds. • 2—1 packet every 4 seconds. • 1—1 packet every 2 seconds. • 0—1 packet every second. • -1—1 packet every 1/2 second, or 2 packets per second. • -2—1 packet every 1/4 second, or 4 packets per second. • -3—1 packet every 1/8 second, or 8 packets per second. • -4—1 packet every 1/16 seconds, or 16 packets per second. • -5—1 packet every 1/32 seconds, or 32 packets per second. • -6—1 packet every 1/64 seconds, or 64 packets per second.
Sync Limit (nanoseconds)	Maximum clock offset value, in nanoseconds, before PTP attempts to resynchronize.
Interface	Physical interface identifier, hyperlinked to the routing information for the interface.
PTP Master Mode	For an interface defined as a master device, the mode used for PTP clocking: • Not Set—The master mode is not used. • Multicast—The interface uses multicast mode for PTP clocking. • Unicast—The interface uses unicast mode for PTP clocking. This mode allows a single destination. • Unicast with Negotiation—The interface uses unicast mode with negotiation for PTP clocking. This mode allows up to 128 destinations.
Clock Destination Addresses	IP addresses of the clock destinations. This field contains IP addresses only when Master mode is enabled.
Domain	Clocking domain.

Viewing Pseudowire Clock Recovery Properties

To view pseudowire clock recovery properties:

Step 1 Choose **Logical Inventory > Clock > Pseudowire Clock Recovery**. The Vision client displays the Virtual CEM information by default. See Figure 26-21.

Figure 26-21 Pseudowire Clock Recovery - Virtual CEM Tab



Step 2 To view more information about a virtual CEM, right-click the virtual CEM, then choose **Properties**. The Virtual CEM Properties window is displayed.

The information that is displayed in the Virtual CEM Properties window depends on whether or not the virtual CEM belongs to a group:

- If a CEM group is not configured on the virtual CEM, the Virtual CEM Properties window contains only the CEM interface name.
- If a CEM group is configured on the virtual CEM, the Virtual CEM Properties window contains the information described in Table 26-20.

Table 26-20 Virtual CEM Group Properties

Field	Description
CEM Interface Name	CEM interface name.
CEM Group Table	
CEM Group	Name of the virtual CEM group.
Framing	Framing mode used for the CEM channel: • Framed—Specifies the channels used for the controller, such as Channels: (1-8), (10-14). The channels that are available depend on the type of controller: T1, E1, T3, or E3. • Unframed—Indicates that a single CEM channel is used for all T1/E1 timeslots. SAToP uses the unframed mode.
Pseudowire	Name of the pseudowire configured on the CEM interface, hyperlinked to the pseudowire properties in logical inventory.
Oper Status	Operational status of the CEM interface: • Dormant—The interface is dormant. • Down—The interface is down. • Not Present—An interface component is missing. • Testing—The interface is in test mode. • Unknown—The interface has an unknown operational status. • Up—The interface is up.
Admin Status	Administrative status of the CEM interface: • Down—The CEM interface is administratively down. • Testing—The administrator is testing the CEM interface. • Unknown—The administrative status is unknown. • Up—The CEM interface is administratively up.

Step 3 To view additional CEM group properties, double-click the required CEM group.

Table 26-21 describes the information displayed in the CEM Group Properties window.

Table 26-21 CEM Group Properties

Field	Description
Oper Status	Operational status of the CEM interface: • Dormant—The interface is dormant. • Down—The interface is down. • Not Present—An interface component is missing. • Testing—The interface is in test mode. • Unknown—The interface has an unknown operational status. • Up—The interface is up.
Idle Pattern	Eight-bit hexadecimal number that is transmitted on a T1 or E1 line when missing packets are detected on the pseudowire (PW) circuit.
Type	Type of CEM group. This is always DS0 Bundle.
Idle CAS Pattern	When CAS is used, the 8-bit hexadecimal signal that is sent when the CEM interface is identified as idle.
Bundle Location	Associated card and slot for the virtual CEM, using the virtual CEM port 24; for example virtual-cem/8/3/24:0.
Dejitter	Size of the dejitter buffer in milliseconds (ms). The range is 4 to 500 ms with a default of 4 ms.
RTP Hdr Compression	Whether RTP header compression is enabled or disabled.
RTP Enabled	Whether RTP compression is enabled or disabled.
Admin Status	Administrative status of the CEM interface: • Down—The CEM interface is administratively down. • Testing—The administrator is testing the CEM interface. • Unknown—The administrative status is unknown. • Up—The CEM interface is administratively up.
ID	DS0 bundle CEM group identifier.
Payload Size	Size of the payload for packets on the CEM interface. The range is 32 to 1312 bytes.

Step 4 To view recovered clock entries, click the Recovered Clock Entries tab. See Figure 26-22.

If no recovered clock entries exist, this tab is not displayed.

Figure 26-22 Pseudowire Clock Recovery - Recovered Clock Entries Tab

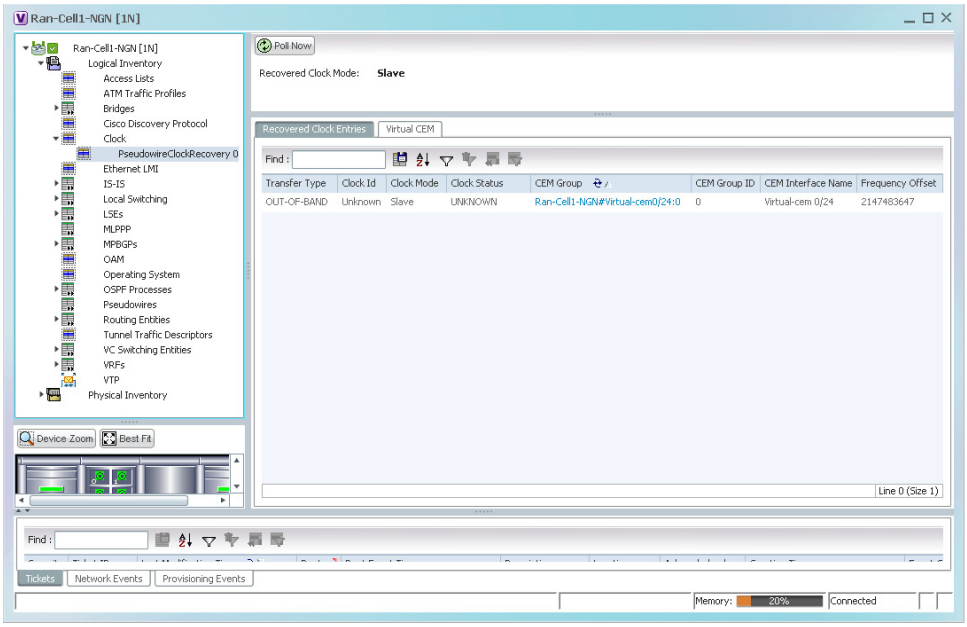


Table 26-22 describes the information displayed for pseudowire clock recovery.

Table 26-22 Pseudowire Clock Recovery Properties

Field	Description
Recovered Clock Source	Interface (slot/subslot) in which clock recovery occurred. Click the hyperlinked entry to view its properties in physical inventory.
Recovered Clock Mode	Recovered clock mode: • Adaptive—The devices do not have a common clock source. The recovered clock is derived from packet arrival. • Differential—The edge devices have a common clock source, and the recovered clock is derived from timing information in packets and the related difference from the common clock. • Synchronous—A GPS or BITS clock source externally synchronizes both end devices. This method is extremely accurate, but is rarely available for all network devices.
Virtual CEM Tab	
CEM Interface Name	Virtual CEM interface associated with the clock.
Recovered Clock Entries Tab	This tab appears if recovered entries exist.
Transfer Type	• In-band—The clocking information is sent over the same pseudowire as the bearer traffic. • Out-of-band—The clocking information is sent over a dedicated pseudowire between the sending and receiving SPAs.

Table 26-22 Pseudowire Clock Recovery Properties (continued)

Field	Description
Clock ID	Clock identifier, if known.
Clock Mode	Clock mode of the recovered clock: • Adaptive—The recovered clock was obtained using ACR. • Primary—The recovered clock was obtained from a clock with the highest priority. • Secondary—The recovered clock was obtained from a clock with a lower priority than the primary clock.
Clock Status	Status of the clock: • Acquiring—The clock is obtaining clocking information. • Acquired—The clock has obtained the required clocking information. • Holdover—The current primary clock is invalid and a holdover timer has started to check whether or not the clock becomes valid within the specified holdover time.
CEM Group	CEM group associated with the clock.
CEM Group ID	Identifier of the CEM group associated with the clock.
CEM Interface Name	Virtual CEM interface associated with the clock.
Frequency Offset	Offset to the clock frequency, in Hz.

Viewing SyncE Properties

With Ethernet equipment gradually replacing SONET and SDH equipment in service-provider networks, frequency synchronization is required to provide high-quality clock synchronization over Ethernet ports. Synchronous Ethernet (SyncE), a recently adopted standard, provides the required synchronization at the physical level.

In SyncE, Ethernet links are synchronized by timing their bit clocks from high-quality, stratum-1-traceable clock signals in the same manner as SONET/SDH. Operations messages maintain SyncE links, and ensure a node always derives timing from the most reliable source.

For configuring SyncE, see Configuring Clock, page 26-55. To view SyncE properties, choose **Logical Inventory > Clock > SyncE**. (See Figure 26-23.)

Figure 26-23 SyncE Properties in Logical Inventory

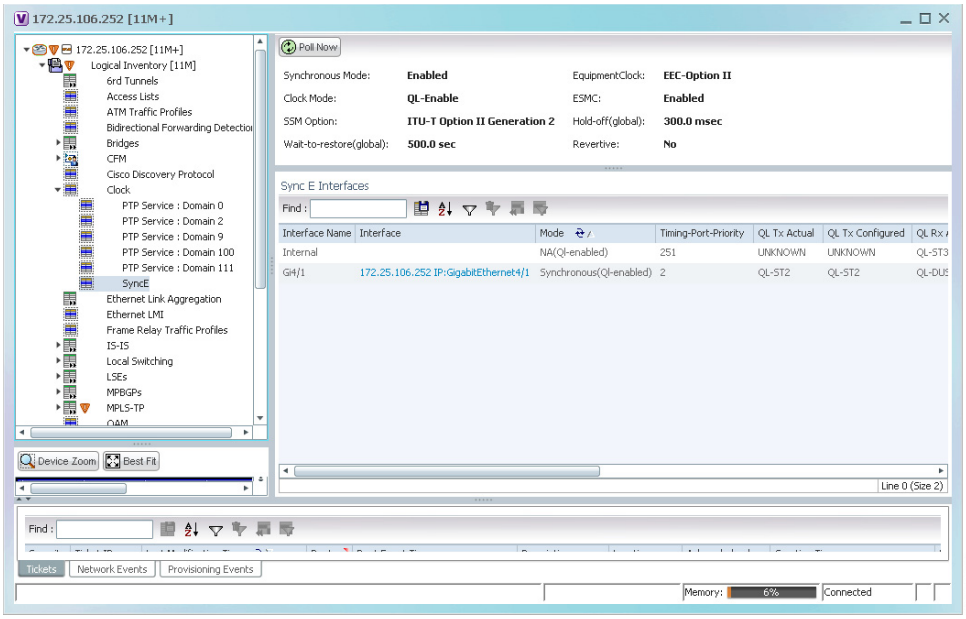


Table 26-23 describes the information that is displayed for SyncE.

Table 26-23 SyncE Properties

Field	Description
Synchronous Mode	Status of the automatic synchronization selection process: Enabled or Disable.
Equipment Clock	Ethernet Equipment Clock (EEC) options: EEC-Option I or EEC-Option II.
Clock Mode	Whether the clock is enabled or disabled for the Quality Level (QL) function: QL-Enabled or QL-Disabled.
ESMC	Ethernet Synchronization Message Channel (ESMC) status: Enabled or Disabled.
SSM Option	Synchronization Status Message (SSM) option being used: • ITU-T Option I • ITU-T Option II Generation 1 • ITU-T Option II Generation 2
Hold-off (global)	Length of time (in milliseconds) to wait before issuing a protection response to a failure event.
Wait-to-restore (global)	Length of time (in seconds) to wait after a failure is fixed before the span returns to its original state.
Revertive	Whether the network clock is to use revertive mode: Yes or No.

Table 26-23 SyncE Properties (continued)

Field	Description
SyncE Interfaces Table	
Interface Name	Name of the Gigabit or 10 Gigabit interface associated with SyncE. If SyncE is not associated with a Gigabit or 10 Gigabit interface, this field contains *Internal*.
Interface	Hyperlinked entry to the interface routing information in the Routing Entity Controller window. For more information, see Viewing Routing Entities, page 17-32. This field does not apply for Internal interfaces.
Mode	Whether the interface is enabled or disabled for the QL function: QL-Enabled or QL-Disabled.
Timing Port Priority	Value used for selecting a SyncE interface for clocking if more than one interface is configured. Values are from 1 to 250, with 1 being the highest priority.
QL Tx Actual	Actual type of outgoing quality level information, depending on the globally configured SSM option: • ITU-T Option I—Available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and QL-DNU. • ITU-T Option II Generation 1—Available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4, and QL-DUS. • ITU-T Option II Generation 2—Available values are QL-PRS, QL-STU, QL-ST2, QL-TNC, QL-ST3, QL-SMC, QL-ST4, and QL-DUS.
QL Tx Configured	Configured type of outgoing quality level information, depending on the globally configured SSM option. See QL Tx Actual for the available values.
QL Rx Actual	Actual type of incoming quality level information, depending on the globally configured SSM option. See QL Tx Actual for the available values.
QL Rx Configured	Configured type of incoming quality level information, depending on the globally configured SSM option. See QL Tx Actual for the available values.
Hold-Off Timer (msecs)	Length of time (in milliseconds) to wait after a clock source goes down before removing the source.
Wait-to-Restore (secs)	Length of time (in seconds) to wait after a failure is fixed before the interface returns to its original state.

Table 26-23 SyncE Properties (continued)

Field	Description
ESMC Tx	Whether ESMC is enabled for outgoing QL information on the interface: Enabled, Disabled, or NA (Not Available).
ESMC Rx	Whether ESMC is enabled for incoming QL information on the interface: Enabled, Disabled, or NA (Not Available).
SSM Tx	Whether SSM is enabled for outgoing QL information on the interface: Enabled, Disabled, or NA (Not Available).
SSM Rx	Whether SSM is enabled for incoming QL information on the interface: Enabled, Disabled, or NA (Not Available).

Applying a Network Clock Service Overlay

A service overlay allows you to isolate the parts of a network that are being used by a particular service. This information can then be used for troubleshooting. For example, the overlay can highlight configuration or design problems when bottlenecks occur and all the site interlinks use the same link.

To apply a network clock overlay:

Step 1 In the Vision client, display the network map on which you want to apply an overlay.

Step 2 From the main toolbar, click **Choose Overlay Type** and choose **Network Clock**.

The Select Network Clock Service Overlay dialog box is displayed.

Step 3 Do one of the following:

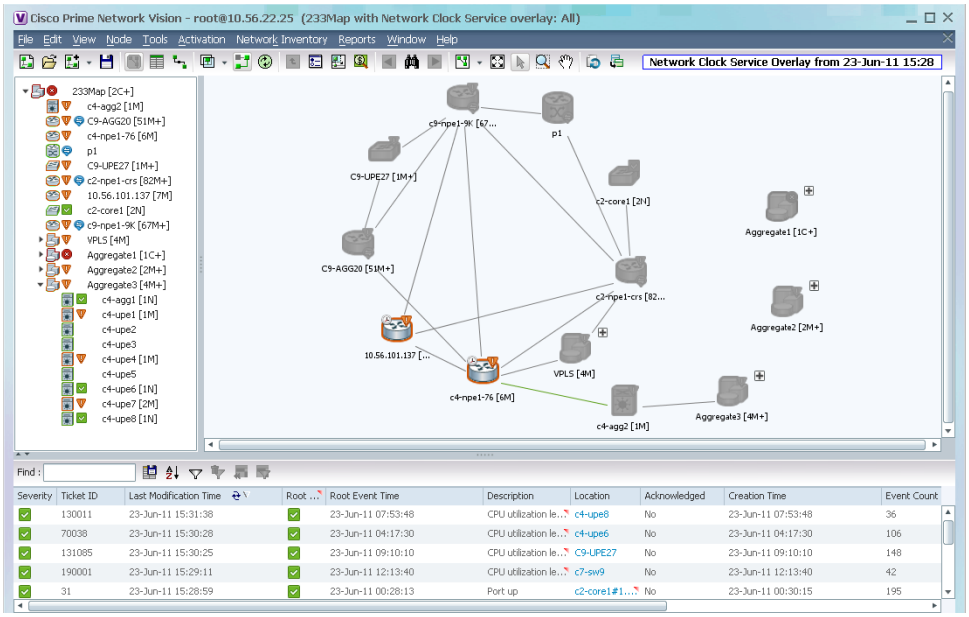
- Choose a search category, enter a search string, then click **Go** to narrow the search results to a range of network clock services or a specific network clock service. Search categories include:
  - Description
  - Name

  The search condition is “contains.” Search strings are case-insensitive. For example, if you choose the Name category and enter “net,” the Vision client displays VPNs “net” and “NET” in the names whether net appears at the beginning, middle, or at the end of the name: for example, Ethernet.
- Choose **Show All** to display all network clock services.

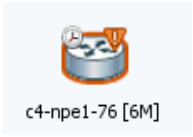
Step 4 Select the network clock service overlay that you want to apply to the map.

The elements and links used by the selected network clock are highlighted in the map, and the overlay name is displayed in the title of the window. (See Figure 26-24.)

Figure 26-24 Network Clock Service Overlay Example



In addition, the elements configured for clocking service display a clock service icon as in the following example:



Note An overlay is a snapshot taken at a specific point in time and does not reflect changes that occur in the service. As a result, the information in an overlay can become stale. To update the overlay, click **Refresh Overlay** in the main toolbar.

Viewing CEM and Virtual CEM Properties

The following topics describe how to view CEM and virtual CEM properties and interfaces:

- Viewing CEM Interfaces, page 26-50
- Viewing Virtual CEMs, page 26-50
- Viewing CEM Groups, page 26-50

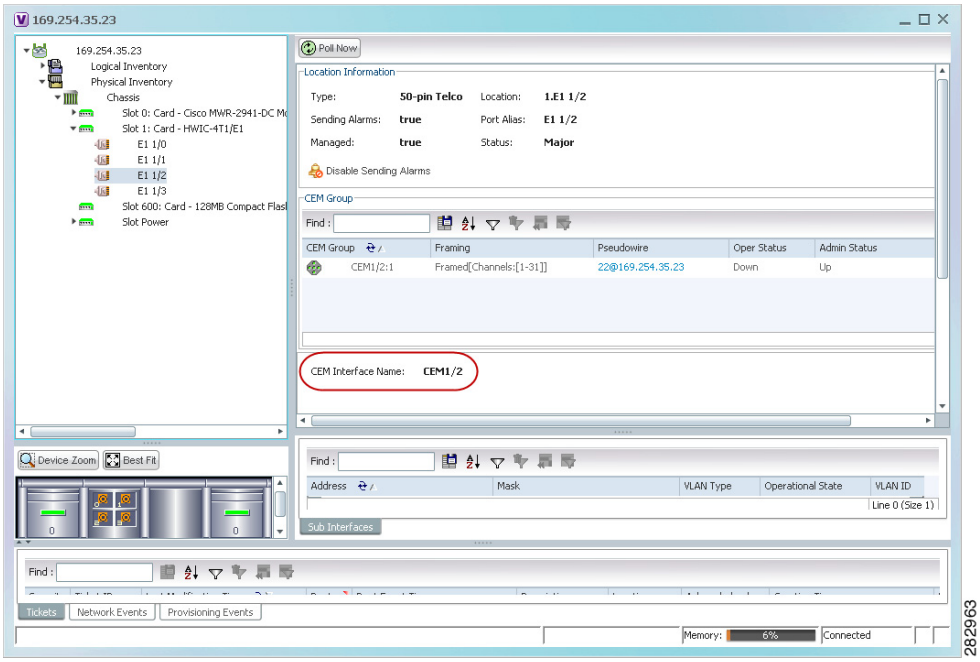
Viewing CEM Interfaces

To view CEM interfaces:

Step 1 In the Vision client, double-click the required device.

Step 2 In the **Inventory** window, choose **Physical Inventory > Chassis >** *slot* **>** *subslot* **>** *interface*. The CEM interface name is displayed in the content pane as shown in Figure 26-25.

Figure 26-25 CEM Interface



Viewing Virtual CEMs

To view virtual CEMs, choose **Logical Inventory > Clock > Pseudowire Clock Recovery**.

The virtual CEM interfaces are listed in the Virtual CEM tab.

Viewing CEM Groups

CEM groups can be configured on physical or virtual CEM interfaces. The underlying interface determines where you view CEM group properties in the Vision client:

- Viewing CEM Groups on Physical Interfaces, page 26-51
- Viewing CEM Groups on Virtual CEM Interfaces, page 26-52

Viewing CEM Groups on Physical Interfaces

When you configure a CEM group on a physical interface, the CEM group properties are displayed in physical inventory for that interface.

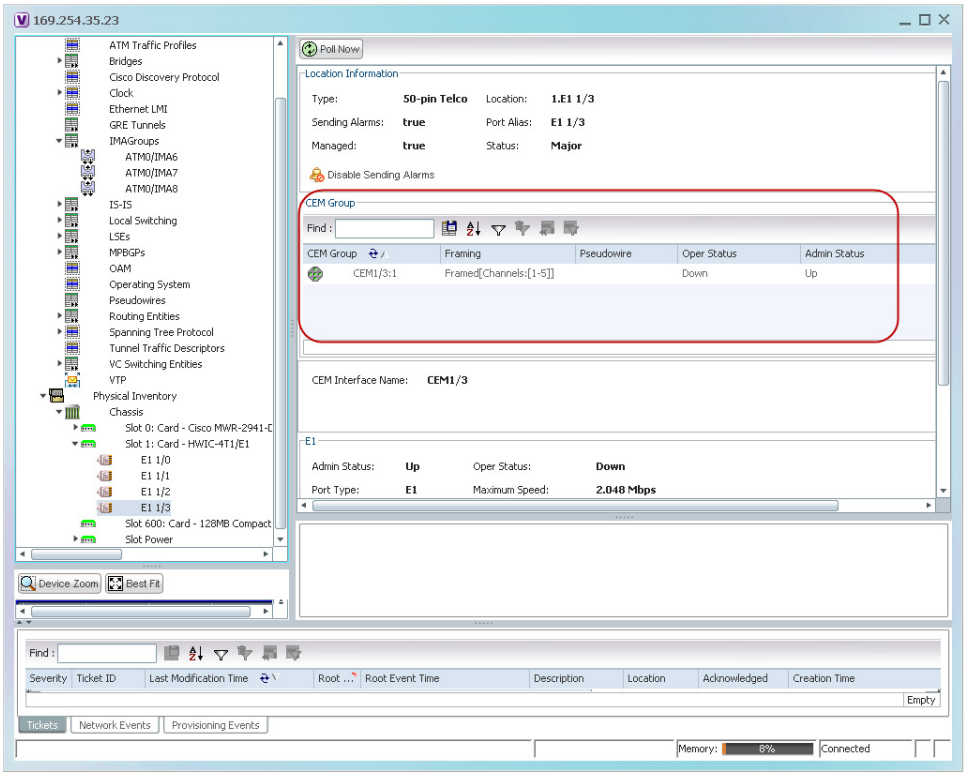
To view CEM groups configured on physical interfaces:

Step 1 In the Vision client, double-click the required device.

Step 2 In the **Inventory** window, choose **Physical Inventory > Chassis >** *slot* **>** *subslot* **>** *interface*.

The CEM group information is displayed in the content pane with other interface properties (Figure 26-26).

Figure 26-26 CEM Group Information

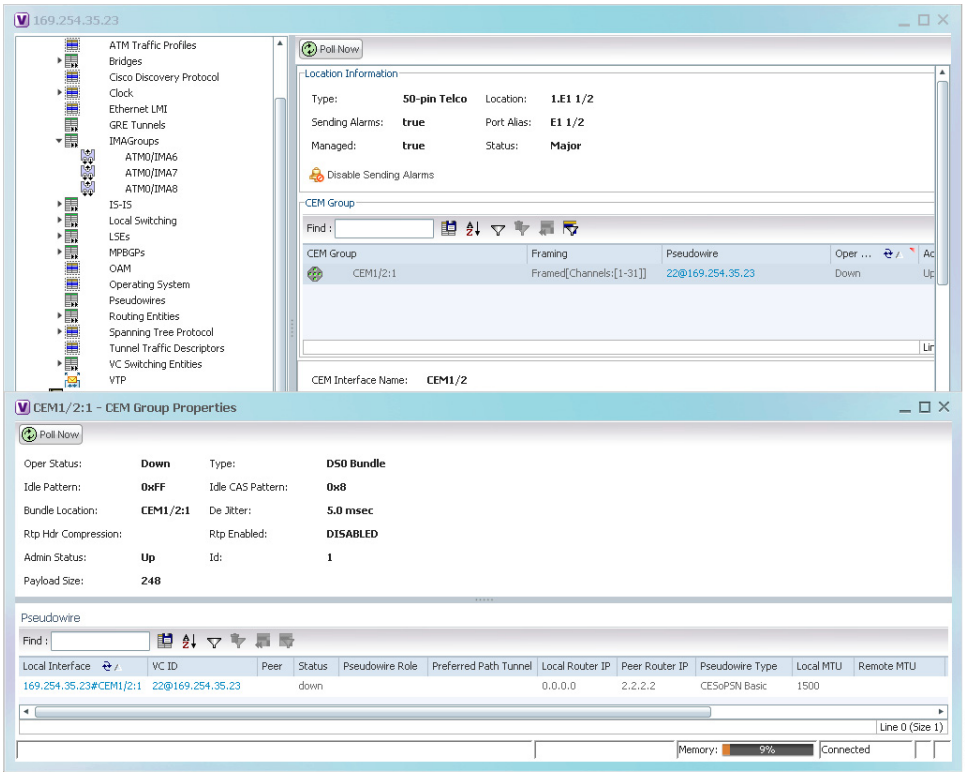


See Table 26-20 for a description of the properties displayed for CEM groups in the content pane.

Step 3 To view additional information, double-click the required group.

The CEM Group Properties window is displayed as shown in Figure 26-27.

Figure 26-27 CEM Group Properties Window



See Table 17-29 on page 17-60for the properties displayed in the Pseudowire table in the CEM Group Properties window.

Viewing CEM Groups on Virtual CEM Interfaces

When you configure a CEM group on a virtual CEM, the CEM group information is displayed below the virtual CEM in logical inventory.

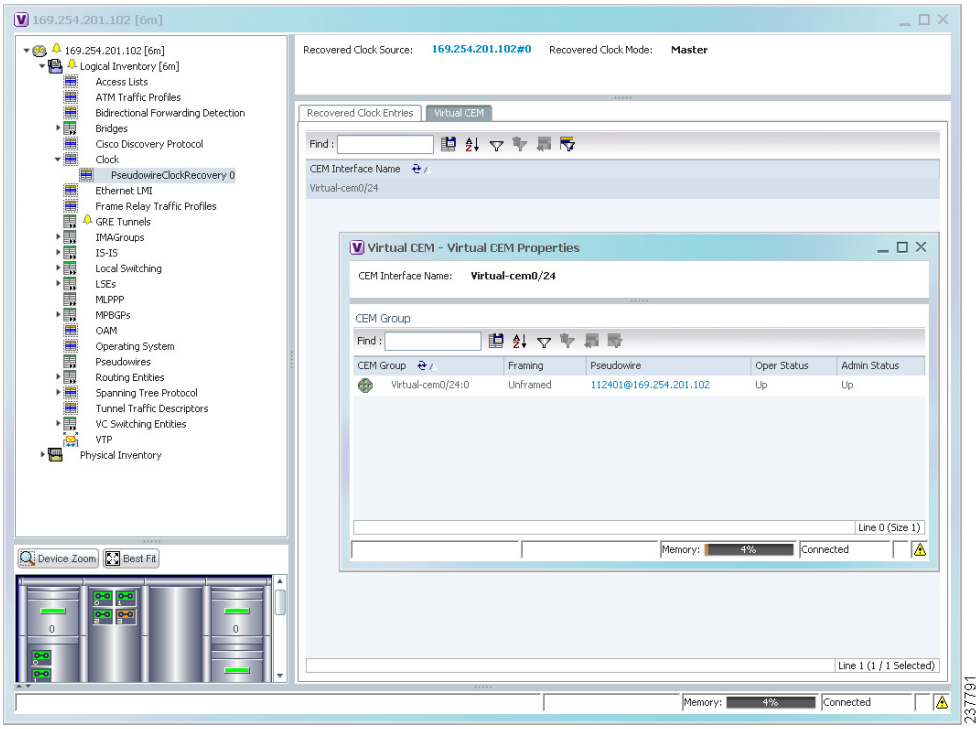
To view CEM groups on virtual CEM interfaces:

Step 1 In the Vision client, right-click the required device, then choose **Inventory**.

Step 2 In the **Inventory** window, choose **Logical Inventory > Clock > Pseudowire Clock Recovery**.

Step 3 In the Virtual CEM tab, right-click the CEM interface name and choose **Properties**. The CEM group properties are displayed in a separate window (Figure 26-28). If a pseudowire is configured on the CEM group for out-of-band clocking, the pseudowire VCID is also shown.

Figure 26-28 CEM Group Properties



Step 4 To view additional CEM group properties, double-click the required CEM group.

Table 26-21 describes the information displayed in the CEM Group Properties window.

Configuring SONET

The table below lists the SONET commands can be launched from the inventory by right-clicking a SONET port and selecting **Commands > SONET**. Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Navigation	Description
BER Threshold	*Right-click on SONET port and select* **Commands > SONET > Show**	Performed from command launch point
Controller Data		
TCA Threshold		
SDH Counters	**Clear > SONET**	N/A; performed from command launch point

Command	Navigation	Description
BER Threshold	*Right-click on SONET port and select* **Commands > SONET > Configure**	BER threshold: • sf-ber—Sets the signal failure BER threshold. Value in the range from 3 to 9. The default value is 6 • sd-ber—Sets the signal degrade BER threshold. Value in the range from 3 through 9. The default value is 3 Bit error rate: 3-9, or default. The default for sf-ber is 3, and the default for sd-ber is 9.
Line Counters	*Right-click on SONET port and select* **Commands > SONET > Show > PM**	Line type: farendline, farendline-history, line, or line-history History interval: 1-96; to view all, enter 0
Medium Counters		N/A; performed from command launch point Path type: farendpath, farendpath-history, path, path-history
Path Counters		Channelized path index: 1-48 (for a particular channel) or 0 (for all channels) History interval: 1-96; to view all, enter 0
Section Counters	*Right-click on SONET port and select* **Commands > SONET > Show > PM**	Section type: section or section-history History interval: 1-96; to view all, enter 0
Trace Details		Card location (for example, 0/5/CPU0) **Note** The device must be managed by Prime Network with device admin privileges.

Command	Navigation	Description
Clock Source	*Right-click on SONET port and select* **Commands > SONET > Configure**	Clock source of sent signal on SONET ports: • internal—Controller will clock its sent data using internal clock. • line—Controller will clock its sent data using the clock recovered from the line's receive data stream. • default—Cancels any clock source setting.
TCA Threshold		TCA threshold: • b1-tca—Threshold for B1 BER TCA, between 3-9 (default is 6). • b2-tca—Threshold for B2 BER TCA, between 3-9 (default is 6). Bit error rate: Value from 3-9 (10 to the negative x), or default.

Configuring Clock

With Ethernet equipment gradually replacing SONET and SDH equipment in service-provider networks, frequency synchronization is required to provide high-quality clock synchronization over Ethernet ports. SyncE and PTP are two widely used clock synchronization protocol used in ethernet based networks.

Clocking configuration commands allows you to configure SyncE and PTP clock configuration on Cisco router. SyncE and PTP clocking configuration is predominantly used in RAN Backhaul (or MToP) network where TDM traffic carried from cell site router to central office via packet switched network.

These commands can be launched from the logical inventory by right-clicking on **Clock** node. Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Navigation	Description
Create PTP Clock Global	*Right-click* **Clock** *node* **> Commands > Configuration** *or* *Right-click* **Clock** *node* **> Commands > Configuration > PTP**	Identify the clock in the network with the highest priority. The clock with the highest priority is referred to as the master clock. All the other devices on the network synchronize their clocks with the master and are referred to as members. Constantly exchanged timing messages between master and members ensure continued synchronization. The PTP clock port commands are used to modify PTP on individual interfaces.
Modify PTP Clock Global	*Expand* **Clock** *node* **>** *right-click PTP Service* **> Commands > Configuration** *or* *Right-click* **Clock** *node* **> Commands > Configuration > PTP**	
Delete PTP Clock Global	*Expand* **Clock** *node* **>** *right-click PTP Service* **> Commands > Configuration**	
Create PTP Clock Port	*Expand* **Clock** *node* **>** *right-click PTP Service* **> Commands > Configuration**	
Show PTP Clock Global	*Expand* **Clock** *node* **>** *right-click PTP Service* **> Commands > Show**	
Modify PTP Clock Port **Delete PTP Clock Port**	*Expand* **Clock** *node* **>** *select* **PTP** *node* **>** *right-click on the selected PTP interface* **> Commands > Configuration**	
Create PTP Interface **Modify PTP Interface**	**Physical inventory > Chassis > Slot >** *Select an interface* **> Commands > Configuration > PTP**	
Create SyncE Global	*Right-click* **Clock** *node* **> Commands > Configuration**	Configure clock properties at the global level such as hold-off time, wait to restore, force switch, and so on, that helps routers to synchronize to the best available clock source. Configure SyncE at the interface level using the SyncE interface commands.
Modify SyncE Global	*Expand* **Clock** *node* **>** *right-click* **SyncE** **> Commands > Configuration** or *Right-click* **Clock** *node* **> Commands > Configuration**	
Create SyncE Interface **Modify SyncE Interface**	*Expand* **Clock** *node* **>** *right-click* **SyncE** **> Commands > Configuration** or **Physical inventory > Chassis > Slot >** *Select an interface* **> Commands > Configuration > SyncE**	

Command	Navigation	Description
Create ESMC Global **Modify ESMC Global**	*Expand* **Clock** *node* **>** *right-click* **SyncE** **> Commands > Configuration**	Configure ESMC for synchronous Ethernet (SyncE) clock synchronization on an interface.
Create ESMC Interface **Disable ESMC Interface**	*Expand* **Clock** *node* **>** *select* **SyncE >** *r*ight-click the *SyncE Interface from the content pane* **> Commands > Configuration**	
Modify ESMC Interface		

Configuring TDM and Channelization

The table below lists the supported TDM and channelization commands and how to launch them. Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Navigation	Description
TDM Commands		
Configure Card Type	*Right-click the device* **> Commands > Configuration**	Configure the card type as SONET/SDH an specify the chassis, slot or the subslot number (for example, for Cisco ASR 9000 series devices). Configure the card type as E1, T1, and specify the location using slot and bay number (for example, for Cisco ASR 901 and Cisco ASR 903 devices).
Modify E1 Controller **Modify T1 Controller**	**Physical Inventory > Chassis > Slot >** *right-click on* **E1 or T1 > Commands > Configuration > E1T1** or **Physical Inventory > Chassis > Slot >** *click on* **SONET >** *double-click on a* **SONET/SDH High Order Path (HOP) >** *right-click* **LOP > Commands > Configuration > E1T1**	Configure E1 and T1 controller as part of the channelization when configuring the low order path (LOP) for the SONET controller (for example, for Cisco ASR 9000 series devices). Configure E1 or T1 controller in either of the following ways while configuring the card type or during the channelization when configuring the low order path (LOP) for the SONET (for example, for Cisco ASR 903 devices). Configure the card type to configure E1 or T1 controller (for example, for Cisco ASR 901 devices).

Command	Navigation	Description
Channelization Commands for SONET/SDH		
Note Channelization commands also include the TDM commands discussed above. Read the description to understand the scenario applicable to your device.		
Configure Framing	**Physical Inventory > Chassis > Slot > Subslot >** *right-click on SONET/SDH-interface* **> Commands > Configuration > SONET**	Configure SDH/SONET framing type using this command.
Configure AUG Mapping		Configuring framing as SDH, configures AU4 by default, but if you want to change the mode of operation as AU3, use the **AUG Mapping** command.
Configure Controller	**Physical Inventory > Chassis > Slot > Subslot >** *right-click on SONET interface* **> Commands > Configuration > SONET**	After configuring SONET/SDH type, configure the controller using additional parameters, like specifying the clock source.
Configure AU3	**Physical Inventory > Chassis > Slot > Subslot >** *click on SONET-interface* **>** right-click the *SONET/SDH HOP* **> Commands > Configuration**	Using these commands, you can configure the parameters for the SDH channelization. When you are configuring the channelized E1/T1 line card for SDH framing, configure AU-3 or AU-4 as the mode of operation. For SDH, both AU-3 and AU-4 AUG mappings are supported.
Delete AU3		
Configure AU4		
Delete AU4		If the AUG mapping is configured to be AU-4, then the following mapping will be used: TUG-3 <--> AU-4 <--> AUG If the mapping is configured to be AU-3, then the following mapping will be used: AU-3 <--> AUG
Configure TUG3 **Delete TUG3**	**Physical Inventory > Chassis > Slot > Subslot >** click on *SONET-interface* **>** *double-click on a* **SONET/SDH High Order Path (HOP) >** *right-click* **LOP > Commands > Configuration**	
Delete STS **Configure STS**	**Physical Inventory > Chassis > Slot > Subslot >** *click on SONET-interface* **>** right-click the *SONET/SDH HOP* **> Commands > Configuration**	Using these commands, you can configure the STS path attributes for the SONET channelization mode.

Configuring Automatic Protection Switching (APS)

APS refers to the mechanism of using a protect interface in the SONET network as the backup for working interface. When the working interface fails, the protect interface quickly assumes its traffic load. The working interfaces and their protect interfaces make up an APS group. SONET APS offers recovery from fiber (external) or equipment (interface and internal) failures at the SONET line layer.

The table below lists the supported APS commands. Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Navigation	Description
Create APS	*Right-click on the device* > **Commands > Configuration > APS** or **Physical Inventory > Chassis >** *slot* **>** *subslot* **>** *SONET interface* **> Commands > Configuration > APS**	Adds an APS group with a specified number and assign a channel for the APS group. 0 designates a protect channel, and 1 designates a working channel.
Modify APS		

Managing Mobile Networks

The following topics provide an overview of mobile technologies and describe how to work with mobile technologies using the Vision client. If you cannot perform an operation that is described in these topics, you may not have sufficient permissions; see Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1

GPRS/UMTS Networks

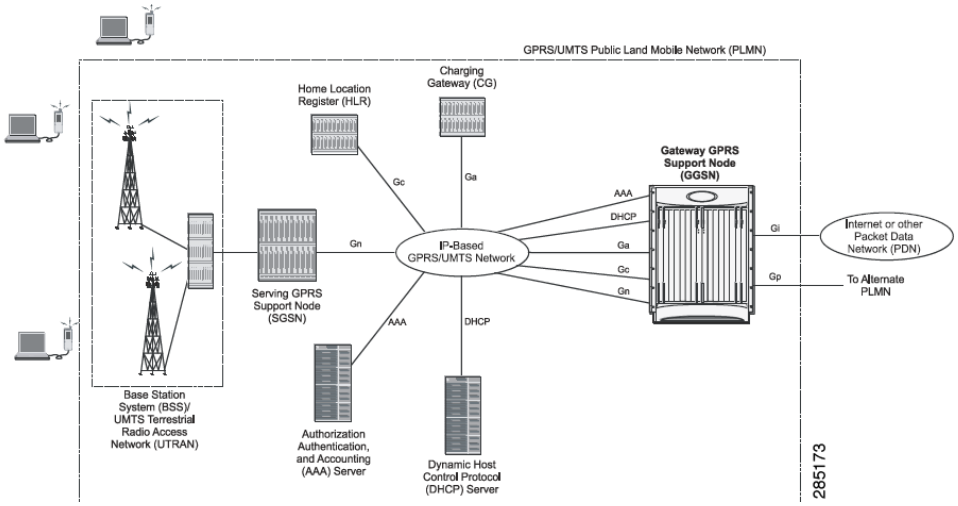
These topics describe how to use Prime Network to manage GPRS/UMTS networks:

Overview of GPRS/UMTS Networks

General Packet Radio Service (GPRS) and Universal Mobile Telecommunication System (UMTS) are evolutions of Global System for Mobile Communication (GSM) networks.

GPRS is a 2.5G mobile communications technology that enables mobile wireless service providers to offer their mobile subscribers packet-based data services over GSM networks. UMTS is a 3G mobile communications technology that provides wideband code division multiple access (CDMA) radio technology. Figure 27-1 shows a basic GPRS/UMTS network topology.

Figure 27-1 Basic GPRS/UMTS Network Topology



The GPRS/UMTS packet core comprises two major network elements:

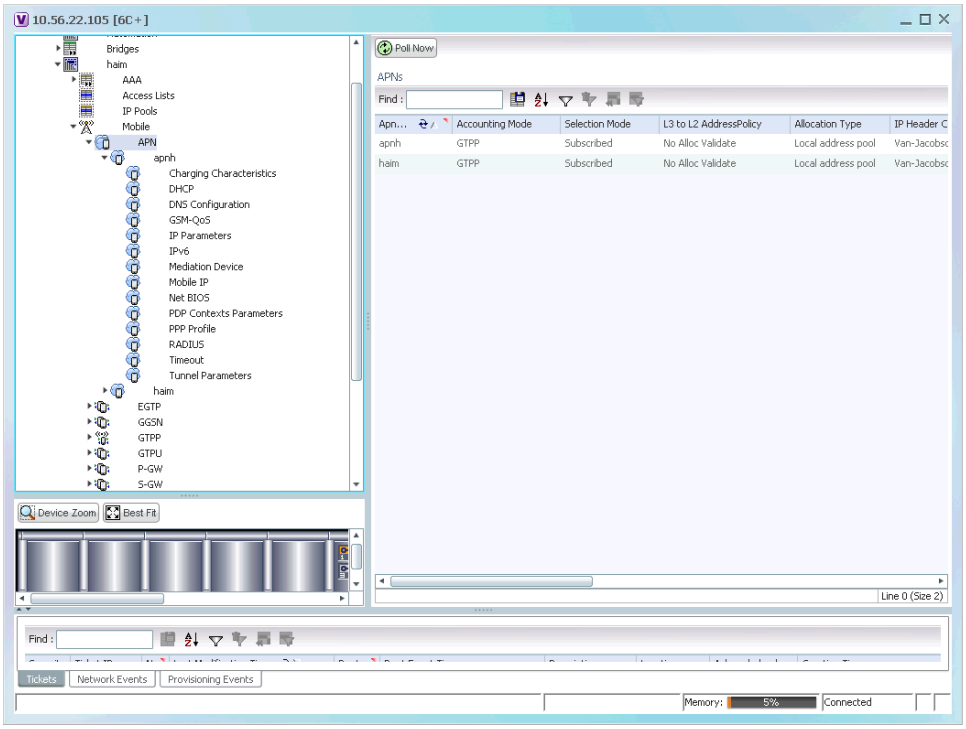
- Gateway GPRS support node (GGSN)—A gateway that provides mobile cell phone users access to a Packet Data Network (PDN) or specified private Internet Protocol (IP) networks.
- Serving GPRS support node (SGSN)—Connects the radio access network (RAN) to the GPRS/UMTS core and tunnels user sessions to the GGSN. The SGSN sends data to and receives data from mobile stations, and maintains information about the location of a mobile station (MS). The SGSN communicates directly with the MS and the GGSN.

PDNs are associated with Access Point Names (APNs) configured on the system. Each APN consists of a set of parameters that dictate how subscriber authentication and IP address assignment is to be handled for that APN.

The Vision client allows you to configure the mobile technologies by using commands and also view the properties configured for the mobile technologies. Figure 27-2 shows an example of the Inventory window with the mobile technology nodes/containers under the Mobile context.

To see which devices support mobile technologies, refer to *Cisco Prime Network 5.3 Supported VNEs*.

Figure 27-2 Mobile Technology Nodes in Logical Inventory



Working With GPRS/UMTS Network Technologies

The following topics explain how to work with GPRS/UMTS network technologies in the Vision client:

- Working with the Gateway GPRS Support Node (GGSN), page 27-3
- Working with the GPRS Tunneling Protocol User Plane (GTPU), page 27-9
- Working with Access Point Names (APNs), page 27-11
- Working with GPRS Tunneling Protocol Prime (GTPP), page 27-22
- Working with the Evolved GPS Tunneling Protocol (eGTP), page 27-29
- Monitoring the Serving GPRS Support Node (SGSN), page 27-31

Working with the Gateway GPRS Support Node (GGSN)

The GGSN works in conjunction with SGSNs within the network to perform the following functions:

- Establish and maintain subscriber Internet Protocol (IP) or Point-to-Point Protocol (PPP) type Packet Data Protocol (PDP) contexts originated by either the mobile or the network.
- Provide charging detail records (CDRs) to the charging gateway ((CG), also known as the Charging Gateway Function (CGF)).
- Route data traffic between the subscriber's Mobile Station (MS) and a PDN such as the Internet or an intranet.

In addition, to providing basic GGSN functionality as described above, the system can be configured to support Mobile IP and/or Proxy Mobile IP data applications in order to provide mobility for subscriber IP PDP contexts. When supporting these services, the system can be configured to function as a GGSN and Foreign Agent (FA), a stand-alone Home Agent (HA), or a GGSN, FA, and HA simultaneously within the carrier's network.

The following topics explain how to work with GGSN in the Vision client:

- Viewing GGSN Properties, page 27-4
- Viewing Additional Characteristics of a GGSN, page 27-6
- GGSN Commands, page 27-8

Viewing GGSN Properties

The Vision client displays the GGSNs in a GGSN container under the Mobile node in the logical inventory. The icon used for representing GGSNs in the logical inventory is explained in NE Logical Inventory Icons, page A-7.

To view GGSN properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > *GGSN Container*.

The Vision client displays the list of GGSNs configured under the container. You can view the individual GGSN details from the table on the right pane or by choosing **Logical Inventory** > *Context* > **Mobile** > *GGSN Container* > *GGSN*.

Table 27-1 describes the details available for each GGSN.

Table 27-1 GGSN Properties in Logical Inventory

Field	Description
Service Name	The name of the GGSN service.
Status	The status of the GGSN service. Value could be Unknown, Running, or Down.
PLMN Policy	The PLMN policy for handling communications from SGSNs that are not configured to communicate with.
Newcall Policy	Specifies whether to accept or reject a new incoming call.
Authentication Server Timeout	The code used by the GGSN as a response message if communication with an authentication server times out. Value could be System Failure or User Authentication Failed.
Accounting Server Timeout	The code used by the GGSN as a response message if communication with an accounting server times out. Value could be System Failure or No Resources.
Accounting Context	The context that processes accounting for PDP contexts handled by the GGSN service
GTPU	The GTPU that is associated with the GGSN and manages the GTP messages between GGSN and a radio access network equipment (RNC).
P-GW	A PDN Gateway (P-GW) is the node that terminates the SGi interface towards the PDN

Table 27-1 GGSN Properties in Logical Inventory (continued)

Field	Description
Associated IPNE Service	The IP Network Enabler (IPNE) service, which defaults to Not Defined.
Associated Peer Map	Specifies the Network side Peer map for the SGW service
S6b IPv6 Reporting	Configures the IPv6 address reporting through Authorization-Authentication-Request (AAR) towards the S6b interface
Local IPv6 Address	The local IPv6 address bounded with the GGSN service.
Maximum Primary Sessions	Configures the maximum number of primary sessions for using this service.
Maximum Secondary Sessions	Configures the maximum number of secondary sessions for using this service.
Unlisted SGSN Rat Type	Specifies the unlisted SGSN rat-type option, which could be gan, geran, hspa, utran, or wlan.
Message Rate [Msgs/Sec]	Specifies the message rate to be in msgs or secs.
Delay Tolerance	Specifies the delay tolerance in secs.
Queue Size	Specifies the size of the queue.
SGSN MCC MNC Preference	Specifies the MCC and MNC portions of PLMN identifier.
Duplicate Subscriber Address Request	Displays how duplicate sessions with same address request are configured.
Duplicate Subscriber Address Request IPV6	Shows how duplicate sessions with same IPv6 address request are configured. The default configuration disables the support to accept duplicate v6 address request.
Gx Li Transport	Displays the Gx LI X3 interface content delivery transport. Default transport is UDP.
Gx Li X3 Interface Context	The Gx LI X3 interface context associated with the service.
Internal QOS Application	The mechanism for deriving the Internal QOS value.
Internal QOS Policy	The derived Internal QOS value for Data Traffic.
DNS Client Context	The context name where a DNS client is configured. The context name associates an existing DNS client configuration with the GGSN to perform a DNS query for P-CSCF, if a P-CSCF query request in an AAA message is received from the Diameter node.
Trace Collection Entity	Shows the configured trace collection entity IP address. Trace collection entity is the destination node to which trace files are transferred and stored.
Path Failure Detection On Gtp Messages	Determines the GTP path-failure behavior on echo or non-echo messages.

Table 27-1 GGSN Properties in Logical Inventory (continued)

Field	Description
MBMS Policy	This command enables or disables the Multimedia Broadcast Multicast Services (MBMS) user service support for multicast or broadcast mode. It also specifies the policy for MBMS user service mode.
Local IP Port	The local UDP port that the GGSN service can use.
Maximum PPP Sessions	Maximum context limits allowed for the service.

If the GGSN is associated with SGSNs and Public Land Mobile Networks (PLMNs), you can view the details from the respective tabs for that GGSN.

Table 27-2 describes the SGSN and PLMN information associated with the GGSN.

Table 27-2 SGSN and PLMN information for a GGSN

Field	Description
SGSNs	
IP Address	The IP address of the SGSN.
Subnet Mask	The subnet mask of the SGSN.
PLMN ID	The PLMN ID associated with the SGSN.
MCC	The mobile country code (MCC) portion of the PLMN.
MNC	The mobile network code (MNC) portion of the PLMN.
PLMN Foreign	Indicates whether the SGSN belongs to a home or foreign PLMN. This field is available only if MCC and MNC are not available.
Reject Foreign Subscriber	Specifies whether to accept or reject foreign subscriber. Value could be True or False.
RAT Type	The type of radio access technology (RAT) that is used for communication.
Description	The description of the SGSN entry in the GGSN service.
PLMNs	
PLMN ID	The ID of the PLMN associated with the GGSN.
Primary	Indicates whether the PLMN ID is the primary PLMN ID for the GGSN. Value could be True or False. When multiple PLMN IDs are configured, the one configured as primary is used for the Authentication, Authorization, and Accounting (AAA) attribute.

Viewing Additional Characteristics of a GGSN

To view additional characteristics of a GGSN:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory > Mobile >** *GGSN Container* **>** *GGSN*.

Step 3 Expand the *GGSN* node. The following list of characteristics configured for the GGSN are displayed:

- Charging Characteristics
- GTPC Characteristics
- Timers And QoS

Step 4 Choose **Charging Characteristics** to view the properties on the right pane. See Table 27-3 for more details on the charging characteristics configured for the GGSN.

Table 27-3 GGSN Charging Characteristics

Field	Description
Profiles	
Profile No	Type of billing. For example: • 1—Hot billing • 2—Flat billing • 4—Prepaid billing • 8—Normal billing All other profiles from 0 - 15 are customized billing types.
Buckets	Denotes container changes in the GGSN Call Detail Record (GCDR).
Prepaid	Prepaid type, which could be Prohibited or Use-rulebase-configuration.
Down Link Octets	Downlink traffic volume of the bucket.
Uplink Octets	Uplink traffic volume of the bucket.
Total Octets	Total traffic volume of the bucket.
Tariff Time Triggers	
Profile No	Type of billing.
Time1, Time2, and so on	First time-of-day time values, and so on, to close the current statistics container.
Intervals	
Profile No	Type of billing.
No. of SGSNs	Number of SGSN changes (inter-SGSN switchovers) resulting in a new Routing Area Identity (RAI) that can occur before closing an accounting record.
Interval	Normal time duration that must elapse before closing an accounting record.
Down Link Octets	Downlink traffic volume reached within the time interval.
Up Link Octets	Uplink traffic volume reached within the time interval.
Total Octets	Total traffic volume reached within the time interval.

Step 5 Under the *GGSN* node, choose **Timers and QoS** to view the properties on the right pane. See Table 27-4 for more details on the Timers and QoS parameters configured for the GGSN.

Table 27-4 GGSN Timers and QoS

Field	Description
Retransmission Timeout	Timeout, in seconds, for retransmission of GTP control packets.
Max Retransmissions	Maximum retries for transmitting GTP control packets.
Setup Timeout	Maximum time, in seconds, allowed for session setup.
Echo Interval	Echo interval, in seconds, for GTP.
Guard Interval	Interval, in seconds, for which the GGSN maintains responses sent to SGSN. This optimizes the handling of retransmitted messages.
QCI to DSCP Mapping	
QoS class index	A set of transport characteristics used to differentiate various packet flows.
DSCP	Differentiated Services Code Point (DSCP), a mechanism for classifying and managing network traffic and providing QoS.
QCI & ARP DSCP Mapping	
QoS class index	A set of transport characteristics used to differentiate various packet flows.
Allocation retention priority	The priority of allocation and retention of the service data flow. This parameter allows prioritizing allocation of resources during bearer establishment and modification. During network traffic congestions, a lower ARP flow is dropped to free up the capacity.
DSCP	A mechanism for classifying and managing network traffic and providing QoS.

GGSN Commands

The following GGSN-related commands can be launched from the inventory by right-clicking a GGSN and choosing *GGSN* **> Commands > Configuration.** Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-5 GGSN Commands

Command	Navigation	Description
Create PLMN Identifier	Right-click the *GGSN group* **> Commands > Configuration**	Use this command to create a PLMN Identifier.
Create SGSN		Use this command to create an SGSN.
Delete GGSN		Use this command to delete a GGSN profile.
Modify GGSN		Use this command to modify a GGSN profile details.

Working with the GPRS Tunneling Protocol User Plane (GTPU)

The GGSN communicates with SGSNs on a Public Land Mobile Network (PLMN) using the GPRS Tunneling Protocol (GTP). The signaling or control aspect of this protocol is referred to as the GTP Control Plane (GTPC) while the encapsulated user data traffic is referred to as the GTP User Plane (GTPU). GTPU is used for transferring user data in separated tunnels for each PDP context.

You can configure various parameters for a GTPU using the configuration commands in the Vision client. You can view the configured parameters for a GTPU in the logical inventory.

The following topics explain how to work with GTPU in the Vision client:

- Viewing GTPU Properties, page 27-9
- GTPU Commands, page 27-10

Viewing GTPU Properties

The Vision client displays the GTPUs in a GTPU container under the Mobile node in the logical inventory. The icon used for representing GTPUs in the logical inventory is explained in NE Logical Inventory Icons, page A-7.

To view GTPU properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > *GTPU Container*.

The Vision client displays the list of GTPUs configured under the container. You can view the individual GTPU details from the table on the right pane or by choosing **Logical Inventory** > *Context* > **Mobile** > *GTPU Container* > *GTPU*.

Table 27-6 describes the details available for each GTPU.

Table 27-6 GTPU Properties in Logical Inventory

Field	Description
Service Name	The name of the GTPU service.
State	The status of the GTPU service. Status could be Unknown, Running, or Down.
Max Retransmissions	The maximum limit for GTPU echo retransmissions. Default value is 4.
Retransmission Timeout	The timeout in seconds for GTPU echo retransmissions. Default value is 5 Secs.
Echo Interval	The rate at which the GTPU echo packets are sent.
IPSEC Tunnel Idle Timeout	The IPSec tunnel idle timeout after which IPSec tunnel deletion is triggered. Default value is 60 Secs.
Allow Error Indication	Specifies whether error indication is dropped or sent without IPSec tunnel. Default value is Disabled.
Include UDP Port Ext Hdr	Specifies whether to include an extension header in the GTPU packet for error indication messages. Default value is False.
IP Address	The list of IP addresses configured on the GTPU. The IP addresses are available only when configured for the GTPU.

Table 27-6 GTPU Properties in Logical Inventory (continued)

Field	Description
Smooth Factor	Configures the smooth-factor used in the dynamic echo timer for GTPU Service, ranging from 1 to 5. Default is 2.
IP QOS DSCP Value	Designates IP Quality of Service - Differentiated Services Code Point.
Source Port Configuration	Configures GTPU data packet source port related parameters.
Path Failure Detection	Specifies policy to be used. Default is GTPU echo message.
Path Failure Clear Trap	Specifies trigger for clearing path failure trap. By default, path failure trap is cleared on receiving first control plane message for that GTPU peer allocation.
UDP Checksum	Detects transmission errors inside GTPU packets.
Echo Interval	Specifies the time of echo interval.
Echo Mode	Specifies the type of echo mode.
Echo Retransmission Timeout	Configures the echo retransmission timeout for GTPU Service, in seconds, ranging from 1 to 20. Default is 5.
Ike Bind Address	Configures an Ike bind address.
Bearer Type	Configures media type supported for the GTPU end point.
Crypto Template	Configures Crypto template for IP-Sec.

Table 27-7 describes the IP address details available for each GTPU.

Table 27-7 GTPU Properties with IP Address Details

Field	Description
IP Address	The list of IP addresses configured on the GTPU. The IP addresses are available only when configured for the GTPU.
Ike Bind Address	Configures an IKE bind address.
Bearer Type	Configures media type supported for the GTPU end point.
Crypto Template	Configures Crypto template for IP-Sec.

GTPU Commands

The following GTPU-related commands can be launched from the inventory by right-clicking a GTPU and choosing **Commands > Configuration.** Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.)

Table 27-8 GTPU Commands

Command	Navigation	Description
Create GTPU Bind IP Address	Right-click the *GTPU defined* > **Commands** > **Configuration**	Use this command to create a bind IP address for GTPU.
Modify GTPU Bind IP Address	Select the **GTPU** node > right-click the *IP address in the content pane* > **Commands** > **Configuration**	Use this command to modify the Bind IP address for GTPU.
Delete GTPU Bind IP Address		Use this command to delete the Bind IP address for GTPU.
Delete GTPU	Right-click the *GTPU defined* > **Commands** > **Configuration**	Use this command to delete a GTPU group.
Modify GTPU		Use this command to modify a GTPU group.

Working with Access Point Names (APNs)

APN is the access point name that is configured in the GGSN configurations. The GGSN's APN support offers the following benefits:

- Extensive parameter configuration flexibility for the APN.
- Extensive QoS support.
- Virtual APNs to allow differentiated services within a single APN. The APN that is supplied by the mobile station is evaluated by the GGSN in conjunction with multiple configurable parameters. Then the GGSN selects an APN configuration based on the supplied APN and those configurable parameters.
- Traffic policing that governs the subscriber traffic flow if it violates or exceeds configured peak or committed data rates. The traffic policing attributes represent a QoS data rate limit configuration for both uplink and downlink directions.

Up to 1024 APNs can be configured in the GGSN. An APN may be configured for any type of PDP context, i.e., PPP, IPv4, IPv6 or both IPv4 and IPv6.

Many parameters can be configured independently for each APN on the device. They are categorized as given below:

- Accounting—Various parameters regarding accounting possibilities, such as, charging characteristics, accounting mode (RADIUS server-based accounting, GTPP-based accounting, and so on.)
- Authentication—Various parameters regarding authentication, such as, protocols used, like, Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or none, default username/password, server group to use, and limit for number of PDP contexts.
- Enhanced Charging—Name of rulebase to use, which holds the enhanced charging configuration (for example, eG-CDR variations, charging rules, prepaid/postpaid options, etc.).
- IP: Method for IP address allocation (e.g., local allocation by GGSN, Mobile IP, Dynamic Host Control Protocol (DHCP), DHCP relay, etc.). IP address ranges, with or without overlapping ranges across APNs.

- Tunneling: PPP may be tunneled with L2TP. IPv4 may be tunneled with GRE, IP-in-IP or L2TP. Load-balancing across multiple tunnels. IPv6 is tunneled in IPv4. Additional tunneling techniques, such as, IPsec and VLAN tagging may be selected by the APN, but are configured in the GGSN independently from the APN.
- QoS: IPv4 header ToS handling. Traffic rate limits for different 3GPP traffic classes. Mapping of R98 QoS attributes to work around particular handset defections. Dynamic QoS renegotiation (described elsewhere).

You can configure the APN parameters using the Vision client. You can view the configured parameters for an APN in the logical inventory. After an APN is determined by the GGSN, the subscriber may be authenticated/authorized with an AAA server. The GGSN allows the AAA server to return Vendor Specific Attributes (VSAs) that override any or all of the APN configuration. This allows different subscriber tier profiles to be configured in the AAA server, and passed to the GGSN during subscriber authentication/authorization.

The following topics explain how to work with APN in the Vision client:

- Viewing APN Properties, page 27-12
- Viewing Additional Characteristics of an APN, page 27-16
- APN Commands, page 27-21

Viewing APN Properties

The Vision client displays the APNs in an APN container under the Mobile node in the logical inventory. You can also view additional characteristics configured on the APN as explained in Viewing Additional Characteristics of an APN, page 27-16. The icon used for representing APNs in the logical inventory is explained in NE Logical Inventory Icons, page A-7.

To view APN properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > *APN Container* > *APN*.

Table 27-9 describes the information that is available for the APN. The information that is displayed depends on the configuration of the APN.

Table 27-9 APN Properties in Logical Inventory

Field	Description
APN Name	The APN name.
Accounting Mode	The accounting protocol in use in the APN. Values are GTPP (GPRS Tunneling Protocol Prime), RADIUS (Remote Authentication Dial In User Service), or None.
Selection Mode	The selection mode in use in the APN. Selection mode indicates the origin of the requested APN and whether or not the Home Location Register (HLR) has verified the user subscription.
L3 to L2 Address Policy	The layer 2 to layer 3 IP address allocation or validation policy.

Table 27-9 APN Properties in Logical Inventory (continued)

Field	Description
Allocation Type	The method by which the APN obtains IP addresses for PDP contexts.
IP Header Compression	IP packet header compression parameters for the APN.
New Call Policy	Specifies whether to accept or reject a new incoming call in case of duplicate session calls with a request for same IP address.

Step 3 To view additional details configured for the APN, use the following tabs:

- Virtual APNs—A virtual APN is a non-physical entity that represents an access point that does not itself provide direct access to a real target network. A virtual APN can be used to consolidate access to multiple, physical target networks through a single access point.
- QCI to DSCP Mapping—Shows the mapping between QoS Class Indices (QCI) to Differentiated Services Code Point (DSCP).
- QCI & ARP DSCP Mapping—Shows the mapping between QCI and Allocation/Retention Priority (ARP) to DSCP.
- QoS Downlink Traffic Policing—Shows the attributes that represent QoS data rate limit configuration for downlink direction within the APN profile.
- QoS Uplink Traffic Policing—Shows the attributes that represent QoS data rate limit configuration for uplink direction within the APN profile.

Table 27-10 Additional Configuration Details for APN

Field	Description
Virtual APNs	
Preference	Specifies the order in which the referenced APNs are compared by the system. Can be configured to any integer value from 1 (highest priority) to 1000 (lowest priority).
APN	Specifies the name of an alternative APN configured on the system that is to be used for PDP contexts with matching properties. Value can be from 1 to 62, alpha and/or numeric characters, and is not case-sensitive. It may also contain dots (.) and/or dashes (-).
Rule Definition	The virtual APN rule definition can be one of the following: • access-gw-address—Specifies the access gateway (SGSN/SGW/Others) address for the virtual APN. The IP address can be an IPv4 or IPv6 address in decimal notation. IPv6 also supports :: notation for the IP address. • bearer-access-service—Specifies the bearer access service name for the virtual APN. • service name—Specifies the service name. Service name is unique across all the contexts. Value is a string of size 1 to 63. • cc-profile—Specifies the APN for charging characteristics (CC) profile index. Value is an integer from 1 to 15. • Domain name—Specifies the subscriber's domain name (realm). Domain name can be from 1 to 79 alpha and/or numeric characters. • MCC—Specifies the MCC portion of the PLMN identifier. Value is an integer between 100 to 999. • MNC—Specifies the MNC portion of the PLMN identifier. Value is an integer between 100 to 999. • msisdn-range—Specifies the APN for this MSISDN range. The starting and ending values of the range is a string of size 2 to 15 with values between 00 and 999999999999999. • Rat-Type—Specifies the rat-type option, which could be gan, geran, hspa, utran, or wlan. • Roaming mode—Specifies the roaming mode, which could be Home, Visiting, or Roaming.
QCI to DSCP Mapping	
QoS class index	Denotes a set of transport characteristics used to differentiate various packet flows.
DSCP	Denotes a mechanism for classifying and managing network traffic and providing QoS.
QCI & ARP DSCP Mapping	
QoS class index	Denotes a set of transport characteristics used to differentiate various packet flows.

Table 27-10 Additional Configuration Details for APN (continued)

Field	Description
Allocation retention priority	Indicates the priority of allocation and retention of the service data flow. This parameter allows prioritizing allocation of resources during bearer establishment and modification. During network traffic congestions, a lower ARP flow is dropped to free up the capacity.
DSCP	Denotes a mechanism for classifying and managing network traffic and providing QoS.
QoS Downlink Traffic Policing	
QCI	A scalar that denotes a set of transport characteristics and used to infer nodes specific parameters that control packet forwarding treatment.
Peak Data Rate	The peak data rate allowed, in bytes, for the downlink direction and QoS traffic class.
Committed Data Rate	The committed data rate allowed, in bytes, for the downlink direction and QoS traffic class.
Negotiate Limit	Indicates whether negotiation limit is enabled or disabled for the downlink direction and Qos traffic class.
Rate Limit	Indicates whether the rate limit is enabled or disabled for the downlink direction and Qos traffic class.
Burst Size Auto Readjust	Indicates whether the auto readjustment of burst size is enabled or disabled. This parameter is used in dynamic burst size calculation, for traffic policing, at the time of PDP activation of modification.
Burst Size Auto Readjust Duration	The burst size readjustment duration in seconds. This parameter indicates the number of seconds that the dynamic burst size calculation will last for. This allows the traffic to be throttled at the negotiated rates.
Peak Burst Size (bytes)	The peak burst size allowed, in bytes, for the downlink direction and QoS class.
Guaranteed Burst Size (bytes)	The guaranteed burst size allowed, in bytes, for the downlink direction and QoS class.
Exceed Action	The action to be taken on packets that exceed the committed data rate, but do not violate the peak data rate. The action could be one of the following: • Drop • Lower IP Precedence • Transmit
Violate Action	The action to be taken on packets that exceed both committed and peak data rates. The action could be one of the following: • Drop • Lower IP Precedence • Shape • Transmit
QoS Uplink Traffic Policing	
QCI	A scalar that denotes a set of transport characteristics and used to infer nodes specific parameters that control packet forwarding treatment.

Table 27-10 Additional Configuration Details for APN (continued)

Field	Description
Peak Data Rate	The peak data rate allowed, in bytes, for the uplink direction and QoS traffic class.
Committed Data Rate	The committed data rate allowed, in bytes, for the uplink direction and QoS traffic class.
Negotiate Limit	Indicates whether negotiation limit is enabled or disabled for the uplink direction and Qos traffic class.
Rate Limit	Indicates whether the rate limit is enabled or disabled for the uplink direction and Qos traffic class.
Burst Size Auto Readjust	Indicates whether the auto readjustment of burst size is enabled or disabled. This parameter is used in dynamic burst size calculation, for traffic policing, at the time PDP.
Burst Size Auto Readjust Duration	The burst size readjustment duration in seconds. This parameter indicates the number of seconds that the dynamic burst size calculation will last for. This allows the traffic to be throttled at the negotiated rates.
Peak Burst Size (bytes)	The peak burst size allowed, in bytes, for the uplink direction and QoS class.
Guaranteed Burst Size (bytes)	The guaranteed burst size allowed, in bytes, for the uplink direction and QoS class.
Exceed Action	The action to be taken on packets that exceed the committed data rate, but do not violate the peak data rate. The action could be one of the following: • Drop • Lower IP Precedence • Transmit
Violate Action	The action to be taken on packets that exceed both committed and peak data rates. The action could be one of the following: • Drop • Lower IP Precedence • Shape • Transmit

Viewing Additional Characteristics of an APN

To view additional characteristics of an APN:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > *APN Container* > *APN*.

Step 3 Expand the APN node. The following list of characteristics configured for the APN are displayed:

- Charging Characteristics—Charging characteristics configured on the APN for different subscribers.
- DHCP—Dynamic Host Control Protocol (DHCP) parameter configured, if the APN supports dynamic address assignment for PDP contexts.
- GSM-QoS—Represents the negotiated QoS attribute reliability class based on the configuration provided for service data unit (SDU) error ratio and residual bit error rate (BER) attributes in the APN.
- IP Parameters—Represents the APN parameters related to IP.
- IPv6—Represents IPv6 configurations and related services for the APN.
- Mediation Device—Represents the mediation device used by the APN for communication with the subscriber.
- Mobile IP—Represents mobile IP configuration of the APN.
- Net BIOS—Represents the NetBIOS server configuration used by the APN.
- PDP Contexts Parameters—Represents the PDP contexts supported by the APN.
- PPP Profile—Represents the PPP profile used by the APN.
- RADIUS—Represents the APN parameters related to communication with the RADIUS server.
- Timeout—Represents the timeout parameters of the APN.
- Tunnel Parameters—Represents the parameters configured for tunneling between the GGSN and an external gateway for the APN.
- DNS Configuration—Represents the Domain Name System (DNS) settings configured on the APN.

Step 4 Click each of one of these characteristics to view its properties on the right pane. See Table 27-11 for more details on the properties of each characteristics configured for the APN.

Table 27-11 APN Characteristics

Field	Description
Charging Characteristics	
Home Bit Behavior	The behavior bit for charging a home subscriber.
Home Profile	The profile index for a home subscriber.
Roaming Bit Behavior	The behavior bit for charging a roaming subscriber.
Roaming Profile	The profile index for a roaming subscriber.
Visiting Bit Behavior	The behavior bit for charging a visiting subscriber.
Visiting Profile	The profile index for a visiting subscriber.
All Bit Behavior	The behavior bit for charging all subscribers. This value is used only if all subscribers are configured to use the same charging characteristics. This value is overridden by the behavior bit set for a subscriber type.
All Profile	The profile index for all subscribers.
Use GGSN	The type of the subscriber using the charging characteristics configured on the APN. Value could be Home, Roaming, Visitor, or None. None indicates that the subscriber is using the charging characteristics from the SGSN.
Use RADIUS Returned	Specifies whether the GGSN accepts charging characteristics returned from the RADIUS server for all subscribers for the APN. Value could be True or False.
DHCP	
Lease Expiration Policy	The action taken when leases for IP addresses assigned to PDP contexts that are facilitated by the APN, are about to expire. For example, auto renew.
GSM-QoS	
SDU Error Ratio Code	The SDU error ratio code based on which the negotiation of QoS attribute reliability class needs to be configured on the APN. Value is an integer between the range 1 and 7. Each code has an assigned value.
Residual BER Code	The residual bit error rate (BER) based on which the negotiation of QoS attribute reliability class needs to be configured on the APN. This value is specified if the SDU error ratio code is 1, 2, 3, or 7. Residual BER code is an integer in the range 1 and 9. Each code has an assigned value.
IP Parameters	
In Access Group	The name of the IPv4/IPv6 access group for the APN when configured for inbound traffic.
Out Access Group	The name of the IPv4/IPv6 access group for the APN when configured for outbound traffic.
Local Address	The static local IP address assigned to the APN.
Next Hop Gateway Address	The IP address of the next hop gateway for the APN. This parameter is available only if it is configured on the APN.
Is Discard Enabled	Specifies whether multicast discard is enabled or disabled. Value could be True or False.

Table 27-11 APN Characteristics (continued)

Field	Description
IPv6	
Inbound Access Group Name	The name of the IPv6 access group for the APN when configured for inbound traffic.
Outbound Access Group Name	The name of the IPv6 access group for the APN when configured for outbound traffic.
Router Advertisement Interval	The time interval (in milliseconds) the initial IPv6 router advertisement is sent to the mobile node. Value is an integer in the range 100 and 16,000. Smaller the advertisement interval greater is the chance of the router being discovered quickly.
Router Advertisement Number	The number of initial IPv6 router advertisements sent to the mobile node. Value is an integer in the range of 1 and 16.
Prefix Pool Name	The name of the IPv6 address prefix pool configured for the subscriber. You can configure upto a maximum of four pools per subscriber.
Egress Address Filtering	Specifies whether filtering of packets not meant for the mobile interface, is enabled or disabled.
Mediation Device	
Mediation Accounting Enabled	Indicates whether mediation accounting is enabled or disabled.
No Early PDUs	Indicates whether protocol data units (PDUs) must be delayed or not until a response to the GGSN's accounting start request is received from the mediation device. If No Early PDUs is ‘true’, the chassis does not send any uplink or downlink data from or to a MS, until it receives a command from the mediation device.
No Interims	Indicates whether radius interim updates are sent to the mediation device or not for the APN for radius accounting.
Delay GTP Response	Indicates whether the GTP response must be delayed or not. If this value is ‘true’, the GTP response is delayed and is sent to the SGSN only if the AAA server is up. If the value is ‘false’, the subscriber will be connected to the SGSN even if the AAA server is down.
Mobile IP	
Home Agent	The IP address of the home agent (HA) used by the current APN to facilitate subscriber mobile IP sessions.
Mobile Node Home Agent SPI	The mobile node Security Parameter Index (SPI) configured for the APN. Value is an integer between 256 and 4294967295.
Mobile Node Home Agent Hash Algorithm	The encryption algorithm used (if any) by the APN for security.
Mobile Node AAA Removal Indication	Specifies whether the system is configured to remove various information elements when relaying registration request (RRQ) messages to HA. Value could be Enabled or Disabled.
Net BIOS	
Primary NBNS Address	Primary service address of the NetBIOS server.
Secondary NBNS Address	Secondary service address of the NetBIOS server.

Table 27-11 APN Characteristics (continued)

Field	Description
PDP Contexts Parameters	
Total Contexts	The total number of primary and secondary PDP contexts that can be supported by the APN. Value is an integer between 1 and 4,000,000.
PDP Type	The type of the PDP contexts supported by the APN.
Primary Contexts	The status of the primary contexts of the APN.
PPP Profile	
Data Compression Protocols	The compression protocol used by the APN for compression of data packets.
Keep Alive	The frequency (in seconds) of sending the Link Control Protocol (LCP) keep alive messages. A value zero denotes that the keep alive messages are disabled completely.
Data Compression Mode	The compression mode used by the compression protocol which could be: • Normal—Packets are compressed using the packet history. • Stateless—Each packet is compressed individually.
MTU (bytes)	The maximum transmission unit (MTU) for packets accessing the APN.
Min. Compression Size (bytes)	The smallest packet to which compression may be applied.
RADIUS	
RADIUS Group	The Authentication, Authorization, and Accounting (AAA) group name for the subscriber. If no group is set, the value is displayed as Default.
RADIUS Secondary Group	The secondary AAA group for the APN. If no group is set, the value is displayed as None.
Returned Framed IP Address Policy	The policy which indicates whether to accept or reject a call when the RADIUS server supplies 255.255.255.255 as the framed IP address and when the MS does not supply an IP address.
Timeout	
Absolute	Absolute timeout of a session, in seconds, for the APN.
Idle	Maximum duration, in seconds, after which the system considers the session as dormant or idle and invokes the long duration timer action.
Long Duration	Maximum duration, in seconds, before the system automatically reports or terminates the session. This is the maximum duration before the specified timeout action is activated for the session.
Long Duration Inactivity	Maximum duration, in seconds, before the session is marked as dormant.
Emergency Inactivity	Timeout duration, in seconds, to check inactivity on the emergency session.
Idle Activity Downlink State	Indicates whether the system must ignore the downlink traffic to consider as activity for idle-timeout. Only uplink packets will be able to reset the idle-timeout.
MBMS Bearer Absolute	Maximum time a Multimedia Broadcast and Multicast Server (MBMS) bearer can exist in active or idle state.
MBMS Bearer Idle	Maximum time an MBMS bearer context can be idle.

Table 27-11 APN Characteristics (continued)

Field	Description
MBMS UE Absolute	Session timeout value for the MBMS user equipment.
IPv6 Init Solicit Wait	IPv6 initial router solicit wait timeout.
Long Duration Action Type	The action taken on long duration sessions. For example, the system performs any of the following actions: • Detects a long duration session and sends an SNMP trap and CORBA notification. • Disconnects the session after sending an SNMP trap and CORBA notification. • Suppresses the SNMP trap and CORBA notification after detecting and disconnecting long duration session.
Tunnel Parameters	
Address Policy	The address allocation / validation policy for all tunneled calls except Layer 2 Tunneling Protocol (L2TP) calls.
Peer Load Balancing	The algorithm that defines how the tunnel peers are selected by the APN when multiple peers are configured in the APN.
DNS Configuration	
Primary DNS Address	The primary DNS server for the APN.
Secondary DNS Address	The secondary DNS server for the APN.

APN Commands

The following commands can be launched from the inventory by right-clicking an APN and choosing **Commands > Configuration**. You can preview a command before executing it, or schedule it to run at a later time. You may be prompted to enter your device access credentials while executing a command.

Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*. (You can also add support for new commands by downloading and installing Prime Network Device Packages (DPs); see the *Cisco Prime Network 5.3 Administrator Guide*.)

Table 27-12 APN Commands

Command	Navigation	Description
Create QoS to DSCP Mapping	Right-click the *APN node* > **Commands** > **Configuration**	Use this command to create the mapping between QoS and DSCP.
Create Virtual APN		Use this command to create a virtual APN.
Delete APN		Use this command to delete an APN profile.
Modify APN		Use this command to delete an APN profile.

Working with GPRS Tunneling Protocol Prime (GTPP)

GPRS Tunneling Protocol Prime (GTPP) is used for communicating accounting messages to CGs. Enhanced Charging Service (ECS) supports different accounting and charging interfaces for prepaid and postpaid charging and record generation. GTPP accounting in ECS allows the collection of counters for different types of data traffic including the data in a GGSN CDR (G-CDR) that is sent to the CGF.

GTPP performs the following functions:

- Transfers CDRs between the Charging Data Function (CDF) and CGF.
- Redirects CDRs to another CGF.
- Advertises to peers about its CDR transfer capability; for example, after a period of service down time.
- Prevents duplicate CDRs that might arise during redundancy operations. The CDR duplication prevention function is carried out by marking potentially duplicated CDR packets, and delegating the final duplicate deletion task to a CGF or the billing domain, instead of handling the possible duplicates solely by GTPP messaging.

Prime Network provides support on gathering the GTPP accounting setup details that are configured in the mobile gateway for transferring the different types of CDRs from charging agent to a GTPP server or accounting server.

GTPP is configured within the accounting context of an APN and is also used by GGSN, P-GW, and S-GW to transmit CDRs to CGF.

The following topics provide details on how to work with GTPP in the Vision client:

- Viewing GTPP Properties, page 27-22
- Viewing Additional Characteristics of a GTPP, page 27-23
- GTPP Commands, page 27-28

Viewing GTPP Properties

the Vision client displays the GTPPs in a GTPP container under the Mobile node in the logical inventory. The icon used for representing GTPPs in the logical inventory is explained in NE Logical Inventory Icons, page A-7.

To view GTPP properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > *GTPP Container*.

The Vision client displays the list of GTPP groups configured under the container. You can view the individual GTPP group details from the table on the right pane or by choosing **Logical Inventory** > *Context* > **Mobile** > *GTPP Container* > *GTPP Group*.

Table 27-13 describes the details available for each GTPP group.

Table 27-13 GTPP Properties in Logical Inventory

Field	Description
Group Name	Name of the GTPP group.
CDR Storage Mode	Storage mode for CDRs, which could be Local or Remote.
CDR Timeout	Maximum amount of time the system waits for a response from the CGF before assuming the packet is lost.
CDR Max Retries	Number of times the system attempts to a CGF that is not responding.
Max CDR Size (bytes)	Maximum payload size of the GTPP packet.
Max CDR Wait Time	Maximum payload size of the GTPP packet. The payload includes the CDR and the GTPP header.
Max CDRs in Message	Maximum number of CDRs allowed in a single packet.
Recover Files Sequence Number	Indicates whether recovery of file sequence number is enabled or not. If enabled, everytime the machine is rebooted, the file sequence number continues from the last sequence number.
Data Request Start Sequence Number	The starting sequence number to be used in the GTPP data record transfer (DRT) record.
Start File Sequence Number	Starting value of the file sequence number.
Source Port Validation	Indicates whether port checking is enabled or disabled for node alive/echo/redirection requests from the CGF.
Dictionary	Dictionary supported by the GTPP group.
Suppress Zero Volume CDRs	Suppress the CDRs with zero byte data count under GTPP group.
Data Record Version Format	Specifies the data record version format.
Accounting Server	
Group	GTPP group, in which the accounting server is configured.
Context Name	Name of the context, in which the CGF is configured.
Primary Accounting Server Address	IPv4 or IPv6 address of the CGF.
Port	UDP port over which the GGSN communicates with the CGF.
State	Status of the CGF, which could be Active or Inactive.
Priority	Relative priority of the CGF. This priority determines which CGF server to send the accounting data to.

Viewing Additional Characteristics of a GTPP

To view additional characteristics of a GTPP:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > *GTPP Container* > *GTPP*.

Step 3 Expand the GTPP node. The following list of characteristics configured for the GGSN are displayed:

- Accounting Server Failure Detection—Attributes of the CGF accounting server within the GTPP server group.
- CDR Attributes Indicator—Indicates whether associated attributes are enabled or disabled for CDR generation.
- CDR Triggers—Attributes that trigger CDR generation.
- Charging Agent— IP address and port of the system interface within the current context used to communicate with the CGF or the GTPP Storage Server (GSS).
- EGCDR Data Generation Configuration—Attributes that represent the GTPP eG-CDR data generation configuration.
- Local Storage—Storage server information, if CDR storage mode is Local.
- MBMS CDR Triggers—Attributes that trigger the MBMS CDR generation.
- Storage Server—Configuration information for the GTPP backup storage server.

Step 4 Click each of one of these characteristics to view its properties on the right pane. See Table 27-14 for more details on the properties of each characteristics configured for the GTPP.

Table 27-14 GTPP Characteristics

Field	Description
Accounting Server Failure Detection	
Detect Dead Server Consecutive Failures	Number of failures that could occur before marking a CGF as dead (down).
Dead Server Suppress CDRs	Indicates whether suppression of CDRs is enabled or disabled when the GTPP server is detected as dead or unreachable.
Dead Time	Maximum duration, in seconds, before marking a CGF as dead on consecutive failures.
Echo Timeout	The amount of time that must elapse before the system attempts to communicate with a CGF that was previously unreachable.
Echo Max Retries	Number of times the system attempts to communicate with a GTPP backup storage server that is not responding.
Redirection Allowed	Indicates whether redirection of CDRs is allowed or not, when the primary CGF is unavailable.
Duplicate Hold Time Minutes	Number of minutes to hold on to CDRs that may be duplicates, when the primary CGF is down.
CDR Attributes Indicator	

Table 27-14 GTPP Characteristics (continued)

Field	Description
Indicators	Indicates whether the following CDR attributes are enabled or not: • PDP Type • PDP Address • Dynamic Flag • Diagnostics • Node ID • Charging Characteristic Selection Mode • Local Record Sequence Number • MSISDN • PLMN ID • PGW PLMN ID • IMEI • RAT • User Location Information • List of Service Data • Served MNAI • Start Time • Stop Time • PDN Connection ID • Served PDP PDN Address Extension • Duration • SGW IPv6 Address • PGW IPv6 Address • SNA IPv6 Address • QOS Max Length • Record Type (SaMOG) • APN AMBR Present • Sponsor ID • SGSN Change Present • Dynamic Address Flag Extension Present • TWAN User Location Information Present • User CSG Information Present • Served PDP PDN Address Prefix Length Present • IMSI Unauthenticated Flag Present

Table 27-14 GTPP Characteristics (continued)

Field	Description
Indicators	• Low Access Priority Indicator • Direct Tunnel Present • Furnish Charging Information Present • APN Selection Mode Present • PCO NAI Present • MS Timezone Present
CDR Triggers	
Triggers	Indicates whether the following CDR triggers are enabled or not: • Volume Limit • Time Limit • Tariff Time Change • Serving Node Change Limit • Intra SGSN Group Change • Inter PLMN SGSN Change • EGCDR Max LOSDV Limit • QOS Change • RAT Change • On RAT Change Generate • MS Timezone Change • Direct Tunnel • Cell Update • PLMN ID Change • Dcca • Service Idle Out • ULI Change • APN AMBR Change
Charging Agent	
IP Address	IP address of the charging agent.
Port	Port of the charging agent.
EGCDR Data Generation Configuration	
Service Interval	The volume octet counts for the generation of the interim eG-CDRs to service data flow container in flow-based charging (FBC).
Service Idle Timeout	Time interval, in seconds, to close the eG-CDR, if the minimum time duration thresholds for service data flow containers are satisfied in FBC.
Delete Service Thresholds	Configured threshold in eG-CDR to be deleted in the service.

Table 27-14 GTPP Characteristics (continued)

Field	Description
Include All LOSDVs	Indicates whether all content IDs are included in the final eG-CDR or not.
LOSDV Max Containers	Maximum number of List of Service Data Volume (LoSDV) containers in one eG-CDR.
LOTDV Max Containers	Maximum number of List of Service Data Volume (LoSDV) containers in one eG-CDR.
Closing Cause Unique	Indicates whether the same closing cause needs to be included for multiple final eG-CDRs or not.
Cause For Record Closing Normal Release	Indicates whether the cause for record closing normal release is enabled or disabled.
Local Storage	
File Format	File format to store CDRs.
File Compression	Type of compression used on CDR files stored locally. None indicates that file compression is disabled.
File Rotation Time Interval	Time duration, in seconds, after which CDR file rotation happens.
File Rotation Volume Limit (MB)	Volume of CDR file, in MB, after which CDR file rotation happens.
File Rotation CDR Count	Number of CDRs to include in a CDR file after which CDR file rotation happens.
Force File Rotation by Time Interval	Indicates whether file rotation is forced or not. If this is enabled, the system is forced to do a file rotation at specified interval, even if there are no CDRs generated.
Purge Processed Files	Indicates whether processed files must be processed or not.
File Transfer Mode	Mode of file transfer for the GTPP service.
MBMS CDR Triggers	
Interval	Specifies the normal time duration that must elapse before closing an accounting record provided that any or all of the following conditions are satisfied: • Down link traffic volume is reached within the time interval • Tariff time based trigger occurred within the time interval • Data volume (uplink and downlink) bucket trigger occurred within the time interval
Buckets	Total number of data buckets configured for MBMS CDR trigger service.
Storage Server	
IP Address	IP address of the backup storage server.
Port	UDP port number over which the GGSN communicates with the backup storage server.
Timeout	Maximum amount of time, in seconds, the system waits for a response from the GTPP backup storage server before assuming the packet is lost.
Max Retries	Number of times the system attempts to communicate with a GTPP backup storage server that is not responding.

GTPP Commands

The following GTPP-related commands can be launched from the inventory by right-clicking a GTPP and choosing **Commands > Configuration** or **Commands > Show.** Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-15 GTPP Commands

Command	Navigation	Description
Create CGF	*Right-click the GTPP group* > **Commands** > **Configuration**	The Charging Gateway Function (CGF) listens to GTP' messages sent from the GSNs on TCP/UDP port 3386. The core network sends charging information to the CGF, typically including PDP context activation times and the quantity of data which the end user has transferred. However, this communication which occurs within one network is less standardized and may, depending on the vendor and configuration options, use proprietary encoding or even an entirely proprietary system. Use this command to create a new CGF.
Create Storage Server		The GTPP Storage Server (GSS) provides an external management solution for the bulk storage of Charging Data Records (CDRs) coming from a GPRS Support Node (GSN) in a GPRS/UMTS network. Use this command to create a storage server.
Modify Storage Server	Right-click the *GTPP group* > **Storage Server**	Use this command to modify storage server configuration details.
Delete Storage Server		Use this command to delete a storage server.

Table 27-15 GTPP Commands (continued)

Command	Navigation	Description
Delete CGF	Right-click the *GTPP group* > **Commands** > **Configuration**	Use this command to delete a CGF.
Delete GTPP		Use this command to delete a GTPP.
Modify CGF		Use this command to modify CGF configuration details.
Modify GTPP		Use this command to modify GTPP configuration details.
Show CGF	Right-click the *GTPP group* > **Properties**. In the GTPP Group Container Properties window, right-click a GTPP Group name and then choose **Commands** > **Show > Show CGF**	Use this command to view and confirm CGF configuration details.

Working with the Evolved GPS Tunneling Protocol (eGTP)

Evolved GPRS Tunneling Protocol (EGTP) formulates the primary bearer plane protocol within an LTE/EPC architecture. It provides support for tunnel management including handover procedures within and across LTE networks.

This topic contains the following sections:

Viewing eGTP Properties

The Vision client displays the EGTPs in an EGTP container under the Mobile node in the logical inventory. The icon used for representing EGTPs in the logical inventory is explained in NE Logical Inventory Icons, page A-7.

To view EGTP properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > *EGTP Container*.

The Vision client displays the list of EGTPs configured under the container. You can view the individual EGTP details from the table on the right pane or by choosing **Logical Inventory** > *Context* > **Mobile** > *EGTP Container* > *EGTP*.

Table 27-16 describes the details available for each EGTP.

Table 27-16 EGTP Properties in Logical Inventory

Field	Description
Service Name	Name of the EGTP service.
Status	Status of the EGTP service.
Message Validation Mode	Mode of message validation for the EGTP service.
Interface Type	Interface type for the EGTP service.
DBcmd When MBreq Pending	Indicates collision handling of DBcmd when MBreq is pending. When No is specified as a Default option, then MB req is aborted and handles DBcmd.
Restart Counter	Restart counter value for the EGTP service.
Max Remote Restart Counter Change	Specifies the counter change after which the P-GW will detect a peer restart. A peer restart is detected only if the absolute difference between the new and old restart counters is less than the value configured.
GTPC Retransmission Timeout	Control packet retransmission timeout for a EGTP service.
GTPC Max Request Retransmissions	Maximum number of request retransmissions for a EGTP service.
GTPC IP QoS DSCP Value	The IP QoS DSCP value for a EGTP service.
GTPC Echo	Indicates whether GTPC echo is configured for the EGTP service or not.
GTPC Echo Interval	GTPC echo interval for a EGTP service.
GTPC Echo Mode	GTPC echo mode, which could be Dynamic or Default.
GTPC Path Failure Detection Policy Echo Timeout	Shows that Path failure is detected when the retries of echo messages times out.
Associated GTPU Service Name	Displays an associated GTPU service for the selected EGTP service.
GTPC Session Uniqueness	Enabled or disabled. When enabled, populates and sends origination timestamp and maximum wait time private extensions in CSReq towards PGW.
GTPC Path Failure Detection Policy Echo Restart Counter Change	Shows that Path failure is detected when the restart counter in echo request or response message changes.
GTPC Path Failure Detection Policy Echo Control Restart Counter Change	Shows that Path failure is detected when the restart counter in control request or response message changes.
GTPC Echo Retransmission Timeout	Displays the echo retransmission timeout for EGTP service in seconds. The ranges are from 1 to 20. Default value is 5.
GTPC Echo Max Retransmission	Displays maximum retries for GTP echo request. Must be followed by integer, ranging from 0 to 15.

eGTP Commands

The following eGTP commands can be launched from the inventory by right-clicking an EGTP and choosing **Commands > Configuration.** Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-17 EGTP Commands

Command	Navigation	Description
Modify EGTP	Right-click the *EGTP group* > **Commands** > **Configuration**	Use this command to modify EGTP configuration details.
Delete EGTP		Use this command to delete the EGTP.

Monitoring the Serving GPRS Support Node (SGSN)

The Serving GPRS Support Node (SGSN) is a very important component of the GPRS network. It is responsible for handling the delivery of data from and to the mobile nodes within its geographical service area, such as packet routing and transfer, mobility management, and authentication of users.

Along with the Radio Access Network (RAN) and Gateway GPRS Support Node (GGSN), the SGSN:

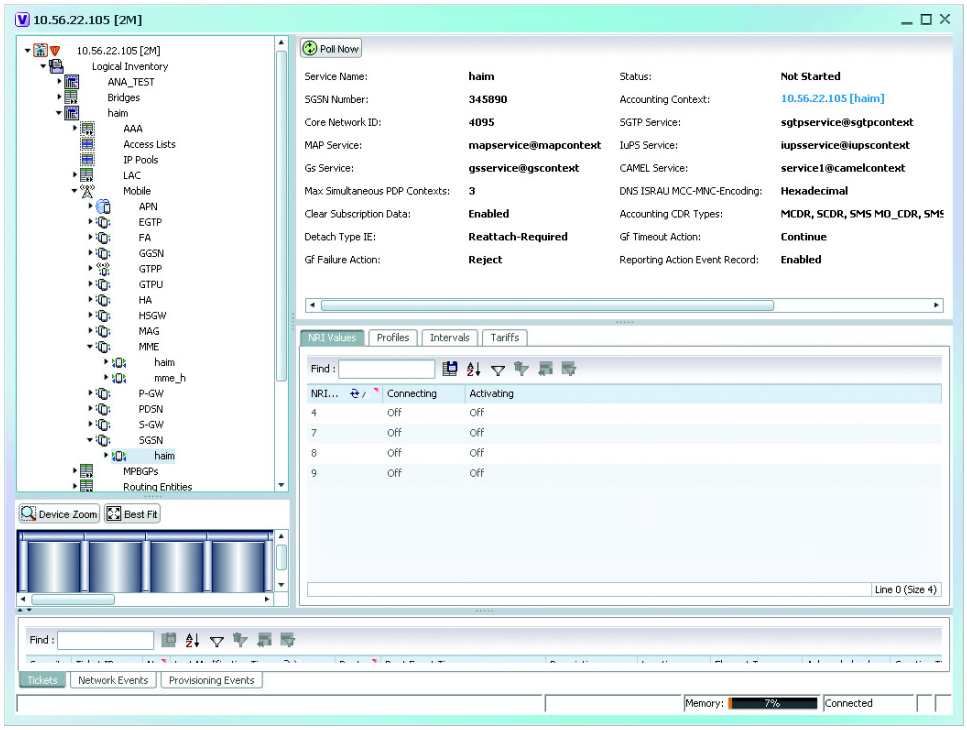
- Communicates with the Home Location Registers (HLR) via a Gr interface and with the mobile Visitor Location Registers (VLR) via a Gs interface to register a subscriber's equipment or authenticate, retrieve and update the subscriber's profile information.
- Supports Gd interface to provide short message service (SMS) and other text-based network services to subscribers.
- Activates and manages IPv4, IPv6 or point-to-point (PPP) type packet data protocol (PDP) contexts for a subscriber session.
- Manages the data plane between the RAN and GGSN providing high speed data transfer with configurable GEA0-3 ciphering.
- Provides mobility management, location management, and session management for the duration of call to ensure smooth handover.
- Provides different types of charging data records (CDR) to attached accounting or billing storage mechanisms
- Provides Communications Assistance for Law Enforcement Act (CALEA) support for lawful intercepts.

Viewing the SGSN Configuration Details

To view the SGSN configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > **SGSN**. The SGSN services configured in Prime Network are displayed in the content pane as shown in the following figure.



Step 3 Under the SGSN node, choose an **SGSN** service. The SGSN service details are displayed in the content pane.

Table 27-18 describes the SGSN service details.

Table 27-18 SGSN Service Details

Field	Description
Service Name	The unique name of the SGSN service. **Note** You can configure only one SGSN service for a chassis.
Status	The status of the SGSN service, which can be any of the following: • Unknown • Initiated • Running • Down • Started • Not Started
SGSN Number	The phone number that is associated with the SGSN service.
Core Network ID	The network code that identifies the core network to connect the SGSN service.
Associated SGTP Service	The name of the STGP service and its context associated to the SGSN service. This service is represented in the following format: <SGTP Service Nameplate Service Context>
Associated MAP Service	The name of the Mobile Application Part (MAP) service and its context that is associated to the SGSN service. This service is represented in the following format: <MAP Service Name>@<MAP Service Context> **Note** MAP is an SS7 protocol that provides an application layer for the various nodes in GSM and UMTS mobile core networks and GPRS core networks to communicate with each other in order to provide services to mobile phone users. It is an application-layer protocol used to access SGSN service.
Associated HSS Service	The name of the Home Subscriber Server (HSS) service and its context that is associated to the SGSN service. This service is represented in the following format: <HSS Service Name>@<HSS Service Context>
Associated IuPS Service	The name of the IuPS service and its context that is associated to the SGSN service. This service is represented in the following format: <IuPS Service Name>@<IuPS Service Context> **Note** The interface between the RNC and the Circuit Switched Core Network (CS-CN) is called Iu-CS and between the RNC and the Packet Switched Core Network is called Iu-PS

Table 27-18 SGSN Service Details (continued)

Field	Description
Associated Gs Service	The name of Gs service and its context that is associated to the SGSN service. This service is represented in the following format: <Gs Service Name>@<Service Context>
Associated CAMEL Service	The name of the Customized Application for Mobile Network Enhanced Logic (CAMEL) service and its context. This service is represented in the following format: <CAMEL Service Name>@<CAMEL Context>
Max Simultaneous PDP Contexts	The maximum number of simultaneous Packet Data Protocol (PDP) contexts per mobile station. This number can be any value between 2 and 11.
Offload T3312 Timeout	The amount of time (in seconds) for sending period RAUs to the mobile station. This time can be any value between 2 and 60.
Override LAC for LI	The Location Area Code (LAC) that is associated with the SGSN service at the time of record opening.
Override RAC for LI	The Routing Area Code (RAC) that is associated with the SGSN service at the time of record opening.
Dns Israu MCC-MNC-Encoding	The format of the MCC and MNC values in the DNS query sent during the Inter-SGSN RAU (ISRAU), which can be any one of the following: • decimal • hexadecimal
Accounting CDR Types	The type of accounting Call Detail Record (CDR) configured for the SGSN service, which can be any one of the following: • MCDR • SCDR • SMS MO_CDR • SMS MT_CDR • SMBMSCDR • LCS MT_CDR • no accounting cdr-types • Unknown Multiple CDR types may be configured for a SGSN service. In such cases, the types are separated by a comma and displayed here.
Clear Subscription Data	Indicates whether the SGSN service will clear subscriber contexts and the subscription database for the attached subscribers whenever the **clear subscribers all** command is issued.
Detach Type IE	The instruction that is included in the Detach-Request message during the Admin-Disconnect procedure, which can be any one of the following: • Reattach-Required • Reattach-Not-Required • Unknown

Table 27-18 SGSN Service Details (continued)

Field	Description
Gf Timeout Action	The action to be taken by the SGSN service when a response is not received from the Equipment Identify Register (EIR) even though a valid EIR configuration exists under the MAP service and the route to the EIR is available. Any one of the following actions is applicable: • Continue • Reject
Gf Failure Action	The action to be taken by the SGSN service when the EIR is temporarily inaccessible even though a valid EIR configuration exists under the MAP service, which can be any one of the following: • Continue • Reject
Reporting Action Event Record	Indicates whether the SGSN service is allowed to enable GGM/SM event logging for 3G services.
Network Global MME ID Management DB	Indicates whether the SGSN service is associated to the Network Global MMEID Management Database, which in turn is configured on the LTE policy.
Tai Management DB	Indicates whether the SGSN service is associated to the Tai Management Database, which in turn is configured on the LTE policy.
LCS Service	The name of the LCS service associated with the SGSN service.
NRI Values tab	
NRI Value	The MS assigned value of the Network Resource Identifier (NRI) to retrieve from the P-TSMI, which is used to identify a SGSN service in a pool. **Note** This value is unique across all pools.
Connecting	Indicates whether the SGSN service will offload subscribers by sending either a “Attach Request” or “RAU Request” message for the corresponding NRI value.
Activating	Indicates whether the SGSN service will offload subscribers by sending an “Activate Request” message for the corresponding NRI value.
Profiles tab	
Profile No.	The type of billing, which can be any one of the following: • 1—Hot billing • 2—Flat billing • 4—Prepaid billing • 8—Normal billing • All other profiles from 0-15 are customized billing types.
Buckets	Denotes container changes in the Call Detail Record (CDR).
Down Link Octets	The downlink traffic volume of the bucket.
Up Link Octets	The uplink traffic volume of the bucket.

Table 27-18 SGSN Service Details (continued)

Field	Description
Total Octets	The total traffic volume of the bucket.
Intervals tab	
Profile No.	The type of billing.
No. of SGSNs	The number of changes to the SGSN (inter-SGSN switchovers) resulting in a new Routing Area Identity (RAI) that can occur before closing an accounting record.
Interval	The amount of time (in seconds) that must elapse before closing an accounting record.
Down Link Octets	The downlink traffic volume reached within the time interval.
Up Link Octets	The uplink traffic volume reached within the time interval.
Total Octets	The total traffic volume reached within the time interval.
Tarrifs tab	
Profile No.	The type of billing.
Time (1 - 6)	The time-of-day values at different times in a day, which is required to close the current statistics container.

SGSN Commands

The following SGSN commands can be launched from the logical inventory by right-clicking a SGSN service and choosing *Context* > **Commands > Configuration.** Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-19 SGSN Commands

Command	Navigation	Description
Modify SGSN	*Right-click the SGSN service* > **Commands** > **Configuration**	Use this command to modify the SGSN service.
Delete SGSN		Use this command to delete the SGSN service.
Create Target NRI		Use this command to create Target NRI.
Show SGSN	*Right-click the SGSN service* > **Commands** > **Show**	Use this command to view details of the selected SGSN service.
Modify Profile	**SGSN service** > **Profiles Tab** > *Right-click the profile* > **Commands** > **Configuration**	Use this command to modify the profile details.
Modify Tariff	**SGSN service** > **Tariffs Tab** > *Right-click the profile* > **Commands** > **Configuration**	Use this command to modify the tariff details.

Table 27-19 SGSN Commands

Command	Navigation	Description
Modify Interval	**SGSN service** > **Intervals Tab** > Right-click the *profile* > **Commands** > **Configuration**	Use this command to modify the interval details.
Modify NRI Values	**SGSN service** > right-click the **NRI Values** > **Commands** > **Configuration**	Use this command to modify NRI value details.
Modify NRI Properties	**SGSN service** > right-click the **NRI Properties** > **Commands** > **Configuration**	Use this command to modify NRI property details.
Modify Target NRI	**SGSN service** > **Target NRI Tab** > right-click the *Target NRI Table* > **Commands** > **Configuration**	Use this command to modify Target NRI details.
Delete Target NRI	Right-click the *SGSN service* > **Commands** > **Configuration**	Use this command to delete Target NRI details.

Viewing SGSN Service Properties

You can also view the following configuration details for SGSN service:

- GPRS Mobility Management—GPRS Mobility Management (GMM) is a GPRS signaling protocol that handles mobility issues such as roaming, authentication, and selection of encryption algorithms. GPRS Mobility Management, together with Session Management (GMM/SM) protocol support the mobility of user terminal so that the SGSN can know the location of a mobile station (MS) at any time and to activate, modify and deactivate the PDP sessions required by the MS for the user data transfer. See GPRS Mobility Management Properties, page 27-37.
- NRI Properties—The Network Resource Identifier (NRI) identifies the specific CN node of the pool. The UE derives the NRI from TMSI, P-TMSI, IMSI or IMEI. See NRI Properties, page 27-39.
- Session Management Properties—The SGSN service performs comprehensive session management, including context activation, modification, deactivation, and preservation. It also provides support for IPv4, IPv6, and PPP PDP context types. In addition, the SGSN's intelligent PDP context preservation feature facilitates efficient radio resource utilization. See Session Management Properties, page 27-40.

GPRS Mobility Management Properties

To view the GPRS Mobility Management details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > **SGSN** > **GPRS Mobility Management**. The GPRS mobility details are displayed in the content pane.

Table 27-20 describes the SGSN service details.

Table 27-20 GPRS Mobility Management Details

Field	Description
Max Identity Retries	The maximum number of retransmissions allowed for identity requests. In other words, it relates to the number of retransmissions allowed before failure of the request. This number can be any value between 1 and 10.
Max Page Retries	The maximum number of retransmissions allowed for page requests. In other words, it relates to the number of retransmissions allowed before failure of the request. This number can be any value between 1 and 5.
Max PTMSI Reloc Retries	The maximum number of retransmissions allowed for P-TMSI relocation procedure. In other words, it relates to the number of retransmissions allowed before failure of the P-TMSI relocation procedure. This number can be any value between 1 and 10.
Perform Identity After Auth	Indicates whether the SGSN service is allowed to perform an identity check to ascertain the IMSI after an authentication failure on a P-TMSI message.
TRAU Timeout	The amount of time (in seconds) that the SGSN service must wait to purge the mobile station's data.This timer is started by the SGSN service after completion of the inter-SGSN RAU.
T3302 Timeout	The amount of time (in minutes) the SGSN service must wait to attach the GPRS or RAU procedure on the mobile station node before retransmitting the message again. This time can be any value between 1 and 186.
T3312 Timeout	The amount of time (in minutes) the SGSN service must wait to initiate the RAU procedure on the network before retransmitting the message again. This time can be any value between 1 and 186.
T3313 Timeout	The amount of time (in seconds) the SGSN service must wait to initiate the GPRS on the network before retransmitting the message again. This time can be any value between 1 and 60.
T3322 Timeout	The amount of time (in seconds) the SGSN service must wait to detach the GPRS on the network before retransmitting the message again. This time can be any value between 1 and 20.
T3350 Timeout	The amount of time (in seconds) the SGSN service must wait to accept the GPRS attach request, RAU attach request, or reallocation request sent with the P-TSMI/TSMI on the network. This time can be any value between 1 and 20.
T3360 Timeout	The amount of time (in seconds) the SGSN service must wait to guard the authentication or cipher request on the network before retransmitting the message again. This time can be any value between 1 and 20.
T3370 Timeout	The amount of time (in seconds) the SGSN service must wait for the identity request before retransmitting the message again. This time can be any value between 1 and 20.
Mobile Reachable Timeout	The amount of time (in minutes) the SGSN service must wait to reach a mobile station on the network before retransmitting the message again. This time can be any value between 4 and 4400.
Implicit Detach Timeout	The amount of time (in seconds) the SGSN service must wait for the implicit detach procedure on the network before retransmitting the message again. This time can be any value between 1 and 3600.

Table 27-20 GPRS Mobility Management Details (continued)

Field	Description
Purge Timeout	The amount of time (in minutes) the SGSN service must wait to detach the mobility management context on the network before retransmitting the message again. This time can be any value between 1 and 20160.
Page Delta Timeout	The page delta timeout associated with the SGSN service.

GPRS Mobility Management Commands

The following GPRS mobility management commands can be launched from the logical inventory by clicking **SGSN** > *Right-clicking on* **GPRS Mobility Management** > **Commands > Configuration.** Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-21 GPRS Mobility Management Commands

Command	Navigation	Description
Modify GPRS Mobility Management	**SGSN** > *Right-click on* **GPRS Mobility Management** > **Commands > Configuration**	Use this command to modify the GPRS mobility management details.

NRI Properties

To view the NRI Properties for an SGSN service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory > *Context* > Mobile > SGSN** > **NRI Properties**. The NRI properties are displayed in the content pane.

Table 27-22 describes the NRI Properties details.

Table 27-22 NRI Properties Details

Field	Description
NRI Length	The number of bits to be used in P-TMSI to define the NRI, which can be any number between 1 and 6. This length also determines the maximum size of the pool. If you do not configure a length for the NRI, then the default value of zero is considered to be the NRI's length.
NRI Null Value	The value of the null NRI, which is unique across all pool areas. If the NRI null value is 0, it indicates that the keyword is not used. Any value between 1 and 63 is used to identify the SGSN service that is to be used for offloading procedure for SGSN pooling.
Non Broadcast MCC	The country code of the mobile, which is basically the first part of the PLMN ID. This code can be any value between 100 and 999.
Non Broadcast MNC	The network code portion of the PLMN ID. This code must be a 2 or 3 digit value between 1 and 999.
Non Broadcast LAC	The location area code associated with an RNC. This code must be any value between 1 and 65535.
Non Broadcast RAC	The remote area code associated with an RNC. This code can be any value between 1 and 255.

Session Management Properties

To view the Session Management properties for an SGSN service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory > *Context* > Mobile > SGSN** > **Session Management Properties**. The Session Management properties are displayed in the content pane.

Table 27-23 describes the Session Management Properties details.

Table 27-23 Session Management Properties Details

Field	Description
Max Activate Retries	The maximum number of retries to activate PDP context, which can be any value between 1 and 10.
Max Modify Retries	The maximum number of retries to modify the PDP context, which can be any value between 1 and 10.
Max Deactivate Retries	The maximum number of retries to deactivate PDP context, which can be any value between 1 and 10.
T3385 Timeout	The amount of time (in seconds) to wait for a network initiated activate request before it is retransmitted again. This time can be any value between 1 and 60.
T3386 Timeout	The amount of time (in seconds) to wait for a network initiated modify request before it is retransmitted again. This time can be any value between 1 and 60.
T3395 Timeout	The amount of time (in seconds) to wait for a network initiated deactivate request before it is retransmitted again. This time can be any value between 1 and 60.
Guard Timeout	The amount of time (in seconds) for retransmission of a GUARD request, which can be any value between 1 and 60.
ARP RP Profile	The status of the ARP packet (request or reply) associated with the SGSN service.

Session Management Commands

The following Session Management commands can be launched from the logical inventory by clicking **SGSN** > *Right-clicking on* **Session Management** > **Commands > Configuration.** Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-24 Session Management Commands

Command	Navigation	Description
Modify Session Management	**SGSN** > *Right-click on* **Session Management** > **Commands > Configuration**	Use this command to modify the session management details.

Viewing SGSN-Global Properties

To view the SGSN-Global configuration details:

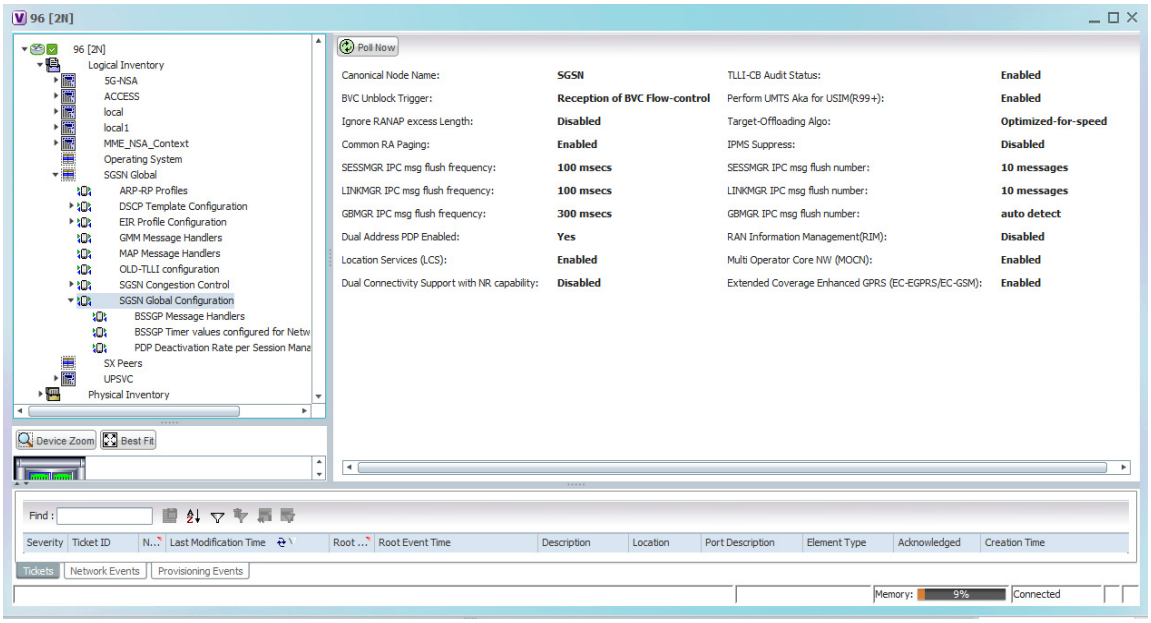
Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory > SGSN Global**. The SGSN-Global configurations for the device are listed.

Note Prime Network supports NSA from StarOS 21.11 onwards.

The following figures and tables show SGSN Global parameters for SGSN Global configurations.

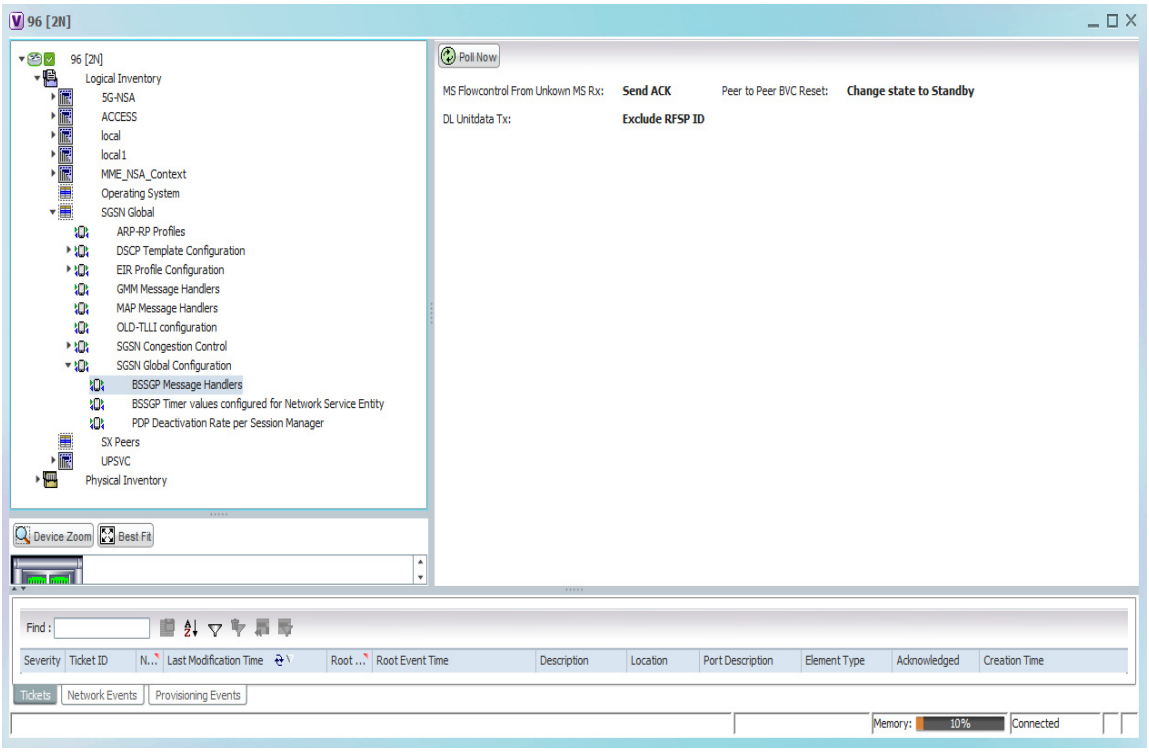
1. SGSN Global > SGSN Global Configuration



Field	Description
Canonical Node Name	Name of the canonical node
TLLI-CB Audit Status	Specifies if the periodic TLLI-CB audit is enabled or disabled
BVC Unblock Trigger	Shows bvc-unblock trigger based on configuration
Perform UMTS AKA for USIM(R99+)	Shows UMTS AKA for USIM(R99+) in case of quintuplet available from HLR
Ignore RANAP excess Length	Shows action on handling of excess length of RANAP messages
Target-Offloading Algo	Shows the algorithm for target-based offloading
Common RA Paging	Specifies if paging across common Routing Area for 2G and 3G is enabled or disabled
IPMS Suppress	Specifies if suppressing of 2G-related IPMS events is enabled or disabled
SESSMGR IPC msg flush frequency	Shows the frequency of flush

Field	Description
SESSMGR IPC msg flush number	Shows the number of IPC messages to be aggregated
LINKMGR IPC msg flush frequency	Shows the frequency of flush
LINKMGR IPC msg flush number	Shows the number of IPC messages to be aggregated
GBMGR IPC msg flush frequency	Shows the frequency of flush
GBMGR IPC msg flush number	Shows the number of IPC messages to be aggregated
Dual Address PDP Enabled	Specifies if the support for dual address PDP is enabled or not
RAN Information Management (RIM)	Specifies if the support for RIM is enabled or disabled
Location Services (LCS)	Specifies if the Location Services are enabled or disabled on the interface
Multi Operator Core NW (MOCN)	Specifies if the support for MOCN for SGSN is enabled or disabled
Dual Connectivity Support with NR capability (DCNR)	Specifies if DCNR is enabled or disabled
Extended Coverage Enhanced GPRS (EC-EGPRS/EC-GSM)	Specifies if the support for EC-GSM (EC-EGPRS) feature is enabled or disabled

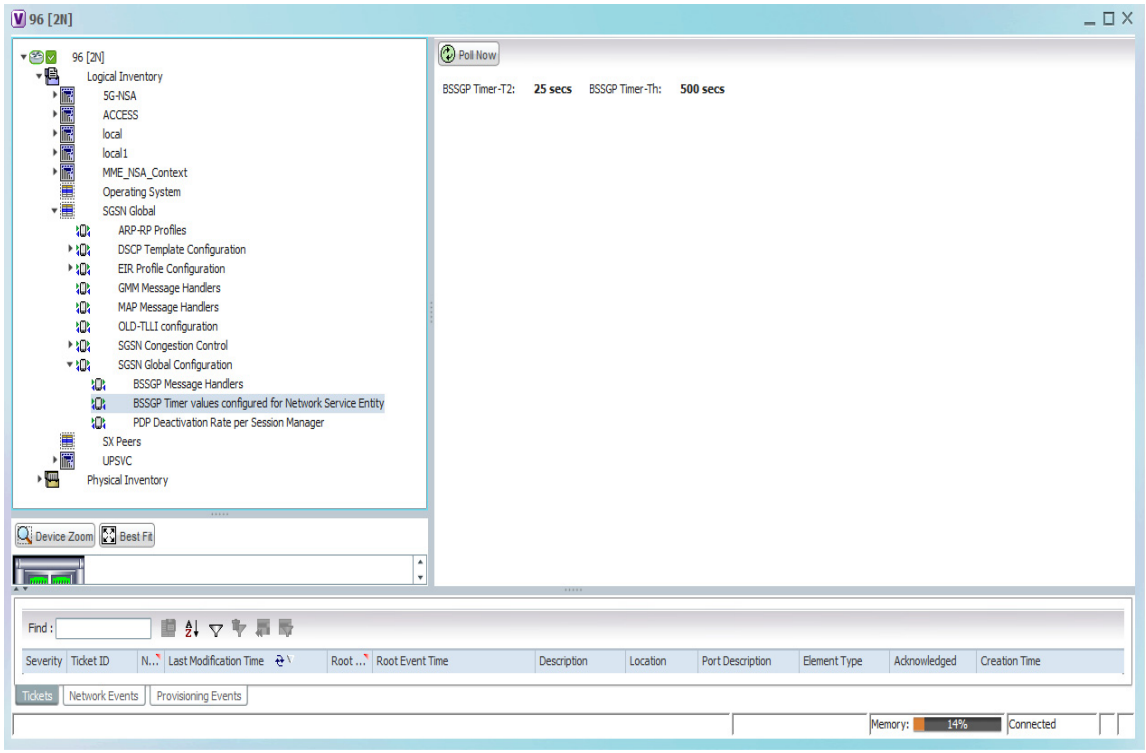
2. SGSN Global > SGSN Global Configuration > BSSGP Message Handlers



Field	Description
MS Flowcontrol from Unknown MS Rx	Specifies the action to be taken for the reception of MS-FLOW-CONTROL message from Unknown MS. By default, SGSN sends BSSGP-STATUS response; Enables the SGSN to send BSSGP-STATUS response; Enables the SGSN to discard the received BSSGP message; Enables the SGSN to send ACK response.

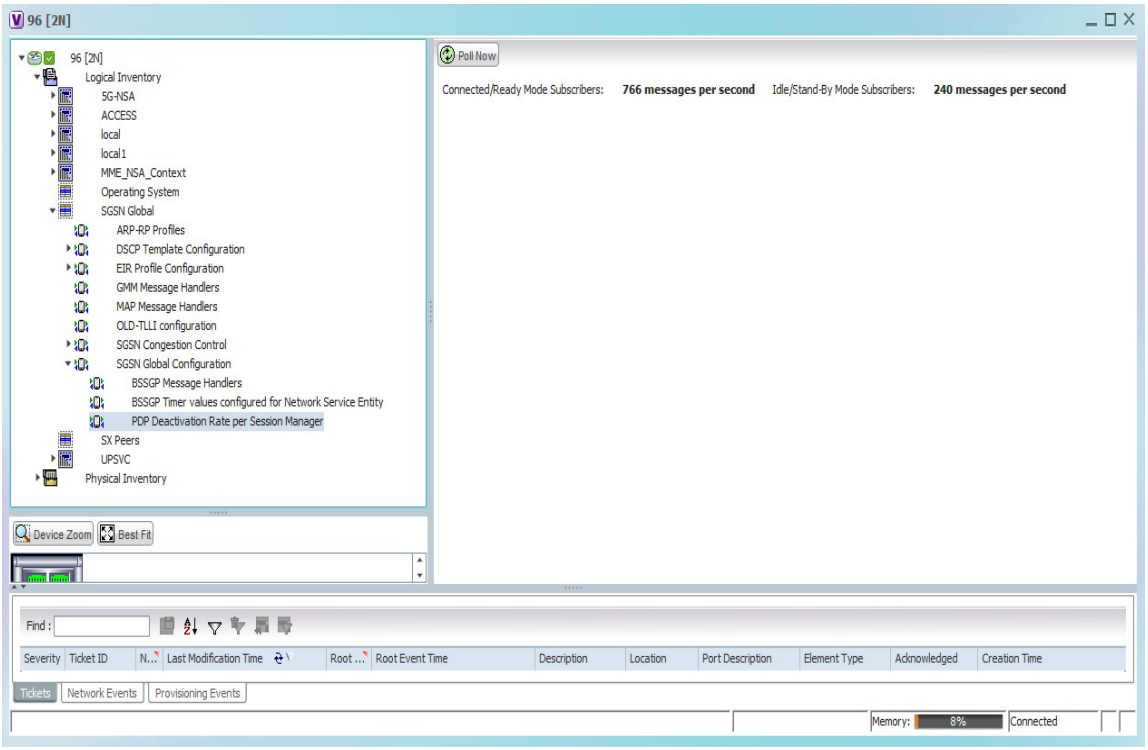
Field	Description
Peer to Peer BVC Reset	Specifies the following: • Action to be taken for the reception of a BSSGP message with particular cause or reason. • Action to be taken for the reception of peer to Peer BVC reset. By default, subscribers continue with the current state. Moves the subscriber to standby state.
DL Unitdata Tx	Specifies the action to be taken for the reception of a BSSGP message with particular cause or reason. Specifies if rfsp-id needs to be excluded in outgoing dl-unitdata. By default, rfsp-id is sent in DL-Unitdata. Exclude RFSP Id in DL-Unitdata message.

3. SGSN Global > SGSN Global Configuration > BSSGP Timer Values configured for Network Service Entity



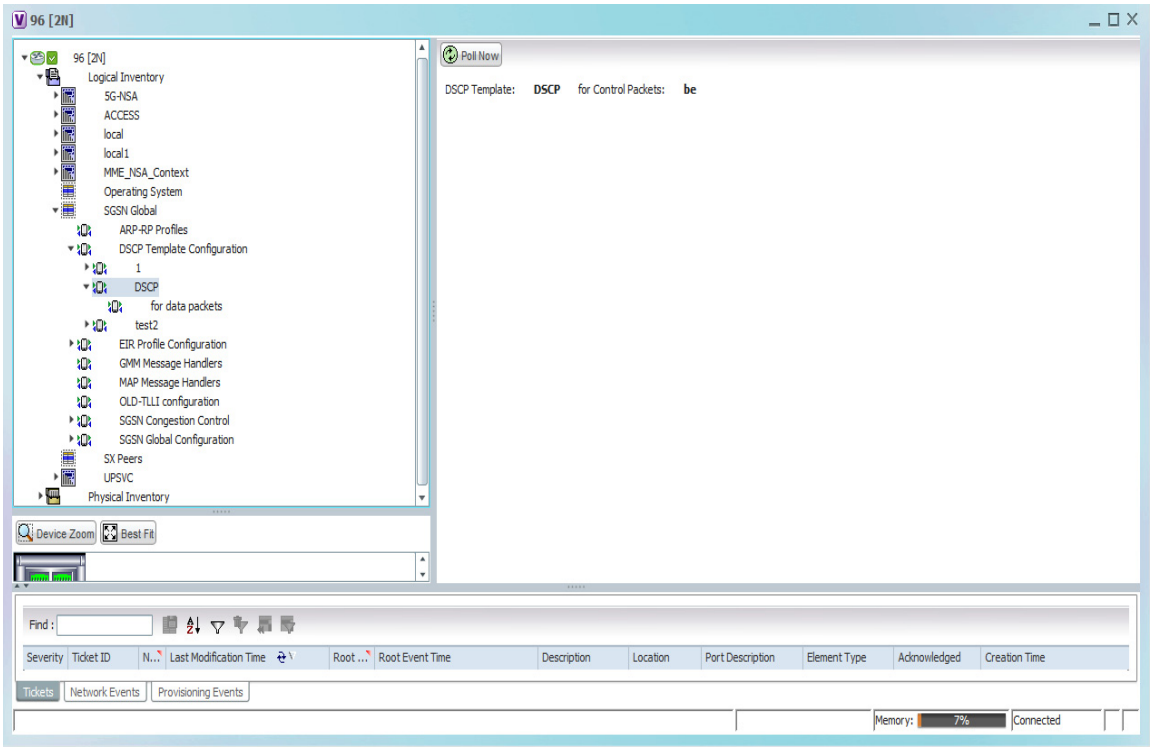
Field	Description
BSSGP Timer-T2	Shows the BVC Reset procedure guard timer.
BSSGP Timer-Th	Shows the MS flow control parameter validity timeouts.

4. SGSN Global > SGSN Global Configuration > PDP Deactivation Rate per Session Manager



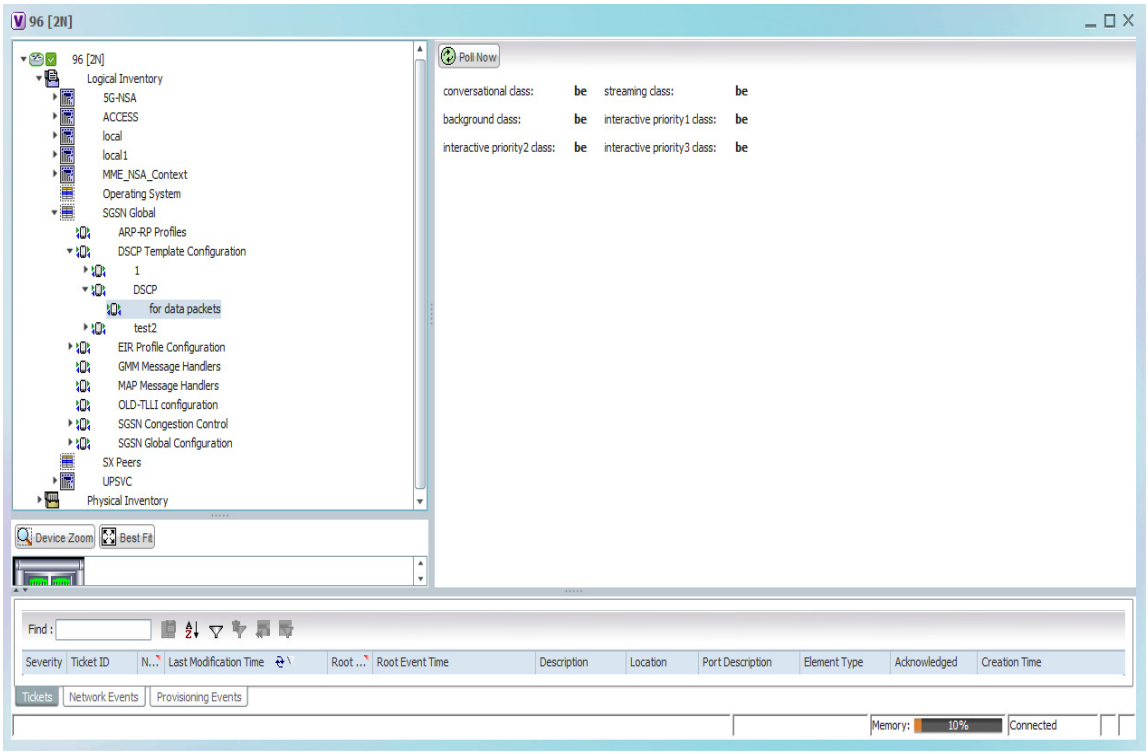
Field	Description
Connected/Ready Mode Subscribers	Shows the message rate for PDP deactivation for Connected/Ready mode subscribers
Idle/Stand-By Mode Subscribers	Shows the message rate for PDP deactivation for Idle/Standby mode subscribers

5. SGSN Global > DSCP



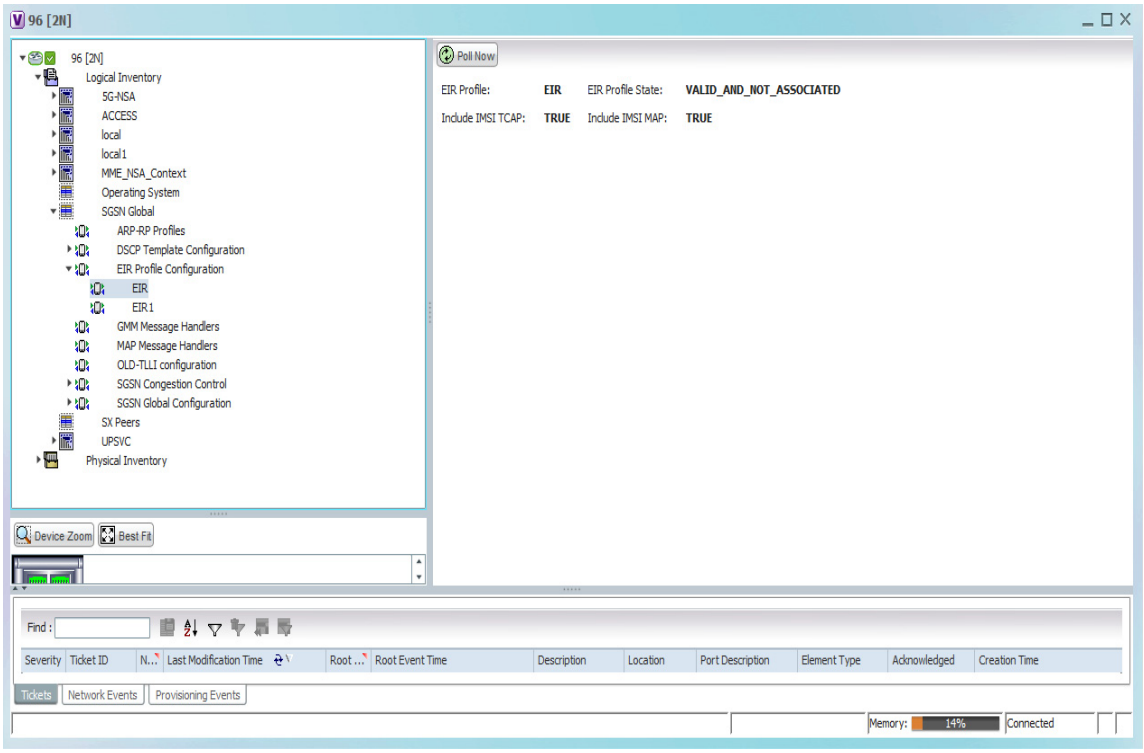
Field	Description
DSCP Template	Shows the name of the DSCP template
for control packets	Shows the DSCP value for the control packet class.

6. SGSN Global > DSCP Template Configuration > DSCP > for data packets



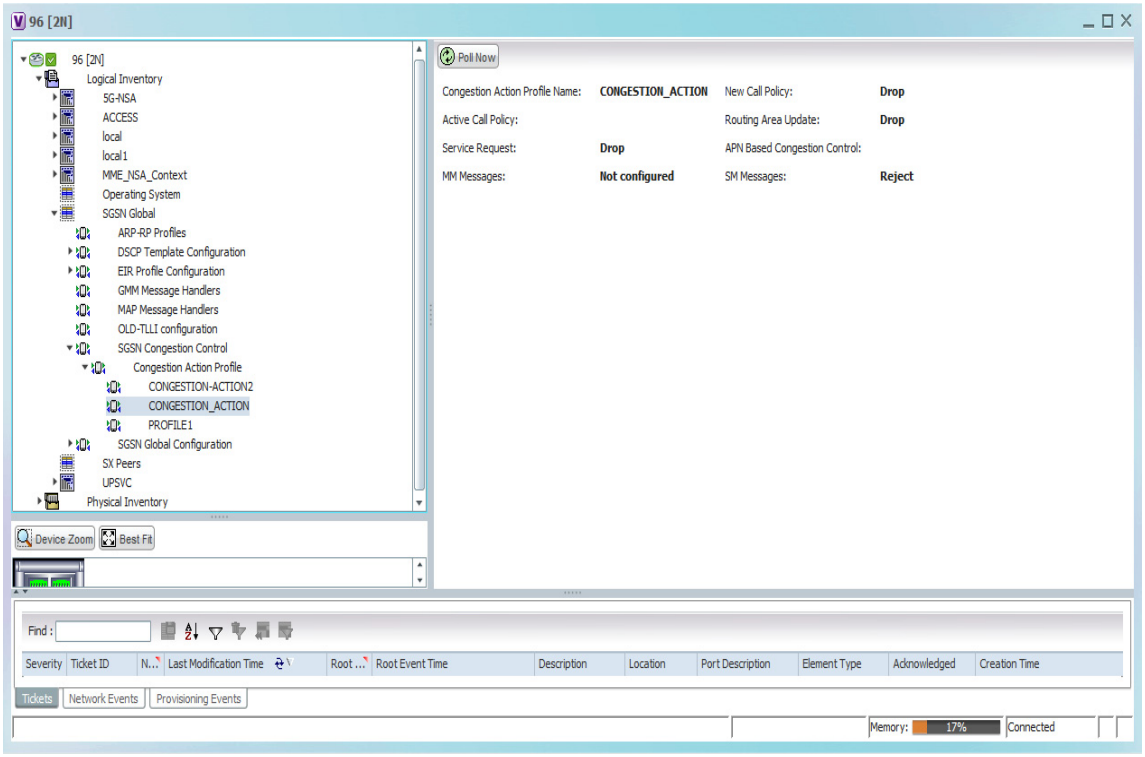
Field	Description
conversational class	Specifies the conversational data packet class
streaming class	Specifies the streaming data packet class
background class	Specifies the background data packet class
interactive priority1 class	Specifies the interactive priority 1 data packet class
interactive priority2 class	Specifies the interactive priority 2 data packet class
interactive priority3 class	Specifies the interactive priority 3 data packet class

7. SGSN Global > EIR Profile Configuration > *EIR Profile*



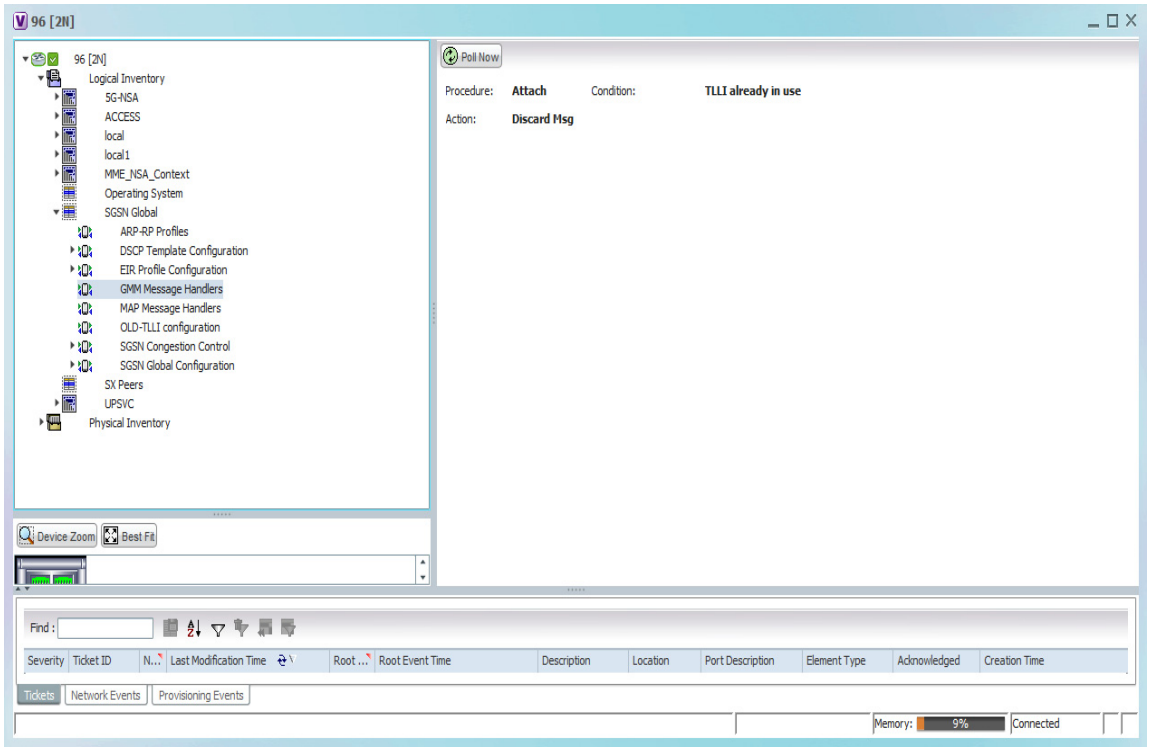
Field	Description
EIR profile	Name of the EIR profile
EIR profile state	State of the EIR profile
Include IMSI TCAP	Specifies if IMSI in TCAP for MAP-CHECK-IMEI operation is included or not
Include IMSI MAP	Specifies if IMSI in MAP for MAP-CHECK-IMEI operation is included or not

8. SGSN Global > SGSN Congestion Control > Congestion Action Profile > *Congestion_Action_Profile*



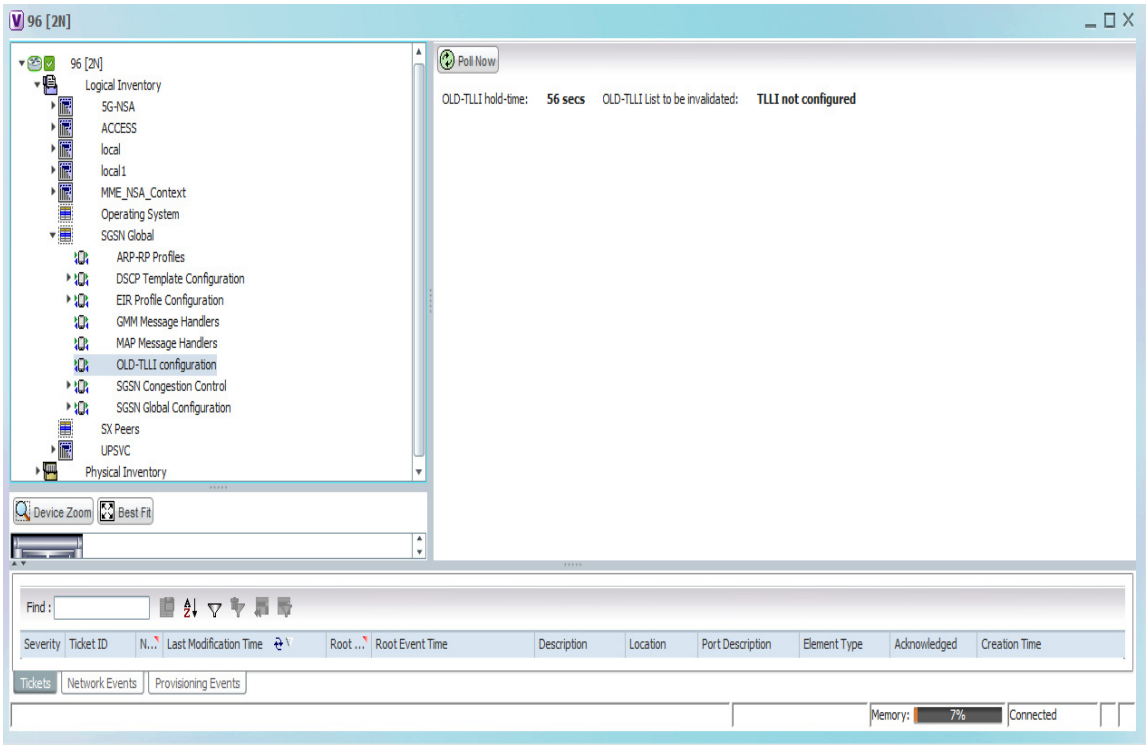
Field	Description
Congestion Action Profile Name	Name of the congestion action profile
New Call Policy	Specifies the congestion control policy for new calls
Active Call Policy	Specifies the congestion control policy for active or existing calls
Routing Area Update	Specifies the congestion control policy for Routing Area Update messages
Service Request	Specifies the congestion control policy for Service Request messages
APN Based Congestion Control	Specifies APN Based congestion control policy
MM messages	Specifies the congestion control policy for for Mobility Management messages
SM messages	Specifies the congestion control policy for Session Management messages

9. SGSN Global >GMM Message Handlers



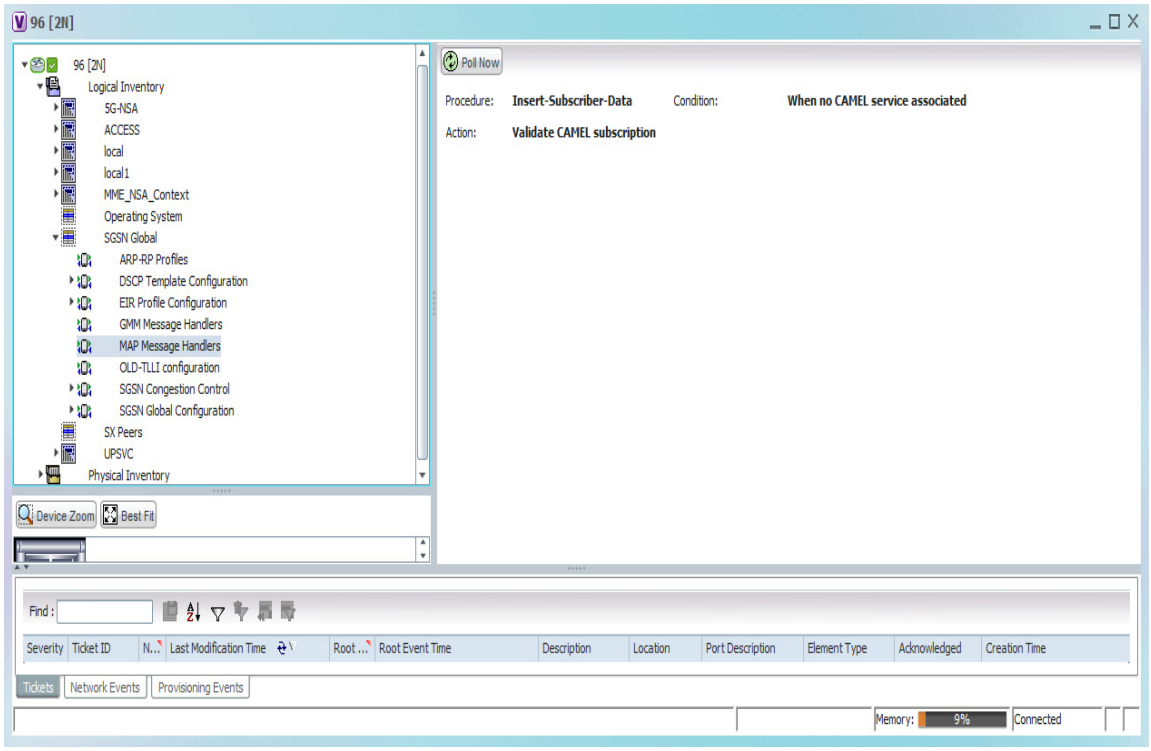
Field	Description
Procedure	Specifies the action to be taken for the reception of a GMM message with particular cause or reason; Specifies the action to be taken for the reception of ATTACH request with TLLI already in use. By default, SGSN process the ATTACH request
Condition	
Action	

10. SGSN Global > OLD-TLLI configuration



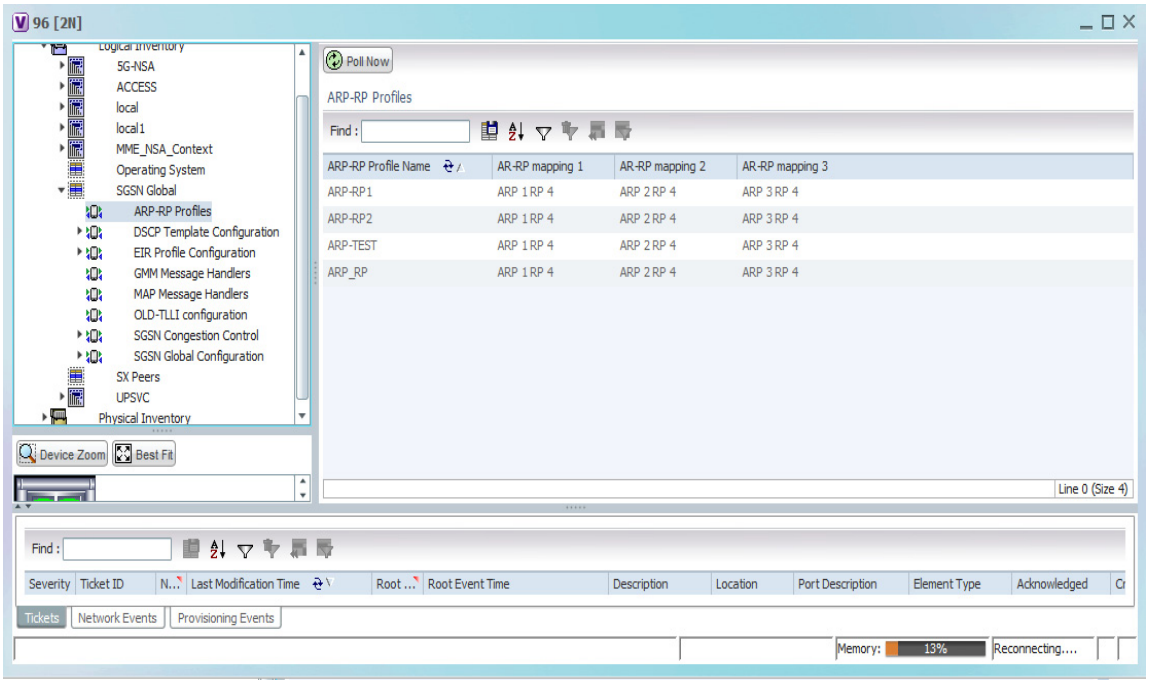
Field	Description
OLD-TLLI hold-time	Timer value to invalidate the old TLLI.
OLD-TLLI List to be invalidated	Specifies the OLD-TLLI list, which is mapped to a subscriber upon time expiry, to be invalidated.

11. SGSN Global > MAP Message Handlers



Field	Description
Procedure	Specifies the following: • Action to be taken on the reception of a MAP message with a particular cause or reason. • Insert Subscriber Data (ISD) message type • Handling of CAMEL subscription information received as part of the ISD message • Action to be taken for the CAMEL subscriber (ISD message with CAMEL subscription) when no camel service associated. By default, it validates for the camel subscription. Ignores the validation of camel subscription if there is no camel service associated.
Condition	
Action	

12. SGSN Global > ARP-RP Profiles



Field	Description
ARP 1 RP 4	Specifies the alloc/reten priority and radio priority
ARP 2 RP 4	
ARP 3 RP 4	

Monitoring the Iu PS Services

The Radio Network Controller (or RNC) is a governing element in the UMTS radio access network (UTRAN) and is responsible for controlling the Node Bs that are connected to it. This is the point where encryption is done before user data is sent to and from the mobile.

The RNC connects to the Circuit Switched Core Network through Media Gateway (MGW) and to the SGSN (Serving GPRS Support Node) in the Packet Switched Core Network. The interface between the RNC and the Circuit Switched Core Network (CS-CN) is called Iu-CS and between the RNC and the Packet Switched Core Network is called Iu-PS.

The Iu PS interface is very important in the UMTS network and it's function include:

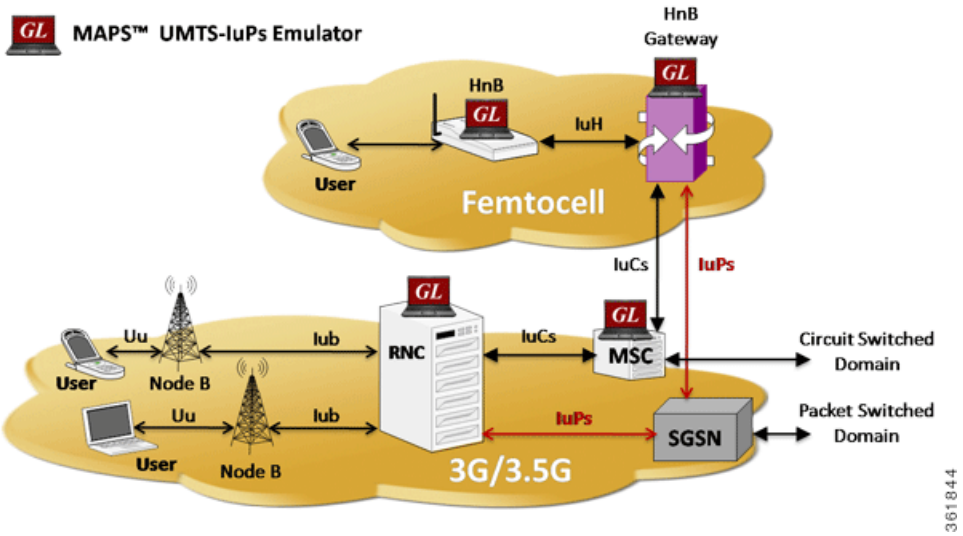
- Radio Access Bearer (RAB) (wireless access bearing) establishment, maintenance and release process
- Changing-over inside the system, changing-over between systems and Serving Radio Network Subsystem (SRNS) reorientation process
- Community radio service process
- Series of general process irrelevant with specific User Equipment (UE)

- Specific signal management for users and separation process on protocol level for each UE
- Transmission process of Network-attached storage (NAS) signal message between UE and CN
- Location service requested from UTRAN to CN and transfer process of position information from UTRAN to CN and resources reserve mechanism

The Iu PS interface mainly analyzes the basic process of the application part of the wireless network, service process of mobility management, service process of conversation management, and statistical values of related Key Performance Indicators (KPI).

Figure 27-3 denotes the architecture of the Iu PS service.

Figure 27-3 Iu PS Service Architecture



To view the Iu PS configuration:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > **Iu PS**. The list of Iu PS Services are displayed in the content pane.

Step 3 In the Iu PS section, double-click on an Iu PS service. The **Iu PS service** window is displayed.

Table 27-25 describes the Iu PS service properties.

Table 27-25 Iu PS Service Properties

Field	Description
Name	The Iu PS service name.
Status	The status of the Iu PS service, which can be any one of the following: • Initiated • Running • Down • Started • Not Started
PLMN ID	The Public Land Mobile Network (PLMN) ID associated with the Iu PS service, which is basically a combination of the Mobile Country Code (MCC) and the Mobile Network Code (MNC).
Network Sharing	Specifies whether network sharing is enabled or disabled.
DSCP Template	Specifies the configuration of the Differentiated Services Code Point (DSCP) for the Iu PS service.
Iu Connection Hold	Specifies whether the Iu connection hold is enabled or disabled. By default, the Iu Connection is held only when requested by MS.
Iu Connection Hold Timer	The time required for the Iu connection hold.
Iu Release Complete Timer	The time interval (in seconds) for which the SGSN waits for Iu release to complete from RNC. The default value is 10 seconds.
Security Mode Complete Timer	The time interval (in seconds) for which the SGSN waits for security mode to complete from MS.
Follow-on for Service Request	Iu established as the result of a Service Request (signaling), the SGSN, by default, waits for the Iu Hold Timer to expire. The service request can be enabled or disabled.
SGSN Initiated Reset	Specifies whether the SGSN RESET procedure initiation is enabled or disabled.
Reset Ack Timer	Specifies the time interval (in seconds) for which the SGSN waits for reset acknowledgment (RESET-ACK) from the RNC.
Reset Maximum Retransmissions	Specifies the maximum retries for the RESET message.
Reset Guard Timer	Specifies the time interval (in seconds) after which the SGSN sends reset acknowledgment (RESET-ACK) to the RNC.
Tin-Tc Timer	Specifies the Tin-Tc time interval (in seconds). SGSN decrements the traffic level of the RNC by one after Tin-Tc interval. The default value is 30 seconds.
Tig-Oc Timer	Specifies the Tig-Oc time interval (in seconds). SGSN ignores any overload messages for Tig-Oc interval after one overload message. The default value is 5 seconds.

Table 27-25 Iu PS Service Properties

Field	Description
RAB Assig Response Timer	The time required to complete the RAB assignment procedure.
SRNS Ctx Response Timer	The time required to wait for a response to the SRNS context request message.
Relocation Complete Timer	The total time required to wait for a response from the relocation request message.
Relocation Alloc Timer	The allocated time required to wait for a response for the relocation request message.
Consecutive sec-fail local messages	Specifies whether intra RAU, service request, or detach requests from local PTMSI is enabled or disabled.
Consecutive sec-fail Non-Local messages	Specifies whether attaches, inter-rat, inter-service RAU is enabled or disabled.
Consecutive sec-fail local messages count	Specifies the number of intra RAU, service request, or detach requests from local PTMSI.
Consecutive sec-fail Non-Local messages count	Specifies the number of attaches, inter-rat, and inter-service RAU.
Security failure during inter-sgsn-rau	Specifies the inter SGSN routing area update status. Enabled or disabled.
MBMS Broadcast mode	Specifies the Multimedia Broadcast Service status. Enabled or disabled.
MBMS Multicast mode	Specifies the Multimedia Multicast Service status. Enabled or disabled.
Empty-CR Procedure	Specifies whether the empty CR procedure is rejected or continued.
Loss of Radio Coverage Detection Cause in Iu Release	Specifies the detection cause number, which will be included in the Iu Release message.The detection cause number identifies the reason for loss of radio coverage (LORC).
RAI validation in Attach	Specifies whether check is done as per 3GPP for MCC or MNC fields of earlier RAI IE in Attach or RAU.
Source-RNC as Target-RNC	Enables source RNC to be used as target RNS during intra-srns.
Network-sharing Failure-code	Configures the reject cause code to be included in network sharing Reject messages.
Check CS/PS Co-ordination	Enables or disables the SGSN service to perform a CS-PS coordination check.
Non-shared Support	Specifies if non-shared area access is Enabled or Disabled. This applies when network-sharing is enabled.
Use Old Location in SCDR and ULI	Displays old value of LAC/RAC/SAC for SCDRs and ULI information to GGSN during intra SRNS procedure.

Step 4 In the **Iu PS** section, double-click on a GTPU Header. The **GTPU Header** window is displayed.

Table 27-26 describes the GTPU header properties.

Table 27-26 GTPU Header Properties

Field	Description
GTP-U Bind Address	Binds Iu PS service GTPU endpoint to IP address.
GTP-U Echo	Specifies whether the GTPU echo is enabled or disabled. By default, it is disabled.
GTP-U Echo Interval	Specifies the echo interval (in seconds) for GTPU. Default is disabled.
GTP-U Max Retries	Specifies the maximum number of transmission retries for GTPU packets.
GTP-U Retransmission Timeout	Specifies the retransmission timeout of GTPU packets, in seconds, ranging from 1 to 20. The default value is 5 seconds.
GTP-U Sync Echo with Peer	Restarts path management when echo request from peer is received.
GTPU Address Blacklisting	Specifies if the GTPU bind address is enabled or disabled. The GTPU bind address (loopback address) will not be used (is blacklisted) in RAB-Assignment requests after a RAB assignment request, with that GTP-U bind address, has been rejected by an RNC with the cause - Unspecified Error. This is a failure at the RNC's GTP-U IP interface.
GTPU Address Blacklist Timer	Specifies the time period that a GTP-U bind address (loopback address) will not be used (is blacklisted) in RAB-Assignment requests after a RAB assignment request, with that GTP-U bind address, has been rejected by an RNC with the cause.

Step 5 In the **RNCs** section, double-click on an RNC ID. The **Radio Network Controller Properties** window is displayed.

Table 27-27 describes the RNC properties.

Table 27-27 Radio Network Controller Properties

Field	Description
ID	The unique code of the RNC configuration, which can be any value between 0 and 65535.
Status	The status of the RNC configuration, which can be any one of the following: • Initiated • Running • Down • Started • Not Started

Table 27-27 Radio Network Controller Properties (continued)

Field	Description
PLMN ID	The PLMN ID associated to the RNC configuration. **Note** All the RNCs associated with an Iu PS service will be assigned the same PLMN ID.
Location and Routing Area Codes	
LAC	The Location Area Code applicable to the RNC. **Note** The area covered by the PLMN ID is divided into different location areas. Each location area is identified by a unique identifier called the Location Area Identity, which is internationally used for updating location of mobile subscribers.
RACs	The Routing Area Code applicable to the RNC, which is used to identify a routing area within a location area.

Step 6 In the **RNCs** section, choose **RNC ID** > **General Characteristics**. The **RNC General Characteristics** window is displayed.

Table 27-28 describes the RNC general characteristics.

Table 27-28 RNC General Characteristics

Field	Description
State	State of the RNC. Up or Down.
ss7-point-code	The SS7 point code in dotted-decimal notation or decimal format.
RNC Description	The description provided for the RNC.
Non-search-ind IE in Paging	Include the non-searching-indication flag in the page-request message.
Direct Tunnel	Restricted or not restricted. Direct Tunnel allows RNC to send data directly to GGSN and also from GGSN to the RNC.
Rab Modify Procedure	Specifies the type of modification procedure to be used to establish the radio access bearer (RAB) assignment.
Rab Asymmetry Indicator	Specifies the RAB asymmetry indicator set in RAB assignment request. For example, Force Asymmetric Bidirectional for Symmetric Bidirectional.
Max IuConId per msg	The Iu-ConIds to be sent in reset resource.

Table 27-28 RNC General Characteristics (continued)

Field	Description
Pooling for Iu-flex	Enabled or Disabled. The Iu-flex, when enabled, creates a pool area. The pool area contains multiple MSC's or SGSN service areas. In the pool area, an UE roams freely without changing the serving core network node. The Iu-flex enables a RAN node to route the information to different CN nodes, and load balances among MSCs and SGSNs.
E-NodeB Direct Data Forwarding	Enabled or Disabled. When enabled, determines the direct forwarding path in the source eNodeB and indicates to the source MME. If X2 connectivity is available between the source and target eNodeBs, a direct forwarding path is available.

Step 7 In the **RNCs** section, choose **RNC ID** > **Overload Control Procedure Actions**. The **Overload Control Procedure Actions** window is displayed.

Table 27-29 describes the Overload Control Procedure Actions.

Table 27-29 Overload Control Procedure Actions

Field	Description
Ptmsi reallocation	Specifies not to perform PTMSI reallocation when it can be skipped. It is performed when the level reaches more than the configured traffic level.
Authentication challenge	Specifies not to perform authentication challenges when it can be skipped. It is performed when the level reaches more than the configured traffic level.
SMS	Specifies not to send SMS-related signaling. It is performed when the level reaches more than the configured traffic level.
Service Request (Data)	Specifies not to accept service request (data, for example, new RABs). It is performed when the level reaches more than the configured traffic level.
Downlink Data Paging	Specifies to ignore downlink data when RABs are not available. No paging for data. It is performed when the level reaches more than the configured traffic level.
Modify PDP Request	Specifies to reject new modify PDP context requests. It is performed when the level reaches more than the configured traffic level.
Activate PDP Request	Specifies to reject new activate PDP context requests. It is performed when the level reaches more than the configured traffic level.
Attach Request	Specifies to reject new attach requests. It is performed when the level reaches more than the configured traffic level.
Srns	Specifies to reject new SMS requests (intra and inter). It is performed when the level reaches more than the configured traffic level.

Step 8 In the **RNCs** section, choose **RNC ID** > **RANAP Characteristics**. The **RANAP Characteristics** window is displayed.

Table 27-29 describes the RANAP Characteristics.

Table 27-30 RANAP Characteristics

Field	Description
Allocation Or Retention Priority	The priority of allocation and retention of the service data flow. The ARP contains information about the priority level, the pre-emption capability and the pre-emption vulnerability. The allocation or retention priority resolves conflicts of demands for network resources. The IE is not included in message.
UE Aggregate Maximum Bit Rate	The aggregate bit rate that can be provided across all Non-GBR PDP contexts of a UE. This attribute enables sending of UE AMBR IE in RAB assignment or Relocation request RANAP messages. The IE is not included in message.
Signalling-Indication IE: Rab Assignment Request	Core Network initiates a Radio Access Bearer (RAB) Assignment. The message specifies the Quality of Service parameters. The IE is included in message.
Signalling-Indication IE: Relocation Request	Relocation request message includes the information received from the source RNC and necessary information for the change of bearer(s). The IE is included in message.
Paging Request	A paging request on all paging channels in the GRA and an indication of which network element initiated the page: CN or GERAN is added to the paging request. Paging Area ID uniquely identifies the area, where the paging message shall be broadcasted. The paging area ID is included in message.
EUTRAN Service Handover	Enables the inclusion of the E-UTRAN Service Handover Information Element in RANAP messages. This results in an elimination of potential service denial or disruption issues, and unnecessary signaling. The IE is not included in message.
RFSP ID	The RFSP Index is mapped by the RNC or BSC to locally defined configuration in order to apply specific RRM strategies. The RFSP Index is UE specific and applies to all the Radio Bearers. The IE is not included in message.

Table 27-30 RANAP Characteristics

Field	Description
Extended MBR	Yes or No. If the RAB ASSIGNMENT REQUEST message contains a request of a RAB configuration with Extended Maximum Bit Rate IE and/or Extended Guaranteed Bit Rate IE respectively, if supported Maximum Bit Rate IE and/or Supported Guaranteed Bit Rate IE are greater than 16 Mbps in RAB parameters IE, the CN should indicate that RAB QoS negotiation is allowed. 8640 kbps value, extended MBR IE is used to send the additional value.
Extended GBR	Yes or No. If the RAB ASSIGNMENT REQUEST message contains a request of a RAB configuration with Extended Maximum Bit Rate IE and/or Extended Guaranteed Bit Rate IE respectively, if supported Maximum Bit Rate IE and/or Supported Guaranteed Bit Rate IE are greater than 16 Mbps in RAB parameters IE, the CN should indicate that RAB QoS negotiation is allowed. 8640 kbps value, extended MBR IE is used to send the additional value.

Step 9 In the **RNCs** section, choose **RNC ID** > **RANAP Global CoreNetwork**. The **RANAP Global Core Network** window is displayed.

Table 27-31 describes the RANAP global core network.

Table 27-31 RANAP Global Core Network Properties

Field	Description
Paging Request	Specifies to enable the CN to send a paging message to a particular UE. The procedure without response is connectionless. When the UE is idle, paging is performed through a common paging channel; when the UE has already had a Radio Resource Control (RRC) connection, paging is performed via its dedicated RRC connection.
Relocation Request	Once resource allocation for relocating the target RNC fails, the target RNC sends a RELOCATION FAILURE message to the CN. Upon receipt of the message by the CN, the CN sends a RELOCATION PREP FAILURE message to the source RNC. The Iu connection for relocating the target RNC is released. The call continues to be held at the source side.
Reset Procedure	RANAP EPs are classified into: connection-oriented and connectionless. The former is supported by a UE specific signaling connection for transport; the latter is supported by a common signaling connection for transport..All other procedures use connection-oriented service to transport except that Reset and Reset Resource.
Reset-Resource Procedure	RANAP EPs are classified into: connection-oriented and connectionless. The former is supported by a UE specific signaling connection for transport; the latter is supported by a common signaling connection for transport. All other procedures use connection-oriented service to transport except that Reset and Reset Resource.

Step 10 In the **RNCs** section, choose **RNC ID** > **RANAP Paging Cause IE**. The **RANAP Paging Cause IE window** is displayed.

Table 27-32 describes the RANAP Paging Cause IE.

Table 27-32 RANAP Paging Cause IE Properties

Field	Description
GMM-Signalling	Sets paging cause due to GMM signaling. The default value is high priority, 5. Terminating High Priority Signalling
SM-Signalling	Sets paging cause due to SM signaling. The default value is high priority, 5. Terminating High Priority Signalling
SMS-Signalling	Sets paging cause due to SMS signaling. The default value is low priority, 4. Terminating Low Priority Signalling
GS-Signalling	Sets paging cause due to VLR paging request. The default value is high priority, 5. Terminating High Priority Signalling
Conversational Data	Sets paging cause due to conversational data. The default value is high priority, 5. Terminating High Priority Signalling
Streaming Data	Sets paging cause due to due to streaming data. The default value high priority, 5. Terminating High Priority Signalling
Interactive Data	Sets paging cause due to interactive data. The default value is interactive, 2. Terminating Interactive Call
Background Data	Sets paging cause due to background data. The default value is background, 3. Terminating Background Call
MME-Signalling	Sets paging cause from MME due to circuit switchfallback (CSFB). Terminating High Priority Signalling

Step 11 In the **RNCs** section, choose **RNC ID** > **RNC 3GPP**. The **RNC 3GPP** window is displayed.

Table 27-33 describes the RNC 3GPP.

Table 27-33 RNC 3GPP Properties

Field	Description
3GPP Release Compliance	Specifies if 3GPP release compliance is adopted by the RNC. There are two releases supported: 1) Pre-release-7—3GPP release 7 and earlier releases. 2) Release-7—3GPP release 7 and later releases.
Mbr-Up	Maximum bit rate is QoS specification attribute, which sets the maximum bit rate for up link. It can be equal or greater than the Guaranteed bit rate.
Mbr-Down	Maximum bit rate is QoS specification attribute, which sets the maximum bit rate for down link. It can be equal or greater than the Guaranteed bit rate.
Gbr-Up	Guaranteed bit rate is QoS specification attribute, which sets Guaranteed bit rate for up link. It can be equal or lesser than the Maximum bit rate.
Gbr-Down	Guaranteed bit rate is QoS specification attribute, which sets Guaranteed bit rate for down link. It can be equal or greater than the Maximum bit rate.

Viewing IU PS Associations

To view the associated Iu PS services for a SGSN:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Mobile > SGSN** > *SGSN service*. The SGSN details are displayed in the content pane.

Step 3 In the content pane, click the **Iu PS Associations** tab.

Table 27-34 describes details relating to Iu Ps Associations for an SGSN.

Table 27-34 SGSN - Iu PS Association Details

Field	Description
Service Name	The name of the Iu PS service associated to the SGSN.
Context	The context of the Iu PS service.

IU PS Associations Commands

The following IU PS associations commands can be launched from the logical inventory by right-clicking a SGSN service and choosing **Commands > Configuration.** Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-35 IU PS Associations Commands

Command	Navigation	Description
Associate IU PS	Right-click the *SGSN service* > **Commands** > **Configuration**	Use this command to associate an IU PS service.
Dissociate IU PS		Use this command to dissociate an IU PS service.

Working with Small Cell Technologies

With the increased demands on the network, service providers are investing in small cell solutions to help optimize and monetize consumer and business services on mobile devices across 3G and 4G networks.

Prime Network offers a portfolio of licensed small cells for home and office to support multiple deployment environments and technologies.

A Home Node B (HNB) is the 3GPP's term for a 3G femtocell. It is a small low-power cellular base station that is very useful for use at home or a small business. It uses a broadband network to connect to the service provider's network.

Note Femtocell is an important technology and service offering that enables new Home and Enterprise service capabilities for Mobile Operators and Converged Mobile Operators (xDSL/Cable/FFTH plus Wireless). The Femtocell network consists of a plug-n-play customer premise device generically called a Home NodeB (HNB) with limited range radio access in home or enterprise. The HNB will auto-configure itself with the network operators and the user can start making voice, data and multimedia calls.

The advantage of using HNB is superior coverage and capacity, especially while indoors. It also provides better voice quality and battery life.

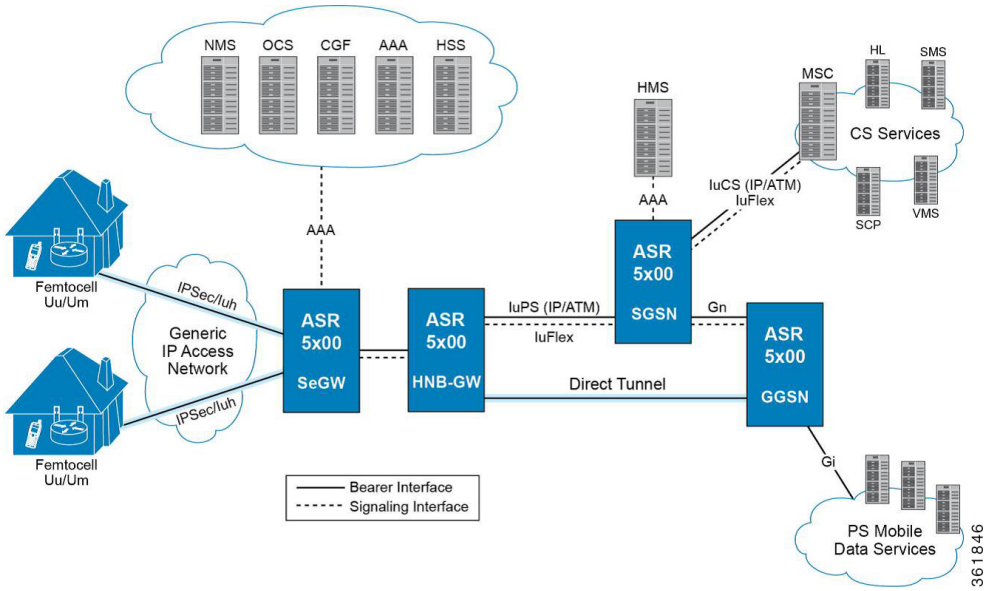
Viewing the Home Node B Gateway Details

The Home Node B Gateway is the HNB network access concentrator that is used to connect the Home Node B (HNBs)/Femto Access Point (FAP) to access the UMTS network through HNB Access Network. It aggregates Home Node-B or Femto Access Points to a single network element and then integrates them into the mobile operators of voice, data and multimedia networks.

The HNB is connected to an existing residential broadband service and provides 3G radio coverage for 3G handsets.

Figure 27-4 depicts the topology of Home Node B Gateway.

Figure 27-4 Home Node B Gateway Topology



Viewing the Home Node B Gateway Configuration

To view the Home Node B Gateway Configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *local* > **Mobile** > **HNB GW**. The HNB GW global configuration details are displayed in the content pane.

Table 27-36 describes the HNB GW Global Configuration details.

Table 27-36 HNB GW Global Configuration Details

Field	Description
NNSF Timer	The NAS (Non-Access Stratum) Node Selection Function (NNSF) timer of the HNB GW, which can be any one of the following values: • any value between 10 and 60 • Disabled **Note** The NNSF timer is used to store the IMSI and the relevant Global-CN-ID. Whenever the MSC sends the paging request with IMSI, the HNB GW stores the Global-CN-ID of the node that issued the request and the timer is started. The HNB GW will store the mapping of the IMSI to the Global-CN-ID until the timer expires.
IMSI Purge Timeout	The purge timeout (in minutes) until which the IMSI White List received from the HMS/BAC during the HNB registration procedure must be maintained in the HNB GW. The field can display any one of the following values: • any value between 1 and 1440 • Immediate • Disabled This field defaults to 1440 (24 hours). The HNB GW waits for the specified time after all referenced HNBs have been de-registered before purging the records.
Alpha RTO	The Alpha Retransmission Timeout (RTO) for the SCTP association between HNB and HNB GW, which can be any value between 0 and 65535.
Beta RTO	The Beta Retransmission Timeout (RTO) for the SCTP association between HNB and HNB GW, which can be any value between 0 and 65535.
Max Incoming Streams	The maximum number of incoming SCTP streams allowed on the HNB GW for an associated HNB-SCTP association. This can be any value between 1 and 16 and defaults to 4.
Max Outgoing Streams	The maximum number of outgoing SCTP streams allowed on the HNB GW for an associated HNB-SCTP association. This can be any value between 1 and 16 and defaults to 4.
Max Re-Tx Association	The maximum number of times the HNB GW is allowed to reach its peer. This number can be any value between 0 and 255, and defaults to 10. **Note** If the number of retransmissions exceed the limit specified here, then the HNB GW considers the peer HNB unreachable and stops transmitting data. The SCTP association is automatically closed.
Max Re-Tx Init	The maximum number of times the HNB GW is allowed to retransmit INIT chunk after the T1-init timer expires. The HNB GW aborts the initialization process once the maximum number of attempts is reached. This can be any value between 0 and 255, and defaults to 5.

Table 27-36 HNB GW Global Configuration Details (continued)

Field	Description
Max Re-Tx Path	The maximum number of times the HNB GW is allowed to access an address after the T3-rtx timer expires. This can be any value between 0 and 255, and defaults to 5. **Note** Every time the T3-rtx timer expires on an address or the Heartbeat sent to an address is not acknowledged, the error counter for that address increases. Once the error counter exceeds the value specified in this field, the destination address is declared inactive.
IU Connection ID Status	Indicates whether the Iu Connection ID status is enabled.
CSG Membership Check	Specifies whether CSG Member check is Enabled or disabled for Non CSG UE's or Non CSG HNB's.
IUPS HNB Session Collocation	Specifies whether the Iu PS interface session is enabled or disabled.
HNBGW Dev Asserts	Enables or disables HNB aggregation support for this HNB gateway service. **Note** Once set, any change in this configuration causes all HNBs in this HNBGW service to get disconnected.
Additional Emergency UEs per HNB	Specifies maximum number of additional emergencies allowed for UE's per HNB in percentage.
IUCS HNB Session Collocation	Specifies whether IuCS interface session is enabled or disabled.

Step 3 In the **Logical Inventory** window, choose **Logical Inventory** > *context* > **Mobile** > **HNB GW**. In the HNB GW node, choose the HNB GW service. The service details are displayed in the content pane.

Table 27-37 describes the HNB GW Service details.

Table 27-37 HNB GW Service Details

Field	Description
Service Name	Specifies the name of the service. The character length of the service name can range from 1 to 63.
CBS Service	The name of the Cell Broadcasting Service (CBS) that is configured to the HNB GW. **Note** CBS is used to reach millions of subscribers instantly with messages. It is very similar to the SMS technology with the added advantage of sending one message to millions of devices instantly. The message is broadcast to all phones connected to the network in the target area.

Table 27-37 HNB GW Service Details (continued)

Field	Description
IPNE Service	The IP Network Enabler (IPNE) service, which defaults to Not Defined. **Note** An IPNE service is used to enable or disable IP based network transfer.
RTP Mux Port	The port number that is allocated to the Real Time Transport Multiplexing protocol.
RTP Mux	Indicates whether Real Time Transport Multiplexing is enabled for the service.
RTP Pool	The IP pool configured to allocate the RTP end point address to the session manager, which can be any value between 1 and 31.
Mismatch Operations	The mismatch handling operation for the HNB GW service.
Open HNB Support	Indicates whether the Open access mode support on the UMTS HNB GW is enabled. **Note** An open access mode provides its services to any subscriber in the femto network. An open access HNB can be deployed in public places to increase indoor coverage or off-load traffic from the macro cell.
Closed HNB Support	Indicates whether the Closed access mode support on the HNB GW is enabled.
Hybrid HNB Support	Indicates whether the Hybrid access mode support on the HNB GW is enabled. **Note** A hybrid access mode provides its services only to those subscribers who are members of the associated access control database.
Status	The status of the HNB GW service, which defaults to Not Defined.
New Call Policy	The new call policy for the security gateway associated to the HNB GW service.
GTP Service	The GPRS Tunneling Protocol (GTP) service associated to the HNB GW service.
Discard OUI	Indicates whether the leading character of the HNB Identification code must be discarded if it contains the Organizational Unique Identifier (OUI).
IURH based Femto-to-Femto handoff	Enables or disables HNB to HNB handoff over IURH for the associated HNB GW service.
IURH handoff guard timer	Guard time, in seconds, for handoff procedure. Default value is 15 seconds.
Override VSA	Enables or disables overriding of particular vendor-specific attributes.
Common Radio PLMN MNC	Specifies the common PLMN ID along with RNC ID.

Table 27-37 HNB GW Service Details (continued)

Field	Description
Multi Operator Core Network (MOCN)	Shows the Common PLMN along with rnc-id. This enables MOCN.
Duplicate Cell-Id Check	Enables or disables the Duplicate-Cell-id validation for a HNBGW-service at HNBGW.
Common Radio PLMN RNC Id	Specifies the common PLMN ID along with RNC ID.
Config Transfer Inner IP Response	Enables or disables the inclusion of inner IP address in HNB configuration that transfer responses for the HNB GW service.
Common Radio PLMN MCC	Specifies the common PLMN ID along with RNC ID.
Common Radio Macro Coverage	Specifies whether to accept or reject registration when the macro coverage IE information is not available in HNB service.
HNB Macro LAI Entries	
MCC	The mobile country code (MCC) portion of the PLMN.
MNC	The mobile network code (MNC) portion of the PLMN.
Location Area Code Start Range	The starting number in the range of LAC.
Location Area Code End Range	The ending number in the range of LAC.

You can also view the following configuration details for a HNB GW service:

- Iu/Iuh—The user data is transferred from HNB to HNB GW through the Iuh interface. Iuh interface is used to carry user traffic and control information whereas the Iu interface is used to transfer CS data as well as PS over IP.
- Paging—The Paging memory management scheme is used to store and retrieve data from a secondary storage.
- SCTP—The Stream Control Transmission Protocol (SCTP) is a transport layer that ensures reliable in sequence transport of messages with congestion control like TCP. It also supports framing of individual message boundaries.
- Security—The policies and configurations specific to security and associated to the HNB GW.
- User Equipment—The user equipment must follow a standard registration procedure to connect to the HNB. This registration process also informs the HNB GW about the location of the HNB where the UE is connected.

Viewing the Iu and Iuh Configuration Details for a Home Node B Gateway Service

To view the Iu or Iuh Configuration details for a HNB GW service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *context* > **Mobile** > **HNB GW >** *hnb gw service* > **Iu** or **Iuh**. The relevant configuration details are displayed in the content pane.

Table 27-38 describes the Iu/Iuh configuration details.

Table 27-38 Iu/Iuh Configuration Details

Field	Description
ScptAny	The Differentiated Services Code Point (DSCP) markings configured over the Iuh interface.
Protocol	The transfer protocol configured for the HNB GW service.
GTPU	The Differentiated Services Code Point (DSCP) configured over the Iu or Iuh interface with the GTPU protocol.
RTP	The DSCP configured over the Iu or Iuh interface with the RTP protocol.
RTCP	The DSCP configured over the Iu or Iuh interface with the RTCP protocol.
Any	The DSCP configured over the Iu or Iuh interface with any protocol.

Viewing the Paging Configuration for a Home Node B Gateway Service

To view the Paging details for a HNB GW service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *context* > **Mobile** > **HNB GW >** *hnb gw service* > **Paging**. The Paging properties are displayed in the content pane.

Table 27-39 describes the Paging details.

Table 27-39 Paging Details

Field	Description
IMSI Life Timer	The International Mobile Subscriber Identity (IMSI) purge time for the HNB GW service, which can be any value between 1 and 12. **Note** The HNB GW maintains IMSI records for a specified period of time, which is usually measured from the time when the user equipment was last de-registered from the HBN GW.
Handle Unknown IMSI (CS)	Indicates whether the CS domain must process or ignore the paging request from the CN node for an IMSI that is not present in the IMSI DB.
Handle Unknown IMSI (PS)	Indicates whether the PS domain must process or ignore the paging request from the CN node for an IMSI that is not present in the IMSI DB.
Last HNB Timeout (CS)	The last known HNB Timeout for the CS domain, which can be any value between 1 and 30.
Last HNB Timeout (PS)	The last known HNB Timeout for the PS domain, which can be any value between 1 and 30.
Paging Grid Fanout Timeout (CS)	The time interval, in seconds, for configuration of grid-based fanout. It is an integer value ranging from 1 to 30. Default timeout value for Circuit Switching (CS) domain and Packet Switching (PS) domain is 5 seconds and 10 seconds, respectively.
Paging Area Fanout Timeout (PS)	The time interval, in seconds, for configuration of area-based fanout. It is an integer value ranging from 1 to 30. Default timeout value for CS domain and PS domain is 5 seconds and 10 seconds, respectively.

Viewing the Radio PLMN Configuration for a Home Node B Gateway Service

To view the Radio PLMN details for a HNB GW service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *context* > **Mobile** > **HNB GW >** *hnb gw service* > **Radio PLMN**. The Paging properties are displayed in the content pane.

Table 27-40 describes the Radio PLMN details.

Table 27-40 Radio PLMN Details

Field	Description
Macro Coverage IE Absent Action	Specifies whether to accept or reject when the macro coverage IE information is not available in HNB.
RNC ID	The unique code used to identify the Radio Network Controller (RNC) connected to the PLMN.
MNC	The mobile network code (MNC) portion of the PLMN.
MCC	The mobile country code (MCC) portion of the PLMN.
HNB Macro LAI Entries	
MCC	The mobile country code (MCC) portion of the PLMN.
MNC	The mobile network code (MNC) portion of the PLMN.
Location Area Code Start Range	The starting number in the range of LAC.
Location Area Code End Range	The ending number in the range of LAC.

Viewing the SCTP Configuration for a Home Node B Gateway Service

To view the SCTP Configuration details for a HNB GW service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *context* > **Mobile** > **HNB GW >** *hnb gw service* > **SCTP**. The SCTP properties are displayed in the content pane.

Table 27-41 describes the SCTP details.

Table 27-41 SCTP Details

Field	Description
Checksum	The type of checksum used to increase data integrity of an SCTP packet, which can be any one of the following: • adler32 • crc32
Connection Timeout	The SCTP association idle timeout (in seconds).
Cookie Life Time	The lifetime of the SCTP cookie (in milliseconds).

Table 27-41 SCTP Details (continued)

Field	Description
Heartbeat Timer	The timer (in milliseconds) of the SCTP heartbeat. **Note** The SCTP heartbeat is sent to a peer to determine reachability. If an acknowledgment is not received from the peer within the specified time, the peer is considered unreachable and further requests are not sent.
Max MTU Size	The maximum size (in bytes) of the Maximum Transmission Unit (MTU) for the SCTP streams allowed by the template, which can be any value between 508 and 65535.
Min MTU Size	The minimum size (in bytes) of the Maximum Transmission Unit (MTU) for the SCTP streams allowed by the template, which can be any value between 508 and 65535.
Start Max MTU	The starting size (in bytes) of the Maximum Transmission Unit (MTU) for the SCTP streams allowed by the template, which can be any value between 508 and 65535.
RTO Initial	The initial time (in milliseconds) for the SCTP Retransmission Timeouts (RTO) allowed by the template, which can be any value between 1 and 1200.
RTO Max	The maximum time (in milliseconds) for the SCTP Retransmission Timeouts (RTO) allowed by the template, which can be any value between 5 and 1200.
RTO Min	The minimum time (in milliseconds) for the SCTP Retransmission Timeouts (RTO) allowed by the template, which can be any value between 1 and 50.
Sack Frequency	The frequency of the SCTP Selective Acknowledgment (sack) allowed by the template, which can be any value between 1 and 5. **Note** Selective Acknowledgment is an extension of SCTP that allows you to acknowledge receipt of specific packets.
Sack Period	The period (in milliseconds) for SCTP selective acknowledgment allowed by the template, which can be any value between 0 and 500.
Binding Address	The binding address associated to the service.
Binding Port	The binding port associated to the service.

Viewing the Security Configuration for a Home Node B Gateway Service

To view the Security details for a HNB GW service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *context* > **Mobile** > **HNB GW >** *hnb gw service* > **Security**. The Security properties are displayed in the content pane.

Table 27-42 describes the Security details.

Table 27-42 Security Configuration Details

Field	Description
Gateway IP Address	The IP Address of the security gateway used by the HNB GW service.
Gateway Context	The name of the context where the AAA server group is defined.
Crypto Template	The crypto template for the security gateway used by the HNB GW service.
IPSec Service	The Internet Protocol Security (IPSec) service used by the HNB GW service.
Newcall Policy	The newcall policy for security gateway in HNB GW service.
IPSec Connection Timeout	The ipsec tunnel idle timeout in hours. Default ipsec tunnel timeout is 4 hrs.

Viewing the User Equipment Configuration for a Home Node B Gateway Service

To view the User equipment details for a HNB GW service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *context* > **Mobile** > **HNB GW >** *hnb gw service* > **UE**. The user equipment properties are displayed in the content pane.

Table 27-43 describes the User equipment details.

Table 27-43 User Equipment Details

Field	Description
Registration Timeout	The timeout interval (in seconds) while connecting the UE with the specified HNB, which can be any value between 60 and 1800.
Handover Status (CS)	Indicates whether the Circuit Switching (CS) handover mode is enabled for the HNB GW service.
Handover Status (PS)	Indicates whether the Packet Switching (PS) handover mode is enabled for the HNB GW service.
Max UEs	The maximum number of user equipment that can be configured for the HNB, which can be any value between 0 and 1000.
Max Unknown UEs	The maximum number of non-access controller user equipment that can be connected to the HNB, which can be any value between 0 and 1000.
Max. UEs Closed	The maximum number of user equipment that can be configured for the HNB in Closed access mode.
Max. UEs Hybrid	The maximum number of user equipment that can be configured for the HNB in Hybrid access mode.
HNB aggregation	Specifies if the HNB aggregation support for the HNB GW service is enabled or disabled.
Maximum number of UEs per HNB	Specifies the maximum number of UEs allowed per HNB, when HNB aggregation is enabled.
Data Path Optimization (CS)	Shows whether the data path optimization for CS domain is enabled or disabled.

Table 27-43 User Equipment Details (continued)

Field	Description
Data Path Optimization (PS)	Shows whether the data path optimization for PS domain is enabled or disabled.
HNB Aggregation Handin	This field is available only when the HNB Aggregation is enabled.

Viewing the Home evolved Node B Gateway Details

The Home evolved Node B (HeNB) provides LTE radio coverage for LTE handsets within a home residential coverage area. A HeNBs incorporate the capabilities of a standard eNodeB.

The Home eNodeB Gateway works as a gateway for HeNBs to access the core networks. The HeNB-GW concentrates connections from a large amount of HeNBs through an interface and terminates the connection to existing Core Networks using the S11 Interface to S-Gateway.

In Prime Network, the following services are available for HeNB GW:

- Access Services—The HeNB GW Access Service is configured to support the interface towards the HeNB(s). This includes the bind address to which the HeNB is connected and which is useful to establish the SCTP associations. If the S1-U relay functionality is enabled for the access service, then the ingress and egress GPRS Tunneling Protocol User Plane (GTPU) services will be associated to this service.
- Network Services—The HeNB GW Network Service is configured to support the interface towards the Mobile Management Entity (MME). This includes the bind address from which HeNB GW will establish SCTP connections to the MME(s). This will support configuration of multiple logical eNodeBs.

To view the Home evolved Node B Gateway Configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *context* > **Mobile** > **HeNB GW**. The HeNB GW configuration details are displayed that includes the HeNB GW Network Services and HeNB GW Access Services tabs. The HeNB GW Network Services tab lists the network services available for HeNB GW and the HeNB GW Access Services tab lists the access services available for HeNB GW.

Step 3 Under the HeNB GW node, choose the *HeNB GW access service*. The access service details are displayed in the content pane.

Table 27-44 describes the HeNB GW Access Services details.

Table 27-44 HeNB GW Access Service Details

Field	Description
Access Service Name	The name of the HeNB GW access service configured on the device.
Status	The status of the access service, which can be any one of the following: • Initiated • Started • Running • Not Started • Down

Table 27-44 HeNB GW Access Service Details (continued)

Field	Description
SCTP IP Address	The SCTP IP Address allocated by the access service to which the HeNB is binded.
SCTP Port	The SCTP port allocated by the access service.
MME Group	The unique code denoting the MME Group that is applicable to the access service.
MME Code	The unique MME Code that is applicable to the access service.
PLMN ID	The Public Land Mobile Network (PLMN) ID that is applicable to the access service.
Security GW Service Address	Designates security gateway address used for HeNBGW access service. Must be followed by IPv4 address, using dotted-decimal notation.
Security GW Context	The context name where crypto template is defined for this HeNBGW access service.
Crypto-Template	Crypto template for security gateway for the associated HeNBGW access service.
Service in IPSec	The name of the service in IPSec.
Associated SCTP Param Template	Parameters allowed by the template for SCTP associations. Refer Table 27-146 for SCTP Template properties.
S1U Relay Status	Indicates whether the S1U Relay is enabled or disabled on the HeNB GW.
X2GW Service	The X2 Gateway (X2GW) service associated with the HeNB access service.
X2GW Context	Context used for X2GW service.

Step 4 Under the selected HeNB GW access service, choose **S1 U Relay Configuration**. The relay configuration details are displayed in the content pane.

Note This node is available only if the S1U Relay Status is enabled for an access service.

Table 27-45 describes the S1 U Relay Configuration details.

Table 27-45 S1 U Relay Configuration Details

Field	Description
GTPU Access Service	The GTPU Access Service available in the HeNB GW. Clicking this link will display the relevant service under the GTPU node.
GTPU Network Service	The GTPU network Service available in HeNB GW. Clicking this link will display the relevant service under the GTPU node.
Downlink QoS	The type of the Downlink DSCP QoS applicable to the S1U Relay on the HeNB GW. For example, be, af11, af12, af13, ef.
Uplink QoS	The type of Uplink DSCP QoS applicable to the S1U Relay on the HeNB GW. For example, af22, af23, af42, af43, ef.

Table 27-45 S1 U Relay Configuration Details (continued)

Field	Description
Downlink QCI DSCP Mapping Table	Name of the QCI-DSCP mapping table to refer the HENBGW ACCESS service towards henb.
Uplink QCI DSCP Mapping Table	Name of the QCI-DSCP mapping table to refer the HENBGW ACCESS service towards sgw.

Step 5 In the **Logical Inventory** window, choose **Logical Inventory** > *context* > **Mobile** > **HeNB GW**. Under the HeNB GW node, choose the *HeNB GW network service*. The network service details, as shown in Table 27-46, are displayed in the content pane.

Table 27-46 HeNB GW Network Service Details

Field	Description
Network Service Name	The name of the HeNB GW network service configured on the device.
Status	The status of the network service, which can be any one of the following: • Initiated • Started • Running • Not Started • Down
ANR Info Retrieval	Automatic Neighbor Relation (ANR) relieves the operator from the complexity of manually managing Neighbor Relations (NRs).This attribute enables the HeNBGW to intercept and respond to the ANR related SON messages with the information requested.
Public Warning System	Public warning system (PWS), which can be any one of the following: Enabled or Disabled.
Default Paging DRX	DRX, a discontinuous reception paging mechanism, decides the procedure that determines sending of messages. Can be v128, v256, v32 and v64.
Paging Rate Control	Maximum paging messages that can be handled by HeNBGW network service per second.
S1AP Max Retransmissions	S1 application protocol provides the signaling service between E-UTRAN and the evolved packet core (EPC), and supports location reporting. Configures the number of times node level S1AP message is retransmitted towards MME.
S1AP Retransmission Timeout	The Node Level S1AP message retransmission timeout in seconds, ranging from 1 to 600. Default is 60 seconds.
SCTP Param Template	Parameters allowed by the template for SCTP associations. Refer Table 27-146 for SCTP Template properties.
PWS Warning Request Timeout	The request timeout value in milliseconds for the PWS.
PWS Kill Request Timeout	The kill request timeout value in milliseconds for the PWS.
PWS Restart Indication Timeout	The restart indication timeout value in milliseconds for the PWS.

Table 27-46 HeNB GW Network Service Details (continued)

Field	Description
Cell Configuration	
PLMN ID	The Public Land Mobile Network (PLMN) ID that is applicable to the network service.
Cell ID	The evolved Node B identification code that is applicable to the network service. **Note** The eNodeB ID allows the HeNB GW to present itself as one or more eNodeBs towards the MME. It is the hardware that is connected to the mobile phone network that communicates directly with the mobile handsets.
SCTP IP Address	The SCTP IP Address applicable to the network service, which represents the bind address to which the HeNB connects and establishes the SCTP associations.
SCTP Port	The SCTP Port applicable to the network service, which helps the HeNB to connect and establish SCTP connection.
TAI List DB	The Tracking Area Identifier (TAI) List applicable to the network service. **Note** Each eNode broadcasts a special tracking area code (TAC) that denotes the tracking area to which the eNode belongs to. The TAI is basically a combination of the PLMN ID and TAC ID.
MME Pool Name	The MME Pool Name applicable to the network service. **Note** The MME Pool Name contains a list of MMEs, which is the key control node for the LTE access network. It is responsible for idle mode user equipment, tracking and paging procedure including retransmissions.
eNodeB Type	Type of eNodeB, which can be one of the following: HOME or MACRO.
SCTP Primary IP Address	The SCTP primary IP address applicable to the network service.
SCTP Secondary IP Address	The SCTP secondary IP address applicable to the network service.
S1 MME IP QoS DSCP	The Quality of Service (QoS) Differentiated Service Code Point (DSCP) used over the S1 MME service.

Configuring Small Cell Technology

The following commands can be launched from the inventory by right-clicking the appropriate node and choosing **Commands** > **Configuration**. Your permissions determine whether you can run these commands. To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Navigation	Input Required and Notes
Create HNB GW	Right-click on a *context* > **Commands** > **Configuration > Small Cell**	Use this command to create a new HNB Gateway service.
Modify HNB GW	*context* > **Mobile** > **HNB GW** > *right-click on a HNB service* > **Commands > Configuration > Modify HNB GW**	Use this command to modify a HNB Gateway service. **Note** You can also delete the CBS service associated to the HNB GW by selecting the **Delete CBS** check box.
Delete HNB GW	*context* > **Mobile** > **HNB GW** > *right-click on a HNB service* > **Commands > Configuration > Delete HNB GW**	Use this command to delete a HNB gateway service.
Show HNB GW	*context* > **Mobile** > **HNB GW** > *right-click on a HNB GW Service* > **Commands > Show**	Use this command to view details of the selected HNB gateway service.
Create PLMN Identifier	*context* > **Mobile** > **HNB GW** > *right-click on a HNB service* > **Commands > Configuration**	Use this command to create a new Public Land Mobile Network (PLMN) for the HNB service.
Modify PLMN Identifier	*context* > **Mobile** > **HNB GW** > *select an HNB service* > In the content pane, *right-click on a PLMN entry* > **Commands** > **Configuration** > **Modify PLMN Identifier**	Use this command to modify PLMN entries for the selected HNB service.
Delete PLMN Identifier	*context* > **Mobile** > **HNB GW** > *select an HNB service* > In the content pane, *right-click on a PLMN entry* > **Commands** > **Configuration** > **Delete PLMN Identifier**	Use this command to delete PLMN entries for the selected HNB service.
Modify Iuh	*context* > **Mobile** > **HNB GW >** Expand the node *hnb gw service* > *right-click* **Iuh** node **> Commands > Configuration**	Use this command to modify IuH interface details for the selected HNB service. **Note** You can delete the protocol for the selected IuH. To delete the protocol, you must specify the Protocol and Payload details.

Command	Navigation	Input Required and Notes
Modify Iu	*context* > **Mobile** > **HNB GW >** expand the *hnb gw service* > *right-click* **Iu** node **> Commands > Configuration**	Use this command to modify Iu Interface details for the selected HNB service.
Modify Paging	*context* > **Mobile** > **HNB GW >** expand the *hnb gw service* > *right-click* **Paging** node **> Commands > Configuration**	Use this command to modify the paging configuration for a HNB GW service.
Modify SCTP	*context* > **Mobile** > **HNB GW >** expand the *hnb gw service* > *right-click* **SCTP** node **> Commands > Configuration**	Use this command to modify the Stream Control Transmission Protocol (SCTP) configuration.
Modify Security	*context* > **Mobile** > **HNB GW >** expand the *hnb gw service* > *right-click* **Security** node **> Commands > Configuration**	Use this command to modify security-specific policies and configurations for the selected HNB service.
Modify UE	*context* > **Mobile** > **HNB GW >** expand the *hnb gw service* > *right-click* **UE** node **> Commands > Configuration**	Use this command to modify the user equipment details for the selected HNB service.
Modify HNB Global	*local* > **Mobile** > *right-click the* **HNB GW** node > **Commands** > **Configuration**	Use this command to modify the HNB Global configuration details.
Show HNB Global	*context* > **Commands** > **Show**	Use this command to view the HNB Global configuration details.
Create HeNB Network	*context* > **Commands** > **Configuration**	Use this command to create a new HeNB network. **Note** You can configure only one HeNB network for a device.
Create Cell Configuration	*context* > **Mobile > HeNB GW >** *right-click the HeNB service* > **Commands > Configuration**	Use this command to create cell configuration details.
Modify Cell Configuration	*context* > **Mobile > HeNB GW >** *networkService* **>** *In the content pane, right-click on the Cell Configuration entry* > **Commands > Configuration**	Use this command to modify cell configuration details.
Delete Cell Configuration		Use this command to delete cell configuration details.
Delete HeNB Network	*context* > **Mobile > HeNB GW >** *right-click on the HeNB service* > **Commands > Configuration**	Use this command to delete an HeNB network.
Show HeNB Network	*context* > **Mobile > HeNB GW >** *right-click on the network service* > **Commands > Show**	Use this command to view HeNB network details.

Command	Navigation	Input Required and Notes
Create HeNB Access	*context* > **Commands** > **Configuration**	Use this command to create HeNB access. **Note** You can configure only one HeNB access for a device.
Modify HeNB Access	*context* > **Mobile** > **HeNB GW** > *right-click the HeNB access service* > **Commands** > **Configuration > Modify HeNB Access** *context* > **Mobile** > **HeNB Access** > *right-click on a HeNB access service* > **Commands > Configuration > Delete HeNB Access**	Use this command to modify HeNB access details.
Delete HeNB Access		Use this command to delete HeNB access details.
Show HeNB Access	*context* > **Mobile** > **HeNB GW** > *right-click the access service* > **Commands** > **Show**	Use this command to view the HeNB access details.
Modify S1U Relay Configuration	*context* > **Mobile** > **HeNB GW** > *HeNB service* > *right-click on the* **S1U Relay Configuration** *node* > **Commands** > **Configuration**	Use this command to modify the S1U Relay Configuration details.

Working with Wireless Security Gateway

The Wireless Security Gateway (WSG) is a highly scalable solution for tunneling femtocell, Unlicensed Mobile Access (UMA)/Generic Access Network (GAN), and 3G/4G macrocell voice and data traffic over fixed broadband networks back to the mobile operator's core network. In a femtocell deployment, WSG uses IP Security (IPsec) to secure the connection between the mobile operator's core network and the "Home Node B" (3G femtocell access point) located at the subscriber's home. In this environment, WSG provides security for trusted hosts (femtocell access points) when they communicate across an external untrusted broadband network such as the Internet. WSG adheres to the latest Third Generation Partnership Project (3GPP) standards for secure remote access over untrusted networks.

In addition to femtocell deployments, WSG can also secure UMA/GAN traffic where the subscriber has a UMA-capable mobile handset that communicates via a Wi-Fi access point over an untrusted network and back to the mobile operator's data center. It can also be deployed to secure 3G/4G base stations that are connected to the mobile operator's network through a third party's carrier Ethernet service.

WSG plays an important role in cost-effectively securing backhaul networks for mobile operators, helping to reduce backhaul costs, which represent a significant part of their operating expenses (OpEx).

To view the security gateway configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> SEC GW**. The Sec GW details are displayed in the content pane.

Table 27-47 describes the Sec GW service details.

Table 27-47 Sec-GW Service Details

Field	Description
Sec GW Lookup tab	
Priority	The priority value for the source and destination subnet size combination, which can be any value between 1 and 6.
Source Net Mask	The subnet size of the source net mask, which can be any value between 1 and 128.
Destination Net Mask	The subnet size of the destination net mask, which can be any value between 1 and 128.
Sec GW Service tab	
Name	The name of the Wireless Security Gateway service.
Status	The status of the WSG service, which can be any one of the following: • Initial • Started
Bind	Indicates whether the WSG service is binded or not. A binded WSG service will have an associated IP Address and Crypto Template.
Max. Sessions	The maximum number of sessions that can be supported by the WSG service, which can be any value between 0 and 8000.
IP Address	The IP address of the WSG service.
UDP Port	The UDP port number of the WSG service.
MTU	The Maximum Transmission Unit (MTU) size before encryption, which can be any value between 576 and 2048.
Crypto Template	The name of the Crypto Template associated with the WSG service.
Deployment Mode	The mode of deployment for the WSG service, which can be any one of the following: • Remote Access—Remote access VPNs connect individual hosts to private networks. Every host must have the VPN client software so that when the host tries to send any traffic, the software encapsulates and encrypts the data before sending it through the VPN gateway at the edge of the target network. • Site to Site—Site to Site VPNs connect networks to each other. In this mode of deployment, the hosts do not have the VPN client software. TCP/IP traffic is sent and received through a VPN gateway, which is responsible for encapsulating and encrypting outbound traffic and sending it to a peer VPN gateway at the target site through a VPN tunnel.
Peer List	The peer list name for WSG service site-to-site mode.
Initiator Mode Duration	The duration WSG tries to initiate or retry a call when peer list is activated (default is 10 seconds).
Responder Mode Duration	The duration WSG waits for the peer to initiate a call when the peer list is activated.
Duplicate Session Detection	Enable duplicate session detection to allow only one IKESA per remote IKE-ID. Default: allow multiple IKESA per remote IKE-ID.

Table 27-47 Sec-GW Service Details (continued)

Field	Description
IPAllocation Type	The IP address from DHCP server.
DHCP Service Name	The DHCP service to be used when the allocation method is dhcp-proxy.
DHCP Context Name	The context in which the DHCP service is configured.
IP Access Group	The name of an access group.
DHCP IPv4	The IPv4 address of the DHCP server to be sent to the peer.
DHCP IPv6	The IPv6 address of the DHCP server to be sent to the peer.

Viewing the Connected Applications Configuration Details

Connected Applications (CA) provide the ability to host third party applications on or adjacent to Cisco networking infrastructure, and enable programmatic access to networking services in a controlled and consistent manner. Enabling CA will allow the ability to host applications on forge blade on an ASR9K platform. The WSG will be the first application to run on the forge blade, which will then interact with the ASR9K device through the CA.

To view the connected applications configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **SEC GW**. The Vision client displays the connected applications details in the content pane.

Table 27-48 describes the connected applications details.

Table 27-48 Connected Applications Details

Field	Description
Session User ID	The ID of the user who has connected into the Connected Application session.
Session Name	The name of the Connected Applications session. The name is configured statically through the StarOS CLI before the session is established.
Session ID	The unique ID of the Connected Applications session. The ID is configured statically through the StarOS CLI before the session is established.
Session IP Address	The IP Address of the Connected Applications session. This address is configured statically through the StarOS CLI before the session is established.
Session Activation	Indicates whether the Connected Applications session is active. **Note** Two different connected applications clients must be able to connect to the same CA server so that one is considered active and the other standby.
RRI Mode	The Recursive Route Injection mode applicable to the Connected Applications session, which can be **RAS**, **S2S**, **Both,** and **None**.
CA Certificate Name	CA Certificate Name in the connected applications session.

Table 27-48 Connected Applications Details (continued)

Field	Description
HA Chassis Mode	The Chassis mode applicable to the Connected Applications session, which can be **Inter**, **Intra**, and **Standalone**.
HA Network Mode	The network mode for the Connected Applications session, which can be **L2**, **L3**, and **NA**.
SRP Status	The Service Redundancy Protocol status of the Connected Applications session, which can be any one of the following: UP, DOWN, ON, OFF, INIT, FAIL, REMOVED, ADMIN DOWN.
SRP State	The state of the connected applications session, which can be any one of the following: UP, DOWN, ON, OFF, INIT, FAIL, REMOVED, ADMIN DOWN.

The following nodes in Prime Network are also configured for WSG:

- Crypto Template—A Crypto Template is a master file that is used to configure an IKEv2 IPSec policy. It includes most of the IPSec parameters and IKEv2 dynamic parameters for cryptographic and authentication algorithms. A security gateway service will not function without a configured crypto template and you can configure only one crypto template for a service.
- Crypto Map—Crypto Maps define the tunnel policies that determine how IPSec is implemented for subscriber data packets. It selects data flows that need security processing and then defines policy for these flows and the crypto peer that traffic needs to go to. It is ultimately applied to an interface.
- IKE SA— Internet Key Exchange (IKE or IKEv2) is the protocol used to set up a security association (SA) in the IPsec protocol suite. The security associations define which protocols and algorithms should be applied to sensitive packets, and also specifies the keying material to be used by the two peers. If IKE is used to establish the security associations, the security associations will have lifetimes set so that they periodically expire and require renegotiation, thus providing an additional level of security.
- Child IPSec SA—A Child-SA is created by IKE for use in Authentication Header (AH) or Encapsulating Security Payload (ESP) security. Two Child-SAs are created as a result of one exchange – Inbound and Outbound. A Child-SA is identified by a single four-byte SPI, Protocol and Gateway IP Address and is carried in each AH/ESP packet.
- Transform Sets—Transform Sets define the negotiable algorithms for IKE SAs (Security Associations) and Child SAs to enable calls to connect to the ePDG. For more information, see Viewing the Transform Set Details, page 27-154.
- CA-Certificates—Certificate or Certification Authority (CA) is an entity that issues digital certificates, which certifies the ownership of a public key by the named subject of the certificate. This allows others (that is, relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. In this model of trust relationships, CA is a trusted third party that is trusted by both the subject (that is, owner) of the certificate and the party relying upon the certificate.

Viewing the Crypto Template Configuration Details

To view the crypto template configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Security Association** > **Crypto Template** > Double click on any template name and check NATT attributes.

Table 27-49 NATT Attributes

Field	Description
NATT Include Header	Specifies that NATT includes header.
NATT	Indicates that the NAT-T initiation is enabled for all security association, which is derived from the crypto map.
NATT Send Keepalive Interval	Shows the NAT-T sending frequency for security gateway keepalive interval in seconds.
NATT Send Keepalive IdleInterval	Displays the waiting period in seconds. The displayed waiting period is before the security gateway starts sending NAT keepalive.
IKEv2 MTU Size IPv4	The MTU size of the IKEv2 payload for IPv4 tunnel.
IKEv2 MTU Size IPv6	The MTU size of the IKEv2 payload for IPv6 tunnel.
CERT Enc Type URL Allowed	Indicates that CERT enc type other than the default type is enabled or not.
Custom FQDN Allowed	Shows whether the custom FQDN is enabled or disabled for a SecGW service.
DNS Handling	Indicates the DNS handling behavior for a crypto template.

Choose > *Context* > **Security Association** > **Crypto Template** > Double-click on any *Crypto Template* > **Payload Tab** > Double Click on any entries and check remaining attributes here. The Vision client displays the details of Crypto Template in the content pane.

Table 27-50 describes the Crypto Template configuration details.

Table 27-50 Crypto Template Properties in Logical Inventory

Field	Description
Type	Indicates the version of the Internet Key Exchange protocol that is configured, which can be IKE v1 or IKE v2.
Status	The completion status of the template, which indicates whether the template is configured with the required properties to establish secure tunnel between local and remote peers. The status can be: • Incomplete–The template needs to be configured further before applying or associating to a security gateway service. • Complete–All properties/attributes are configured.

Table 27-50 Crypto Template Properties in Logical Inventory (continued)

Field	Description
Access Control List	The status of the blacklist/whitelist subscribers attached to the crypto template, which can be **enabled** or **disabled**. **Note** The Blacklist or Whitelist is a list based on which the ISP allows traffic or denies services to a particular subscriber. Rules are configured on each list, and this list is then applied to the traffic.
Remote Secret List	The remote secret list applicable to the crypto template. **Note** The remote secret list contains a list of secret IP addresses. When an authorization request is received, peer ID is checked in this list
OCSP Status	Indicates whether the Online Certificate Status Protocol applicable to the crypto template is enabled or disabled. **Note** The OCSP is an Internet protocol that is used to obtain the revocation status of an x.509 digital certificate.
OCSP Nonce Status	Indicates whether the OCSP nonce applicable to the crypto template is enabled or disabled. **Note** An OCSP may contain a nonce request extension to improve security against replay attacks.
Self Certificate Validation	Indicates whether the self certificate validation for the crypto template is enabled or disabled. **Note** Self Certificate Validation indicates the certificate that is signed by the entity whose identity it certifies.
Dead Peer Detection	Indicates whether the Dead Peer Detection for the crypto template is enabled or disabled. **Note** The Dead Peer Detection method detects a dead Internet Key Exchange peer and reclaims the lost resource. This method uses IPSec traffic patterns to minimize the number of messages required to confirm the availability of a peer. It is also used to perform IKE peer failover.
Payload Identifier	The name of the payload, which can be any one of the following: • Phase-1—contains IPv4 Address and Key ID as the payload values. • Phase-2 SA—contains IPv4 Address and Subnet as the payload values.

Table 27-50 Crypto Template Properties in Logical Inventory (continued)

Field	Description
IKE Mode	The Internet Key Exchange (IKE) mode for the crypto template, which can be any one of the following: • Main Mode–In this mode, the initiator sends a proposal to the responder. In the first exchange, the initiator proposes the encryption and authentication algorithms to be used and the responder chooses the appropriate proposal. In the second exchange, the Diffie-Hellman public keys and other data are exchanged. In the last and final exchange, the ISAKMP session is authenticated. Once the IKE SA is established, IPSec negotiation begins. • Aggressive Mode–In this mode, the initiator sends three packets that contain the IKE SA negotiation along with the data required by the security association. The responder chooses the proposal, key material, and ID and authenticates the session in the next packet. The initiator replies to this by authenticating the session. When compared to the Main Mode, negotiation is much quicker in this mode.
Perfect Forward Secrecy	The Perfect Forward Secrecy (PFS) value for the crypto template. **Note** To ensure that derived session keys are not compromised and to prevent a third party discovering a key value, IPSec uses PFS to create a new key value based on values supplied by both parties in the exchange.
Number of IPSec Transforms	The number of IPSec transforms applicable for the crypto template. **Note** An IPSec transform specifies a single IPSec security protocol (either AH or ESP) with its corresponding security algorithms and mode. For example, the AH protocol with HMAC with MD5 authentication algorithm in tunnel mode is used for authentication.
Local Gateway Address	The IP Address of the responder, which represents the local end of the security associations.
Remote Gateway Address	The IP address of the initiator, which represents the remote end of the security associations.
Payload Attributes	
IPv4 PCSCF Payload Value	Defines the IPv4 PCSCF payload value.
IPv6 PCSCF Payload Value	Defines the IPv6 PCSCF payload value.
IMEI Payload Value	Defines the IMEI payload value.
IPv4 Fragment Type	The fragment type when User Payload is ipv4 type and DF bit is not set.
Maximum Child SA	The maximum number of IPsec child security associations, which is derived from a single IKEve IKE security association.
Ignore Rekeying Requests	Ignores rekeying requests for IPsec SA

Table 27-50 Crypto Template Properties in Logical Inventory (continued)

Field	Description
Lifetime	The lifetime in seconds for IPsec Child Security Associations derived from a Crypto Template.
Lifetime (KB)	Shows the lifetime in kilo bytes for IPsec Child Security Associations derived from a Crypto Template.
TSI Start Address	The starting address for the IKEv2 initiator traffic selector payload.
TSI End Address	The ending address for the IKEv2 initiator traffic selector payload.
TSR Start/End Address	The starting or ending address for the IKEv2 responder traffic selector payload.

Viewing the Crypto Map Configuration Details

To view the crypto map configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Security Association > Crypto Map >** *Crypto Maps*. The Vision client displays the map details in the content pane.

Table 27-51 describes the crypto map configuration details.

Table 27-51 Crypto Map Properties in Logical Inventory

Field	Description
Name	The unique name of the crypto map.
Status	The current status of the crypto map, which can be **Complete** or **Incomplete**.
Type	The type of the crypto map, which can be any one of the following: • IPSEC IKEv2 over IPv4 • IPSEC IKEv2 over IPv6
OCSP Status	Indicates whether the OCSP request status is enabled for the crypto map.
Local Authentication	The local authentication method to be used by the crypto map, which can be **Certificate**, **Pre-shared-key**, or **EAP_Profile**.
Remote Authentication	The remote authentication method to be used by the crypto map, which can be **Certificate**, **Pre-shared-key**, or **EAP_Profile**.
OCSP Nonce Status	Indicates whether the OCSP Nonce Status is enabled for the crypto map.
Don’t Fragment	The Control Don’t Fragment number that is available in the IPSec outer header.
Remote Gateway	The IP Address of the remote gateway that is configured in the peer parameters.

Table 27-51 Crypto Map Properties in Logical Inventory (continued)

Field	Description
Access Control List	The status of the blacklist/whitelist subscribers attached to the crypto template, which can be **enabled** or **disabled**. **Note** The Blacklist or Whitelist is a list based on which the ISP allows traffic or denies services to a particular subscriber. Rules are configured on each list, and this list is then applied to the traffic.
Crypto Map Payload tab	
Name	The name of the crypto map payload.
IKESA Transform Sets tab	
Id	The unique ID of the crypto map IKSEA transform set.
Encryption	The encryption algorithm and encryption key length for the IKEv2 IKE security association. This field defaults to AESCBC-128.
PRF	The PRF associated to the crypto map. **Note** The PRF is used to generate keying material for all cryptographic algorithms used in IKE SA and the child SAs. This PRF produces a string that an attacker cannot distinguish from random bit without the secret key.
HMAC	The Hash Message Authentication Code applicable for the crypto map. The HMAC is used to simultaneously verify both data integrity and the authentication of the message.
DH Group	The Diffie-Hellman group that is associated to the crypto map. This group is used to determine the length of the base prime numbers used during the key exchange in IKEv2. The cryptographic strength of any derived key partly depends on the DH group upon which the prime number is based.

Step 3 In the Crypto map Payload tab, right-click a Payload name and select **Properties**. The Crypto Map Payload Properties window is displayed.

Table 27-52 describes the crypto map configuration details.

Table 27-52 Crypto Map Payload Properties

Field	Description
IPSecSA Transform Sets tab	
ID	The unique ID that identifies the crypto map IPSecSA transform set.
Protocol	The transport protocol used at the inbound site, which can be ESP or AH.
Encryption	The encryption algorithm and encryption key length for the IKEv2 IKE security association. This field defaults to **AESCBC-128**.
HMAC	The Hash Message Authentication Code applicable for the crypto map.
DH Group	The Diffie-Hellman group that is associated to the crypto map.

Viewing the IKE SA Configuration Details

To view the IKE SA configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Security Association** > **IKE IPSec SA**. The Vision client displays a list of IKE Security Associations in the content pane.

Step 3 Right-click a IKE SA and choose **Properties**. The IKE IPSec Security Association – Properties window is displayed.

Table 27-53 describes the IKE SA configuration details.

Table 27-53 IKE SA Configuration Details

Field	Description
Remote IP Address	The IP address of the remote gateway.
Local IP Address	The IP address of the local gateway.
Remote WSG Port	Port number of the remote gateway.
Local WSG Port	Port number of the local gateway.
Crypto Map Name	The name of the Crypto Map facilitating the security association.
Authentication Status	The status of the IKE Security Association. This is defined based on the authentication of phase 1 and phase 2 of the SA establishment and can be any one of the following: • Authentication Completed–if authentication is successful for both phase 1 and phase 2. • Authentication Initialization–if authentication is successful for phase 1 but awaiting request from IKE peer for phase 2.
Redundancy Status	The redundancy status of the IKE security association, which can be any one of the following: • Original tunnel—Session recovery is successful. • Recovered tunnel—Session recovery is configured and the IPSec manager instance, on which the tunnel is created, is killed.
Role	The role of the entity that is establishing the security association, which can be any one of the following: • Initiator–The entity that initiated the security association. • Responder–The entity that is responding to the security association.
IPSec Manager	The IPSec manager of the IKE Security Association, which is created and associated to a tunnel.
Send Rekey Requests	Indicates whether the rekey request to be sent to the peer host is enabled. **Note** Rekey refers to the process of changing the encryption key of the ongoing communication, which helps to limit the amount of data encrypted using the same key.
Process Rekey Requests	Indicates whether the rekey request must be processed.

Table 27-53 IKE SA Configuration Details (continued)

Field	Description
Soft Lifetime	The soft lifetime of the IKE security association. When this lifetime expires, a warning message is given to implement the setup for the SA. Setting up involves refreshing the encryption or authentication keys. **Note** The security gateway initiates the rekey request after the soft lifetime expires. This lifetime is calculated as 90 percent of the hard lifetime.
Hard Lifetime	The hard lifetime of the IKE security association. The current SA is deleted on expiration of the hard lifetime. The policies accessing the SA will exist, but they are not associated to an SA.
Dead Peer Detection	Indicates whether the dead peer detection feature is enabled for the security association. **Note** This feature is used to detect dead IKE peer. It also reclaims lost resources if the peer is found dead.
Initiator Cookie	The cookie of the entity that initiated the SA establishment, notification or deletion.
Responder Cookie	The cookie of the entity that is responding to the establishment, notification or deletion request.
Algorithms tab	
DH Group	The Diffie-Hellman group for the IKE SA.
HMAC	The Hash Message Authentication Code applicable for the IKE SA.
Encryption	The encryption algorithm for the IKE security association, which is used to encrypt the data. Information is made into meaningless cipher text, and you need a key to transform this text back into the original form.
PRF	The PRF associated to the IKE SA.
Child-SA Parameters tab	
Current Child-SA Instantiations	The number of instantiations for the child security association.
Total Child-SA Instantiations	The total number of times the child security association is instantiated.
Lifetime	The number of times the child security association is deleted due to lifetime expiration.
Terminations (Other)	The number of times the child security association is deleted due to reasons other than lifetime expiration.
NAT tab	
Sent	Indicates whether the Network Address Translator (NAT) payload can be sent from a peer to NAT gateway.
Received	Indicates whether the NAT payload can be received by the NAT gateway from the peer.
Behind Local	Indicates whether the NAT is available for the local entity.

Table 27-53 IKE SA Configuration Details (continued)

Field	Description
Behind Remote	Indicates whether the NAT is available for the remote entity.
Encapsulation in Use	Indicates whether encapsulation of payload is enabled for IKE SA.
IKEv2 Fragmentation	Indicates whether IKESA fragmentation or re-assembly support.
Child SAs tab	
Id	The unique code of the child security association that is associated to the IKE SA.
SPI	The Security Parameter Index (SPI) that is added to the header while using IP Security for tunneling the traffic. This tag helps the kernel to distinguish between two traffic streams that use different encryption rules and algorithms.

Viewing the Child IPSec SA Configuration Details

To view the Child IPSec SA Configuration Details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Security Association** > **Child IPSec SAs**. The Vision client displays a list of IPSec Security Associations in the content pane.

Step 3 Right-click an IPSec SA and choose **Properties**. The Child IPSec Security Association Properties window is displayed.

Table 27-54 describes the Child IPSec SA configuration details.

Table 27-54 Child IPSec SA Configuration Details

Field	Description
IP Address	The IP address of the local wireless security gateway service that is facilitating the security association.
Remote Peer Address	The IP address of the remote WSG service that is facilitating the security association.
Outbound SPI	The Security Parameter Index (SPI) of the outbound security association.
Inbound SPI	The SPI of the inbound security association.
SA Status	The status of the security association, which can be any one of the following: • Established • Not Established • No SAs
Redundancy Status	The redundancy status of the security association, which can be any one of the following: • Original Tunnel–No failure has occurred. • Recovered Session–A failure has occurred and a recovery session has been created.

Table 27-54 Child IPSec SA Configuration Details (continued)

Field	Description
Crypto Map Name	The name of the crypto map facilitating the security association. This name is derived from the crypto template that is applied to the transform set parameters.
Crypto Map Type	The type of crypto map facilitating the security association, which can be any one of the following: Manual Tunnel, MIP Tunnel, L2TP Tunnel, Subscriber Tunnel, IKEv2 Simulator Tunnel, Dynamic Tunnel, IKEv1 Tunnel, IKEv2 Tunnel, IKEv2 IPv4 Tunnel, IKEv2 IPv6 Tunnel, IKEv2 Simulator Tunnel, IKEv2 Subscriber, IKEv2 IPv4, IKEv2 IPv6, CSCF Subscriber, IMS CSCF Template, IKEv2 Template, IKEv2 Simulator Template.
Allocated Address	The IP address allocated to the Network Access Identifiers (NAI) of the users.
ESN	Enable Extended Sequence Number (ESN) for IPSec (ESP/AH).
Network Address Identifier	The Network Address Identifier (NAI) applicable to the security association, which is used to identify the user as well as to assist in routing the authentication request.
IPSec Manager Instances	The number of IPSec managers facilitating the security association.
Rekeying	Indicates whether rekeying is applicable for the security association.
Rekey Count	The total number of times the tunnel has been rekeyed.
DH Group	The Diffie-Hellman group to which the security association belongs.
Inbound/Outbound tab	
SPI	The SPI of the inbound/outbound security association.
Protocol	The transport protocol used at the inbound/outbound side, which can be any one of the following: • ESP – Encapsulating Security Payload • AH – Authentication Header • PCP – Payload Compression Payload
HMAC Algorithm	The keyed HMAC used for the inbound/outbound security association, which can be **shal-96** or **md5-96**.
Encryption Algorithm	The encryption algorithm used for the inbound/outbound security association, which can be **Null**, **des**, **3des**, **aes-cbc-128**, or **aes-cbc-256**.
Hard Lifetime	The hard lifetime of the security association, on the expiration of which the currently used security association will be deleted.
Soft Lifetime	The soft lifetime of the security association, on the expiration of which WSG initiates a rekey.

Table 27-54 Child IPSec SA Configuration Details (continued)

Field	Description
Anti Replay	Indicates whether the anti replay feature is enabled for the security association. **Note** Anti replay is a sub-protocol of IPSec that prevents hackers from injecting or making changes in packets that travel from a source to destination.
Anti Replay Window Size	The window size (in bits) of the anti-replay feature, which can be 32, 64, 128, 256, 384 and 512.
Traffic Selectors tab	
Id	The unique ID assigned to the traffic selector. **Note** A packet arriving at an IPSec subsystem must be protected through the IPSec tunneling. This is accomplished through the traffic selector, which allows two endpoints to share their information from the SDPs.
Role	The role of the IKE security association, which can be Initiator or Responder.
Protocol ID	The protocol ID for the security association.
Port Range	The range of ports applicable for the security association.
IP Range	The range of IP addresses applicable for the security association.

Viewing the CA Certificate Configuration Details

To view the CA certificate configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Security Association** > **CA Certificates**. The Vision client displays a list of CA Certificates in the content pane.

Step 3 Right-click the CA Certificate and choose **Properties**. The **CA Certificate Properties** window is displayed.

Table 27-55 describes the CA certificate configuration details.

Table 27-55 CA Certificate Configuration Details

Field	Description
Name	The name of the CA certificate.
Status	The status of the CA certificate, which can Valid or Invalid. **Note** A certificate can become invalid if there is an error during the download process, or if the file gets corrupted locally or remotely.

Table 27-55 CA Certificate Configuration Details (continued)

Field	Description
Version	The version of the CA certificate. This version indicates the functionality supported in each version.
Serial Number	The serial number of the CA certificate that is used to uniquely identify it.
Signature Algorithm	The algorithm used to sign the certificate issued with any public key algorithm supported by the CA. For example, ECC signing certificate can sign both ECC and RSA certificates as long as both these algorithms are supported by CA.
Issuer	The details of the CA certificate issues, such as the country, state, location, and organization.
Public Key Algorithm	The public key algorithm that is used to sign the digital signature supported by the CA.
Subject	The details of the owner of the CA certificate, such as the country, state, location, and organization.
Validity Start Time	The date and time from when the CA certificate is valid.
Validity End Time	The date and time up to which the CA certificate is valid.

Configuring Wireless Security Gateway

The following commands can be launched from the inventory by right-clicking AAA group and then choosing **Commands** > **Configuration**. Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the Cisco Prime Network 5.3 Supported Cisco VNEs.

Command	Navigation	Input Required and Notes
Create Sec GW	Right-click a *context* > **Commands** > **Configuration**	Use this command to create a new security gateway.
Modify Sec GW	*context* > **Sec GW** > right-click a *Sec GW service* > **Commands > Configuration**	Use this command to modify a security gateway service.
Delete Sec GW		Use this command to delete a security gateway service.
Show Sec GW	*context* > **Sec GW** > right-click a *Sec GW service* > **Commands > Show**	Use this command to view details of the selected security gateway service.
Create Sec GW Lookup	Right-click the *device* > **Commands > Configuration**	Use this command to create a new security gateway Lookup.
Modify Sec GW Lookup	*context* > **SEC GW** > In the **Sec GW Lookup** tab in the content pane, right-click the ***Priority*** *field* > **Commands > Configuration**	Use this command to modify security gateway Lookup details.
Delete Sec GW Lookup		Use this command to delete security gateway Lookup.

Command	Navigation	Input Required and Notes
Show SEC GW Lookup	Right-click the *device* > **Commands > Show** > **Show SEC GW Lookup** -OR- context > **SEC GW** > In the **Sec GW Lookup** tab in the content pane, right-click the **Priority** field > **Commands > Show**	Use this command to view security gateway lookup details.
Create Crypto Template	Right-click the *context* **> Commands > Configuration**	Use this command to create a new crypto template.
Modify Crypto Template	*context* > **IP Security** > **Crypto Template** > right-click a *crypto template* **> Commands > Configuration**	Use this command to modify details of the selected crypto template.
Delete Crypto Template		Use this command to delete a crypto template.
Show Crypto Template	*context* > **IP Security** > **Crypto Template** > right-click a *crypto template* **> Commands > Show**	Use this command to view crypto template details.
Add Payload	*context* > **IP Security** > **Crypto Template** > right-click a *crypto template* **> Commands > Configuration**	Use this command to add a payload.
Modify Payload	*context* > **IP Security** > **Crypto Template** > select a *crypto template* **>** In the ***Crypto Template Payloads*** tab in the content pane, right-click a *Payload instance* **> Commands > Configuration**	Use this command to modify payload details.
Delete Payload		Use this command to delete a payload.
Modify Crypto Template IKESA	context > **IP Security** > **Crypto Template** > right-click a crypto template **> Commands > Configuration**	Use this command to modify details of the selected Crypto Template IKESA.
Create CA Certificate	Right-click the *device* > **Commands** > **Configuration**	Use this command to create a new CA certificate.
Delete CA Certificate	*context* **> IP Security > CA Certificate** > right-click a *certificate* > **Commands** > **Configuration**	Use this command to delete the selected CA certificate.
Show CA Certificate	*context* **> IP Security > CA Certificate** > right-click a *certificate* > **Commands** > **Show**	Use this command to view the CA certificate details.
Show IKE SAs	context **> IP Security >** right-click **IKE IPsec SA > Commands** > **Show**	Use this command to view details of the selected IKE SA.
Create IKEv2 Transform Set	Right-click the *context* **> Commands > Configuration**	Use this command to create a new IKEv2 transform set.
Modify IKEv2 Transform Set	*context* **> IP Security > Transform Set > IKEv2 >** right-click a *transform set* **> Commands Configuration**	Use this command to modify the IKEv2 transform set details.
Delete IKEv2 Transform Set		Use this command to delete the selected IKEv2 transform set.

Command	Navigation	Input Required and Notes
Show IKEv2 Transform Set	*context* **> IP Security > Transform Set > IKEv2 >** right-click a *transform set* **> Commands** > **Show**	Use this command to view the IKEv2 transform set.
Create IKEv2 IPSec Transform Set	Right-click the *context* **> Commands > Configuration**	Use this command to create a new IKEv2 IPSec transform set.
Modify IKEv2 IPSec Transform Set	*context* > **IP Security** > **Transform Set** > **IKEv2 IPSec >** right-click a *transform set* > **Commands** > **Configuration**	Use this command to modify the details of the selected IKEv2 IPSec transform set.
Delete IKEv2 IPSec Transform Set		Use this command to delete the selected IKEv2 IPSec transform set.
Show IKEv2 IPSec Transform Set	*context* > **IP Security** > **Transform Set** > **IKEv2 IPSec >** right-click a *transform set* > **Commands** > **Show**	Use this command to view details of the selected IKEv2 IPSec transform set.
Modify Connected Apps	Right-click the device > **Commands** > **Configuration**	Use this command to modify the connected application details.
Show Connected Apps	Right-click the device > **Commands** > **Show > Show Connected Apps**	Use this command to view the connected application details.
Create Crypto Map	Right-click the *context* > **Commands** > **Configuration**	Use this command to create a new crypto map.
Modify Crypto Map	*context* > **IP Security** > **Crypto Map** > right-click a *crypto map* > **Commands** > **Configuration**	Use this command to modify the crypto map details.
Delete Crypto Map		Use this command to delete the selected crypto map.
Show Crypto Map	*context* > **IP Security** > **Crypto Map** > right-click a *crypto map* > **Commands** > **Show**	Use this command to view details of the selected crypto map.
Create Crypto Map Payload	*context* > **IP Security** > **Crypto Map** > right-click a *crypto map* > **Commands** > **Configuration**	Use this command to create a new crypto map payload.
Modify Crypto Map Payload	*context* > **IP Security** > **Crypto Map** > select a *crypto map* > In the **Crypto Map Payload** tab in the content pane, right-click the **Name** > **Commands** > **Configuration**.	Use this command to modify details of the selected crypto map payload.
Delete Crypto Map Payload		Use this command to delete the crypto map payload.
Show IPSec SAs	context **> IP Security >** right-click **IKE IPsec SA > Commands** > **Show**	Use this command to view details of the selected IPSec SA.

LTE Networks

These topics describe how to use Prime Network to monitor LTE networks and technologies:

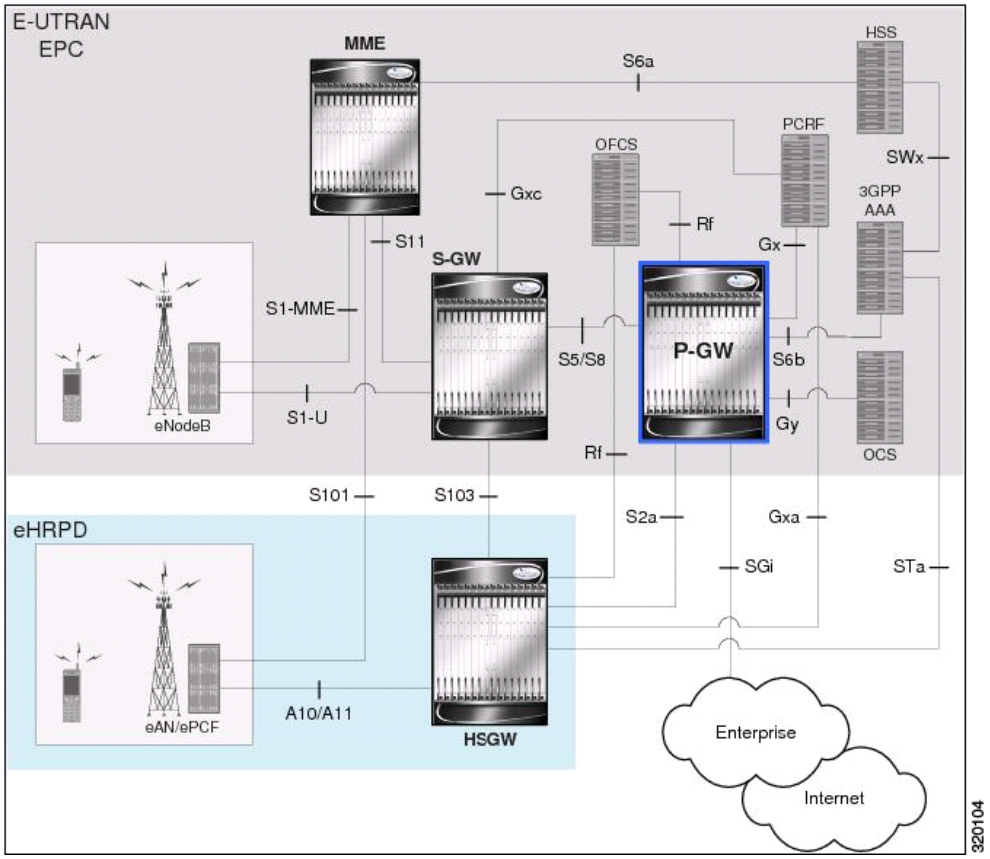
Overview of LTE Networks

Long Term Evolution (LTE) is the latest step in moving forward from the cellular 3G services, such as GSM to UMTS to HSPA to LTE or CDMA to LTE. LTE is based on standards developed by the Third Generation Partnership Project (3GPP). LTE may also be referred more formally as Evolved UMTS Terrestrial Radio Access Network (E-UTRAN). Following are the main objectives of an LTE network.

- Increased downlink and uplink peak data rates
- Scalable bandwidth
- Improved spectral efficiency
- All IP network

Figure 27-5 provides the topology of a basic LTE network.

Figure 27-5 Basic LTE Network Topology



Working with LTE Network Technologies

The E-UTRAN uses a simplified single node architecture consisting of the eNodeBs (E-UTRAN Node B). The eNB communicates with the Evolved Packet Core (EPC) using the S1 interface, specifically with the Mobility Management Entity (MME) and Serving Gateway (S-GW) using S1-U interface. The PDN Gateway (P-GW0 provides connectivity to the external packet data networks.

Following sections provide more details on these services and their support in Prime Network:

Monitoring System Architecture Evolution Networks (SAE-GW)

Systems Architecture Evolution (SAE) has a flat all-IP architecture with separation of control plane and user plane traffic. The main component of SAE architecture is the Evolved Packet Core (EPC), also known as SAE Core. The EPC serves as an equivalent to GPRS networks by using its subcomponents Mobility Management Entities (MMEs), Serving Gateway (S-GW), and PDN Gateway (P-GW).

Mobility Management Entity (MME)

MME is the key control node for a Long Term Evolution (LTE) access network. It is responsible for idle mode User Equipment (UE) tracking and paging procedure including retransmissions. It is involved in the bearer activation/deactivation process and is also responsible for choosing the S-GW for a UE at the initial attach and at time of intra-LTE handover involving Core Network (CN) node relocation. The MME also provides the control plane function for mobility between LTE and 2G/3G access networks with the S3 interface terminating at the MME from the SGSN.

Serving Gateway (S-GW)

The S-GW routes and forwards user data packets, while also acting as the mobility anchor for the user plane during inter-eNodeB handovers and as the anchor for mobility between LTE and other 3GPP technologies. For idle state UEs, the S-GW terminates the downlink data path and triggers paging when downlink data arrives for the UE. It manages and stores UE contexts, such as parameters of the IP bearer service, network internal routing information, and so on. It also performs replication of the user traffic in case of lawful interception. For more information, see Working with Serving Gateway (S-GW), page 27-107.

PDN Gateway (P-GW)

The P-GW provides connectivity from the UE to external packet data networks by being the point of exit and entry of traffic for the UE. A UE may have simultaneous connectivity with more than one P-GW for accessing multiple PDNs. The P-GW performs policy enforcement, packet filtering for each user, charging support, lawful interception, and packet screening. Another key role of the P-GW is to act as the anchor for mobility between 3GPP and non-3GPP technologies such as WiMAX and 3GPP2. For more information, see Working with PDN-Gateways (P-GW), page 27-101.

Running S-GW and P-GW services together as a SAE-GW provides the following benefits:

- Higher capacity—For a UE with one PDN connection that is passing through standalone S-GW and P-GW services consumes 2 license units because both S-GW and P-GW services account for it separately. SAE-GW as a single node consumes only one license unit for the same, thus increasing the capacity.
- Cohesive configuration—Configuration and management of SAE-GW as a node is simpler to follow and logical to explain.

See Viewing SAE-GW Properties, page 27-100 for details on how to view SAE-GW properties in the Vision client.

Viewing SAE-GW Properties

The Vision client displays the SAE-GWs in a SAE-GW container under the Mobile node in the logical inventory. The icon used for representing SAE-GW in the logical inventory is explained in NE Logical Inventory Icons, page A-7.

To view SAE-GW properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > *SAE-GW Container*.

The Vision client displays the list of SAE-GW services configured under the container. You can view the individual SAE-GW service details from the table on the right pane or by choosing **Logical Inventory** > *Context* > **Mobile** > *SAE-GW Container* > *SAE-GW*.

Table 27-56 describes the details available for each SAE-GW.

Table 27-56 SAE-GW Properties in Logical Inventory

Field	Description
Service Name	Name of the SAE-GW service.
Service ID	ID of the SAE-GW service.
Status	Status of the SAE-GW service.
P-GW Service	The P-GW service associated with the SAE-GW.
S-GW Service	The S-GW service associated with the SAE-GW.
New Call Policy	Specifies if the new call related behavior of SAE-GW service is enabled or disabled, when duplicate sessions with same IP address request is received.
GTPU Service	The GTPU service associated with the SAE-GW.
Sx Service	The Sx service associated with the SAE-GW.
CUPS Enabled	Specifies if CUPS is enabled or disabled.

SAE-GW Commands

The following SAE-GW commands can be launched from the inventory by right-clicking a SAE-GW and choosing **Commands > Configuration.** Your permissions determine whether you can run these commands (seePermissions Required to Perform Tasks Using the Prime Network Clients, page B-1). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-57 SAE-GW Commands

Command	Navigation	Description
Create SAE GW	*Logical Inventory* > right-click the *context* > **Commands** > **Configuration**	Use this command to create SAE GW.
Delete SAE GW	Right-click the *SAE GW* > **Commands** > **Configuration**	Use this command to delete or modify the configuration details for a SAE GW.
Modify SAE GW		

Working with PDN-Gateways (P-GW)

A PDN Gateway (P-GW) is the node that terminates the SGi interface towards the PDN. If a user equipment (UE) is accessing multiple PDNs, there may be more than one P-GW for that UE. The P-GW provides connectivity to the UE to external packet data networks by being the point of exit and entry of traffic for the UE. A UE may have simultaneous connectivity with more than one P-GW for accessing multiple PDNs.

The P-GW facilitates policy enforcement, packet filtering for each user, charging support, lawful interception, and packet screening. The features of P-GW include:

- Integration of multiple core network functions in a single node
- Multiple instances of P-GW can enable call localization and local breakout
- High performance across all parameters like, signaling, throughput, density, and latency
- Integrated in-line services

- Support for enhanced content charging, content filtering with blacklisting, dynamic network-based traffic optimization, application detection and optimization, stateful firewall, NAT translation, and lawful intercept
- High-availability helps to ensure subscriber satisfaction

The following topics explain how to work with P-GW in the Vision client:

- Viewing P-GW Properties, page 27-102
- P-GW Commands, page 27-106

Viewing P-GW Properties

The Vision client displays the P-GWs in a P-GW container under the Mobile node in the logical inventory. The icon used for representing P-GW in the logical inventory is explained in NE Logical Inventory Icons, page A-7.

To view P-GW properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > *P-GW Container*.

The Vision client displays the list of P-GW services configured under the container. You can view the individual P-GW service details from the table on the right pane or by choosing **Logical Inventory** > *Context* > **Mobile** > *P-GW* Container > *P-GW*.

Figure 27-6 P-GW Properties

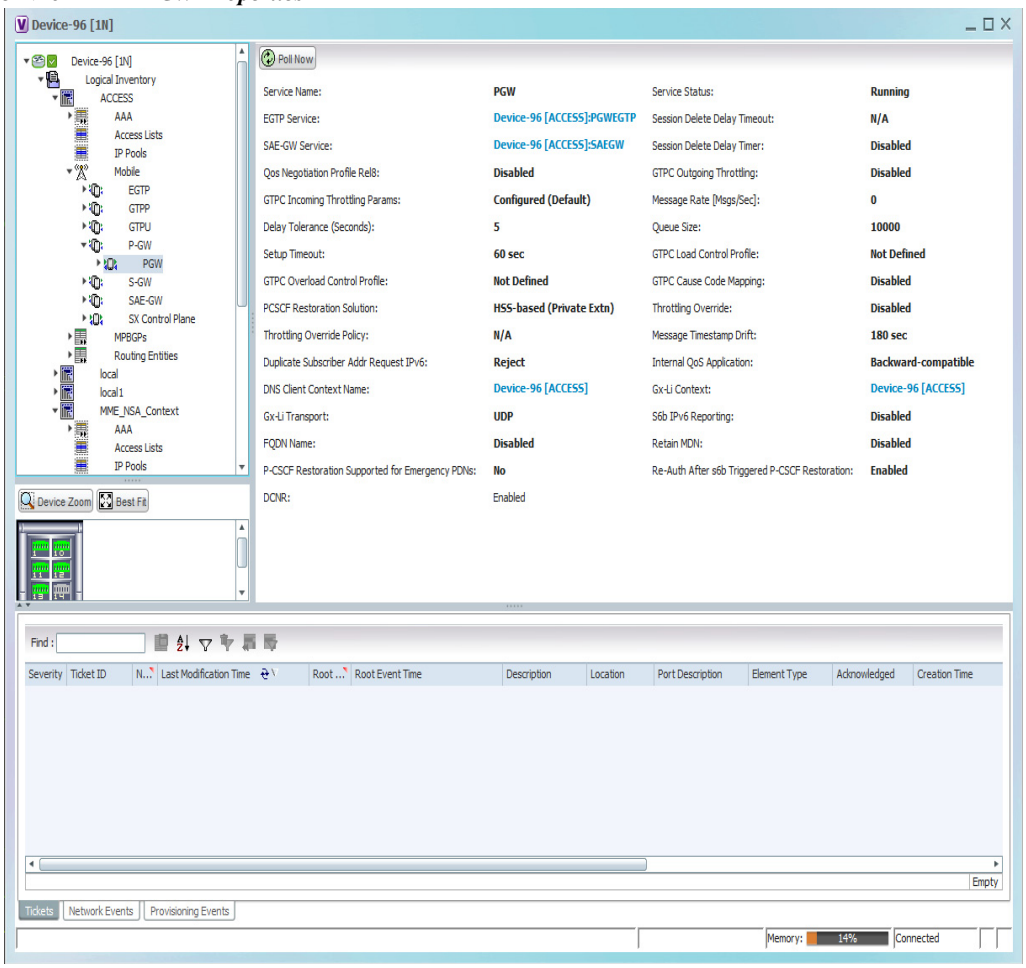


Table 27-58 describes the details available for each P-GW.

Table 27-58 P-GW Properties in Logical Inventory

Field	Description
Service Name	Name of the P-GW service.
Service Status	Status of the P-GW service.
EGTP Service	Evolved GPRS Tunneling Protocol (EGTP) service associated with the P-GW. EGTP provides tunneling support for the P-GW.
GGSN Service	GGSN service associated with the P-GW.
LMA Service	Local Mobility Anchor (LMA) that facilitates proxy mobile IP on the P-GW.
QCI QoS Mapping Table Name	Table name of QoS class indices that enforce QoS parameters.
New Call Policy	Specifies if the new call related behavior of P-GW service is enabled or disabled, when duplicate sessions with same IP address request is received.
Session Delete Delay Timeout	Duration, in seconds, to retain a session before terminating it.

Table 27-58 P-GW Properties in Logical Inventory (continued)

Field	Description
SAE-GW Service	Systems Architecture Evolution (SAE) gateway service associated with the P-GW.
Setup Timeout	The timeout (duration in seconds) for setting up the session. Ranges from 1 to 120. Default is 60 seconds.
GTPC Load Control Profile	Specifies the GTPC load control profile for the P-GW service.
GTPC Overload Control Profile	Specifies the GTPC overload control profile for the P-GW service.
GTPC Cause Code Mapping	Specifies the GTPC cause code mapping for the P-GW service.
PCSCF Restoration Solution	Specifies the mechanism to support PCSCF restoration, which can be one of the following: HSS-based (Private Extension) and HSS-based (Release12).
Throttling Override	Specifies throttling override.
Throttling Override Policy	Specifies the throttling override policy.
Message Timestamp Draft	Displays the message timestamp for the P-GW service.
Duplicate Subscriber Addr Request IPV6	Shows how duplicate sessions with same IPv6 address request are configured. The default configuration disables the support to accept duplicate v6 address request.
Internal Qos Application	Specifies whether the internal Qos application is enabled or disabled for P-GW service.
Event Reporting	Shows reporting of events.
Internal Qos Policy	Specifies the internal Qos policy for P-Gw service.
DNS Client Context Name	Displays the DNS client context name for P-Gw service.
Gx-Li Context	Displays Gx LI X3 interface context that is associated with the service.
Gx-Li Transport	Displays Gx LI X3 interface content delivery transport. Default transport is UDP.
Authorize	This command enables or disables subscriber session authorization through a Home Subscriber Server (HSS) over an S6b Diameter interface. This feature is required to support the interworking of GGSN with P-GW and HA.
S6b IPV6 Reporting	Enables ipv6 reporting through AAR towards s6b interface.
Fqdn Name	Designates PGW FQDN host and realm as a string between 1 and 255 alpha-numeric characters.
Subscriber Map Name	The subscriber map name associated with the P-GW service is available or not.
Session Delete Delay Timer	The session delete timeout.
Retain MDN	Shows the retained value of either MSISDN or MDN value retained, which is negotiated during the call setup for the lifetime of call.

Table 27-58 P-GW Properties in Logical Inventory (continued)

Field	Description
P-CSCF Restoration Supported for Emergency PDNs	Enables P-CSCF restoration for emergency PDNs.
Re-Auth After s6b Triggered P-CSCF Restoration	Enables Re-Auth after S6b triggered P-CSCF restoration of WLAN. This is applicable only for S2a and S2b. **Note** By default, Re-Auth is performed for P-CSCF restoration extension on S6b.
DCNR	Enables Dual Connectivity with the New Radio (DCNR) to support 5G Non-Standalone (NSA).

Step 3 If the P-GW is associated with PLMNs, you can view the details of the PLMNs on clicking the specified P-GW.

eGTP Characteristics

The Vision client displays the EGTP characteristics in an EGTP container under the Mobile node in the logical inventory. The icon used for representing EGTPs in the logical inventory is explained in NE Logical Inventory Icons, page A-7.

To view EGTP characteristics:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > *EGTP Characteristics*.

Table 27-59 describes the EGTP Characteristics.

Table 27-59 EGTP Characteristics

Field	Description
Overcharging Properties	Overcharge protection is described as temporarily not charging during loss of radio coverage.
Drop Policy	The drop policy is enabled while over charging protection is enabled. There are two drop policies: • **drop-all** —Configures overcharge protection to drop all packets. • **received transmit-all** —Configures overcharge protection to send all received packets
SGW Restoration Handling	Configuration is related to SGW-restoration.
Session Hold Timer	Session time hold for SGW-restoration. It can be configured only when SGW-restoration is enabled.
Timeout	It specifies session hold timer in seconds when the SGW-restoration is enabled. Value range: 1 - 3600

Field	Description
Modify Bearer Cmd Negotiate QoS	It prefers **PCRF Authorized QoS** rather than **Requested QoS** in Modify-bearer-command procedure.
Bit Rate in Rounded Down Kbps	The rounded down Kbps value of Bit Rate is enabled or disabled on GTP interface.
Suppress Update Bearer Request	Enables the P-GW to suppress the Update Bearer Request (UBR) message UBR, if the bit rate is the same after the round-off.
EGTP Cause Code Handling	Enables eGTP Cause Code Handling when the P-GW receives a temporary failure response from peer (cause code 110). **Note** All transactions that are moved to a pending queue due to temporary cause failure is re-attempted.

P-GW Commands

The following P-GW commands can be launched from the inventory by right-clicking a P-GW and choosing **Commands > Configuration.** Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-60 P-GW Commands

Command	Navigation	Description
Create P-GW PLMN	Right-click the *P-GW service* > **Commands** > **Configuration** > **Mobility**	Use this command to create a PLMN for P-GW.
Delete P-GW		Use this command to delete a P-GW.
Modify P-GW		Use this command to modify the configuration details for a P-GW.

Enabling DCNR in P-GW Service

Follow these steps to enable DCNR to support 5G NSA:

Note Prime Network supports NSA from StarOS 21.11 onwards.

Step 1 Install NSA license on the ASR 5500 device for which you want to enable 5G NSA:

```
20000 5G NSA feature Set 100k Sess VPCSW Active
```

Step 2 Once the license is enabled, the **DCNR** option is available in **pgw-service** configuration mode. Enable **DCNR** option from the device.

Step 3 The **DCNR** field is now visible in the Vision GUI. See P-GW Properties.

Working with Serving Gateway (S-GW)

In a Long Term Evolution (LTE) / Systems Architecture Evolution (SAE) network, a Serving Gateway (S-GW) acts as a demarcation point between the Radio Access Network (RAN) and core network, and manages user plane mobility. It serves as the mobility anchor when terminals move across areas served by different eNode-B elements in Evolved UMTS Terrestrial Radio Access Network (E-UTRAN), as well as across other 3GPP radio networks such as GSM EDGE Radio Access Network(GERAN) and UTRAN. S-GW buffers downlink packets and initiates network-triggered service request procedures. Other functions include lawful interception, packet routing and forwarding, transport level packet marking in the uplink and the downlink, accounting support for per user, and inter-operator charging. The S-GW routes and forwards user data packets, while also acting as the mobility anchor for the user plane during inter-eNode-B handovers and as the anchor for mobility between LTE and other 3GPP technologies.

For idle state user equipment (UE), the S-GW terminates the downlink data path and triggers paging when downlink data arrives for the UE. It manages and stores UE contexts, such as parameters of the IP bearer service, network internal routing information, and so on. It also performs replication of the user traffic in case of lawful interception.

The following topics provide details on how to work with S-GWs in the Vision client:

- Viewing S-GW Properties, page 27-107
- S-GW Commands, page 27-110

Viewing S-GW Properties

The Vision client displays the S-GWs in a S-GW container under the Mobile node in the logical inventory. The icon used for representing S-GW in the logical inventory is explained in NE Logical Inventory Icons, page A-7.

To view S-GW properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > *S-GW Container*.

The Vision client displays the list of S-GW services configured under the container. You can view the individual S-GW service details from the table on the right pane or by choosing **Logical Inventory** > *Context* > **Mobile** > *S-GW* Container > *S-GW*.

Table 27-61 describes the details available for each S-GW.

Table 27-61 S-GW Properties in Logical Inventory

Field	Description
Service Name	Name of the S-GW service.
Service Status	Status of the S-GW service.
Accounting Context	Name of the context configured on the system that processes accounting for service requests handled by the S-GW service.
Accounting GTPP Group	Name of the accounting GTPP group associated with the S-GW service. This will hold the configured GTPP server group (for GTPP servers redundancy) on a S-GW service for CGF accounting functionality.

Table 27-61 S-GW Properties in Logical Inventory (continued)

Field	Description
Accounting Mode	Accounting protocol, which could be GTPP or Radius-Diameter.
Egress Protocol	Egress protocol used for the S-GW service, which could be GTP, GTP-PMIP, or PMIP.
Ingress EGTP Service	Ingress EGTP service associated with the S-GW. EGTP provides tunneling support for the S-GW.
Egress Context	Context used for S-GW service egress.
Egress ETGP Service	Ingress EGTP service associated with the S-GW. EGTP provides tunneling support for the S-GW.
Egress Mag Service	Mobile Access Gateway (MAG) egress service through calls are routed to the S-GW.
IMS Authorization Service	IMS authorization service associated with the S-GW.
Accounting Policy	Accounting policy configured for the S-GW.
Accounting Stop Trigger	The trigger point for accounting stop CDR. Default is on session deletion request.
Peer Map	Configuration of the Network side peer map for the S-GW service.
Access Peer Map	Configuration of the Access side peer map for the S-GW service.
Temporary Failure Handling	Configuration related to handling temporary failure from peer.
EGTP NTSR	Configuration related to handling EGTP procedure and NTSR.
EGTP NTSR Timeout	Configures a timer to hold the session after path failure is detected at the MME (for Network Triggered Service Restoration (NTSR)).
Timeout	Configuration related to the subscriber's time-to-live (TTL) settings.
Session Hold Timer	Configuration related to session hold for NTSR.
Include PGW Control FTEID	Controls the sending of the PGW Fully Qualified Tunnel Endpoint Identifier (FTEID) for relocation Create Session Response procedures with an S-GW change.
Page UE for PGW Initiated Procedures	Enable paging UE for PGW initiated procedures (CBR/UBR) when UE is Idle/during handoff and sends failure response to PGW with cause code 110 (Temporary Failure). Default behaviour is Disabled.
Idle Seconds Deemed	Specifies the time duration, in seconds, after which a session state is deemed to have changed from active to idle or idle to active, and a micro-checkpoint is then sent from the active to the standby chassis. time_in_seconds must be an integer from 10 to 1000.
Idle Checkpoint Periodicity	Specifies the micro-checkpoint Periodicity for idlesecs, in seconds. time_in_seconds must be an integer from 10 to 10000 seconds.
New Call Policy	Specifies if the new call related behavior of S-GW service is enabled or disabled, when duplicate sessions with same IP address request is received.
QCI QoS Mapping Table	Table name of QoS class indices that enforce QoS parameters.

Table 27-61 S-GW Properties in Logical Inventory (continued)

Field	Description
SAE GW Service	Systems Architecture Evolution (SAE) gateway service associated with the S-GW.
Idle Timeout	The maximum duration a session can remain idle in seconds. Default value is 0.
Idle Timeout Micro Checkpoint Periodicity	Specifies the micro checkpoint periodicity for the S-GW service.
GTPC Load Control Profile	Specifies the GTPC load control profile for the S-GW service.
GTPC Overload Control Profile	Specifies the GTPC overload control profile for the S-GW service.
Internal Qos Policy	Specifies the internal Qos policy for the S-GNW service.
Internal Qos Application	Specifies the internal Qos application for the S-GNW service.
Event Reporting	Shows reporting of events.
Subscriber Map Name	Specifies subscriber map name associated with the S-GW service.

Step 3 Choose **Logical Inventory >** *Context* **> Mobile >** *S-GW Container* > **S-GW** > **DDN Throttling Characteristics**.

Table 27-62 describes the details of DDN throttling characteristics for each S-GW.

Table 27-62 DDN Throttling Characteristics for S-GW

Field	Description
Throttling	Specifies the status of the DDN throttling characteristics. The status can be **Enabled** or **Disabled**.
Feature Packet Drop Time	Specifies the feature packet drop time for the S-GW service.
Arp Watermark	Specifies the throttle ARP watermark. If the arp watermark is configured and if an MME/SGSN sends the throttling factor and delay in a DDN ACK message, all the DDNs, which have an ARP value greater than the configured value will be throttled by the throttle factor for the specified delay.
Increment Factor	Specifies the percentage by which the DDN throttling should be increased.
Rate Limit	Specifies the rate limit.
Time Factor	Specifies time duration during which the S-GW makes throttling decisions.
Stab Time in Hours	Specifies time period in hours over which the system is stabilized, throttling will be disabled.
Throttle Time In Hours	Specifies DDN throttling time in hours.
Success Action Retry Time	Specifies the success action retry time for the S-GW service.
ISR Sequential Paging Delay Time	Specifies the ISR sequential paging delay time for the S-GW service.

Table 27-62 DDN Throttling Characteristics for S-GW (continued)

Field	Description
Throttle Factor	Specifies the DDN throttling factor.
Poll Interval	Specifies the polling interval in DDN throttling.
Stab Time In Seconds	Specifies the DDN throttling stabilization time in seconds.
Throttle Time In Seconds	Specifies the DDN throttling time in seconds.
Stab Time in Minutes	Specifies the DDN throttling stabilization time in minutes.
Throttle Time in Minutes	Specifies the DDN throttling time in minutes.

Step 4 If the S-GW is associated with PLMNs, you can view the PLMN entries on clicking the specified S-GW.

S-GW Commands

The following S-GW commands can be launched from the inventory by right-clicking an S-W and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-63 S-GW Commands

Command	Navigation	Description
Create S-GW PLMN	Right-click the *S-GW service* > **Commands** > **Configuration**	Use this command to create a PLMN for S-GW.
Delete S-GW		Use this command to delete a S-GW.
Modify S-GW		Use this command to modify the configuration details for a S-GW.

Viewing QoS Class Index to QoS (QCI-QoS) Mapping

The QoS Class Index (QCI) to QoS mapping configuration mode is used to map Indexes to enforceable QoS parameters. Mapping can occur between the RAN and the S-GW, the MME, and/or the P-GW in an LTE network or between the RAN and the harped Serving Gateway (HSGW) in an eHRPD network. This is a global configuration. These maps can be imported by P-gateway and S-gateway to enforce these parameters on upstream/downstream traffic.

The Vision client displays the QCI-QoS mapping information under the Mobile node in the logical inventory. See Figure 27-22.

Note QCI-QoS mapping is applicable only for the ‘local’ context in the logical inventory.

To view QCI-QoS mapping:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

In the **Logical Inventory** window, choose **Logical Inventory** > *local* > **Mobile** > **QCI-QoS Mapping**.

the Vision client displays the list of QCI-QoS mapping records configured under the container. You can view the individual record from the table on the right pane or by choosing **Logical Inventory** > *Context* > **Mobile** > **QCI-QoS Mapping** > *Mapping Name.*

Table 27-64 describes the QCI-QoS mapping details.

Table 27-64 QCI-QoS Mapping

Field	Description
Mapping Name	Name of the QCI-QoS mapping record.
QCI-QoS Mapping Table	
QCI Number	QCI number.
QCI Type	QCI type.
Uplink	DSCP marking to be used for encapsulation and UDP for uplink traffic
Downlink	DSCP marking to be used for encapsulation and UDP for downlink traffic
Max Packet Delay	Maximum packet delay, in milliseconds, that can be applied to the data.
Max Error Rate	Maximum error loss rate of non congestion related packet loss.
Delay Class	Packet delay.
Precedence Class	Indicates packet precedence.
Reliability Class	Indicates packet reliability.
Traffic Policing Interval	Traffic policing interval.

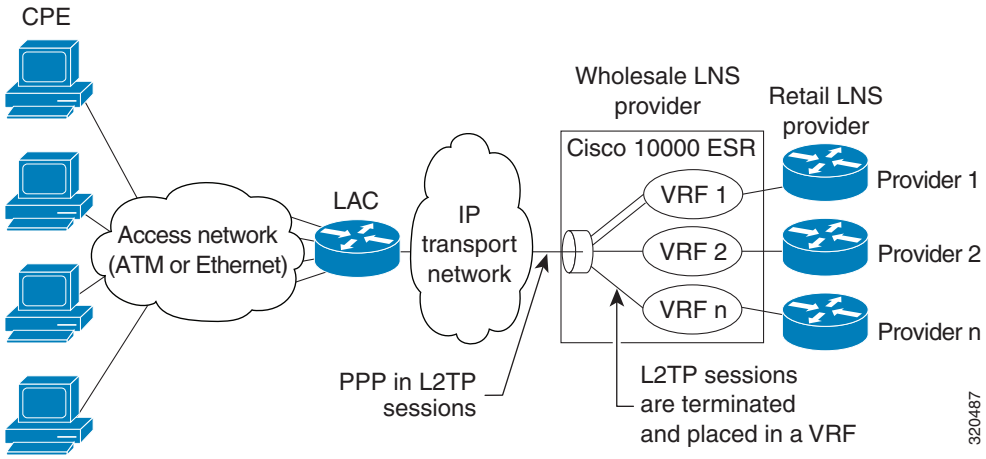
Viewing Layer 2 Tunnel Access Concentrator Configurations (LAC)

In computer networking, Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself; it relies on an encryption protocol that it passes within the tunnel to provide privacy. The entire L2TP packet, including payload and L2TP header, is sent within a User Datagram Protocol (UDP) datagram. It is common to carry Point-to-Point Protocol (PPP) sessions within an L2TP tunnel.

The two endpoints of an L2TP tunnel are called the LAC (L2TP Access Concentrator) and the LNS (L2TP Network Server). The LAC is the initiator of the tunnel while the LNS is the server, which waits for new tunnels. Once a tunnel is established, the network traffic between the peers is bidirectional.

LAC allows users and telecommuters to connect to their corporate intranets or extranets using L2TP. In other words, it forwards packets to and from the LNS and a remote system. It connects to the LNS using a local area network or wide area network and directs subscriber sessions into L2TP tunnels based on the domain of each session. Figure 27-7 denotes the LAC architecture.

Figure 27-7 LAC Architecture



The packets that are exchanged within an L2TP tunnel can be categorized as control packets and data packets.

To view the LAC configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **LAC.** The list of LAC services configured in Prime Network is displayed in the content pane.

Step 3 From the **LAC** node, choose an LAC service. The LAC service details are displayed in the content pane as shown in Figure 27-8.

Figure 27-8 LAC Service Details

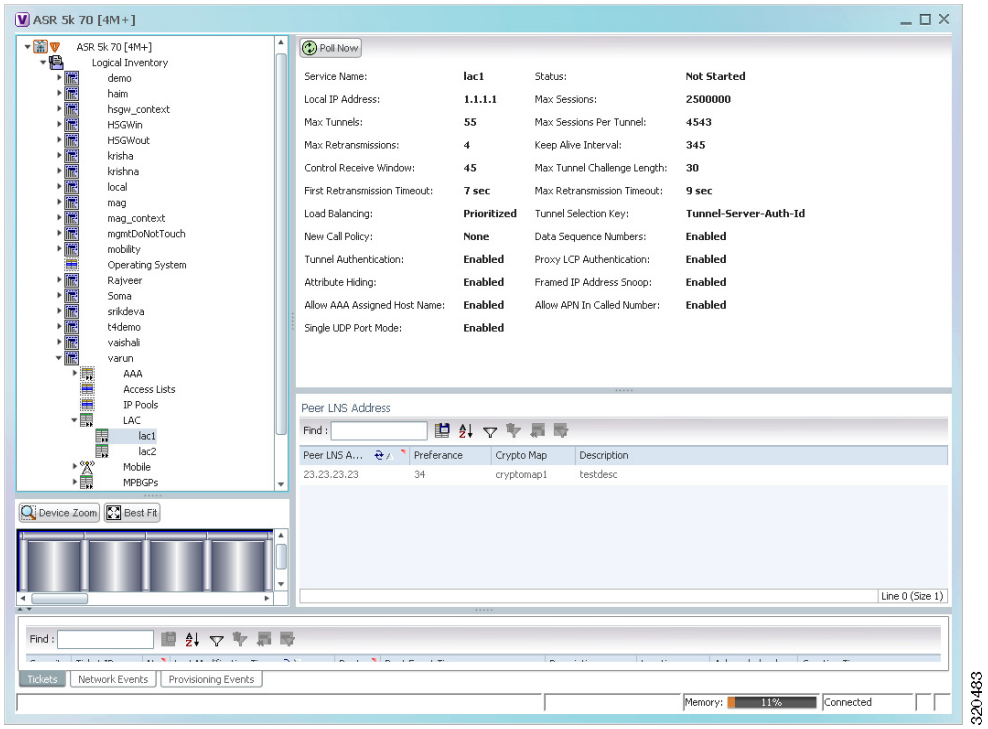


Table 27-65 displays the LAC configuration details.

Table 27-65 LAC Configuration Details

Field	Description
Service Name	The unique identification string for the LAC service.
Status	The status of the LAC service, which can be any one of the following: • Initiated • Running • Down • Started • Nonstarted • Unknown
Local IP Address	The local IP address bound with the LAC service.
Max Sessions	The maximum number of subscribers connected to this service at any time, which can be any value between 1 and 2500000. This field defaults to 2500000.
Max Tunnels	The maximum length (in bytes) of the tunnel challenge. **Note** The tunnel challenge is basically used to authenticate tunnels at the time of creation.

Table 27-65 LAC Configuration Details (continued)

Field	Description
Max Sessions Per Tunnel	The maximum number of sessions that can be handled by a single tunnel at one point of time, which can be any value between 1 and 65535. This field defaults to 512.
Max Retransmissions	The maximum number of times a control message is retransmitted to a peer, before clearing the tunnel and its sessions.
Keep Alive Interval	The amount of time after which a keep alive message is sent.
Control Receive Window	The number of control messages the remote peer LNS can send before an acknowledgement is received.
Max Tunnel Challenge Length	The maximum length (in bytes) of the tunnel challenge.
First Retransmission Timeout	The initial timeout before retransmitting a control message. **Note** Each tunnel maintains a queue of control messages that must be transmitted to its peer. If an acknowledgement is not received after the specified period, then the control message is retransmitted.
Max Retransmission Timeout	The maximum amount of time between two retransmitted messages.
Load Balancing	The type of load balancing to select LNS for the LAC service, which can be any one of the following: • Balanced • Prioritized • Random
Tunnel Selection Key	The selection key to create tunnels between the L2TP service and the LNS server, based on the value of the \u2015Tunnel-Server-Auth-ID\u2016 attribute received from the AAA server.
New Call Policy	The new call policy for busy-out conditions, which can be any one of the following: • None • Accept • Reject
Data Sequence Numbers	Indicates whether data sequence numbering for sessions that use the current LAC service is enabled. This option is enabled by default.
Tunnel Authentication	Indicates whether tunnel authentication is enabled. **Note** If this option is enabled, a configured shared secret is used to ensure that the LAC service is communicating with an authorized peer LNS. The shared secret is configured by the command in the LAC service configuration mode, the command in the subscriber configuration mode, or the Tunnel-Password attribute in the subscribers RADIUS profile.

Table 27-65 LAC Configuration Details (continued)

Field	Description
Proxy LCP Authentication	Indicates whether the option to send proxy LCP authentication parameters to the LNS is enabled.
Attribute Hiding	Indicates whether certain attributes in control messages sent from the LAC to the LNS is hidden. **Note** The LAC hides these attributes only if the tunnel authentication option is enabled between the LAC and LNS.
Framed IP Address Snoop	Indicates whether the LAC can detect IPCP packets exchanged between the mobile node and the LNS and extract the framed-I-address assigned to the mobile node. **Note** The address that is extracted is reported in the accounting start/stop messages and will be displayed for each subscriber session.
Allow AAA Assigned Host Name	Indicates whether the Tunnel-Client-Auth ID assigned by AAA is used as the Host name AVP in the L2TP tunnel setup message. **Note** If the tunnel parameters are not received from the RADIUS server, then the parameters configured in APN are considered for LNS peer selection. When the parameters in APN are considered, the local-hostname configured with the APN command for the LNS peer is used as the LAC Host name.
Allow APN in Called Number	Indicates whether the APN name in Called number AVP is sent as part of the Incoming-Call Request (ICRQ) message sent to the LNS. If this keyword is not configured, then the Called number AVP will not be included in the ICRQ message sent to the LNS>
Single UDP Port Mode	Indicates whether the standard L2TP port 1701 is used as a source port for all L2TP control and data packets that originate from the LAC node.
Peer LNS Address	
Peer LNS Address	The IP address of the peer LNS for the current LAC service, which is usually in standard IPv4 dotted decimal notation.
Preference	The priority of the peer LNS, which can be any number between 1 and 128. This priority is used when multiple peer LNS are configured.
Crypto Map	The name of crypto map that is configured for the selected context.
Description	The description of the specified peer LNS.

Monitoring the HRPD Serving Gateway (HSGW)

The HRPD Serving Gateway (HSGW) is a component in the evolved High Rate Packet Data (eHRPD) mobile network. It is an evolution option for CDMA operators that helps ensure converged mobility and management between HRPD and LTE networks.

The HSGW terminates the eHRPD access network interface from the Evolved Access Network (eAN) or Evolved Packet Core Function (ePCF) and routes UE-originated or terminated packet data traffic. It provides interworking with the eAN/ePCF and the PDN Gateway (P-GW) within the Evolved Packet Core (EPC) or LTE/SAE core network.

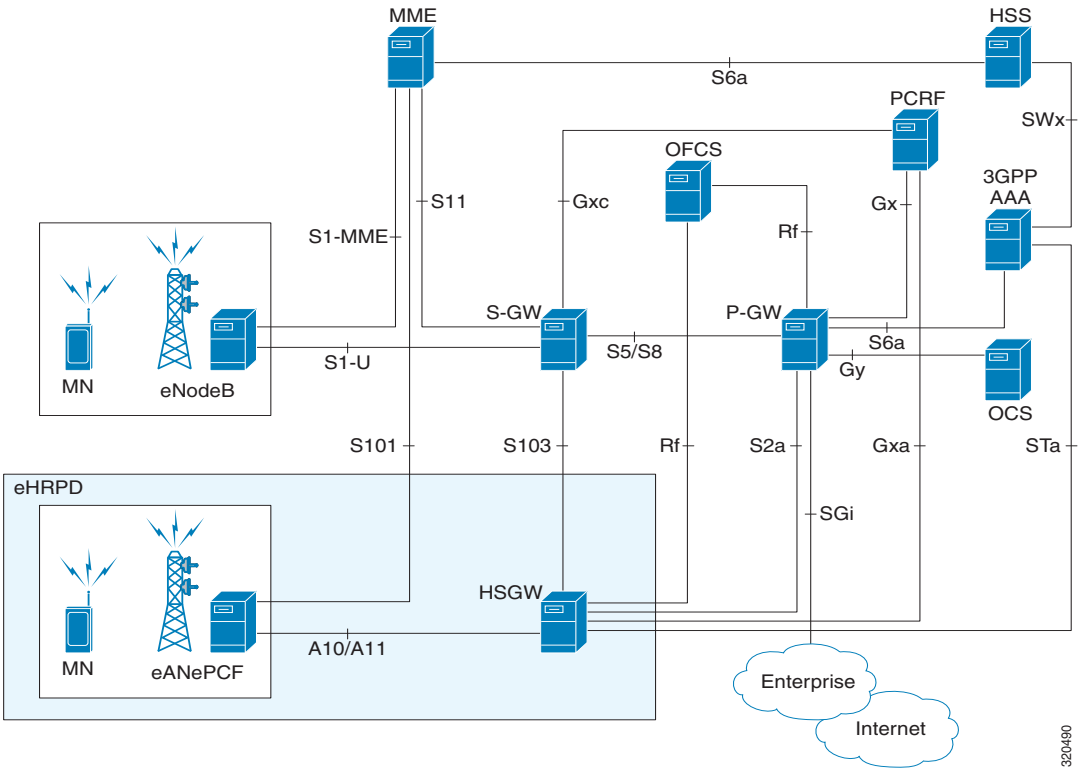
HSGW performs the following functions:

- Mobility anchoring for inter-eAN handoffs
- Transport level packet marking in the uplink and the downlink. For example, setting the DiffServ Code Point, based on the QCI of the associated EPS bearer
- Uplink and downlink charging per UE, PDN, and QCI
- Downlink bearer binding based on policy information
- Uplink bearer binding verification with packet dropping of UL traffic that does not comply with established uplink policy
- MAG functions for S2a mobility (i.e., Network-based mobility based on PMIPv6)
- Support for IPv4 and IPv6 address assignment
- EAP Authenticator function
- Policy enforcement functions defined for the Gxa interface
- Robust Header Compression (RoHC)
- Support for VSNCP and VSNP with UE
- Support for packet-based or HDLC-like framing on auxiliary connections
- IPv6 SLACC, generating RAs responding to RSs

An HSGW also establishes, maintains and terminates link layer sessions to UEs. The HSGW functionality provides interworking of the UE with the 3GPP EPS architecture and protocols. This includes support for mobility, policy control and charging (PCC), access authentication, and roaming. The HSGW also manages inter-HSGW handoffs.

The topology of the HSGW network is shown in the following figure:

Figure 27-9 HSGW Topology



Basic Features of HSGW

The basic features supported by HSGW can be categorized as follows:

- Authentication
- IP Address Allocation
- Quality of Service
- AAA, Policy and Charging

The **Authentication** features supported by HSGW are:

- EAP over PPP
- UE and HSGW negotiates EAP as the authentication protocol during LCP
- HSGW is the EAP authenticator
- EAP-AKA' (trusted non-3GPP access procedure) as specified in TS 33.402
- EAP is performed between UE and 3GPP AAA over PPP/STa

The **IP Address Allocation** features supported by HSGW are:

- Support for IPv4 and IPv6 addressing
- Types of PDNs - IPv4, IPv6 or IPv4v6
- IPv6 addressing
  - Interface Identifier assigned during initial attach and used by UE to generate it's link local address

  - HSGW sends the assigned /64 bit prefix in RA to the UE
  - Configure the 128-bits IPv6 address using IPv6 SLAAC (RFC 4862)
  - Optional IPv6 parameter configuration via stateless DHCPv6(Not supported)
- IPv4 address
  - IPv4 address allocation during attach
  - Deferred address allocation using DHCPv4(Not supported)
  - Option IPv4 parameter configuration via stateless DHCPv4(Not supported)

The **Quality of Service** features supported by HSGW include:

- HRPD Profile ID to QCI Mapping
- DSCP Marking
- UE Initiated Dedicated Bearer Resource Establishment
- QCI to DSCP Mapping

The **AAA, Policy and Charging** features supported by HSGW include:

- EAP Authentication (STa)
- Rf Diameter Accounting
- AAA Server Groups
- Dynamic Policy and Charging: Gxa Reference Interface
- Intelligent Traffic Control

Viewing the HSGW Configuration

To view the HSGW configuration:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > **HSGW**. The list of HSGW services configured in Prime Network are displayed in the content pane.

Step 3 From the **HSGW** node, choose a HSGW service. The HSGW service details are displayed in the content pane as shown in Figure 27-10.

Figure 27-10 HSGW Service Details

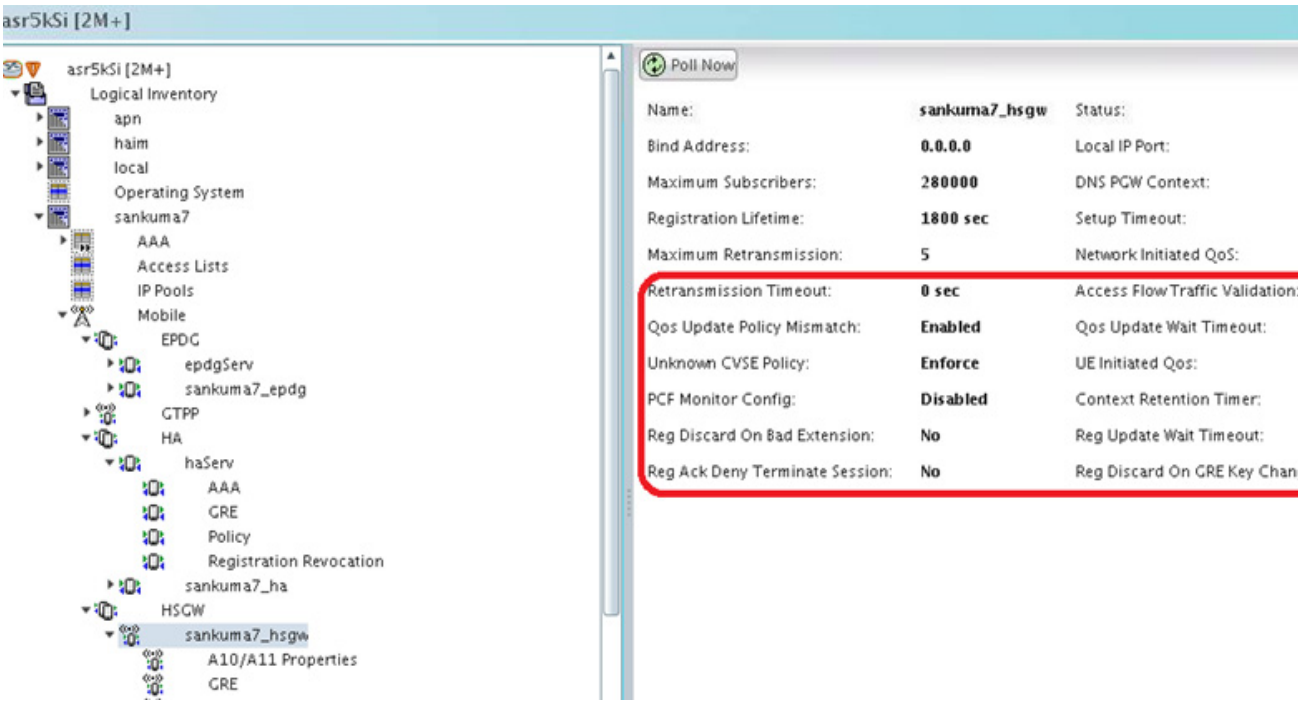


Table 27-66 displays the HSGW service details.

Table 27-66 HSGW Service details

Field	Description
Name	The name of the HSGW service.
Status	The status of the service, which can be any one of the following: • Started • Not Started This field defaults to **Not Started**.
Bind Address	The IPv4 address to which the service is bound to. This field defaults to Null if binding is not done.
Local IP Port	The User Datagram Protocol (UDG) port for the R-P interface of the IP socket.
Maximum Subscribers	The maximum number of subscriber sessions that the service can support.
MAG Service	The Mobile Access Gateway (MAG) service associated with the HSGW service. Clicking this link will take you to the relevant MAG service under the MAG node.
DNS PGW Context	The location of the Domain Name System (DNS) client, which is used to identify the Fully Qualified Domain Name (FQDN) for the peer P-GW.
Registration Lifetime	The registration lifetime that is configured for all the subscribers.
Setup Timeout	The maximum amount of time (in seconds) allowed for session setup.

Table 27-66 HSGW Service details (continued)

Field	Description
Context Retention Timeout	The maximum number of time (in seconds) that the UE session context is maintained by the HSGW service before it is torn down. **Note** The UE session context includes the Link Control Protocol (LCP), authentication and the A10 session context for a given UE.
Maximum Retransmission	The maximum number of times the HSGW service will try to communicate with the eAN or PCF before it declares it as unreachable.
Network Initiated QoS	Indicates whether the Network Initiated QoS feature is supported by the HSGW service.
Retransmission Timeout	Configures the maximum allowable time for the HSGW service to wait for a response from the eAN/PCF before it attempts to communicate with the eAN/PCF again (if the system is configured to retry the PCF), or marks the eAN/PCF as unreachable.
QOS Update Policy Mismatch	Sets QOS update parameters for policy mismatches or wait timeouts.
Unknown CVSE Policy	Configures unknown; CVSE Policy value
PCF Monitor Config	Enables the monitoring of all the PCFs that have sessions associated with it.
Reg Discard on Bad Extension	Configures Discard on Bad Extension option
Reg Ack Deny Terminate Session	Configures Acknowledgement Deny Terminate Session option
Access Flow Traffic Validation	If access-flow traffic-validation is enabled for the service and the subscriber, then the flows are checked against the filter rules. If the packets does not match the filter rules, and N violations occur in K seconds, the rp connection is downgraded to best-effort flow, if it is already not a best-effort flow.
QOS Update Wait Timeout	Sets QOS update parameters for policy mismatches or wait timeouts.
UE Initiated QOS	Configures the HSGW behavior for UE initiated QOS requests.
Context Retention Timer	Configures the maximum number of consecutive seconds that a UE session context (which includes the LCP, authentication and A10 session context for a given UE) is maintained by the HSGW before it is torn down.
Reg Update Wait Timeout	Configures Update Wait Timeout option
Reg Discard on GRE Key Change	Configures Discard on GRE key change option
Unauthorized Flow QoS Timeout	The amount of time (in seconds) the service must wait before a QoS update is triggered to downgrade an unauthorized flow.
SPI tab	
SPI Number	The unique Security Parameter Index (SPI) number, which indicates a security context between the services.
Remote Address	The IP address of the source service, which can be an IPv4 dotted decimal notation or IPv6 colon separated notation.

Table 27-66 HSGW Service details (continued)

Field	Description
Zone ID	The PCF zone id that must be configured for the HSGW service.
Netmask	The subnet mask of the service.
Hash Algorithm	The hash algorithm used between the source and destination services.
Time Stamp Tolerance	The difference (tolerance) in timestamps that is acceptable. If the actual difference in the timestamps exceeds this difference, then the session is rejected.
Replay Protection	The replay-protection scheme that must be implemented by the service.
Description	The description of the SPI.
PLMN tab	
PLMN ID	The unique id of the Public Land Mobile Network (PLMN), which is used to determine if a mobile station is visiting, roaming, or belongs to the network.
Primary	Indicates whether the PLMN Id must be used as the default and primary ID.
Overload Policies tab	
IP Address	The IP address of an alternate PDSN, which is in the IPv4 dotted decimal notation.
Weight	The weightage of the IP address, which determines the order in which the IP address is used in case of multiple IP addresses.

You can also view the following configuration details for a HSGW service:

- A10/A11 Properties—The A10/A11 interface (also known as R-P interface for RAN-to-PDSN) supports the A10 protocol for user data transport between the PCF and PDSN, and the A11 protocol for the associated signaling. A11 signaling messages are also used for passing accounting related and other information from the PCF to the PDSN. The A10/A11 interfaces support mobility between PCFs under the same PDSN. See Viewing the A10/A11 Configuration Details, page 27-122.
- GRE Parameters—Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork. See Viewing the GRE Parameters, page 27-123.
- IP Source Violation—IP source violations occur when the PDSN receives packets from a subscriber where the source address is not the same as the address given to the subscriber, and hence get discarded. See Viewing the IP Source Violation Details, page 27-125.

Viewing the ROHC Properties Details

To view the ROHC Properties details for a HSGW service:

Step 1 Right-click the required device in the Vision client and choose Inventory.

Step 2 In the Logical Inventory window, choose Logical Inventory > Context > Mobile > HSGW > ROHC Properties. The details are displayed in the content pane.

Table 27-68 displays the ROHC properties details.

Table 27-67 ROHC Properties Details

Field	Description
ROHC IP Header Compression	Indicates whether the Robust Header Compression (ROHC) is enabled for headers in the IP packets that are being sent by or sent to the PDSN. By default, this option is disabled.
Max Received Reconstructed Unit	Specifies the size of the largest reconstructed reception unit that the decompressor is expected to reassemble from segments. The size includes the CRC. If maximum received reconstructed unit (MRRU) is negotiated to be 0, no segment headers are allowed on the channel.
Profile ID(s)	Specifies the header compression profiles to use. A header compression profile is a specification of how to compress the headers of a specific kind of packet stream over a specific kind of link. At least one profile must be specified
Max Cid	Specifies the highest context ID number to be used by the compressor as an integer from 0 through 15 when small packet size is selected, and 0 through 31 when large packet size is selected. Default: 15
Cid Mode	This mode allows you to configure options that apply during ROHC compression for the service.

Viewing the A10/A11 Configuration Details

To view the A10/A11 configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >***Context* **>Mobile >HSGW >***HSGW service* **>A10/A11 Properties**. The configuration details are displayed in the content pane.

Table 27-68 displays the A10/A11 configuration details.

Table 27-68 A10 A11 Configuration Details

Field	Description
Overload Policy	The method used by the HSGW service to handle overload conditions, which can be any one of the following: • Reject • Redirect
New Call Policy	The new call policy configured for the HSGW service, which can be any one of the following: • None • Reject • Accept This field defaults to **None**.
Data Available Indicator Enabled	Indicates whether the data available indicator in A10/A11 registration reply messages is enabled.
Data Over Signalling	Indicates whether the data over signaling marking feature for A10 packets is enabled.
Airlink Bad Sequence	The behavior for airlink related parameters configured for the HSGW service, which can be any one of the following: • Accept • Deny
Airlink Bad Sequence Deny Code	The reason for denying airlink bad sequence, which can be any one of the following: • Unsupported vendor ID • Poorly formed request
Handoff With No Connection Setup	Indicates whether the HSGW service must accept or deny handoff R-P sessions that do not have an Airlink Connection setup record in the A11 registration request.
RSVP Retransmission Timeout	The maximum amount of time (in seconds) in which RP control packets must be retransmitted.
RSVP Maximum Retransmission Count	The maximum number of times the RP control packets can be retransmitted.
Maximum MSID Length	The maximum length of the MSID configured for the A10 A11 service. This length can be any value between 10 and 15, and defaults to 15.
Minimum MSID Length	The minimum length of the MSID configured for the A10 A11 service. This length can be any value between 10 and 15, and defaults to 10.

Viewing the GRE Parameters

To view the GRE Parameters for the HSGW service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >***Context* **>Mobile >HSGW >***HSGW service* **>GRE Parameters**. The relevant details are displayed in the content pane.

Table 27-69 displays the GRE parameter details.

Table 27-69 GRE Parameter Details

Field	Description
Checksum	Indicates whether insertion of GRE checksum in outgoing GRE data packets is enabled.
Checksum Verify	Indicates whether verification of GRE checksum in incoming GRE packets is enabled.
Reorder Timeout	The maximum amount of time (in milliseconds) to wait before reordered out-of-sequence GRE packets are processed.
Sequence Mode	The method to handle incoming out-of-sequence GRE packets, which can be any one of the following: • Reorder • None
Sequence Numbers	Indicates whether the option to insert or remove GRE sequence numbers in GRE packets is enabled.
Flow Control	Indicates whether flow control is supported by the selected HSGW service. By default, this option is disabled.
Flow Control Timeout	The amount of time (in milliseconds) to wait for an Transmitter On (XON) indicator from the RAN. This time can be any value between 1 and 1000000, and defaults to 10000 milliseconds.
Flow Control Action	The action that must be taken when the timeout limit is reached, which can be any one of the following: • disconnect-session • resume-session.
Protocol Type	The tunnel type for the GRE routing. This field defaults to **Any**.
Is 3GPP Extension Header QoS Marking	Indicates whether the 3GG Extension Header QoS Marking is enabled for the selected HSGW feature. **Note** If this feature is enabled and the PCF negotiation feature is enabled in A11 RRQ, then the HSGW will include QoS optional data attribute in the GRE 3GPP2 Extension Header.
MTU	The maximum transmission unit (MTU) for packets accessing the APN.
IP Header DSCP	The Differential Service Code Point (DSCP) value in the IP header that marks the GRE IP Header encapsulation. This can be any value between 0x0F and 0X3F, and defaults to 0X0F.

Table 27-69 GRE Parameter Details (continued)

Field	Description
IP Header DSCP Packet Type	Indicates whether the IP Header DSCP Value packet type is specified for the packets, which can be any one of the following: • all-control-packets—Indicates that DSCP marking for GRE IP header encapsulation will be applied for all control packets for the session. • setup-packets-only—Indicates that DSCP marking for GRE IP header encapsulation will be applied only for session setup packets.
GRE Segmentation	Indicates whether segmentation of GRE packets is enabled. By default, this option is disabled.

Viewing the IP Source Violation Details

To view the IP source Violation configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >***Context* **>Mobile >HSGW >***HSGW service* **>IP Source Violation**. The configuration details are displayed in the content pane.

Table 27-70 displays the IP Source Violation configuration details.

Table 27-70 IP Source Violation Configuration Details

Field	Description
Renegotiation Limit	The number of source violations that are allowed within a specified detection period, after which a PPP renegotiation is forced.
Drop Limit	The number of source violations that are allowed within a specified detection period, after which a call disconnect is forced.
Clear On Valid PDU	Indicates whether the service must reset the renegotiation limit and drop limit counters if a properly addressed packet is received.
Period	The amount of time (in seconds) for the source violation detection period. Once this value is reached, the drop limit and renegotiation limit counters are decremented.

Configuration Commands for HSGW

The following HSGW commands can be launched from the logical inventory by choosing the *Context* > **Commands** > **Configuration** or *Context* > **Commands** > **Show**. Your permissions determine whether you can run these commands. To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-71 HSGW Configuration Commands

Command	Navigation	Description
Create HSGW	*Right-click context* > **Commands** > **Configuration > Mobility**	Use this command to create a new HSGW service.
Modify HSGW **Delete HSGW**	*Expand* **HSGW** *node* > *Right-click HSGW service* > **Commands** > **Configuration**	Use this command to modify/delete the configuration details of an HSGW service.
Show HSGW	*Expand* **HSGW** *node* > *Right-click HSGW service* > **Commands** > **Show**	Use this command to view and confirm the configuration details of an HSGW service.
Create SPI	*Expand* **HSGW** *node* > *right-click HSGW service* > **Commands** > **Configuration**	Use this command to create a new Security Parameter Index (SPI) for the HSGW service.
Modify SPI **Delete SPI**	*Expand* **HSGW** *node* > *HSGW service* > *In content pane, click* **SPI** *tab* > *Right-click on SPI No. field* > **Commands** > **Configuration**	Use this command to modify/delete the SPI configuration details for the HSGW service.
Create PLMN entries	*Expand* **HSGW** *node* > *Right-click HSGW service* > **Commands** > **Configuration**	Use this command to create a new Public Land Mobile Network (PLMN) for the HSGW service.
Modify PLMN entries **Delete PLMN entries**	*Expand* **HSGW** *node* > *HSGW service* > *In content pane, click* **PLMN** *tab* > *Right-click on PLMN ID field* > **Commands** > **Configuration**	Use this command to modify/delete the PLMN configuration details for the HSGW service.
Create Overload Policy	*Expand* **HSGW** *node* > *right-click HSGW service* > **Commands** > **Configuration**	Use this command to create a new overload policy for the HSGW service.
Modify Overload Policy **Delete Overload Policy**	*Expand* **HSGW** *node* > *HSGW service* > *In content pane, click* **Overload Policies** *tab* > *Right-click on IP address field* > **Commands** > **Configuration**	Use this command to modify/delete the overload policy details for the HSGW service.
Modify A10 A11 Interface	*Expand* **HSGW** *node* > *HSGW service* > *Right-click A10/A11 Properties* > **Commands** > **Configuration**	Use this command to modify the A10/A11 configuration details for the HSGW service.
Modify GRE	*Expand* **HSGW** *node* > *HSGW service* > *Right-click GRE* > **Commands** > **Configuration**	Use this command to modify the GRE configuration details for the HSGW service.
Modify IP Source Violation	*Expand* **HSGW** *node* > HSGW service > *Right-click IP Source Violation* > **Commands** > **Configuration**	Use this command to modify the IP source violation details for the HSGW service.

Viewing the MAG Configuration for HSGW

A Mobile Access Gateway (MAG) performs mobility-related signaling on behalf of the mobile nodes (MN) attached to its access links. MAG is the access router for the MN; that is, the MAG is the first-hop router in the localized mobility management infrastructure

A MAG performs the following functions:

- Obtains an IP address from a Local Mobility Anchor (LMA) and assigns it to an MN
- Retains the IP address of an MN when the MN roams across MAGs
- Tunnels traffic from an MN to LMA

To view the MAG configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > **MAG** > *MAG service*. The configuration details are displayed in the content pane.

Table 27-72 displays the configuration details for a MAG service.

Table 27-72 MAG Service Configuration Details

Field	Description
Name	The unique name of the MAG service.
Status	The status of the MAG service, which can be any one of the following: • Started • Not Started This field defaults to **Not Started**.
Bind Address	The IP address to which the MAG service is bound to.
Maximum Subscribers	The maximum number of subscribers supported by the service.
PMIP Maximum Retransmission	The maximum number of times the MAG service will communicate with the LMA, before it is declared unreachable.
Registration Lifetime	The registration lifetime configured for all the subscribers who have subscribed to this service.
PMIP Retransmission Timeout	The maximum amount of time (in milliseconds) the MAG service must wait for a response from the LMA.
PMIP Renewal Time	Indicates the percentage of the registration lifetime when the registration renewal is sent to the LMA for subscribers using this service.
PMIP Retransmission Policy	The retransmission policy for PMIP control messages, which can be any one of the following: • Normal • Exponential backoff

Table 27-72 MAG Service Configuration Details

Field	Description
New Call Policy	The method for handling new calls, which can be any one of the following: • Accept • Reject This field defaults to **None**.
PMIPv6 Tunnel Encapsulation	The encapsulation type used for PMIPv6 tunnel data between the MAG and the LMA.
Information Set	The mobility options to be used in Proxy Binding Update (PBU) messages, for those messages sent between MAG and LMA.
Mobility Option Type	The mobility option type used in the mobility messages.
Signalling Packets IP Header DSCP	The Differential Services Code Point (DSCP) value in the IP Header of the signalling packets.
Local IPv4 Address	The IPv4 address of the MAG service.
Local IP Port	The binding port for the MAG service.
PBU Option	The mobility / BSID option to be included in Proxy Binding Update (PBU) messages, for those messages sent between MAG and PGW.
Mobility Header Checksum Type	The checksum type used to calculate the outbound mobility messages from MAG to LMA or inbound mobility messages from LMA to MAG, which can be any one of the following: • RFC3775 • RFC6275 This field defaults to **RFC3775**.
Heartbeat Support	Indicates the option to enable the heartbeat support.
Heartbeat Interval	The time interval in seconds to configure the heartbeat support. Ranges from 30 to 3600. Default value is 60 seconds.
Heartbeat Retransmission Timeout	The timeout in seconds for heartbeat retransmission.Ranges from 1 to 20. Default value is 3 seconds.
Heartbeat Max Retransmissions	The maximum limit for heartbeat retransmission. Ranges from 0 to 50. Default value is 3.

Viewing the Profile-QCI Mapping Details

You can view the configured mapping entries between a Rendezvous Point (RP) QoS Profile and the LTE QoS Class Index (QCI).

A QCI is a scalar that is used as a reference to access node-specific parameters that control bearer level packet forwarding treatment (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.), and that have been pre-configured by the operator owning the access node.

To view the Profile-QCI mapping entries:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *local* > **Mobile** > **Profile** > **Profile-QCI Mapping** > *Profile-QCI Mapping*. The mapping details are displayed in the content pane.

Table 27-73 displays the Profile-QCI Mapping details.

Table 27-73 Profile-QCI Mapping Details

Field	Description
Profile Name	The name of the Profile-QCI Mapping profile that is associated with the HSGW.
Profile-QCI Mapping Table	
QCI ID	The QCI ID to which the profile is mapped.
Profile ID	The profile ID to which the QCI ID is mapped.
Uplink GBR	The Guaranteed Bit Rate (GBR) for the uplink data flow, which can be any value between 0 and 4294967295.
Downlink GBR	The GBR for the downlink data flow, which can be any value between 0 and 4294967295.
Uplink MBR	The Maximum Bit Rate (MBR) for the uplink data flow, which can be any value between 0 and 4294967295.
Downlink MBR	The MBR for the downlink data flow, which can be any value between 0 and 4294967295.
Priority Level	The priority level of the profile for the QCI, which can be any value between 1 and 15.
Preemption Capability	The preemption capability of the profile.

Configuration Commands for MAG

The following MAG commands can be launched from the logical inventory by choosing the *Context* > **Commands** > **Configuration** or *Context* > **Commands** > **Show**. Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-74 MAG Configuration Commands

Command	Navigation	Description
Create MAG	*Right-click context* > **Commands** > **Configuration** > **Mobility**	Use this command to create a new Mobile Access Gateway (MAG) service for the selected context.
Modify MAG **Delete MAG**	*Expand MAG Node* > *Right-click MAG service* > **Commands** > **Configuration**	Use this command to modify the MAG configuration details/delete the MAG profile for the selected context.

Table 27-74 MAG Configuration Commands

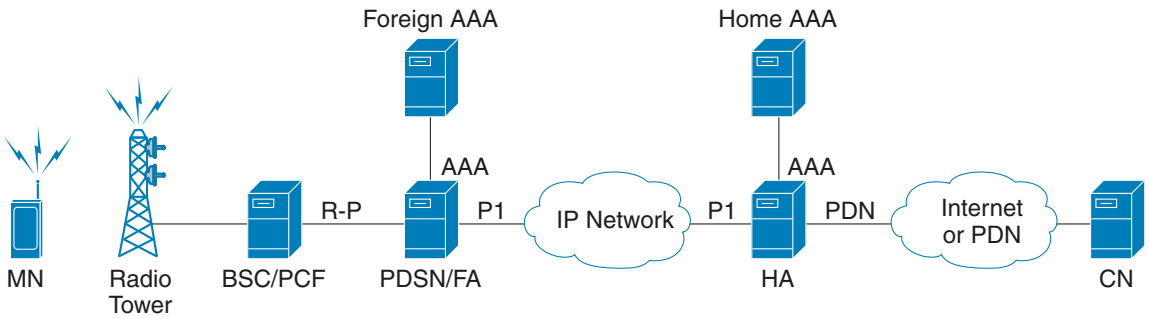
Command	Navigation	Description
Show MAG	*Expand MAG Node* > *Right-click MAG service* > **Commands** > **Show**	Use this command to view and confirm the configuration details for the selected MAG service.
Create Profile QCI-Mapping	*Right-click on context* > **Commands** > **Configuration** > **Mobility** > **Create Profile QCI-Mapping**	Use this command to create a QCI profile.
Delete Profile QCI Mapping	*Expand Profile node* > and then Profile-QCI Mapping node > *Right-click the local context* > **Commands** > **Configuration** > **Delete Profile QCI Mapping**	Use this command to delete QCI profile.
Create Profile	*Expand Profile node* > and then Profile-QCI Mapping node > *Right-click the local context* > **Commands** > **Configuration** > **Create Profile**	Use this command to create an entry for the QCI mapping profile.
Modify Profile **Delete Profile**	*Expand Profile node* > *profile* > *Right-click on profile entry* > **Commands** > **Configuration**	Use these commands to modify/delete the entry for the QCI mapping profile.

Monitoring Home Agent (HA)

A Home Agent (HA) stores information about the mobile nodes whose permanent home address is in the home agent's network. When a node wants to communicate with the mobile node, it sends packets to the permanent address. Because the home address logically belongs to the network associated with the HA, normal IP routing mechanisms forward these packets to the home agent.

When a mobile node moves out of the home network, the HA still manages to deliver the packets to the mobile node. This is done by interacting with the Foreign Agent (FA) that the mobile node is communicating with using the Mobile IP (MIP) Standard. Such transactions are performed through the use of virtual private networks that create MIP tunnels between the HA and FA. The following figure displays the configuration between the FA and HA network deployment.

Figure 27-11 Home Agent Topology



When functioning as a HA, the system can either be located within the carrier's 3G network or in an external enterprise or ISP network. The FA terminates the mobile subscriber's PPP session, and then routes data to and from the appropriate HA on behalf of the subscriber.

In accordance with Request for Comments (RFC) 2002, the FA is responsible for mobile node registration with, and tunneling of data traffic from/to the subscriber's home network. The HA is also responsible for tunneling traffic, but it maintains subscriber location information separately in the Mobility Binding Records (MBR).

Viewing the Home Agent Configuration

To view the Home Agent configuration:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > **Home Agent**. The list of home agent services configured in Prime Network are displayed in the content pane.

Step 3 From the **Home Agent** node, choose a home agent service. The home agent service details are displayed in the content pane as shown in Figure 27-12.

Figure 27-12 Home Agent Service Details

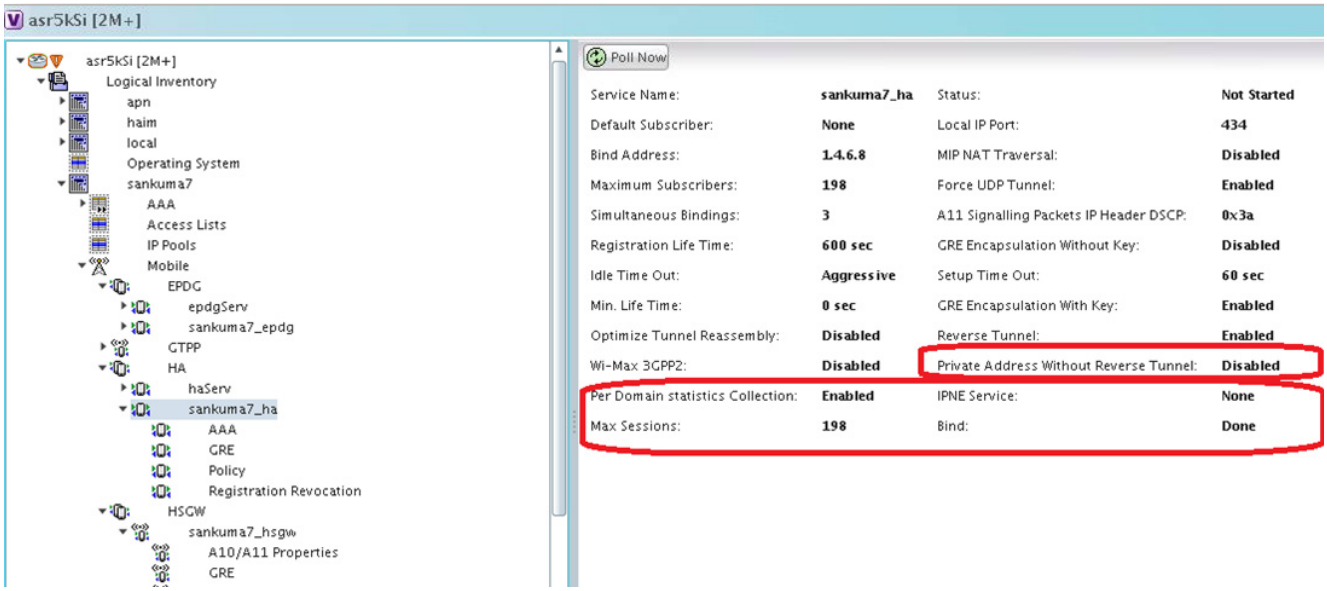


Table 27-75 displays the Home Agent service details.

Table 27-75 Home Agent Service Details

Field	Description
Service Name	The name of the home agent service.
Status	The status of the home agent service, which can be any one of the following: • Down • Running • Initiated • Unknown This field defaults to **Down**.
Default Subscriber	The name of the subscriber template that is applied to the subscribers.
Local IP Port	The User Datagram Protocol (UDP) port for the R-P interface of the IP socket. This IP port can be any value between 1 and 65535 and defaults to 699.
Bind Address	The IP address to which the service is bound to. This can be any address in the IPV4/IPv6 range.
MIP NAT Traversal	Indicates whether the acceptance of UDP tunnels for NAT traversal is enabled.
Max. Subscribers	The maximum subscriber sessions that could be supported.

Table 27-75 Home Agent Service Details (continued)

Field	Description
Force UDP Tunnel	Indicates whether HA would accept requests when Network Address Translation (NAT) is not detected but the Force bit is set in the Registration Request (RRQ) with the UDP Tunnel Request.
Simultaneous Bindings	The maximum number of care of addresses that can be simultaneously bound for the same user identified by Network Access Identifier (NAI) and Home address.
Destination Context	The name of the context to assign to the subscriber, after authentication.
A11 Signalling Packets IP Header DSCP	The Differential Services Code Point (DSCP) value in the IP header.
Registration Life Time	The registration lifetime configured for all the subscribers to the service.
GRE Encapsulation Without Key	Indicates whether Generic Routing Encapsulation (GRE) without encapsulation key is used during Mobile IP sessions with FA.
Idle Time Out	The method the HA service uses to determine the time to reset a session idle timer, which can be any one of the following: • Aggressive • Handoff • Normal
SPI List	The Security Parameter Index (SPI) between the HA service and the FA.
Optimize Tunnel Reassembly	Indicates whether the option to optimize tunnel reassembly is enabled.
Wi-Max 3GPP	Indicates whether the Worldwide Interoperability for Microwave Access (Wi-Max)-3GPP option is enabled for the Home agent service.
Private Address without Reverse Tunnel	This allows calls with private addresses and there is no reverse tunneling.
Per Domain Statistics Collection	This enables/disables per-domain statistics collection.
Max Sessions	Configures the maximum number of subscribers that can use this service. Default is 800000.
IPNE Service	Configures associated IPNE Service.
Bind	Binds Home Agent service to IP address of interface.
Radius Accounting Dropped Pkts	Indicates that the RADIUS accounting related configuration is enabled or disabled for dropped packets. By default this feature is disabled.
Setup Time Out	The maximum time (in seconds) allowed for session setup.
Reverse Tunnel	Indicates whether the reverse tunnel feature is enabled for the home agent feature. **Note** A reverse tunnel is a tunnel that starts at the care-of address of the mobile node and terminates at the home agent. A mobile node can request a reverse tunnel between the foreign agent and the home agent when the mobile node registers.

Table 27-75 Home Agent Service Details (continued)

Field	Description
Min. Life Time	The minimum registration life time for a mobile IP session.
GRE Encapsulation With Key	Indicates whether GRE is used during mobile IP sessions with an FA.
FA HA SPIs / MN HA SPIs tab	
SPI Number	The number to indicate the security context between services.
Remote Address	The IP address of the source service.
Hash Algorithm	The hash algorithm used between the source and destination services.
Time Stamp Tolerance	The acceptable allowable difference in time stamps. If this difference is exceeded, then the session is rejected.
Replay Protection	The replay protection scheme that should be implemented by the service.
Permit Any Hash Algorithm	Indicates whether verification of MN-HA authenticator using other hash algorithms is allowed, on failure of the configured hash algorithm. **Note** This field is available only in the **MN HA SPIs** tab.
Description	The description of the SPI.
IPSEC Crypto Maps	
Map Name	The name of the crypto map that is configured in the same context that defines the IPSec tunnel properties.
Peer FA Address	The IP address of the Peer FA to which the IPSEC SA will be established.
Skey Expiry	The expiry information of the secret key.

Viewing the AAA Configuration for Home Agent Service

In order to support Packet Data Serving Node (PDSN), FA, and HA functionality, the system must be configured with at least one source context and at least two destination contexts as shown in the following figure.

The source context will facilitate the PDSN service(s), and the R-P interfaces. The AAA context will be configured to provide foreign/home AAA functionality for subscriber sessions and facilitate the AAA interfaces.

To view the AAA configuration:

Step 1 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Mobile > Home Agent** > *Home agent service* > **AAA**. The AAA configuration details are displayed in the content pane.

Table 27-76 displays the AAA configuration for a home agent service.

Table 27-76 AAA Configuration for Home Agent Service

Field	Description
AAA Context	The AAA context for the home agent service. Click this link to view the relevant AAA context.
AAA Accounting	Indicates whether the Home Agent can send AAA accounting information for subscriber sessions.
AAA Accounting Group	The AAA Accounting group for the Home agent service.
AAA Distributed MIP Keys	Indicates the usage of AAA distributed MIP keys for authenticating RRQ for WiMax HA calls.
DMU Refresh Key	Indicates whether the Home Agent is allowed to retrieve the MN-HA key again from the AAA during the call and use this freshly retrieved key value to recheck authentication.
IMSI Authentication	Indicates whether MN-AAA or MN-FAC extensions are present in the RRQ.
MN HA Authentication Type	Indicates whether the HA service looks for an MN-HA authentication in the RRQ.
MN AAA Authentication Type	The method used to send authentication request to AAA for each re-registration attempt. **Note** The initial registration request and de-registrations are handled normally.
PMIP Authentication	Indicates whether the HA service looks for an PMIP authentication in the RRQ.
Stale Key Disconnect	Indicates whether the call must be disconnected immediately on failure of MN-HA authentication.
Skew Lifetime	The IKE pre-shared key\u2018s time skew.

Viewing the GRE Configuration for Home Agent Service

To view the GRE configuration:

Step 1 In the **Logical Inventory** window, choose **Logical Inventory > *Context* > Mobile > Home Agent** > *Home agent service* > **GRE**. The GRE configuration details are displayed in the content pane.

Table 27-77 displays the GRE configuration for a home agent service.

Table 27-77 GRE Configuration for Home Agent Service

Field	Description
Checksum	Indicates whether insertion of GRE checksum in outgoing GRE data packets is enabled.
Checksum Verify	Indicates whether verification of GRE checksum in incoming GRE packets is enabled.
Reorder Timeout	The maximum amount of time (in milliseconds) to wait before reordered out-of-sequence GRE packets are processed.

Table 27-77 GRE Configuration for Home Agent Service (continued)

Field	Description
Sequence Mode	The method to handle incoming out-of-sequence GRE packets, which can be any one of the following: • Reorder • None
Sequence Numbers	Indicates whether the option to insert or remove GRE sequence numbers in GRE packets is enabled.

Viewing the Policy Configuration for Home Agent Service

To view the Policy configuration:

Step 1 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Mobile > Home Agent** > *Home agent service* > **Policy**. The Policy configuration details are displayed in the content pane.

Table 27-78 displays the Policy configuration for a home agent service.

Table 27-78 Policy Configuration for Home Agent Service

Field	Description
BC Response Code	The response code for a binding cache (BC) query result in response to a network failure or error.
NW-Reachability Policy	The action to be taken on detection of an upstream network-reachability failure.
Over Load Policy	The overload policy within the HA service.
New Call Policy	The new call policy within the HA service.
Null Username Policy	Configures Null Username Policy to HA service
Over Load Redirect / NW-Reachability Redirect	
IP Address	The IP address associated with the policy.
Weight	The weightage of the IP address associated with the policy.

Viewing the Registration Revocation Details for a Home Agent Service

To view the Registration revocation configuration details:

Step 1 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Mobile > Home Agent** > *Home agent service* > **Registration Revocation**. The configuration details are displayed in the content pane.

Table 27-79 displays the Registration Revocation configuration for a home agent service.

Table 27-79 Registration Revocation configuration for Home Agent Service

Field	Description
Registration Revocation State	Indicates whether the Registration Revocation Status is enabled.
Revocation IBit	Indicates whether the Revocation Ibit feature is enabled.
Send NAI Extension	Indicates whether the option to send NAI extension in the revocation message is enabled.
Handoff Old FA	Indicates whether the option to send a revocation message from the HA to the FA is enabled. **Note** The revocation message is sent from the HA to the FA when an inter-access gateway or FA handoff of the MIP session occurs.
Idle Timeout	Indicates whether the HA must send a revocation message to the FA when the session times out.
Revocation Max Retries	The number of times the revocation message can be retransmitted.
Revocation Timeout	The maximum amount of time (in seconds) to wait for the receipt of an acknowledgement from the FA before the revocation message is transmitted again.

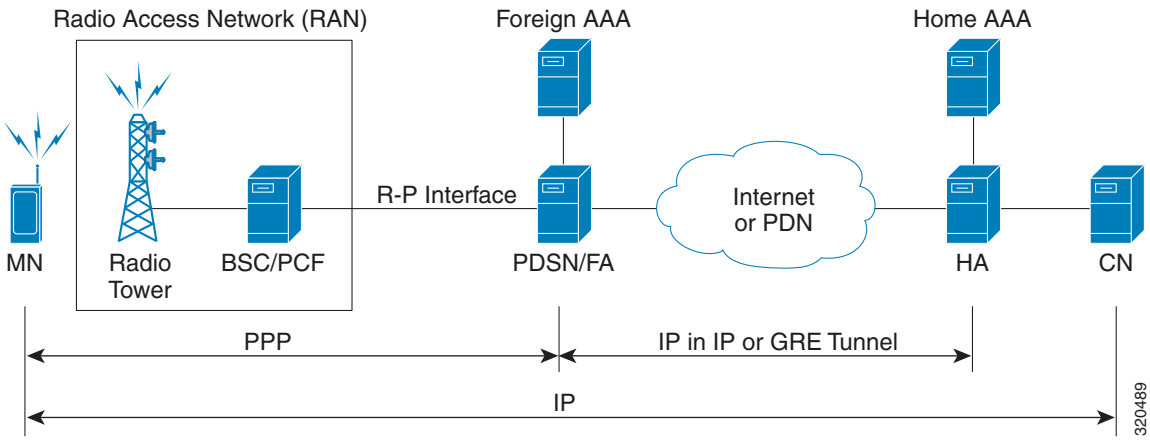
Monitoring the Foreign Agent (FA)

A Foreign Agent (FA) is basically a router on a mobile node's visited network that provides routing services to the mobile node. The FA acts as a mediator between the mobile node and it's home agent (HA). When the mobile node moves out of its home network, the FA registers the mobile node with a Care of Address (CoA). It also facilitates routing information to the mobile node's home agent, which contains the permanent address of the node.

When a node tries to communicate with a mobile node that is roaming, it sends packets to the permanent address. The HA interacts with the FA and delivers the packets to the mobile node using the COA.

Figure 27-13 depicts the function of a foreign agent in a network and the different components that it interacts with.

Figure 27-13 Foreign Agent Architecture



Viewing the Foreign Agent Configuration Details

To view the Foreign Agent configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > **FA.** The list of Foreign agents configured in Prime Network are displayed in the content pane.

Step 3 From the **FA** node, choose a FA service. The FA service details are displayed in the content pane as shown in Figure 27-14.

Figure 27-14 Foreign Agent Service Details

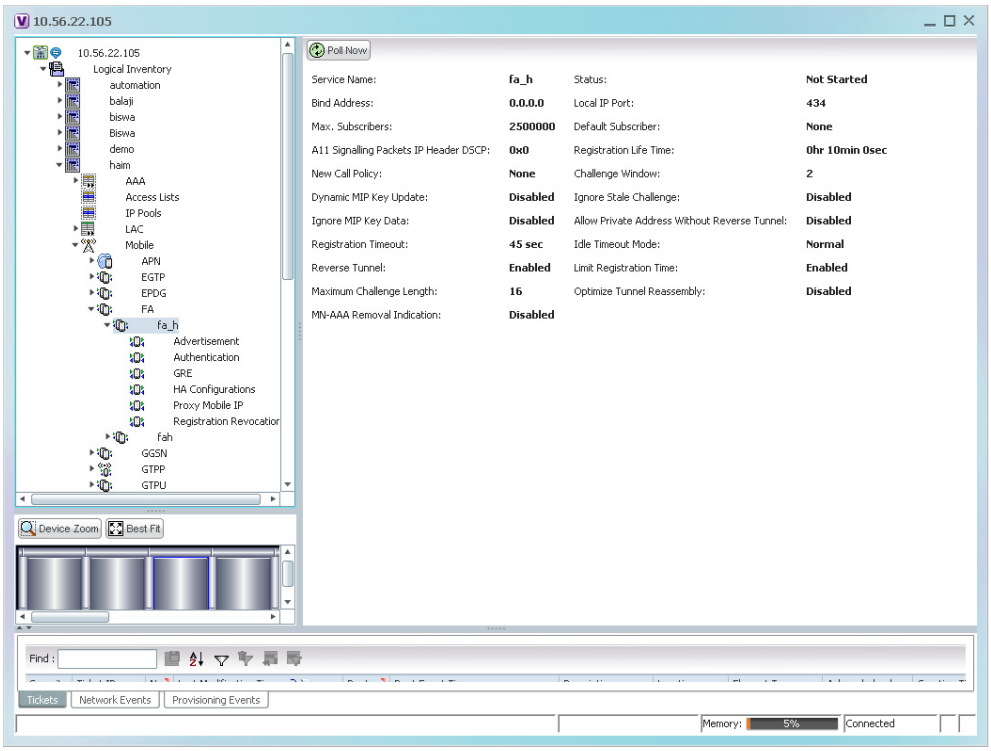


Table 27-80 displays the Foreign Agent configuration details.

Table 27-80 FA Configuration Details

Field	Description
Service Name	The unique name to identify the FA service.
Status	The status of the FA service, which can be any one of the following: • Down • Running • Initiated • Unknown This field defaults to **Down**.
Bind Address	The IPv4 address to which the service is bound.
Local IP Port	The UDP port for the R-P Interface of the IP socket. This port can be any value between 1 and 65535, and defaults to 434.
Max. Subscribers	The maximum subscriber sessions that is supported by the service. This can be any value between 0 and 2500000, and defaults to 2500000.
Default Subscriber	The name of the subscriber template that is applicable to the subscribers using this domain alias.
A11 Signalling Packets IP Header DSCP	The Differential Service Code Point (DSCP) value in the IP header. This value can range between 0x0 and 0x3F, and defaults to 0x0F. **Note** The Differentiated Services (DS) field of a packet contains 6 bits that represents the DSCP value. Out of these 6 bits, five of them represent the DSCP. Hence, you can assign upto 32 DSCPs for various priorities.
Registration Life Time	The amount of time (in seconds) that an A10 connection can exist before its registration expires. This time can be any value between 1 and 65534, and defaults to 1800 seconds.
New Call Policy	The call policy for one or all the services, which can be any one of the following: • Reject • None This field defaults to **None**.
Challenge Window	The number of challenges that can be handled by the FA.
Dynamic MIP Key Update	The status of the Dynamic Mobile IP Key update feature. This option is disabled by default.
Ignore Stale Challenge	The status of the Ignore Stale Challenge in MIP RRQ. This option is disabled by default.
Ignore MIP Key Data	The status of the Ignore MIP Key data. This option is disabled by default.
Allow Private Address Without Reverse Tunnel	Indicates whether the mobile node can use reverse tunnel for a private address. This option is disabled by default.
Registration Timeout	The amount of time (in seconds) for the registration reply timeout.

Table 27-80 FA Configuration Details (continued)

Field	Description
Idle Timeout Mode	The idle timeout method, which can be any one of the following: • Normal • Aggressive
Reverse Tunnel	Indicates whether reverse tunneling is applicable for client mobile IP sessions. This option is enabled by default.
Limit Registration Time	Indicates whether MIP registration lifetime is shorter than session idle, absolute, and long-duration timeouts. By default, this option is enabled.
Maximum Challenge Length	The maximum length of the FA challenge.
Optimize Tunnel Reassembly	Indicates whether tunnel reassembly is optimized for fragmented large packets passed between HA and FA. By default, this option is disabled.
MN-AAA Removal Indication	Indicates whether the FA can remove MN-FAC and MN-AAA extensions from RRQs. By default, this option is disabled.
Max Sessions	The maximum number of subscriber sessions allowed.
Standalone FA Service	Shows the standalone FA service status. If the status is enabled then, the system performs only as a standalone FA.

You can also view the following configuration details for a Foreign Agent service:

- Advertisement—Foreign agents advertise their presence on their attached links by periodically multicasting or broadcasting messages called agent advertisements. Mobile nodes listen to these advertisements and determine if they are connected to their home link or foreign link. Rather than waiting for agent advertisements, an MN can also send an agent solicitation. This solicitation forces any agents on the link to immediately send an agent advertisement.
- Authentication—Authentication verifies users before they are allowed access to the network and network services.
- GRE—Generic routing encapsulation (GRE) is a tunneling protocol used by Mobile IP. The GRE tunnel interface creates a virtual point-to-point link between two routers at remote points over an IP internetwork. If the GRE for Cisco Mobile Networks feature is enabled, the mobile router will request GRE encapsulation in the registration request only if the FA advertises that it is capable of GRE encapsulation (the G bit is set in the advertisement). If the registration request is successful, packets will be tunneled using GRE encapsulation. If the GRE for Cisco Mobile Networks feature is enabled and the mobile router is using collocated care-of address (CCoA), the mobile router will attempt to register with the HA using GRE encapsulation. If the registration request is successful, packets will be tunneled using GRE encapsulation.
- HA Configurations—Once the mobile node roams to a new network, it must register with the home agent as being away from home. Its registration is sent by way of the Foreign Agent (FA), the router providing service on the foreign network. A security association between the home agent (HA) and the foreign agent (FA) is mandatory.

- Proxy Mobile IP—Proxy Mobile IP supports Mobile IP for wireless nodes without requiring specialized software for those devices. The wireless access point acts as a proxy on behalf of wireless clients that are not aware of the fact that they have roamed onto a different Layer 3 network. The access point handles the IRDP communications to the foreign agent and handles registrations to the home agent.
- Registration Revocation—Registration Revocation is a method by which a mobility agent (one that provides Mobile IP services to a mobile node) can notify the other mobility agent of the termination of a registration due to administrative reasons or MIP handoff. When a mobile changes its point of attachment (FA), or needs to terminate the session administratively, the HA sends a registration revocation message to the old FA. The old FA tears down the session and sends a registration revocation acknowledgement message to the HA. Additionally, if the PDSN/FA needs to terminate the session administratively, the FA sends a registration revocation message to the HA. The HA deletes the binding for the mobile, and sends a registration revocation acknowledgement to FA.

Viewing the Advertisement Configuration Details

To view the Advertisement configuration details for a foreign agent:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Mobile > FA** > *FA service* > **Advertisement.** The details are displayed in the content pane.

Table 27-81 displays the Advertisement configuration details.

Table 27-81 Advertisement Configuration Details

Field	Description
Advertisement Delay	The time delay (in milliseconds) for the first advertisement for a WiMax call. This time can be any value between 10 and 5000, and defaults to 1000.
Advertisement Interval	The advertisement interval time (in milliseconds). This time can be any value between 100 and 1800000, and defaults to 5000 milliseconds.
Advertisement Life Time	The maximum registration life time (in seconds) of the advertisement. This time can be any value between 1 and 65535, and defaults to 600 seconds.
Number of Advertisements Sent	The number of initial agent advertisements sent. This number can be any value between 1 and 65535, and defaults to 5.
Prefix Length Extension	Indicates whether the service address of the FA must be included in the Router Address field of the agent advertisement. If this field is set to **Yes**, then a prefix-length extension is appended to the router address field. By default, this option is set to **No**.

Viewing the Authentication Configuration Details

To view the Authentication configuration details for a foreign agent:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Mobile > FA** > *FA service* > **Authentication.** The details are displayed in the content pane.

Table 27-82 displays the Authentication configuration details.

Table 27-82 Authentication Configuration Details

Field	Description
MN AAA Authentication Policy	The MN AAA Authentication policy, which can be any one of the following: • Ignore-after-handoff • Init-reg • Init-reg-except-handoff • Always • Renew-reg-noauth • Renew-and-dereg-noauth This field defaults to Always.
MN HA Authentication Policy	The policy to authenticate Mobile Node HA in the RRP, which can be any one of the following: • Always • Allow-noauth This field defaults to **Allow-noauth**.
AAA Distributed MIP Keys Override	Indicates whether the AAA distributed MIP Keys Override option is enabled. In other words, if this feature is enabled, then the authentication parameters for the FA service will override the dynamic keys from AAA with static keys. **Note** This feature supports those MIP registrations with an HA that does not support dynamic keys.
MN AAA Optimized Retries	Indicates whether the authentication request must be sent to the AA for each re-registration.

Viewing the GRE Configuration Details

To view the Generic Routing Encapsulation (GRE) configuration details for a foreign agent:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Mobile > FA** > *A service* > **GRE.** The details are displayed in the content pane.

Table 27-83 displays the GRE configuration details.

Table 27-83 GRE Configuration Details

Field	Description
Checksum	Indicates whether the Checksum feature is enabled in outgoing GRE packets. By default, this option is disabled.
GRE Encapsulation	Indicates whether GRE is used when establishing a Mobile IP session. If this option is enabled, the FA requests HA to use GRE when establishing a MIP session. If this option is disabled, the FA will not set the GRE bit in agent advertisements to the mobile node.
Checksum Verify	Indicates whether the checksum field must be verified in the incoming GRE packets. By default, this option is disabled.
Reorder Timeout	The maximum time (in milliseconds) to wait before processing the GRE packets that are out of sequence. This time can be any value between 0 and 5000, and defaults to 100 milliseconds.
Sequence Mode	The mode used to handle the incoming out-of-sequence packets, which can be any one of the following: • Reorder • None This field defaults to **None**.
Sequence Numbers	Indicates whether GRE sequence numbers must be inserted into the data that is about to be transmitted over the A10 interface. This option is disabled by default.

Viewing the HA Configuration Details

To view the HA configuration details for a foreign agent:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Mobile > FA** > *FA service* > **HA.** The details are displayed in the content pane.

Table 27-84 displays the HA configuration details.

Table 27-84 HA Configuration Details

Field	Description
HA Monitoring	The HA monitoring status of the FA. This option is disabled by default.
AAA-HA Override	Indicates whether AAA HA can override Mobile Node during call establishment for HA assignment.
Dynamic HAFailover	Indicates whether failover during call establishment for Home Agent assignment is allowed.
HA Monitor Interval	The time interval (in seconds) to send HA monitoring requests. This time can be any value between 1 and 36000, and defaults to 30 seconds.
HA Monitor Maximum Inactivity Time	The maximum amount of time (in seconds) when there is no MIP traffic between FA and HA, which triggers the HA monitoring feature. This time can be any value between 30 and 600, and defaults to 60 seconds.
HA Monitor Retry Count	The number of times HA monitoring requests are sent before deciding that the HA is not reachable. This count can be any value between 0 and 10, and defaults to 5.
FA SPI List Name	The name of the SPI list linked with the FA service and configured for the selected context. Clicking on this link will take you to the relevant list under the **SPI** node.
IKE	
Peer HA Address	The IP address of the peer home agent.
Crypto Map Name	The IKE crypto map for the peer home agent.
SPI	
SPI Number	The unique SPI number that indicates a security context between the services. This number can be any value between 256 and 4294967295.
Remote Address	The IP address of the source service, which is expressed either in the IPv4 dotted decimal notation or IPv6 colon separated notation.
Hash Algorithm	The hash algorithm used between the source and destination services.
Time Stamp Tolerance	The acceptable time difference (in seconds) in timestamps, which can be any value between 0 and 65535. **Note** If the actual timestamp difference exceeds the value here, then the session is rejected. If this value is 0, then the timestamp tolerance checking is disabled at the receiving end.
Replay Protection	The replay protection scheme that is implemented by the service.
Description	The description of the SPI.
Net Mask	The net mask for the IP address of the SPI. This field defaults to 255.255.255.255.
HA Monitor	Indicates whether HA monitoring is enabled.

Viewing the Proxy Mobile IP Configuration Details

To view the Proxy Mobile IP configuration details for a foreign agent:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Mobile > FA** > *FA service* > **Proxy Mobile IP.** The details are displayed in the content pane.

Table 27-85 displays the Proxy Mobile IP configuration details.

Table 27-85 Proxy Mobile IP Configuration Details

Field	Description
Proxy MIP	Indicates the status of the Proxy Mobile IP.
Encapsulation Type	The data encapsulation type to be used in PMIP call for specific FA services, which can be any one of the following: • IPIP • GRE This field defaults to **IPIP**.
HA Failover	The failover status of the FA. This option is disabled by default.
HA Failover Max Attempts	The maximum number of times for HA Failover. This can be any value between 1 and 10, and defaults to 4.
HA Failover Timeout	The timeout (in seconds) for the HA failover. This time can be any value between 1 and 50, and defaults to 2.
HA Failover Attempts Before Switching	The number of times HA Failover was attempted, before switching over to an alternate HA. This can be any value between 1 and 5, and defaults to 2.
HA Failover Reply Code Trigger	The action to be taken on receipt of the configured reject code.
Max Retransmissions	The maximum number of times the FA is allowed to retransmit Proxy Mobile IP registration requests to the HA. This number can be any value between 1 and 4294967295, and defaults to 5.
Retransmission Timeout	The retransmission timeout (in seconds) for Proxy Mobile IP messages on event of failover. This time can be any value between 1 and 100, and defaults to 3.
Renew Time	The percentage of lifetime at which point the renewal is sent. This percent can be between 0 and 100, and defaults to 75.

Viewing the Registration Revocation Configuration Details

To view the Registration Revocation configuration details for a foreign agent:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Mobile > FA** > *FA service* > **Registration Revocation.** The details are displayed in the content pane.

Table 27-86 displays the Registration Revocation configuration details.

Table 27-86 Registration Revocation Configuration Details

Field	Description
Registration Revocation State	Indicates the status of the registration revocation. If this feature is enabled, then the FA can send a revocation message to the HA when revocation is negotiated with the HA and MIP binding is terminated. This feature is disabled by default.
Revocation IBit	The status of the Ibit on the registration revocation. If this feature is enabled, the FA can negotiate the Ibit via PRQ/RRP messages and process the Ibit revocation messages. This feature is disabled by default.
Internal Failure	Indicates whether a revocation message must be sent to the HA for those sessions that are affected by internal task failure.
Revocation Maximum Retries	The maximum number times a revocation message must be retransmitted before failure. This value can be any value between 0 and 10, and defaults to 3.
Revocation Timeout	The time period (in seconds) to wait for an acknowledgement from the HA before the revocation message is retransmitted. This time can be any value between 1 and 10, and defaults to 3.

Configuration Commands for Foreign Agent

To enable Mobile IP services on your network, you must determine which home agents will facilitate the tunneling for selected IP address, and where these devices or router will be allowed to roam. The areas, or subnets, into which the hosts are allowed to roam determine where foreign agent services need to be set up.

Use the following commands to manage foreign agents. These commands can be launched from the logical inventory by choosing the *Context* > **Commands** > **Configuration** or *Context* > **Commands** > **Show**. Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-87 Foreign Agent Configuration Commands

Command	Navigation	Description
Create FA	Right-click the *context* > **Commands** > **Configuration** > **Mobility**	Use this command to create a new foreign agent service for the selected context.
Modify FA **Delete FA**	*Expand FA node* > *Right-click FA service* > **Commands** > **Configuration**	Use these commands to modify/delete an existing foreign agent service configured for the selected context.
Show FA	*Expand FA node* > *Right-click FA service* > **Commands** > **Show**	Use this command to view and confirm the foreign agent configuration details.
Create SPI	*Expand FA node* > *Right-click FA service* > **Commands** > **Configuration**	Use this command to configure Security Parameter Index (SPI) for a foreign agent service.

Table 27-87 Foreign Agent Configuration Commands (continued)

Command	Navigation	Description
Modify SPI **Delete SPI**	*Expand FA node* > *Expand FA service node* > **HA Configuration >** *Right-click on SPI Number in content pane* > **Commands** > **Configuration**	Use these commands to modify and delete an existing SPI configured for a foreign agent service.
Create IKE	*Expand FA node* > *Right-click FA service* > **Commands** > **Configuration**	Use this command to configure Internet Key Exchange (IKE) for a foreign agent service. If foreign agent reverse tunneling creates a tunnel that transverses a firewall, any mobile node that knows the addresses of the tunnel endpoints can insert packets into the tunnel from anywhere in the network. It is recommended to configure Internet Key Exchange (IKE) or IP Security (IPSec) to prevent this.
Modify IKE **Delete IKE**	*Expand FA node* > *Expand FA service node* > **HA Configuration >** *right-click on IKE Number in content pane* > **Commands** > **Configuration**	Use these commands to modify and delete an existing IKE configured for a foreign agent service.
Modify Advertisement	*Expand FA node* > *FA service* > *right-click* **Advertisement** > **Commands** > **Configuration**	Use this command to modify the advertisement configuration settings specified for a foreign agent.
Modify Authentication	*Expand FA node* > *FA service* > *right-click* **Authentication** > **Commands** > **Configuration**	Use this command to modify the authentication configuration settings specified for a foreign agent.
Modify GRE	*Expand FA node* > *FA service* > *right-click* **GRE** > **Commands** > **Configuration**	Use this command to modify the Generic Routing Encapsulation (GRE) configuration settings specified for a foreign agent.
Modify HA Configuration	*Expand FA node* > *FA service* > *right-click* **HA Configuration** > **Commands** > **Configuration**	Use this command to modify the Home Agent configuration settings specified for a foreign agent.
Modify Proxy Mobile IP	*Expand FA node* > *FA service* > *right-click* **Proxy Mobile IP** > **Commands** > **Configuration**	Use this command to modify the Proxy Mobile IP configuration settings specified for a foreign agent.
Modify Registration Revocation	*Expand FA node* > *FA service* > *right-click* **Registration Revocation** > **Commands** > **Configuration**	Use this command to modify the Registration revocation configuration settings specified for a foreign agent.

Monitoring Evolved Packet Data Gateway (ePDG)

In today's market, there are multiple access networks for mobile technologies. For example, the following access networks are available for 3rd Generation Partnership Project (3GPP) network:

- General Packet Radio Service (GPRS). See GPRS/UMTS Networks, page 27-1.

- Global System for Mobile communication (GSM)
- Universal Mobile Telecommunication System (UMTS). See GPRS/UMTS Networks, page 27-1.

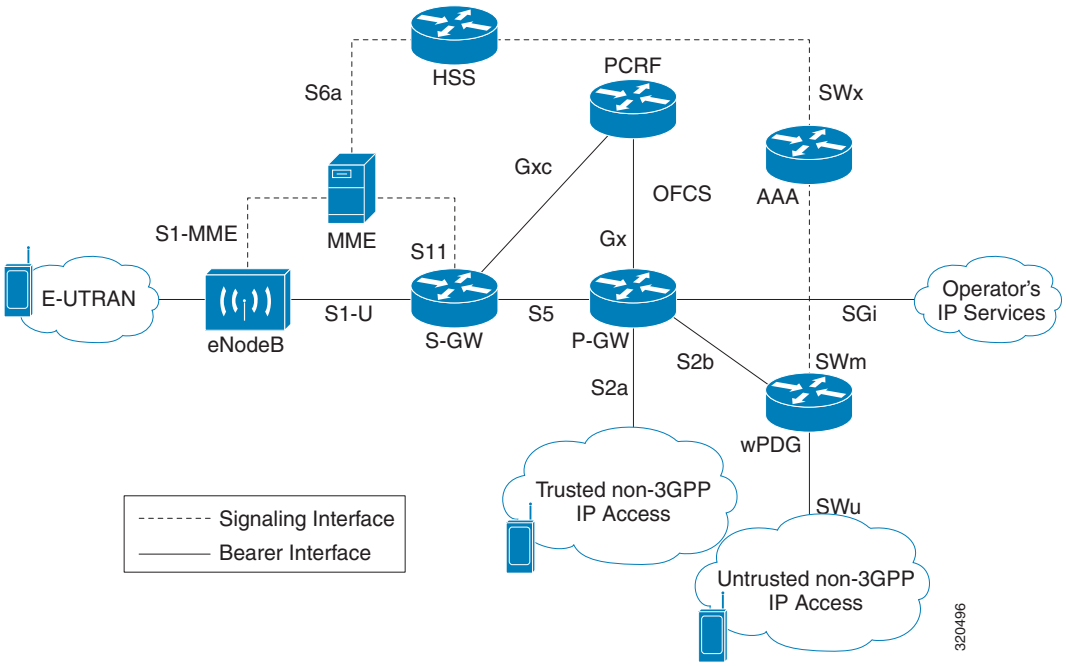
The following access network are available for Non-3GPP network:

- Worldwide Interoperability for Microwave Access (WiMAX)
- CDMA2000
- Wireless local area network (WLAN)
- Fixed networks

The Non-3GPP networks can be categorized into two—Trusted and Untrusted. While the trusted non-3GPP networks can interact directly with the Evolved Packet Core (EPC), the untrusted networks are required to pass through a security gateway to gain access to the EPC. This security gateway is called the Evolved Packet Data Gateway or ePDG.

When a user transmits data to the EPC using an untrusted non-3GPP network access, the ePDG must act as a termination node of IPSec tunnels established with the user equipment and secure the data being sent. Figure 27-15 shows the ePDG architecture.

Figure 27-15 ePDG Architecture



IP Security (IPSec)

Internet Protocol Security or IPSec is a protocol suite that interacts with one another to provide secure private communications across IP networks. These protocols allow the system to establish and maintain secure tunnels with peer security gateways. In accordance with the following standards, IPSec provides a mechanism for establishing secure channels from mobile subscribers to pre-defined end points (such as enterprise or home networks):

- RFC 2401, Security Architecture for the Internet Protocol
- RFC 2402, IP Authentication Header (AH)

- RFC 2406, IP Encapsulating Security Payload (ESP)
- RFC 2409, The Internet Key Exchange (IKE)
- RFC-3193, Securing L2TP using IPSEC, November 2001

IPSec can be implemented for the following applications:

- **PDN Access**: Subscriber IP traffic is routed over an IPSec tunnel from the system to a secure gateway on the packet data network (PDN) as determined by access control list (ACL) criteria.
- **Mobile IP**: Mobile IP control signals and subscriber data is encapsulated in IPSec tunnels that are established between foreign agents (FAs) and home agents (HAs) over the Pi interfaces.

IKEv2 and IPSec Encryption

ePDG supports Internet Key Exchange Version 2 (IKEv2) and IP Security Encapsulating Security Payload (IPSec ESP) encryption over IPv4 transport. The IKEv2 and IPSec encryption takes care of network domain security for all IP packet switched networks. It uses cryptographic techniques to ensure ensures confidentiality, integrity, authentication, and anti-replay protection.

ePDG Security

In Prime Network, the following security services are available for ePDG:

- Crypto template—Used to define the IKEv2 and IPSec policies. In other words, it includes IKEv2 and IPSec parameters for keepalive, lifetime, NAT-T and cryptographic and authentication algorithms.
- EAP Profile—Defines the EAP authentication method and associated parameters.
- Transform Set—Define the negotiable algorithms for IKE SAs (Security Associations) and Child SAs to enable calls to connect to the ePDG.

Viewing the Crypto Template Service Details

To view the Crypto template details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory > *Context* > Security Association > Crypto Template.** The list of crypto templates are displayed in the content pane.

Step 3 In the **Crypto Template** node, choose the crypto template. The template details are displayed in the content pane. Figure 27-16 displays the crypto template details.

Figure 27-16 Crypto Template Details

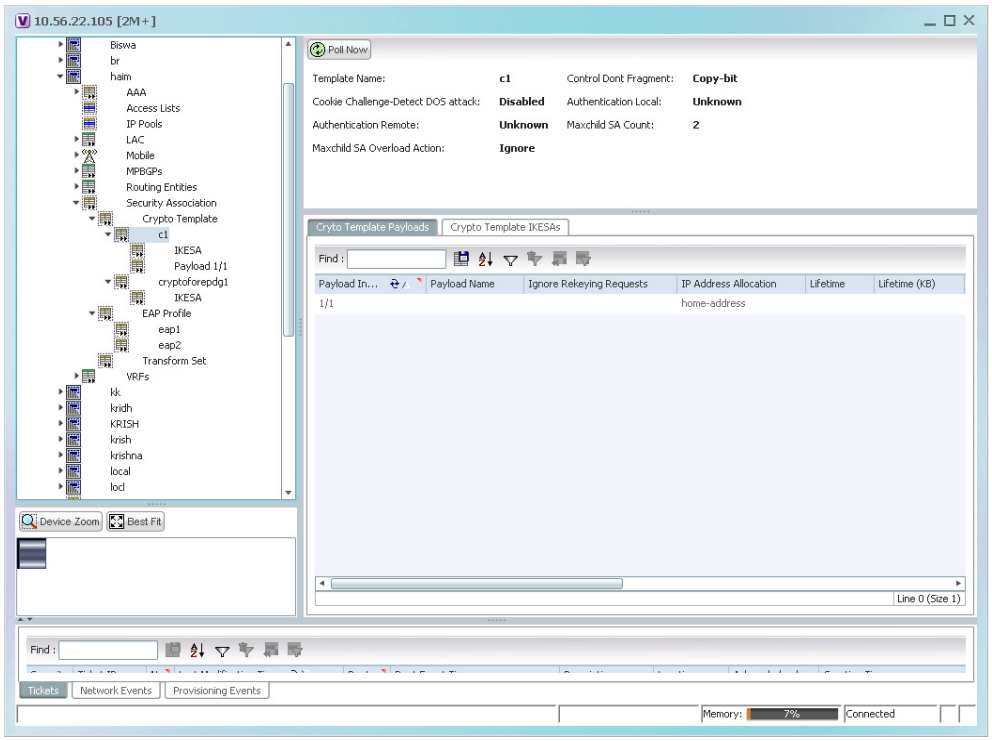


Table 27-88 displays the Crypto template details.

Table 27-88 Crypto Template Details

Field	Description
Template Name	The unique name of the template.
Control Don't Fragment	The Don't Fragment (DF) bit in the IPSec tunnel data packet, which is encapsulated in the IPSec headers at both ends. The values for this field are: • clear-bit—Clear DF Bit • copy-bit—Copy DF bit from inner header • set-bit—Set DF Bit This field defaults to **copy-bit**.
Cookie Challenge-Detect DOS Attack	The cookie challenge parameters for the crypto template, which is used to prevent malicious Denial of Service (DOS) attacks against the server. **Note** This feature prevents DOS attacks by sending a challenge cookie. If the response from the sender does not incorporate the expected cookie data, the packets are dropped.

Table 27-88 Crypto Template Details (continued)

Field	Description
Notify Payload - Half Open Session Start	The initial count of the number of half-open sessions per IPSec manager. Transmission of information will start only when the number of half-open sessions currently open exceed the starting count. **Note** A session is considered half open if a Packet Data Interworking Function (PDIF) has responded to an IKEv2 INIT request with an IKEv2 INIT response, but no further messages were received on the particular IKE SA.
Notify Payload - Half Open Session End	The maximum count of half open sessions per IPSec manager. Transmission of information will stop when the number of half-open sessions currently open is less than this count.
Authentication Local	The local gateway key used for authentication.
Authentication Remote	The remote gateway key used for authentication.
Keepalive Interval	The period of time (in seconds) that must elapse before the next keepalive request is sent.
Keepalive Retries	The period of time (in seconds) that must elapse before the keepalive request is resent.
Keepalive Timeout	The keepalive time (in terms of seconds) for dead peer detection.
Maxchild SA Count	The maximum number of child SA per IKEv2 policy, which can be any value between 1 and 4.
Maxchild SA Overload Action	The action to be taken when the specified soft limit for the maximum number of SA is reached, which can be any one of the following: Ignore—The IKEv2 stack ignores the specified soft limit for the SA and allows new SA to be created. Terminate—The IKEv2 stack does not allow new child SA to be created when the specified soft limit is reached.
NAI CustomIDr	The unique user specified identification number to be used in the crypto template for Network Access Identifier (NAI).
Crypto Template Payloads	
Payload Instance	The payload instance configured for the crypto template.
Payload Name	The unique name of the crypto template payload.
Ignore Rekeying Requests	Indicates whether IKESA rekeying requests must be ignored.
IP Address Allocation	The IP Address Allocation scheme configured for the crypto template payload.
Lifetime	The lifetime (in seconds) for the IPSec Child Security Associations derived from the crypto template.
Lifetime (KB)	The lifetime (in kilo bytes) for the IPSec Child Security Associations derived from the crypto template.
Crypto Template IKESA	
IKESA Instance	The IKESA instance configured for the crypto template.

Table 27-88 Crypto Template Details (continued)

Field	Description
Allow Empty IKESA	Indicates whether empty IKESA is allowed. By default, empty IKESA is not allowed.
Certificate Sign	The certificate sign to be used. This field defaults to pkcs1.5.
Ignore Notify Protocol ID	Indicates whether the IKEv2 Exchange Notify Payload Protocol-ID values must be ignored for strict RFCA 4306 compliance.
Ignore Rekeying Requests	Indicates whether IKESA rekeying requests must be ignored.
Keepalive User Activity	Indicates whether the user inactivity timer must be reset when keepalive messages are received from the peer.
Max Retransmission Count	The maximum number of retransmissions of an IKEv2 IKE exchange request that is allowed if a corresponding IKEv2 IKE exchange response is not received.
Policy Congestion Rejection Notify Status	Indicates whether an error notification message must be sent in response to an IKE_SA INIT exchange, when IKESA sessions cannot be established anymore.
Policy Error Notification	Indicates whether an error notification message must be sent for invalid IKEv2 exchange message ID and syntax.
Rekey	Indicates whether IKESA rekeying must occur before the configured lifetime expires (which is approximately at 90% of the lifetime interval). By default, rekeying is not allowed.
Retransmission Timeout	The time period (in milliseconds) that must elapse before a retransmission of an IKEv2 IKE exchange request is sent when a corresponding response is not received.
Setup Timer	The number of seconds before a IKEv2 security association, which is not fully established, is terminated.
Mobike	Indicates that Mobike attribute is enabled for IKESA.
RFC Notification	Shows that RFC 5996 notifications is sent or received.
Ignore Notify Protocol ID	Indicates that IKEv2 Informational Exchange Notify Payload protocol ID is ignored for strict RFC 4306 compliance.
Notify Payload Error Message Attributes	
Notify UE	Displays the value for UE related errors.
Network Transient Minor	Displays the value for minor transient network errors.
Network Transient Major	Displays the value for major transient network errors.
Network Permanent	Displays the value for permanent network errors.
OCSP Attributes	
OCSP Responder Address	Displays the OCSP responder IPv4 address.
OCSP Responder Port	Displays the OCSP responder IPv4 port.
OCSP HTTP Version	Shows a http version 1.0 or 1.1 that is used for OCSP responder.

Viewing the EAP Profile Details

To view the EAP Profile details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Security Association > EAP Profile.** The list of profiles are displayed in the content pane.

Step 3 In the **EAP Profile** node, choose the profile. The profile details are displayed in the content pane.

Table 27-89 displays the EAP Profile details.

Table 27-89 EAP Profile Details

Field	Description
Name	The unique name of the EAP Profile.
Mode	The operative mode of the EAP profile, which can be any one of the following: • **Authenticator Pass Through**—Indicates that the EAP Authentication Requests must be passed to an external EAP Server. • **Authenticator Terminate**—Indicates that the EAP must act as an EAP Authentication Server.
Authentication Method	The EAP Authentication method to be used for the profile, which can be any one of the following: • If the Mode is **Authenticator Pass Through**: – eap-aka – eap-gtc – eap-md5 – eap-sim – eap-tls • If the Mode is Authenticator Terminate: – eap-gtc – eap-md5

Viewing the Transform Set Details

To view the Transform Set details for IKEv2 IPSec/IKEv2:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Security Association > Transform Set > IKEv2 IPSec Transform Set** or **IKEv2 Transform set.** The list of profiles are displayed in the content pane.

Step 3 In the **IKEv2 IPSec Transform Set** or **IKEv2 Transform set** node, choose the transform set. The relevant details are displayed in the content pane.

Table 27-90 displays the IKEv2 IPSec Transform set or IKEv2 Transform set details.

Table 27-90 IKEv2 IPSec Transform Set/IKEv2 Transform set Details

Field	Description
Name	The name of the transform set.
DH Group	The Diffie-Hellman (DH) group for the transform set, which can be any one of the following: • 1—Configure Diffie-Hellman Group 1:768-bit MODP Group • 14—Configure Diffie-Hellman Group 14:2048-bit MODP Group • 2—Configure Diffie-Hellman Group 2:1024-bit MODP Group • 5—Configure Diffie-Hellman Group 5:1536-bit MODP Group This field defaults to **2—Configure Diffie-Hellman Group 2:1024-bit MODP Group**. **Note** The DH group is used to determine the length of the base Prime numbers used during the key exchange process in IKEv2. The cryptographic strength of any key derived, depends in part, on the strength of the DH group upon which the prime numbers are based.
Cipher	The appropriate encryption algorithm and encryption key length for the IKEv2 IKE security association, which can be any one of the following: • 3des-cbc • aes-cbc-128 • aes-cbc-256 • des-cbc • Null This field defaults to AESCBC-128.
HMAC	The Hash Message Authentication Code (HMAC) for the IKEv2 IPSec transform set, which can be any one of the following: • aes-xcbc-96 • md5-96 • sha1-96 • sha2-256-128 • sha2-384-192 • sha2-512-256 This field defaults to **sha1-96**. **Note** HMAC is a type of message authentication code calculated using a cryptographic hash function in combination with a secret key to verify both data integrity and message authenticity. A hash takes a message of any size and transforms it into a message of fixed size (the authenticator value), which is truncated and transmitted.

Table 27-90 IKEv2 IPSec Transform Set/IKEv2 Transform set Details

Field	Description
Mode	The encapsulation mode for the transform set, which can be any one of the following: • transport • tunnel
ESN	Enable Extended Sequence Number (ESN) for IPSec (ESP/AH).
PRF	The Pseudo-random Function (PRF) for the transform set, which can be any one of the following: • aes-xcbc-128 • md5 • sha1 • sha2-256 • sha2-384 • sha2-512 This field defaults to SHA1. This field is applicable only for IKEv2 transform sets. **Note** This function is used to generate keying material for all cryptographic algorithms. It produces a string of bits that cannot be distinguished from random bit strings without the secret key.
Life Time	The time period for which the secret keys used for various aspects of a configuration is valid (before it times out). This field is applicable only for IKEv2 transform sets.

Viewing the ePDG Configuration Details

To view the ePDG configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory > *Context* > Mobile > EPDG.** The list of EPDG services configured in Prime Network are displayed in the content pane.

Step 3 From the **EPDG** node, choose an EPDG service. The EPDG service details are displayed in the content pane.

Table 27-91 displays the EPDG service details.

Table 27-91 EPDG Service Details

Field	Description
Service Name	The unique name of the ePDG service.
Status	The status of the ePDG service, which can be any one of the following: • Initiated • Running • Down • Started • Nonstarted
IP Address	The IPV4 address of the ePDG service.
UDP Port	The User Datagram Protocol (UDP) port of the ePDG service.
Crypto Template	The name of the IKEv2 crypto template to be used by the ePDG service. This template is used to define the cryptographic policy for the ePDG service.
Max Sessions	The maximum number of sessions allowed for the ePDG service.
PLMN ID	The unique identification code of the Public Land Mobile Network (PLMN) for the ePDG service. This id is made up of the Mobile Country Code (MCC) and the Mobile Network Code (MNC).
MAG Service Context	The name of the context where the Mobile Access Gateway (MAG) services are configured. If a MAG service is not configured for the ePDG service, then one of the MAG services defined in the context is selected.
MAG Service	The name of the MAG service that handles the mobile IPv6 sessions.
Setup Timeout	The maximum time (in seconds) allowed for the session setup.
DNS PGWClient Context	The name of the context where the Domain Name System (DNS) client is configured for the Packet Data Network Gateway (PWG) selection.
DNS PGW Selection	The criteria to select a PGW service from the DNS. This criteria is based on the topology and/or weight from the DNS.
FQDN	The Fully Qualified Domain Name (FQDN), which is used for longest suffix match during dynamic allocation.
PGW Selection Agent Info Error Action	The action to be taken when the expected MIP6 agent information is not received from Authentication, Authorization, and Accounting (AAA) or Hosting Solution Software (HSS).
User Name MAC Address Stripping	Indicates whether the MAC address in the username obtained from the user equipment must be stripped.
User Name MAC Address Validation	Indicates whether the MAC address in the username obtained from the user equipment must be validated.
User Name MAC Address Validation Failure Action	Indicates the action that must be taken on failure of the validation of the MAC address in the user name obtained from the user equipment.
New Call Policy	Indicates the busy-out policy that must be followed to reject the incoming calls from individual users.

Table 27-91 EPDG Service Details

Field	Description
PGW Selection Mechanism	The ePDG service should be configured indicating preferred method of PGW selection, whether local configuration or DNS/AAA server based PGW selection. Local Configuration based PGW selection as fallback mechanism is default configuration behavior.
QCI QOS Mapping	It indicates the associated QCI QOS Mapping Table.
MAC Address Delimiter	Configures MAC Address Delimiter for username.
Subscriber Map	Configures subscriber map association to get PGW address locally.
IP Fragment Chain Timeout	This command configures Internet Protocol (IP) parameters. This option configures ip fragment chain settings during TFT handling. This is the time to hold an ip fragment chain. Secs is an integer value between 1 and 10. The default value is 5.
Max Out of Order Fragment	This is the number of fragments to buffer per fragment chain for out-of-order reception before receiving first fragment (for L4 packet filtering). Fragments are an integer value between 0 and 300.
Bind	Binds the service to an ip and associated max-subscribers.
Custom SWm-SWu Error Mapping	Customized mapping of SWm errors with SWu Notify Error Type.
Custom S2b SWu Error Mapping	Allows duplicate precedence in a TFT for a S2b ePDG session.
Data Buffering	Allows downlink packets to be buffered, while session is in the connecting state. By default it is enabled.
PDN Type	Specifies the PDN type of IPv6 parameters for the ePDG service.
GTPC Load Control Profile	Associates the GTPC load control profile for ePDG.
GTPC Overload Control Profile	Associates the GTPC overload control profile for ePDG.
Idle Timeout	The subscriber's time-to-live (TTL) settings for the EPDG service.
Ebi End Value	Indicates end value for ebi range. The end value can range greater than or equal to the start value.
Reporting Action event Record	Shows reporting of events.
Micro Checkpoint Periodicity	The micro checkpoint periodicity for a subscriber.
Micro Checkpoint Deemed Idle	The micro checkpoint duration when UE is deemed idle for a subscriber.
Ebi Start Value	Indicates Start value of ebi range for bearer-id allocation (applicable only for GTPv2-S2b).

Viewing EPDG S2b Service Interface Properties

To view the ePDG S2b configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Mobile > EPDG.** The list of EPDG services configured in Prime Network are displayed in the content pane.

Step 3 From the **EPDG** node, choose S2b Service Interface. The EPDG S2b Service Interface details are displayed in the content pane.

Table 27-92 displays the EPDG S2b Service Interface details.

Table 27-92 EPDG S2b Service Interface Details

Field	Description
Vendor Specific DNS Server Request	Configures the vendor-specific-attributes values on PMIP based S2b interface. Configures the DNS Server Address to be present in PCO/APCO IE. Default setting is to use the APCO IE.
Duplicate Precedence in TFT	Allows duplicate precedence in a TFT for an S2b ePDG session.
Vendor Specific PCSCF Server Request	The vendor-specific-attributes values on PMIP based S2b interface. Configures the PCSCF Server Address to be present in APCO/PrivateExtn IE. Default setting is to use PrivateExtension IE.

Configuration Commands for ePDG

The following ePDG commands can be launched from the logical inventory by choosing the *Context* > **Commands** > **Configuration** or *Context* > **Commands** > **Show**. Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-93 ePDG Configuration Commands

Command	Navigation	Description
Create ePDG Service	*Right-click context* > **Commands** > **Configuration** > **Mobility** > **Create ePDG**	Use this command to create a new ePDG service.
Modify ePDG Service	*Expand EPDG Node* > *right-click EPDG service* > **Commands** > **Configuration**	Use this command to modify the configuration details for an ePDG service.
Delete ePDG Service	*Expand EPDG Node* > *right-click EPDG service* > **Commands** > **Configuration**	Use this command to delete an ePDG service.
Show ePDG Service	*Expand EPDG Node* > *right-click EPDG service* > **Commands** > **Show**	Use this command to view and confirm the configuration details of an ePDG Service.

Monitoring Packet Data Serving Node (PDSN)

Packet Data Serving Node, or PDSN, is a component of the Code Division Multiple Access (CDMA) 2000 mobile network. It acts as a connection point between the Radio Access Network (RAN) and IP Network. PDSN also manages PPP sessions between the mobile provider's core IP network and the mobile node.

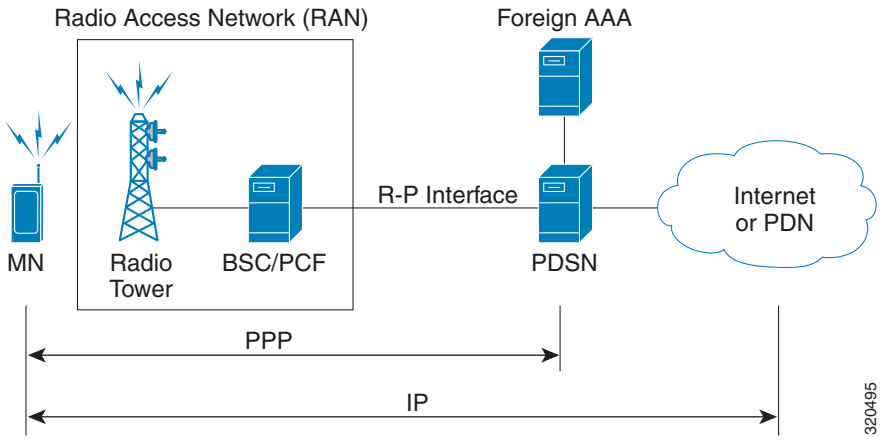
In other words, it provides access to the Internet, intranets, and applications servers for mobile stations that utilize a CDMA2000 RAN. Acting as an access gateway, PDSN provides simple IP and mobile IP access, foreign agent support, and packet transport for virtual private networking. It acts as a client for Authentication, Authorization, and Accounting (AAA) servers and provides mobile stations with a gateway to the IP network.

PDSN Configurations

The following paragraphs list the different configurations for PDSN:

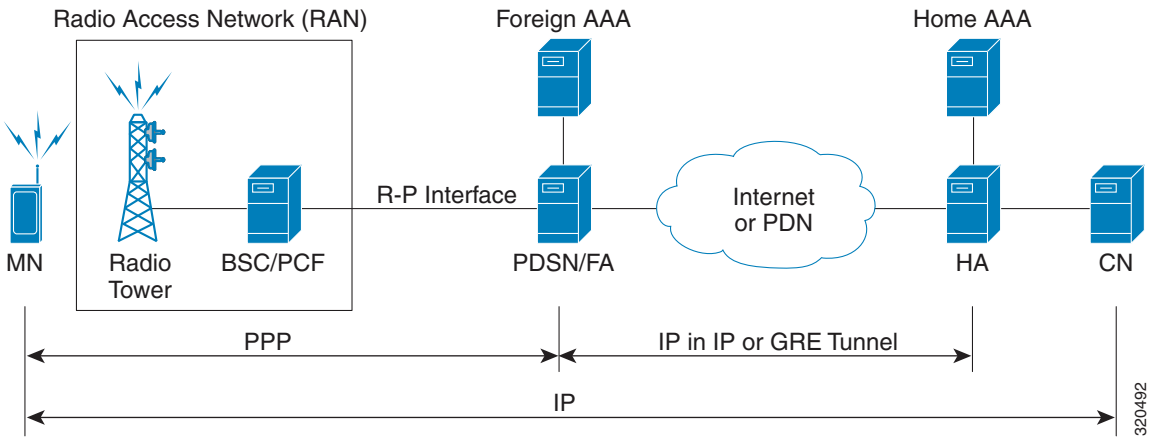
- Simple IP—In this protocol, the mobile user is assigned an IP address dynamically. The user can use this IP address within a defined geographical area, which is lost when the user moves out of the area. If the user moves out of the designated area, they must register with the service provider again to obtain a new IP address. Figure 27-17 depicts the working of this protocol.

Figure 27-17 Simple IP configuration for PDSN



- Mobile IP—In this protocol, the mobile user is assigned a static or dynamic IP address, which is basically the "home address" assigned by the user's Home Agent (HA). Even if the user moves out of the home network, the IP address does not change or is not lost. This enables the user to use applications that require seamless mobility such as transferring files. How does this work? The Mobile IP protocol provides a network-layer solution that allows mobile nodes to receive IP packets from their home network even when they are connected to a visitor network. The PDSN in the visitor's network performs as a Foreign Agent (FA), which assigns a Care-of-Address (CoA) to the mobile node and establishes a virtual session with the mobile node's HA. IP packets are encapsulated into IP tunnels and transported between the FA, HA and mobile node. Figure 27-18 depicts the working of this protocol.

Figure 27-18 Mobile IP Configuration for PDSN



- Proxy Mobile IP—This protocol provides a mobility solution for subscribers whose mobile nodes do not support the Mobile IP protocol. On behalf of the mobile node, PDSN proxies the Mobile IP tunnel with the HA. In turn, the service provider or the home agent assigns an IP address to the subscriber. This IP address does not change or is not lost even if the user moves out of the home network.

Viewing the PDSN Configuration Details

To view the PDSN configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > **PDSN.** The list of PDSN services configured in Prime Network are displayed in the content pane.

Step 3 From the **PDSN** node, choose a PDSN service. The PDSN service details are displayed in the content pane as shown in Figure 27-19.

Figure 27-19 PDSN Service Details

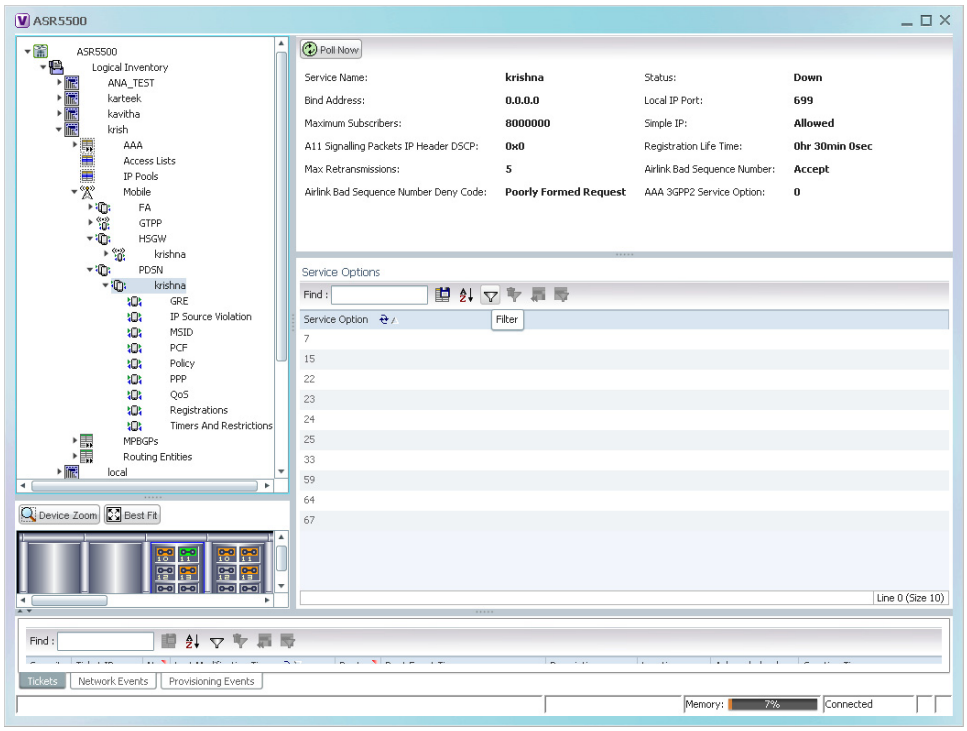


Table 27-94 displays the PDSN service details.

Table 27-94 PDSN Service Details

Field	Description
Service Name	The unique name of the PDSN service.
Status	The status of the PDSN service, which can be any one of the following: • Initiated • Running • Down • Started • Nonstarted • Unknown
Bind Address	The IP address to which the service is bound. This can be a IPv4 or IPv6 address. **Note** Multiple IP addresses belonging to the same IP interface can be bound to different PDSN services, but one address can be bound to only one service.
Local IP Port	The User Datagram Protocol (UDP) port for the R-P interface of the IP socket. This IP port can be any value between 1 and 65535 and defaults to 699.

Table 27-94 PDSN Service Details (continued)

Field	Description
Mobile IP	The IP address of the Foreign agent that is configured for the PDSN service.
Simple IP	Indicates whether the Simple IP configuration is available for the PDSN service, which can be any one of the following: • Allowed • Not Allowed (default value)
Max Subscribers	The maximum number of subscribers that the PDSN service can support.
Registration Life Time	The registration lifetime configured for all the subscribers to the service.
Max Retransmissions	Maximum retries for transmitting RP control packets. This count can be any value between 1 and 1000000 and defaults to 5.
A11 Signalling Packets IP Header DSCP	The Differential Services Code Point (DSCP) value in the IP header.
NAI Construction Domain	The Network Access Identifier for the PDSN service. This field is made up of the Mobile Station Identifier (MSID) of the subscriber, a separator character and a domain name. **Note** The domain name used here can be either the name supplied as part of the subscriber's name or the domain alias.
Airlink Bad Sequence Number	The action to be taken when the PDSN receives an airlink record with a bad sequence number, which can be any one of the following: • Accept (default value) • Reject **Note** At the time of the R-PA10 connection setup, an airlink record is assigned a unique sequence number.
Airlink Bad Sequence Number Deny Code	The reason for rejecting the airlink record with a bad sequence number, which can be any one of the following: • Poorly Formed Request • Unsupported Vendor ID
AAA 3GPP2 Service Option	The service options for which AAA 3GPP2 authentication is applicable.
Service Option Entries	
Service Option Number	The service option numbers applicable for the PDSN service. **Note** Each service option relates to a standard data service. Hence, these numbers determine the data services that are supported by the PDSN service.

You can also view the following configuration details for a PDSN service:

- GRE

- IP Source Violation
- MSID
- PCF
- Policy
- PPP
- QoS
- Registrations
- Timers and Restrictions

Viewing the GRE Configuration Details

To view the Generic Routing Encapsulation (GRE) configuration details for a PDSN service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Mobile > PDSN** > *PDSN service* > **GRE.** The GRE details are displayed in the content pane.

Table 27-95 displays the GRE configuration details.

Table 27-95 GRE Configuration Details

Field	Description
Checksum	Indicates whether the Checksum field is applicable for outgoing GRE packets.By default, this option is disabled.
Checksum Verify	Indicates whether the verification of the Checksum field is enabled for incoming GRE packets.
Reorder Time Out	The maximum time (in milliseconds) for processing the GRE packets that are coming out of order. This time can be any value between 0 and 5000, and defaults to 100 milliseconds.
Sequence Mode	The mode in which incoming out-of-sequence GRE packets are handled, which can be any one of the following: • Reorder • None This field defaults to **None**.
Sequence Numbers	Indicates whether GRE sequence numbers are inserted in data that is about to be transmitted over the A10 interface. By default, this option is disabled.
Flow Control	Indicates whether flow control is supported by the selected PDSN service. If this option is enabled, PDSN sends flow control enabled Normal Vendor Specific Extensions (NSVE) in A11 RRPs. By default, this option is disabled.
Flow Control Time Out	The amount of time (in milliseconds) to wait for an Transmitter On (XON) indicator from the RAN. This time can be any value between 1 and 1000000, and defaults to 1000 milliseconds.

Table 27-95 GRE Configuration Details (continued)

Field	Description
Flow Control Action	The action that must be taken when the timeout limit is reached, which can be any one of the following: • disconnect-session • resume-session.
Protocol Type	The tunnel type for the GRE routing. This field defaults to **Any**.
Is 3GPP Ext Header QoS Marking	Indicates whether the 3GPP Extension Header QoS Marking is enabled for the selected PDSN feature. **Note** If this feature is enabled and the PCF negotiation feature is enabled in A11 RRQ, then the PDSN will include QoS optional data attribute in the GRE 3GPP2 Extension Header.
IP Header DSCP Value	The Differential Service Code Point (DSCP) value in the IP header that marks the GRE IP Header encapsulation. This can be any value between 0x0F and 0X3F, and defaults to 0X0F.
IP Header DSCP Value Packet Type	Indicates whether the IP Header DSCP Value packet type is specified for the packets. By default, this option is disabled.
GRE Segmentation	Indicates whether segmentation of GRE packets is enabled. By default, this option is disabled.

Viewing the IP Source Violation Details

A Source violation occurs when a mobile device sources packets to the PDSN with a IP address that is different from the one specified during setup. Using this feature, the packets that need not be sent over the network are dropped when it tries to pass through PDSN.

To view the IP Source Violation configuration details for a PDSN service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Mobile > PDSN** > *PDSN service* > **IP Source Violation.** The details are displayed in the content pane.

Table 27-96 displays the IP Source Violation configuration details.

Table 27-96 IP Source Violation Configuration Details

Field	Description
Clear on Valid Packet	Indicates whether the service to reset the negotiation and drop limit counters upon receipt of properly addressed packet is enabled. By default, this feature is disabled.
Drop Limit	The maximum number of IP source violations within the detection period, before the call is dropped. This number can be any value between 0 and 1000000, and defaults to 10.
Period	The detection period (in seconds) for the IP source violation. This field can be any value between 1 and 1000000, and defaults to 120.
Renegotiation Limit	The maximum number of IP source violations within the detection period before renegotiating PPP for the call. This field can be any value between 1 and 1000000, and defaults to 5.

Viewing the MSID Configuration Details

To view the Mobile Station ID (MSID) configuration details for a PDSN service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Mobile > PDSN** > *PDSN service* > **MSID.** The details are displayed in the content pane.

Table 27-97 displays the MSID configuration details.

Table 27-97 MSID Configuration Details

Field	Description
MSID Length Max	The maximum length of the MSID configured for the PDSN service. This length can be any value between 10 and 15, and defaults to 15.
MSID Length Min	The minimum length of the MSID configured for the PDSN service. This length can be any value between 10 and 15, and defaults to 10.
MSID Authentication	Indicates whether the MSID authentication feature is enabled.
MSID Length Check	Indicates whether MSID length is enabled for the PDSN service. By default, this option is disabled. **Note** This configuration is required to reject the A11-RRQs with illegal International Mobile Station Identification (IMSI).

Viewing the PCF Configuration Details

To view the Packet Control Function (PCF) configuration details for a PDSN service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Mobile > PDSN** > *PDSN service* > **PCF.** The details are displayed in the content pane.

Table 27-98 displays the PCF configuration details.

Table 27-98 PCF Configuration Details

Field	Description
PCF Monitor Num Retries	The maximum number of retries before deciding that the PCF service is down.
PCF Session ID Change Restart PPP	Indicates whether the PPP must be restarted if there is a change in the session ID of an existing session.
New Call Conflict Terminate Old Session	Indicates whether the session with a PCF must be terminated when a new call request for an existing session is received from another PCF.
PDSN Security Entries	
SPI Number	The unique Security Parameters Index number that indicates a security context between the services.
Remote Address	The IP address of the source service.
Netmask	The subnet mask of the source service.
Zone ID	The ID of the zone to which the IP address belongs to.
Hash Algorithm	The hash algorithm used to encrypt the data.
Time Stamp Tolerance	The acceptable difference (in seconds) in the timestamps. **Note** If the actual difference exceeds the difference specified here, then the session is rejected. If this difference is 0, the timestamp tolerance checking is disabled at the receiving end.
Replay Protection	The replay protection schemes that is implemented by the service.
Description	The description of the security profile.

Viewing the Policy Configuration Details

To view the Policy configuration details for a PDSN service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Mobile > PDSN** > *PDSN service* > **Policy.** The details are displayed in the content pane.

Table 27-99 displays the Policy configuration details.

Table 27-99 Policy Configuration Details

Field	Description
Unknown CVSE Policy	Indicates whether the unknown Critical Vendor Specific Extension (CVSE) policy is enforced.
RRQ MEI From Current PCF	Indicates whether PPP must be restarted after getting MEI in RRQ.
New Call Policy	The call policy for one or all the services, which can be any one of the following: • Accept • Reject • Redirect • Reject on MSID • Redirect on MSID • None This field defaults to **None**.
Overload Policy	The action to be taken by the PDSN service in case of an overload condition.
Overload Policy Reject Code	The reject code for the overload policy.
Service Option Policy	The policy followed by PDSN for configuring services.
Reject MSID	The Mobile Station Identifier (MSID) for which new calls are rejected. **Note** If the **New Call Policy** field is set to **Reject MSID**, then this field will display the relevant MSID.

Viewing the PPP Configuration Details

To view the Point-to-Point Protocol details for a PDSN service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory > *Context* > Mobile > PDSN** > *PDSN service* > **PPP.** The details are displayed in the content pane.

Table 27-100 displays the PPP configuration details.

Table 27-100 PPP Configuration Details

Field	Description
Context Name	The destination context where the Layer 2 Tunneling protocol Access Concentrator (LAC) service is configured. **Note** This context is the same as the PPP tunneling context.
Tunnel Type	The type of the PPP tunnel established between the PDSN and the PFC, which can be any one of the following values: • L2TP • None This field defaults to **None**.
Fragment State	Indicates whether the PPP fragmentation is enabled. By default, this is option is disabled.
Alt PPP	Indicates whether the Alternate Point-to-Point (PPP) protocol sessions are enabled for the PDSN service. By default, this option is disabled.
Allow No Authentication	Indicates whether subscribers can gain network access even if they have not been authenticated.
Authentication	The authentication mode and priority when multiple modes are selected, which can be any one of the following: • **chap**—Uses the Challenge Handshake Authentication Protocol (CHAP) for authentication. Must be followed by a priority value, which can be any value between 0 and 1000 with a lower number indicating higher preference. This protocol is enabled by default and commands the highest priority. • **mschap**—Uses the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) for authentication. Must be followed by a priority value, which can be any value between 0 and 1000 with a lower number indicating higher preference. This protocol is disabled by default. • **pap**—Uses Password Authentication Protocol (PAP) for authentication. Must be followed by a priority value, which can be any value between 0 and 1000 with a lower number indicating higher preference. This protocol seconds CHAP in terms of priority. This protocol is enabled by default.

Viewing the QoS Configuration Details

To view the Quality of Service configuration details for a PDSN service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Mobile PDSN** > *PDSN service* > **QoS.** The details are displayed in the content pane.

Table 27-101 displays the QoS configuration details.

Table 27-101 QoS Configuration Details

Field	Description
Policy Mismatch	Indicates whether the PDSN must raise a Traffic FLow Template (TFT) violation if there is a policy mismatch of QoS.
Qos Wait	Indicates whether parameters related to QoS are enabled. **Note** While configuring parameters for QoS, the minimum and maximum waiting time for transmission are also specified. Also, the action to be performed when the minimum time elapses is also specified.
Associate	The unique identification number of the associated QoS Profile that is configured for the selected context.
QoS Profile tab	
ID	The unique code of the QoS profile.
Description	The description of the QoS profile.
Uplink Bandwidth	The uplink bandwidth (in kbps) of your profile.
Downlink Bandwidth	The downlink bandwidth (in kbps) of your profile.
Latency	The latency (in milliseconds) of the profile.
Drop Rate	The maximum drop rate percent of the packet.
QoS Class	The type of QoS class associated with the profile.

Viewing the Registration Details

To view the Registration details for a PDSN service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory > *Context* > Mobile > PDSN** > *PDSN service* > **Registrations.** The details are displayed in the content pane.

Table 27-102 displays the Registration details.

Table 27-102 Registration Details

Field	Description
Accept Session Disconnect In Progress	Indicates whether A11 registration request messages must be accepted from the PCF when a session disconnection is in progress.
Ask Deny Terminate Session on Error	Indicates whether A11 sessions must be terminated when a registration acknowledgement is received from PCF with an error status.
Max Deny Reply Limit	Maximum number of retries for an erroneous registration request message from PCF, before PDSN terminates the session.
Deny Mismatched COA Address	Indicates whether RP Requests must be denied, when the Care of Address field does not match the source address of the requests.
Deny New Call Connection Setup Record Absent	Indicates whether new calls that do not have airlink connection setup record in the RRQ must be denied.
Deny New Call Connection Setup Record Absent Deny Code	The reason for denying new calls that do not have airlink connection setup record in RRQ.
Deny New Call Connection Reverse Tunnel Unavailable	Indicates whether new calls whose GRE key is the same as that of another user must be denied.
Deny Session Already Active	Indicates whether renew requests that have Airlink Start record for already active R-P sessions must be denied.
Deny Session Already Closed	Indicates whether renew and de registration requests for closed R-P sessions must be denied.
Deny Session Already Dormant	Indicates whether renew requests that have Airlink Start record for already dormant R-P sessions must be renewed.
Deny Terminate Session On Error	Indicates whether termination of session on receipt of erroneous registration request message must be denied.
Deny Use Zero GRE Key	Indicates whether the GRE key must be initialized to 0 when denying a new R-P session.
Discard Bad Extension	Indicates whether A11 registration request messages containing bad extensions must be discarded.
Discard GRE Key Change	Indicates whether A11 registration request messages for an existing A11 session that contain a different GRE key must be discarded.
Update Wait Timeout	The time taken (in seconds) by A11 RRQ for QoS changes.

Viewing the Timers and Restrictions Details

To view the Timers and Restrictions details for a PDSN service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Mobile > PDSN** > *PDSN service* > **Timers and Restrictions.** The details are displayed in the content pane.

Table 27-103 Timers and Restrictions Details

Field	Description
Inter PDSN Handoff	Indicates whether the Inter-PDSN handoff feature off is enabled. Inter-PDSN handoff relates to the handoff between two PCFs with connectivity to different PDSNs. **Note** Inter-PDSN handoff can be of two types: Fast Handoff and Dormant Handoff. Fast Handoff uses a GRE tunnel between two PDSNs to transport user data for a single service instance. Dormant Handoff occurs when a mobile station with a dormant packet session determines that it has crossed a packet zone boundary.
Inter PDSN Handover Use CANIDPANID	Indicates whether usage of Current Access Network ID (CANID) or Previous Access Network ID (PAN) is supported during an Inter-PDSN handover.
Data Available Indicator	Indicates whether data transfer is available.
PMA Capability Indicator	The Proxy Mobile Agent capability (PMA) indicator, which determines whether PMIP is supported by Prime Network. **Note** PDSN sends the capability indicator through RADIUS to the AAA server as an access-request packet to indicate to the AAA server that PDSN supports PMIP. If the capability indicator attribute is missing, then PMIP is not supported by PDSN.
Direct LTE Indicator	Indicates whether PDSN can send Direct LTE indicator in the Access Request.
Data Over Signalling	Indicates whether data transfer over a10 signalling channel instead of bearer or subscriber channels from PCF or PDSN is allowed. By default, this feature is not allowed.
Dormant Transition	Indicates whether dormant transition of the RP link during the initial setup of the subscriber session is allowed. If this option is disabled, then the subscriber session will be disconnected if the RP link becomes dormant during the initial setup.
ROHC IP Header Compression	Indicates whether the Robust Header Compression (ROHC) is enabled for headers in the IP packets that are being sent by or sent to the PDSN. By default, this option is disabled.
Always On Indication	Indicates whether the Always On feature is enabled for a subscriber. **Note** When the idle-time out limit runs out for a subscriber, the IP/PPP session remains connected as long as the subscriber is reachable. By default, this feature is disabled.
Setup TimeOut	The maximum time (in seconds) allowed for a session to be setup between PCF and PDSN. This time can be any value between 1 and 1000000, and defaults to 60 seconds.

Table 27-103 Timers and Restrictions Details (continued)

Field	Description
Retransmission TimeOut	The timeout period (in seconds) for retransmission of RP control packets. This time can be any value between 1 and 1000000 and defaults to 3 seconds.
Pdsn Type0 Tft	Indicates whether Traffic Flow Template (TFT) of the PDSN is changed from type 0 TFT to type 1 TFT.
Tft Validation TimeOut	The TFT validation timeout (in seconds) for QoS changes. This time can be any value between 1 and 100000, and defaults to 0.
Access Flow Traffic Violations	The number of violations that are permitted in the access flow traffic.
Access Flow Traffic Violations Interval	The time interval between two subsequent access flow traffic violations.
Cid Mode	This mode allows you to configure options that are applied during ROHC compression for the service. This sets the RoHC packet size Large or Small.
Max Cid	Configures the highest context ID number to be used by the compressor as an integer from 0 and 15 when small packet size is selected, and 0 and 31 when large packet size is selected. Default is 15.
Max Received Reconstructed Unit	Configures the size of the largest reconstructed reception unit that the decompressor is expected to reassemble from segments. The size includes the CRC. If maximum received reconstructed unit (MRRU) is negotiated to be 0, no segment headers are allowed on the channel.
Radius Accounting Dropped Packets	Indicates whether radius accounting dropped packets are enabled or not for a PDSN service.
Profile ID(s)	Configures the header compression profiles to use. A header compression profile is a specification of how to compress the headers of a specific kind of packet stream over a specific kind of link. At least one profile must be specified.
Radius Accounting Dropped Packets	Indicates if radius accounting for dropped packets is enabled.

Configuration Commands for PDSN

The following PDSN commands can be launched from the logical inventory by choosing the *Context* > **Commands** > **Configuration** or *Context* > **Commands** > **Show**. Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-104 PDSN Configuration Commands

Command	Navigation	Description
Create PDSN	Right-click the *context* > **Commands** > **Configuration** > **Mobility**	Use this command to create a new PDSN service for the selected context.
Modify PDSN **Delete PDSN**	*Expand PDSN node* > *Right-click PDSN service* > **Commands** > **Configuration**	Use these commands to modify/delete an existing PDSN service configured for the selected context.
Show PDSN	*Expand PDSN node* > *Right-click PDSN service* > **Commands** > **Show**	Use this command to view and confirm the PDSN service configuration details.
Modify GRE	*Expand PDSN node* > *PDSN service* > *right-click* **GRE > Commands > Configuration**	Use this command to modify the Generic Routing Encapsulation (GRE) configuration settings for a specified PDSN service.
Modify IP Source Violation	*Expand PDSN node* > *PDSN service* > *Right-click IP Source Violation* > **Commands > Configuration**	Use this command to modify the IP Source Violation configuration details for the specified PDSN service.
Modify MSID	*Expand PDSN node* > *PDSN service* > *Right-click MSID* > **Commands > Configuration**	Use this command to modify the mobile station ID (MSID) configuration details for the specified PDSN service.
Modify PCF Parameters	*Expand PDSN node* > *PDSN service* > *Right-click PCF* > **Commands > Configuration**	Use this command to modify the Packet Control Function (PCF) configuration details for the specified PDSN service.
Create PCF Security Entry	*Expand PDSN node* > *Right-click PDSN service* > **Commands** > **Configuration**	Use this command to create a new PCF security entry.
Modify PCF Security Entry **Delete PCF Security Entry**	*Expand PDSN node* > *PDSN service* > **PCF** > *Under Security Profiles tab n the content pane, right-click SPI Number* > **Commands** > **Configuration**	Use these commands to modify/delete the PCF security entry details.
Modify Policy	*Expand PDSN node* > *PDSN service* > *Right-click* **Policy > Commands > Configuration**	Use this command to modify the policy configuration details for the PDSN service.
Modify PPP	*Expand PDSN node* > *PDSN service* > *Right-click* **PPP > Commands > Configuration**	Use this command to modify the Point-to-Point Protocol configuration details for the selected PDSN service.
Modify Registrations	*Expand PDSN node* > *PDSN service* > *Right-click* **Registrations > Commands > Configuration**	Use this command to modify the registration details for the selected PDSN service.
Modify Timers and Registrations	Expand *PDSN node* > *PDSN service* > *Right-click* **Timers and Registrations > Commands > Configuration**	Use this command to modify the timers and registration details for the selected PDSN service.

Viewing the Local Mobility Anchor Configuration (LMA)

Proxy Mobile IPv6 (or PMIPv6, or PMIP) is a network-based mobility management protocol for building a common access technology independent of mobile core networks, accommodating various access technologies such as WiMAX, 3GPP, 3GPP2 and WLAN based access architectures.

The PMIPv6 provides network-based IP Mobility management to a mobile node, without requiring the participation of the MN in any IP mobility-related signaling. The mobility entities in the network track the movements of the MN, initiate the mobility signaling, and set up the required routing state.

The major functional entities of PMIPv6 are Mobile Access Gateways (MAGs), Local Mobility Anchors (LMAs), and Mobile Nodes (MNs).

The Local Mobility Anchor (LMA) is the home agent for a mobile node in a Proxy Mobile IPv6 (PMIPv6) domain. It is the topological anchor point for mobile node home network prefixes and manages the binding state of an mobile node. An LMA has the functional capabilities of a home agent as defined in the Mobile IPv6 base specification (RFC 3775) along with the capabilities required for supporting the PMIPv6 protocol.

To view the LMA configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *Context* **> Mobile > LMA.** The list of LMA services configured in Prime Network is displayed in the content pane.

Step 3 From the **LMA** node, choose an LMA service. The LMA service details are displayed in the content pane.

Figure 27-20 LMA Service Details

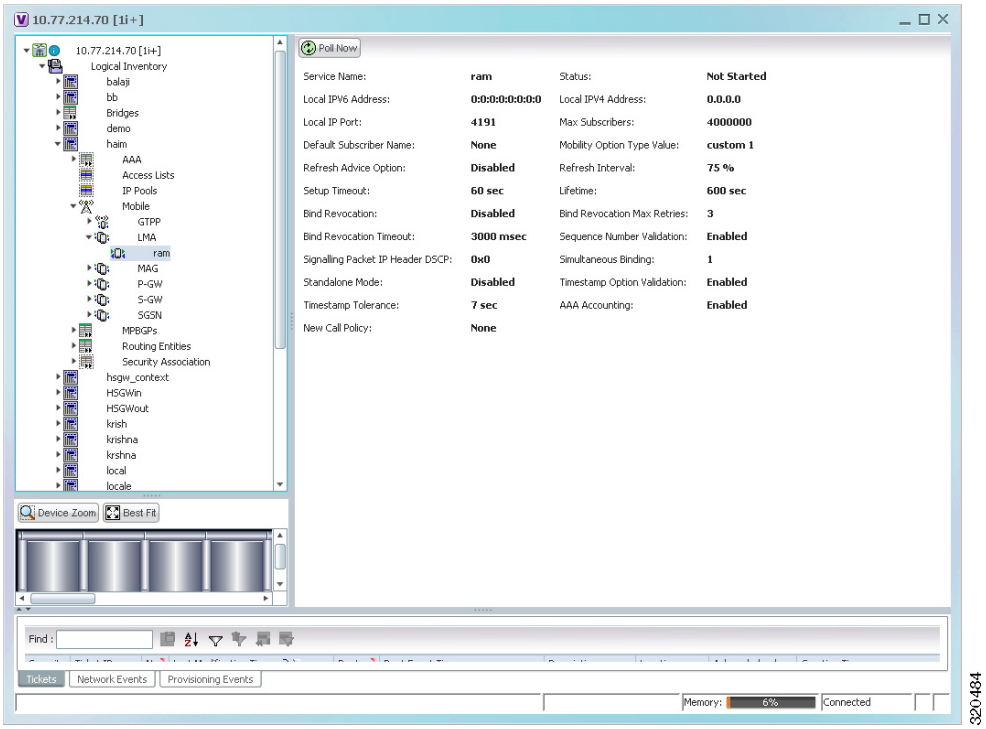


Table 27-105 displays the LMA service details.

Table 27-105 LMA Service Details

Field	Description
Service Name	The unique service name of the LMA.
Status	The status of the LMA service, which can be any one of the following: • Down • Running • Initiated • Unknown. • Not Started This field defaults to **Down**.
Local IPv6 Address	The IP address of the interface serving as S2a (that is connected to HSGW) or S5/S8 (that is connected to S-GW) interface.
Local IPv4 Address	The IP address of the interface connected to HA/P-GW.
Local IP Port	The User Datagram Protocol (UDP) port for the LMA service.
Max Subscribers	The maximum number of subscribers that the LMA service can support. This number can be any value between 0 and 12000000 based on the below listed platforms and card types: – SSI SMALL card on QvPC-SI platform—range is 0 to 120000. – SSI MEDIUM card on QvPC-SI platform—range is 0 to 280000. – SSI FORGE card on QvPC-SI platform—range is 0 to 240000. – SSI LARGE card on QvPC-SI platform—range is 0 to 640000. – ASR5000 PSC, ASR5000 PPC card on ASR5k platform—range is 0 to 4000000. – SCALE MEDIUM on QvPC-DI platform—range is 0 to 4000000. – ASR5000 PSC2, ASR5000 PSC3 on ASR5k platform—range is 0 to 4500000. – ASR5500 DPC on ASR5500 platform—range is 0 to 4500000. – ASR5500 DPC2 on ASR5500 platform— range is 0 to 12000000. – SCALE LARGE on QvPC -DI platform— range is 0 to 12000000.
Default Subscriber Name	The name of the subscriber template to be used for subscribers who are using this domain alias.
Mobility Option Type Value	The mobility option type used in mobility messages, which can be any one of the following: • Custom 1 • Custom 2 • Custom 3 • Standard

Table 27-105 LMA Service Details (continued)

Field	Description
Refresh Advice Option	Indicates whether refresh advice option must be included in the Binding Acknowledgment sent by the LMA service. By default, this option is disabled.
Refresh Interval	The percent of granted lifetime to be used in the Refresh Interval Mobility option pertaining to the Binding Acknowledgment sent by the LMA service. This percentage can be any value between 1 and 99 and defaults to 75.
Setup Timeout	The maximum time (in seconds) allowed for the session to setup. This field defaults to 60.
Lifetime	The registration lifetime (in seconds) of the mobile IPv6 session. This number can be any value between 1 and 262140.
Bind Revocation	Indicates whether the binding revocation support is available for the LMA service. By default, this option is disabled.
Bind Revocation Max Retries	The maximum number of retries for the binding revocation, which can be any value between 1 and 10. This field defaults to 3.
Bind Revocation Timeout	The time interval (in milliseconds) of the retransmission of the binding revocation, which can be any value between 500 and 10000. This field defaults to 3000.
Sequence Number Validation	Indicates whether the sequence number of the MIPv6 control packet received by the LMA service must be validated. This option is enabled by default.
Signaling Packet IP Header DSCP	The Differentiated Services Code Point (DSCP) marking that is applicable to the IP header that is carrying outgoing signalling packets.
Simultaneous Binding	The maximum number of Care of addresses that can be bound for the same user as identified by their Network Access Identifier (NAI) and home address. This can be any value ranging from 1 to 3. This field defaults to 1.
Standalone Mode	Indicates whether the LMA service can be started in the standalone mode. This option is disabled by default.
Timestamp Option Validation	Indicates whether the Timestamp option in the Binding Acknowledgment must be validated. This option is disabled by default.
Timestamp Tolerance	The time (in seconds) to validate Timestamp reply protection, which can be any value between 0 and 65535. This field defaults to 7 seconds.
AAA Accounting	Indicates whether the AAA Accounting information for subscriber sessions must be sent. This option is enabled by default.
New Call Policy	Indicates whether the new call policy must be accepted or rejected. By default, this field is set to **None**.
Heartbeat support	Indicates whether the heartbeat support associated with the LMA Service is enabled or disabled.
Heartbeat Interval	Indicates heartbeat interval. Default value is 60 seconds.
Heartbeat Retransmission Timeout	Indicates heartbeat retransmission timeout. Default value is 3 seconds.
Heartbeat Max Retransmissions	Indicates maximum heartbeat retransmissions. Default value is 3 seconds.

Table 27-105 LMA Service Details (continued)

Field	Description
Alternate CoA	Configuration to allow alternate Care-of-address for data traffic through alternate-care-of-address mobility options in PBU.
Timestamp Replay Protection	Designates timestamp replay protection scheme as per RFC 4285.

View Additional Mobility Options for MPN Service on the LMA Platform

Prime Network 5.3 supports PMIPv6/LMA inventory and faults, as well as performance statistics. Additional mobility options that are needed for supporting the MPN service is supported on the ASR9K platform. You can discover active PMIPv6/LMA function on ASR9K, view LMA service information in logical inventory and the associated VPN, tunnels and so on. For example, you can view service attributes such as terminating IP address, maximum sessions, and thresholds in logical inventory. SNMP traps and Syslog that are associated with the function of the service emphasis on any service-impacting events.

Note Make sure to configure the LMA Service in ASR9K Device after modeling the VNE in PN.

To view additional mobility options, follow the procedural steps:

Step 1 Right-click the required device in the Vision client and choose Inventory.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > **Mobile** > **LMA**. The list of LMA services configured in Prime Network is displayed in the content pan.

Step 3 Click the **Peers** tab to view the following details specified in the Table 27-106.

Table 27-106 Peers Entry Details for LMA Service

Field	Description
Peer MAGs	Shows MAG within LMA.
Auth option	Shows authentication option between PMIPV6 entities.
Encap type	Shows encapsulation option between PMIPV6 entities.

Step 4 To view the networks entries for LMA service, click the **Networks** tab. Table 27-107 displays the network details.

Table 27-107 Network Details for LMA Service

Field	Description
Network	Shows the network name for the selected LMA service.
IPv4 Pool prefix	Shows IPV4 pool configurations for the mobile network.

Table 27-107 Network Details for LMA Service

Field	Description
IPv6 Pool prefix	Shows IPV6 pool configurations for the mobile network.
No of Mobile Nwks Pools	Shows the count for mobile network pools that are configured.

Step 5 To view the bindings entries for LMA service, click the **Bindings** tab. Table 27-108 displays the binding details.

Table 27-108 Bindings Details for the LMA Service

Field	Description
State	Shows the Binding state.
NAI	Shows the network access identifier.
HOA	Shows the redistribute home address.
Prefix	Shows the redistribute HOA host prefix routes.
HNP	Shows the home network prefix.
IPV4 Mobile Network Prefixes	Shows the IPV4 mobile network prefixes.
IPV6 Mobile Network Prefixes	Shows the IPV6 mobile network prefixes.
LLID	Shows the Link layer identifier.
ID	Shows the MAG identifier.
COA	Shows CoA address.
Lifetime	Shows lifetime interval of the binding.
Tunnel	Shows outgoing interface.

Step 6 To view the heartbeat entries for peers, click the **Peer Heartbeats** tab. Table 27-109 displays the heartbeat entries for peers.

Table 27-109 Heartbeat Details for Peers

Field	Description
VRF	Shows the VRF of a customer.
Peer	Shows the customer specific LMA IPv4 or IPv6 addresses.
Time Interval	Specifies the interval between two heartbeat messages in seconds.

Table 27-109 Heartbeat Details for Peers

Field	Description
Retries	In the absence of reply from the peer, specify the number of retries.
Timeout	Specifies the time-out value to wait for a response from the peer after which the request is declared as timed out.

Step 7 To view the heartbeat path details, click the **Heartbeat Path Information** tab.Table 27-110 displays the heartbeat path details.

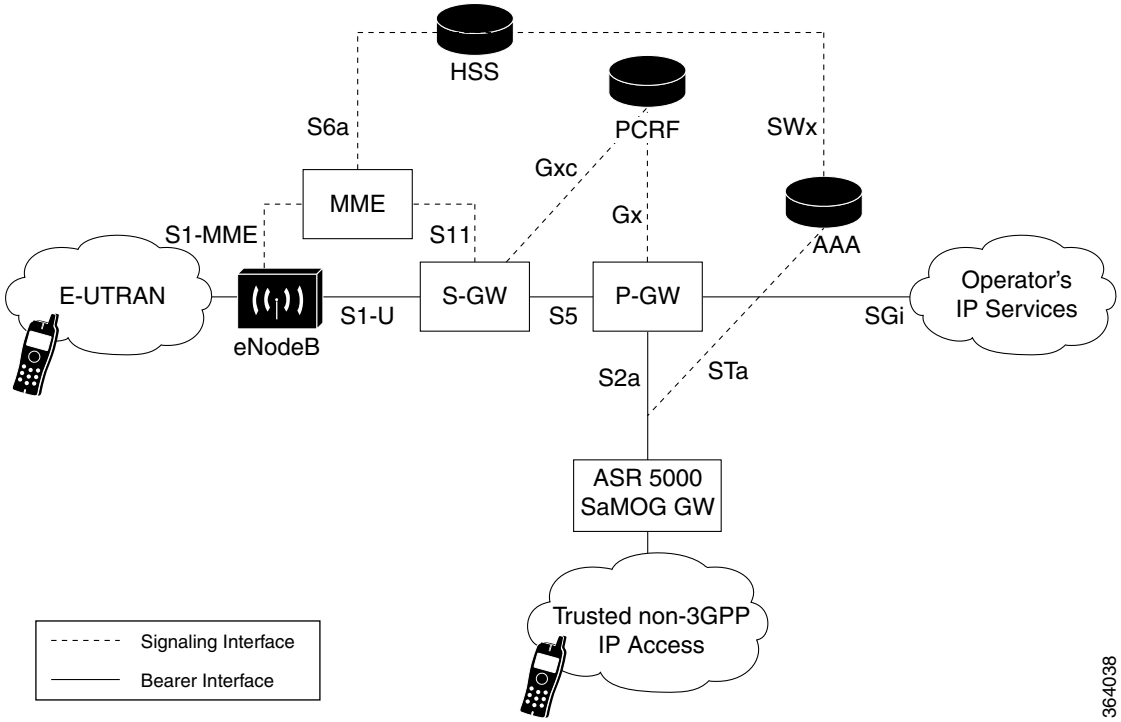
Table 27-110 Heartbeat Path Details

Field	Description
State	Shows the heartbeat state.
VRF	Shows the VRF of a customer.
Source Address	Shows the source address of the heartbeat for the peer.
Destination Address	Shows the destination address of the heartbeat for the peer.
Source Port	Shows the source port of the heartbeat for the peer.
Destination Port	Shows the destination port of the heartbeat for the peer.

Monitoring the SaMOG Gateway Configuration

The SaMOG (S2a Mobility Over GTP) Gateway runs on a Cisco ASR 5000 chassis with the StarOS operating system as shown in Figure 27-21.

Figure 27-21 SaMOG Gateway Topology



The SaMOG Gateway enhances the network services in the following ways:

- Provides seamless mobility between the 3GPP EPC network and WLANs for EPS (Evolved Packet System) services via the GTPv2-based S2a interface.
- Functions as a 3GPP Trusted WLAN Access Gateway (TWAG) as the Convergence Gateway (CGW) service. The CGW service terminates the S2a interface to the P-GW and acts as the default router for the WLAN UEs on its access link, and as a DHCP server for the UE. When the TWAN provides access to EPC for an UE, it forwards packets between the UE-TWAG point-to-point link and the S2a tunnel for that UE. The association in the TWAN between UE-TWAG point-to-point link and S2a tunnel is based on the UE MAC address.
- Functions as a 3GPP Trusted WLAN AAA Proxy (TWAP) as the Multi Radio Management Entity (MRME) service. The MRME service terminates the STa interface to the 3GPP AAA server and relays the AAA information between the WLAN IP access network and the AAA server, or AAA proxy in the case of roaming. It establishes the binding of UE subscription data (including IMSI) with UE MAC address on the WLAN Access Network. The function provides the TWAG with UE subscription data during initial attach or at UE subscription data modification.

The services supported on the SaMOG gateway are:

- SaMOG service
- CGW service
- MRME service

SaMOG Service

The SaMOG Gateway acts as the termination point of the WLAN access network. The SaMOG service enables the WLAN UEs in the trusted non-3GPP IP access network to connect to the EPC network via Wireless LAN Controllers (WLCs). During configuration, the SaMOG service gets associated with two services: the Convergence Gateway (CGW) service and the Multi Radio Mobility Entity (MRME) service. These collocated services combine to enable the SaMOG Gateway functionality.

CGW Service

The Convergence Gateway (CGW) service functions as a 3GPP Trusted WLAN Access Gateway (TWAG), terminating the S2a interface to the P-GW and acts as the default router for the WLAN UEs on its access link.

The CGW service has the following key features and functions:

- Functions as a Local Mobility Anchor (LMA) towards the WLCs, which functions as a Mobile Access Gateway (MAG) with Proxy MIP capabilities per RFC 5213 and 3GPP TS 29.275 V11.5.
- Enables the S2a interface towards the P-GW for session establishment per 3GPP TS 29.274 V11.5.
- Routing of packets between the P-GW and the WLAN UEs via the Wireless LAN Controllers (WLCs).
- Support for PDN type IPv4.
- Interacts with the MRME service to provide user profile information to establish the GTP-variant S2a interface towards the P-GW per 3GPP TS 29.274.
- Provides a Generic Routing Encapsulation (GRE) data path towards the WLCs per RFCs 1701 and 1702 for tunneling of data towards the WLCs. Also follows RFC 5845 for exchanging GRE keys with WLC-based PMIP signaling.
- Receives and sends GTPU data packets towards the P-GW per 3GPP TS 29.281 V11.5.

MRME Service

The Multi Radio Mobility Entity (MRME) service functions as a 3GPP Trusted WLAN AAA Proxy (TWAP), terminating the STa interface to the 3GPP AAA server. The service relays the AAA information between the WLAN IP access network and the AAA server, or AAA proxy in the case of roaming.

The MRME service has the following key features and functions:

- Relays the AAA information between the Wireless LAN Controllers (WLCs) and the 3GPP AAA server.
- Supports EAP-over-RADIUS between the SaMOG Gateway and the WLCs to authenticate the WLAN UEs per RFC 3579.
- Supports the Diameter-based STa interface between the 3GPP AAA server/proxy and the SaMOG Gateway per 3GPP TS 29.273 V11.
- Supports the exchange of EAP messages over the STa interface per RFC 4072.
- Functions as a RADIUS accounting proxy for WLC-initiated accounting messages.
- Supports RADIUS Dynamic Authorization Extensions per RFC 3576 to handle HSS/AAA-initiated detach and Diameter re-authorization procedures.
- Supports authentication between the WLAN UEs and the 3GPP AAA server using EAP-AKA, EAP-AKA', and EAP-SIM.

- Supports static and dynamic P-GW selection after the authentication procedures.
- Supports PDN type IPv4.
- Maintains a username database to reuse existing resources when the CGW service receives PMIPv6 procedures initiated by the WLCs.
- Interacts with the CGW service to provide user profile information to establish the GTP-variant S2a interface towards the P-GW per 3GPP TS 29.274.

Viewing the SaMOG Configuration Details

To view the SaMOG configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *context* > **Mobile** > **SaMOG**. The SaMOG configuration details are displayed in the content pane.

Table 27-111 describes the SaMOG configuration details.

Table 27-111 SaMOG Configuration Details

Field	Description
Name	The name of the SaMOG service configured on the device.
Status	The status of the service, which can be any one of the following: • Initiated • Started • Running • Not Started • Down
CGW Service	The name of the CGW service configured on the device.
DHCP Service	The name of the service configured for DHCP interface support in SaMOG service.
DHCPv6 Service	The name of the service configured for DHCPv6 interface support in SaMOG service.
MRME Service	The name of the MRME service configured on the device.
Subscriber Map	The subscriber map name associated with the SaMOG service.
Max Sessions	The maximum number of sessions the SaMOG service can support.
Setup Timeout	The maximum amount of time (in seconds) allowed for session setup. Default is 60 seconds.
Absolute Timeout	The maximum duration of the session before the system automatically terminates the session. Default is 0.
Idle Timeout	The maximum duration a session can remain idle before the system automatically terminates the session. Default is 0.
Serving PLMN MCC	The mobile country code portion of the Serving PLMN.

Table 27-111 SaMOG Configuration Details

Field	Description
Serving PLMN MNC	The mobile network code portion of the Serving PLMN.
New Call Policy	The new call policy that the SaMOG service can support. When a new call policy is enabled, the policy redirects or rejects new calls in anticipation of the chassis reload that completes the upgrade process.

SaMOG Configuration Commands

The following SaMOG commands can be launched from the logical inventory by choosing the *Context* > **Commands** > **Configuration > Small Cell** or *Context* > **Commands** > **Show**. Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-112 SaMOG Configuration Commands

Command	Navigation	Description
Modify SaMOG **Delete SaMOG**	*Expand* **SaMOG** *node* > *Right-click* SaMOG *service* > **Commands** > **Configuration**	Use this command to modify/delete the configuration details of a SaMOG service.
Show SaMOG	*Expand* **SaMOG** *node* > *Right-click* SaMOG *service* > **Commands** > **Show**	Use this command to view and confirm the configuration details of a SaMOG service.

Viewing the CGW Service Configuration Details

To view the CGW service configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *context* **> Mobile > CGW Service.** The CGW Service configuration details are displayed in the content pane**.**

Table 27-113 describes the CGW service configuration details.

Table 27-113 CGW Service Configuration Details

Field	Description
Name	The name of the service configured on the device.
Status	The status of the service, which can be any one of the following: • Initiated • Started • Running • Not Started • Down
IPv4 Bind Address (IP Address)	The Bind IP address for Local Mobility Anchor (LMA) driver. Designates address of the LMA service.
IPv6 Bind Address (IP Address)	The Bind IP address for the LMA driver. Designates address of the LMA service.
Egress EGTP Service	The associated (Evolved GPRS Tunneling Protocol) EGTP Service.
PGW Service	The name of the context in which the PGW service is configured.
GGSN Service	The name of the context in which the GGSN service is configured.
SGTP Service	The associated (SGSN GPRS Tunneling Protocol) SGTP Service.
Subscriber Map	The subscriber map name associated with the CGW service.
qci-qos-mapping	The associated QoS Class Index (QCI) QOS Mapping Table.
Registration Lifetime	The mobile IPV6 session registration lifetime ranging from 1 to 262140. Default is 600 seconds.
Binding Revocation	Shows whether binding revocation support for a specific CGW service is Enabled or Disabled.
Bind-Revocation Max-Retries	The maximum number of retransmissions of bind revocation.
Bind Revocation Timeout	The retransmission timeout for bind revocation.
Session Delete Delay Timer	Configures CGW to retain the session on receiving a termination request till configured delay time for session continuity in case of break-before-make scenario. Timer is Disabled by default.
Session Delete Delay Timeout	Configures CGW to retain the session until the configured time when the timer is enabled. Default timeout when enabled is 10000 milliseconds.
Timestamp Option Validation	The validation of timestamp option in binding update messages. By default timestamp is I10:I31.
Timestamp Replay Protection	The timestamp replay protection scheme as per RFC 4285.
Timestamp Tolerance	The acceptable difference in timing (between timestamps) before rejecting packet. Ranges from 0 to 65535. Default is 7 seconds.
MAG Service	The MAG service associated with the CGW service.
GGSN Service	The GGSN service associated with the CGW service.

Table 27-113 CGW Service Configuration Details (continued)

Field	Description
GRE Sequence Numbers	Indicates whether the option to insert or remove GRE sequence numbers in GRE packets is enabled.
GGSN Context	The GGSN context associated with the CGW service.
Egress EGTP Service Context	The associated EGTP service context for CGW service.

CGW Configuration Commands

The following CGW commands can be launched from the logical inventory by choosing the *Context* > **Commands** > **Configuration** or *Context* > **Commands** > **Show**. Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-114 CGW Commands

Command	Navigation	Description
Modify CGW **Delete CGW**	*Expand* **CGW** *node* > *Right-click* CGW *service* > **Commands** > **Configuration**	Use this command to modify/delete the configuration details of a CGW service.
Show CGW	*Expand* **CGW** *node* > *Right-click* CGW *service* > **Commands** > **Show**	Use this command to view and confirm the configuration details of a CGW service.

Viewing the MRME Service Configuration Details

To view the MRME service configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *context* > **Mobile** > **MRME Service**. The MRME Service configuration details are displayed in the content pane.

Table 27-115 describes the MRME service configuration details.

Table 27-115 MRME Service Configuration Details

Field	Description
Name	The name of the service configured on the device.
Status	The status of the service, which can be any one of the following: • Initiated • Started • Running • Not Started • Down
IPv4 Bind Address (IP Address)	The designated address of the MRME service in the RADIUS server mode. Must be followed by IPv4 address, using dotted-decimal notation.
Authentication Port	The authentication port number.
Accounting Port	The accounting port number.
Disconnection Delay Time	The maximum time allowed to retain the session on receiving an accounting stop and session continuity further on receiving an accounting start for roaming scenarios. Default is 10 seconds.
Disconnection Wait Time	The maximum time allowed to wait for accounting stop before clearing the call and after sending disconnect message to WLC. Default is 30 seconds.
DNS-PGW Context	The name of the context where the Domain Name System (DNS) client is configured for the Packet Data Network Gateway (PGW) selection.
DNS PGW Selection	The PGW DNS selection criteria.
FQDN	The designated MRME Fully Qualified Domain Name (FQDN), which is used for longest suffix match during dynamic allocation.
Associated SaMOG service	The associated SaMOG service.
Sta Attribute ANID	The STa interface attribute. Format for Access Network ID (ANID). This attribute contains the access network identifier used for key derivation at the Home Subscriber Server (HSS).
MRME operation mode	The MRME operation mode.
Sta Attribute Calling Station Id	The STa interface attribute that carries the Layer-2 address of the UE in the format of calling station identifier.
Preferred PGW Selection Mechanism	Indicates that the local PGW selection as the preferred mechanism. This is applicable for initial attach. **Note** By default, DNS based selection is displayed.
PGW-ID Selection Fallback	Allows you to PGW- selection Fallback when AAA provided PGW-ID selection fails.
ANID for AAR (Non-EAP Session)	Allows you to include ANID in AAR message for non-eap session.

Table 27-115 MRME Service Configuration Details (continued)

Field	Description
AAA Send Framed-MTU Size	The size of Framed MTU Attribute Value Pairs to be sent in authentication request.
Bind IPv6 Address	Specifies the IPv6 address of the MRME service in the RADIUS server mode.

MRME Configuration Commands

The following MRME commands can be launched from the logical inventory by choosing the *Context* > **Commands** > **Configuration** or *Context* > **Commands** > **Show**. (see Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-116 MRME Configuration Commands

Command	Navigation	Description
Modify MRME **Delete MRME**	*Expand* **MRME** *node* > *Right-click* MRME *service* > **Commands** > **Configuration**	Use this command to modify/delete the configuration details of a MRME service.
Show MRME	*Expand* **MRME** *node* > *Right-click* MRME *service* > **Commands** > **Show**	Use this command to view and confirm the configuration details of a MRME service.

Scheduling 3GPP Inventory Retrieval Requests

The 3GPP Inventory Management Web Services for Prime Network Integration Layer (PN-IL) retrieves the physical and logical inventory data from the Prime Network managed devices. For details on supported network elements, see *Cisco Prime Network 5.3 Supported Cisco VNEs*. For more details on the 3GPP inventory management and the web services, refer to the *Cisco Prime OSS Integration Guide, 2.0*.

Prime Network allows you to schedule a web service operations for Prime Network Integration Layer to run immediately or at a later point in time. Using Prime Network - Web Service Scheduler option, you can do the following:

- Select the inventory request type based on which the inventory data will be retrieved from either all the supported devices or from the specified devices under Prime Network.
- Schedule the 3GPP inventory management web service operations to initiate the inventory request and executes it according to the specified schedule.

To schedule web services:

Step 1 In the Vision client, Events client, or Administration client, choose **Tools > Web Service Scheduler**.

Step 2 In the Web Service Scheduler window, select **General** tab and select the inventory request type.

Table 27-117 describes the details of the Web Service Scheduler - General tab.

Table 27-117 General Tab in Web Service Scheduler

Field	Description
Operation	Select from the following inventory request: • **getAllInventory** - This inventory request is used to retrieve Inventory data for all supported devices under Prime Network. One notification will be issued by Prime Network Integration Layer upon completion of file creation for all supported network elements • **getManagedElement** - This inventory request is used to retrieve the inventory data for a specific managed element. One notification will be sent by the Prime Network Integration Layer for the specific managed element. **Note** For information on how to subscribe to a notification, see the *Cisco Prime OSS Integration Guide, 2.0.* **Note** The API **getManagedElement** reports the network functions of the mobility devices.
Managed Element	This options appears only if the inventory request type selected is of getManagedElement type. This option allows you to select a specific managed element, i.e, ASR5000, Security GW, or ASR5500 for which inventory data will be retrieved.

Step 3 Click **Execute** to initiate the inventory request and check the output files as specified in the Response message.

Step 4 Click the **Scheduling** tab to schedule the web services to run later or click on Run Now option to run web services immediately.

Step 5 To schedule the web services for a later date/time:

a. Select the **Schedule Job** radio button. The scheduling options Once and Recurring are enabled.

b. To execute the webservice operation once, select the **Once** radio button and specify the date and time.

c. To schedule the web services operation execution on a recurring basis, select the **Recurring** radio button and specify the following:

– The date and time range for the recurrence.

– How often you want to initiate the inventory request within that time range - every X minutes, daily, weekly, or monthly.

Step 6 Specify comments, if required and click **Schedule**. Prime Network initiates the inventory request and executes it according to your scheduling specifications. Go to the **Scheduled Jobs** page (**Tools** > **Scheduled Jobs**), to check that your inventory request job has been created. You can use the Scheduled Jobs page to monitor the job status and to reschedule a job if necessary. You can also clone a scheduled job and edit the criteria, if required.

MTOSI Inventory Support for Small Cell Integration using Network Function APIs

To retrieve a specific network function supported by the device, the APIs used are

- getNetworkFunctionNamesByType
- getNetworkFunction

getNetworkFunctionNamesByType

This API is used to return all the network functions names for a particular network function type like mobility function supported by the device.

Following are the supported mobility network function service types,

- GGSN Services
- SGSN Services
- MME Services
- HeNB Gateway Services
  - HeNB Gateway Access services
  - HeNB Gateway Network Services
- HNB Services
- Sec Gateway Services

getNetworkFunction

This API is used to return details of mobility network function supported by getNetworkFunctionNamesByType API.

Note Any addition, deletion, or change in the attributes supported by PNIL for the H(e)NB GW,MME,PGW, GSN, or Security GW services should be informed to the client subscribed for MTOSI notifications.

Viewing Operator Policies, APN Remaps, and APN Profiles

Operator policy provides mechanisms to fine tune the behavior of subsets of subscribers above and beyond the behaviors described in the user profile. It can also be used to control the behavior of visiting subscribers in roaming scenarios, enforcing roaming agreements, and providing a measure of local protection against foreign subscribers.

An operator policy associates APNs, APN profiles, an APN remap table, and a call-control profile to ranges of International Mobile Subscriber Identities (IMSIs). These profiles and tables are created and defined within their own configuration modes to generate sets of rules and instructions that can be reused and assigned to multiple policies. In this manner, an operator policy manages the application of rules

governing the services, facilities, and privileges available to subscribers. These policies can override standard behaviors and provide mechanisms for an operator to get around the limitations of other infrastructure elements, such as DNS servers and HSSs.

Note Operator policies and APN profiles are applicable only for the 'local' context in the logical inventory.

The following topics explain how to view operator policies, APN remaps, and APN profiles in the Vision client:

- Viewing Operator Policies, page 27-192
- Viewing APN Remaps, page 27-194
- Viewing APN Profiles, page 27-196

Viewing Operator Policies

Operator policies provide an operator with a range of control to manage the services, facilities, and privileges available to subscribers. By configuring the various components of an operator policy, the operator fine tunes any desired restrictions or limitations needed to control call handling and this can be done for a group of callers within a defined IMSI range or per subscriber.

Besides enhancing operator control through configuration, the operator policy feature minimizes configuration by drastically reducing the number of configuration 5.3 needed. Operator policy maximizes configurations by breaking them into the following reusable components that can be shared across IMSI ranges or subscribers:

- Call-control profiles
- IMEI profiles (SGSN only)
- APN profiles
- APN remap tables
- Operator policies
- IMSI ranges

To view operator policies in logical inventory:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory > *local* > Mobile > Policy > Operator Policies**

The Vision client displays the list of operator policies configured under the container. You can view the individual policy details from the table on the right pane or by choosing **Logical Inventory** > *local* > **Mobile > Policy > Operator Policies >** *Policy*.

Table 27-118 describes the details available for each operator policy.

If an operator policy is configured with IMEI ranges and APN entries, the details are displayed in the respective tabs IMEI Ranges and APN Entries on the content pane.

Table 27-118 Operator Policies in Logical Inventory

Field	Description
Name	Name of the operator policy.
Description	Description of the operator policy.
Call Control Profile Name	Name of the call control profile associated with the operator policy.
Call Control Validity	Indicates whether the call control profile name associated with the operator policy is valid or is not created yet (invalid).
APN Remap Table Name	Name of the APN remap table associated with the operator policy.
APN Remap Table Validity	Indicates whether the APN remap table name associated with the operator policy is valid or is not created yet (invalid).
Default APN Profile Name	Name of the default APN profile associated with the operator policy.
Default APN Profile Validity	Indicates whether the default APN profile name associated with the operator policy is valid or is not created yet (invalid).
IMEI Ranges	
Start Range	The starting number in the range of IMEI profiles.
To Range	The ending number in the range of IMEI profiles.
Software Version	Software version to fine tune the IMEI definition.
Profile Name	Name of the IMEI profile associated with the IMEI range. Displays ‘None’, if no profile is associated with the range.
Validity	Validity of the IMEI profile.
APN Entries	
NI	APN network identifier.
NI APN Profile	Name of the APN profile associated with the network identifier. An APN profile groups a set of APN-specific parameters that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, the parameter values configured in the associated APN profile are applied.
NI APN Profile Validity	Indicates whether the NI APN profile associated with the operator policy is valid or is not created yet (invalid).
OI	APN operator identifier.
OI APN Profile	Name of the APN profile associated with the operator identifier. An APN profile groups a set of APN-specific parameters that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, the parameter values configured in the associated APN profile are applied.
OI APN Profile	Indicates whether the OI APN profile associated with the operator policy is valid or is not created yet (invalid).

Viewing APN Remaps

An APN remap tables allow an operator to override an APN specified by a user, or the APN selected during the normal APN selection procedure, as specified by 3GPP TS 23.060. This level of control enables operators to deal with situations such as:

- An APN is provided in the activation request that does not match with any of the subscribed APNs; either a different APN was entered or the APN could have been misspelled. In such situations, the SGSN rejects the activation request. It is possible to correct the APN, creating a valid name so that the activation request is not rejected.
- In some cases, an operator might want to force certain devices or users to use a specific APN. For example, a set of mobile users may need to be directed to a specific APN. In such situations, the operator needs to override the selected APN.

An APN remap table group is a set of APN-handling configurations that may be applicable to one or more subscribers. When a subscriber requests an APN that has been identified in a selected operator policy, the parameter values configured in the associated APN remap table are applied. For example, an APN remap table allows configuration of the following:

- APN aliasing—Maps incoming APN to a different APN, based on partial string match (MME and SGSN) or matching charging characteristic (SGSN only).
- Wildcard APN—Allows APN to be provided by the SGSN, when wildcard subscription is present and the user has not requested an APN.
- Default APN—Allows a configured default APN to be used, when the requested APN cannot be used.

APN remap tables are configured with commands in the APN Remap Table configuration mode. A single APN remap table can be associated with multiple operator policies, but an operator policy can only be associated with a single APN remap table.

To view APN remap properties in logical inventory:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory > *local* > Mobile > Profile > APN Remaps**

The Vision client displays the list of APN remaps configured under the container. You can view the individual APN remap details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Profile > APN Remaps >** *APN Remap.*

Table 27-119 describes the details available for each APN remap.

If an APN remap is configured with charging characteristics and NI and OI entries, the details are displayed in the respective tabs Charging Characteristics, Network And Operator Identifier Entries, and Default APN Entries on the content pane.

Table 27-119 APN Remap Properties in Logical Inventory

Field	Description
Name	Name of the APN remap.
Description	Description of the APN remap.
APN When No APN Requested	APN network identifier that will be used when no APN is requested.

Table 27-119 APN Remap Properties in Logical Inventory (continued)

Field	Description
Wildcard APN for IPv4	Wildcard APN included in the subscriber record, with PDP type as IPv4 context.
Wildcard APN for IPv6	Wildcard APN included in the subscriber record, with PDP type as IPv6 context.
Wildcard APN for IPv4v6	Wildcard APN included in the subscriber record, with PDP type as both IPv4 and IPv6 contexts.
Wildcard APN for PPP	Wildcard APN included in the subscriber record, with PDP type as PPP context.
Charging Characteristics	
Profile Index	Profile index in charging characteristics.
Behavior Bit Value	Behavior bit in charging characteristics.
APN For Overriding	Name of the APN profile that the charging characteristic attributes must be applied to, to generate CDRs.
Network And Operator Identifier Entries	
Requested NI	The old network identifier that is being mapped for replacement.
Mapped to NI	The new network identifier.
NI Wildcard Replace String	When a wildcard character is included in the old APN network identifier, this parameter identifies the information to replace the wildcard in the new APN network identifier.
Requested OI	The old operator identifier that is being mapped for replacement.
Mapped to OI	The new operator identifier.
OI MNC Replace String	When a wildcard character is included in the MNC portion of the old APN operator identifier, this parameter identifies the information to replace the wildcard in the new APN operator identifier.
OI MCC Replace String	When a wildcard character is included in the MCC portion of the old APN operator identifier, this parameter identifies the information to replace the wildcard in the new APN operator identifier.
Default APN Entries	
Default APN	Name of the default APN.
Require Subscription	Indicates whether the configured default APN can be used or not, if there is no APN in the request.
Use Default APN When No APN Is Required	Indicates whether the configured default APN can be used or not, if DNS query fails.
Use Default APN When DNS Query Fails	A fallback APN to be used when the configured default APN is not present in the subscription, so that activation does not fail.
Fallback APN To Use	Indicates whether APN from the first subscription record must be used, when the configured default APN is not available.
Fallback APN In First Subscription	Indicates whether APN from the subscription record must be used, if it is the only record available and the normal APN selection fails.
Use APN From Single Subscription Record	Indicates whether APN from the subscription record must be used, if it is the only record available and the normal APN selection fails.

Note If a default APN is configured for the remap, click the **Default APN** tab to view the APN details. In the APN remap table you can configure four default APNs.

Viewing APN Profiles

APN Profile defines a set of parameters controlling the SGSN or MME behavior, when a specific APN is received or no APN is received in a request. An APN profile is a key element in the Operator Policy feature. An APN profile is not used or valid unless it is associated with an APN and this association is specified in an operator policy.

Essentially, an APN profile is a template which groups a set of APN-specific commands that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, then the set of commands in the associated APN profile will be applied. The same APN profile can be associated with multiple APNs and multiple operator policies.

An APN profile groups a set of APN-specific parameters that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, the parameter values configured in the associated APN profile are applied. For example:

- Enable or disable a direct tunnel (DT) per APN (SGSN).
- Define charging characters for calls associated with a specific APN.
- Identify a specific GGSN to be used for calls associated with a specific APN (SGSN).
- Define various quality of service (QoS) parameters to be applied to calls associated with a specific APN.
- Restrict or allow PDP context activation on the basis of access type for calls associated with a specific APN.

A single APN profile can be associated with multiple operator policies.

To view APN profile properties in logical inventory:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory > *local* > Mobile > Profile > APN Profiles.**

The Vision client displays the list of APN profiles configured under the container. You can view the individual APN profile details from the table on the right pane or by choosing **Logical Inventory >** *local* **> Mobile > Profile > APN Profiles >** *APN Profile.*

Table 27-120 describes the details available for each APN remap.

If additional properties are configured for the APN profile, you can click the respective tabs on the content pane to view the details:

- Gateway Entries
- RANAP ARP Entries
- QoS Class Entries
- Uplink Traffic Policing Entries/Downlink Traffic Policing Entries

Table 27-120 APN Profile Properties in Logical Inventory

Field	Description
Name	Name of the APN profile.
Description	Description of the APN profile.
QoS Service Capping Prefer Type	Operational preferences for QoS parameters, specifically QoS bit rates. Value could be one of the following: • both-hlr-and-local—Instructs the SGSN to use the locally configured QoS or HLR subscription. • hlr-subscription—Instructs the SGSN to use QoS bit rate from HLR configuration and use the same for session establishment. • local—Instructs the SGSN to use the locally configured QoS bit rate and use the same for session establishment.
Address Resolution Mode	Address resolution mode of the APN profile, which could be one of the following: • fallback-for-dns—Uses DNS query for address resolution. • local—Uses locally configured address.
CC Preferred Source	Charging characteristic settings to be used for S-CDRs, which could be one of the following: • hlr-value-for-scdrs—Instructs the system to use charging characteristic settings received from the HLR for S-CDRs. • local-value-for-scdrs—Instructs the profile preference to use only locally configured/stored charging characteristic settings for S-CDRs.
CC Local SCDR Behavior Bit	Value of the behavior bit for the charging characteristics for S-CDRs.
CC Local SCDR Behavior Profile Index	Value of the profile index for the charging characteristics for S-CDRs.
GGSN Algorithm Applicable	Selection algorithm for GGSNs. This parameter allows the operator to configure multiple GGSN pools by assigning the GGSN to a secondary pool of GGSNs.

Table 27-120 APN Profile Properties in Logical Inventory (continued)

Field	Description
IP Source Validation	Configures settings related to IP source violation detection with one of the following criteria: • deactivate—Deactivates the PDP context with one of the following conditions: – Deactivates all PDP contexts of the MS/UE. Default is to deactivate errant PDP contexts. – Excludes packets having an invalid source IP address from the statistics used in the accounting records. – Deactivates all associated PDP contexts (primary/secondary). Default is to deactivate errant PDP contexts. – Configures maximum number of allowed IP source violations before the session is deactivated. • discard—Discards errant packets and excludes packets having an invalid source IP address from the statistics used in the accounting records. • ignore—Ignores checking of packets for MS/UE IP source violation.
IP Source Validation Tolerance Limit	Maximum number of allowed IP source violations before the session is deactivated.
Direct Tunnel	Permission for direct tunnel establishment by GGSNs, which could be not-permitted-by-ggsn or remove.
Private Extension LORC IE to GGSN	Indicates whether GTPC private extension is enabled or not for the over charging protection feature of the GGSN.
Private Extension LORC IE to SGSN	Indicates whether GTPC private extension is enabled or not for the over charging protection feature of the SGSN.
Idle Mode Access Control List IPV4	Group of IPv4 Access Control Lists (ACLs) that define rules to apply to downlink data destined for UEs in an idle mode.
Idle Mode Access Control List IPV6	Group of IPv6 ACLs that define rules to apply to downlink data destined for UEs in an idle mode.
DNS Query with MSISDN Start Offset Position	The position of the first digit in the MSISDN to start an offset and create a new APN DNS query string that is intended to assist roaming subscribers to use the local GGSN.
DNS Query with MSISDN End Offset Position	The position of the last digit in the MSISDN to be part of the offset.
DNS Query with LAC or RAC	Indicates whether geographical information must be appended to the APN string that is sent to the DNS query or not. This information is used during the DNS query process to select the geographically closest GGSN.
DNS Query with RNC ID	Indicates whether the SGSN must include the ID of the calling RNC in the APN DNS query string or not.
DNS Query with Charging Characteristics	Indicates whether charging characteristic configuration is enabled for the APN profile or not.

Table 27-120 APN Profile Properties in Logical Inventory (continued)

Field	Description
DNS Query Charging Characteristics ID Format	Format of the charging characteristic information to be included.
Gateway Entries	
Gateway Entry	Gateway entry configured for the APN profile.
IP Address	IPv4 or IPv6 addresses of the gateway configured.
Priority	Priority of the gateway to consider during address selection.
Weight	Weightage or importance assigned to the gateway for load balancing.
Pool	Gateway pool assigned.
Gateway Type	Type of gateway configured, which could be GGSN or P-GW.
RANAP ARP Entries	
Traffic Class	Traffic class of the Radio Access Network Application Part (RANAP) configuration.
Subscription Priority	Subscription priority of the traffic class; the lowest number denoting the highest priority.
Priority Level	Priority level for the subscription priority.
Preemption Capability	Preemption capability value of the traffic class.
Preemption Vulnerability	Preemption vulnerability value of the traffic class.
Queuing Allowed	Indicates whether queuing is allowed for the traffic class or not.
QoS Class Entries	
Class Name	Traffing class of the QoS configuration.
Service Delivery Unit Delivery Order	Indicates whether bearer should provide in-sequence delivery of service data units (SDUs) or not.
Delivery of Erroneous Service Delivery Units	Indicates whether SDUs detected as erroneous should be delivered or discarded.
Max Bit Rate Uplink	Maximum bit rate, in kbps, allowed for uplink between MS and the core network.
Max Bit Rate Downlink	Maximum bit rate, in kbps, allowed for downlink between MS and the core network.
Allocation Retention Priority	Relative importance compared to other Radio Access Bearers (RABs) for allocation and retention of the RAB.
Traffic Handling Priority	Relative importance for traffic handling when compared to other RABs.
SDU Max Size	Maximum allowed SDU size, in bytes.
SDU Error Ratio	Fraction of SDUs lost or detected as erroneous.
Guaranteed Bit Rate Uplink	Uplink bit rate, in kbps, that is assured for a given RAB between MS and the core network.
Guaranteed Bit Rate Downlink	Downlink bit rate, in kbps, that is assured for a given RAB between MS and the core network.

Table 27-120 APN Profile Properties in Logical Inventory (continued)

Field	Description
Minimum Transfer Delay	Minimum transfer delay, in milliseconds.
Residual BER	Undetected bit error ratio (BER) in the delivered SDUs.
MBR Map Down	Attribute that maps or converts the received HLR maximum bit rate (MBR) (from value) to a locally configured downlink MBR value (to value).
MBR Map Up	Attribute that maps or converts the received HLR MBR (from value) to a locally configured uplink MBR value (to value).
Uplink Traffic Policing Entries/Downlink Traffic Policing Entries	
Traffic Class	Traffic class of the QoS configuration.
Burst Size Auto Readjust	Indicates whether the auto readjustment of burst size is enabled or disabled. This parameter is used in dynamic burst size calculation, for traffic policing, at the time of PDP activation or modification.
Burst Size Auto Readjust Duration	The burst size readjustment duration in seconds. This parameter indicates the number of seconds that the dynamic burst size calculation will last for. This allows the traffic to be throttled at the negotiated rates.
Peak Burst Size (bytes)	The peak burst size allowed, in bytes, for the uplink/downlink direction and QoS class.
Guaranteed Burst Size (bytes)	The guaranteed burst size allowed, in bytes, for the uplink/downlink direction and QoS class.
Exceed Action	The action to be taken on packets that exceed the committed data rate, but do not violate the peak data rate. The action could be one of the following: • Drop • Lower IP Precedence • Transmit
Violate Action	The action to be taken on packets that exceed both committed and peak data rates. The action could be one of the following: • Drop • Lower IP Precedence • Shape • Transmit

Viewing Additional Characteristics of an APN Profile

To view additional characteristics of an APN profile:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *local* **> Mobile > Profile > APN Profiles >** *APN Profile*.

Step 3 Expand the *APN Profile* node. The following list of characteristics configured for the APN profile are displayed:

- PDP Inactivity Actions—Attributes related to PDP data inactivity. Once a data communication is in progress there are cases where this data communication can be inactive after some time, for example, when the user has locked the phone after browsing the internet or when the battery suddenly drains out. In such a case, the SGSN can take a configured action based on this inactivity. The inactivity timeout and the actions that can be taken based on certain conditions are modeled in this configuration.
- QoS to DSCP Mapping (Downlink) / Qos to DSCP Mapping (Uplink)—Mapping of QoS parameters to DSCP. Configuration of the local values for the traffic class (TC) parameters for QoS configured for the APN.
- PDP Restrictions (UMTS) / PDP Restrictions (GPRS)—Activation restrictions on PDP.

Step 4 Click each of one of these characteristics to view its properties on the right pane. See Table 27-121 for more details on the properties of each characteristics configured for the APN profile.

Table 27-121 APN Profile Additional Characteristics

Field	Description
PDP Inactivity Actions	
PDP Inactivity Idle Timeout	Timeout duration for PDP inactivity. PDP context is deactivated, if it is inactive for the given duration.
PDP Inactivity Idle Timeout Action	Action to be taken when the PDP data communication is inactive for the timeout duration.
PDP Inactivity Idle Timeout Action Condition	Condition when the GPRS detach procedure should be executed on the PDP context, when the timeout is reached or exceeded.
PDP IPV4 IPV6 Override	PDP type to use, per APN, if dual PDP type addressing is not supported by the network.
QoS to DSCP Mapping (Downlink) / Qos to DSCP Mapping (Uplink)	
Conversational	Real time conversational traffic class of service, which is reserved for voice traffic.
Streaming	Streaming traffic class of service, which handes one-way, real-time data transmission, such as streaming video or audio.
Interactive Threshold Priority 1/2/3	Interactive traffic class of service with threshold priorities 1, 2, and 3.
Background	Background traffic class of service. This best-effort class manages traffic that is handled as a background function, such as e-mail, where time to delivery is not a key factor.
Interactive TP1 Alloc P1/P2/P3	Interactive traffic class of service, with threshold priority 1 and allocation priorities 1, 2, and 3.
Interactive TP2 Alloc P1/P2/P3	Interactive traffic class of service, with threshold priority 2 and allocation priorities 1, 2, and 3.
Interactive TP3 Alloc P1/P2/P3	Interactive traffic class of service, with threshold priority 3 and allocation priorities 1, 2, and 3.
PDP Restrictions (UMTS) / PDP Restrictions (GPRS)	

Table 27-121 APN Profile Additional Characteristics (continued)

Field	Description
QoS Class Background	Indicates whether background traffic class of service is enabled or not.
QoS Class Interactive	Indicates whether interactive traffic class of service is enabled or not.
QoS Class Streaming	Indicates whether streaming traffic class of service is enabled or not.
QoS Class Conversational	Indicates whether conversational traffic class of service is enabled or not.

Working with Active Charging Service

Enhanced Charging Service (ECS), also known as Active Charging Service (ACS), is an in-line service, which is integrated within the platform and provides mobile operators the ability to offer tiered, detailed, and itemized billing to subscribers. Data packets flow through the ECS subsystem and relevant actions are performed based on the configured rules. Charging records (xCDRs) will be generated and forwarded to ESS or billing systems for prepaid and post paid billing.

The major components and functions of an ECS solution are given below.

Content Service Steering

Content Service Steering (CSS) enables directing selective subscriber traffic into the ECS subsystem. CSS uses Access Control Lists (ACLs) to redirect selective subscriber traffic flows. ACLs control the flow of packets into and out of the system. ACLs consist of rules (ACL rules) or filters that control the action taken on packets matching the filter criteria.

ACLs are configurable on a per-context basis and apply to a subscriber through either a subscriber profile (for PDSN) or an APN profile (for GGSN) in the destination context.

Protocol Analyzer

Protocol analyzer stack is responsible for analyzing the individual protocol fields during packet inspection. The analyzer supports the following types of packet inspection:

- Shallow Packet Inspection—Inspection of the Layer 3 (IP header) and Layer 4 (for example, UDP or TCP header) information.
- Deep Packet Inspection—Inspection of Layer 7 and above information. This functionality includes:
  - Detection of Uniform Resource Identifier (URI) information at level 7 (example, HTTP)
  - Identification of true destination in the case of terminating proxies, where shallow packet inspection only reveals the destination IP address/port number of a terminating proxy

Rule Definitions

Rule definitions (ruledefs) are user-defined expressions, based on protocol fields and protocol states, which define what actions to take when specific field values are true.

Most important rule definitions are related to Routing and Charging as explained below:

- Routing Ruledefs—Routing ruledefs are used to route packets to content analyzers. Routing ruledefs determine which content analyzer to route the packet to, when the protocol fields and/or protocol states in ruledef expression are true.

- Charging Ruledefs—Charging ruledefs are used to specify what action to take based on the analysis done by the content analyzers. Actions can include redirection, charge value, and billing record emission.

Rule Base

A rule base is a collection of rule definitions and their associated billing policy. The rule base determines the action to be taken when a rule is matched. Rule bases can also be used to apply the same rule definitions for several subscribers, which eliminate the need to have unique rule definition for each subscriber. We can set priority, default bandwidth policy, type of billing for subscriber sessions, for a rule definition or group of rule definitions in the rule base.

Content Filtering

ACS also offers a content filtering mechanism. Content filtering is an in-line service available for 3GPP and 3GPP2 networks to filter HTTP and WAP requests from mobile subscribers, based on the URLs in the requests. Content filtering uses the DPI feature of ECS to discern HTTP and WAP requests. This enables operators to filter and control the content that an individual subscriber can access, so that subscribers are inadvertently not exposed to universally unacceptable content and/or content inappropriate as per the subscribers' preferences.

The content filtering service offers the following solutions:

- URL Blacklisting—With this solution, all HTTP/WAP URLs in subscriber requests are matched against a database of blacklisted URLs. If there is a match, the flow is discarded, redirected, or terminated as configured. If there is no match, subscribers view the content as they would normally.
- Category-based Content Filtering
  - Category-based Static Content Filtering—In this method, all HTTP/WAP URLs in subscriber requests are matched against a static URL categorization database. Action is taken based on a URL's category, and the action configured for that category in the subscriber's content filtering policy. Possible actions include permitting, blocking, redirecting, and inserting content.
  - Category-based Static-and-Dynamic Content Filtering—In this method, each URL first undergoes static rating. If the URL cannot be rated by the static database or if the URL static rating categorizes a URL as either Dynamic or Unknown, the requested content is sent for dynamic rating; wherein the requested content is analyzed and categorized. Action is taken based on the category determined by dynamic rating, and the action configured for that category in the subscriber's content filtering policy. Possible actions include permitting, blocking, redirecting, and inserting content.

Note ACS is applicable only for the 'local' context in the logical inventory.

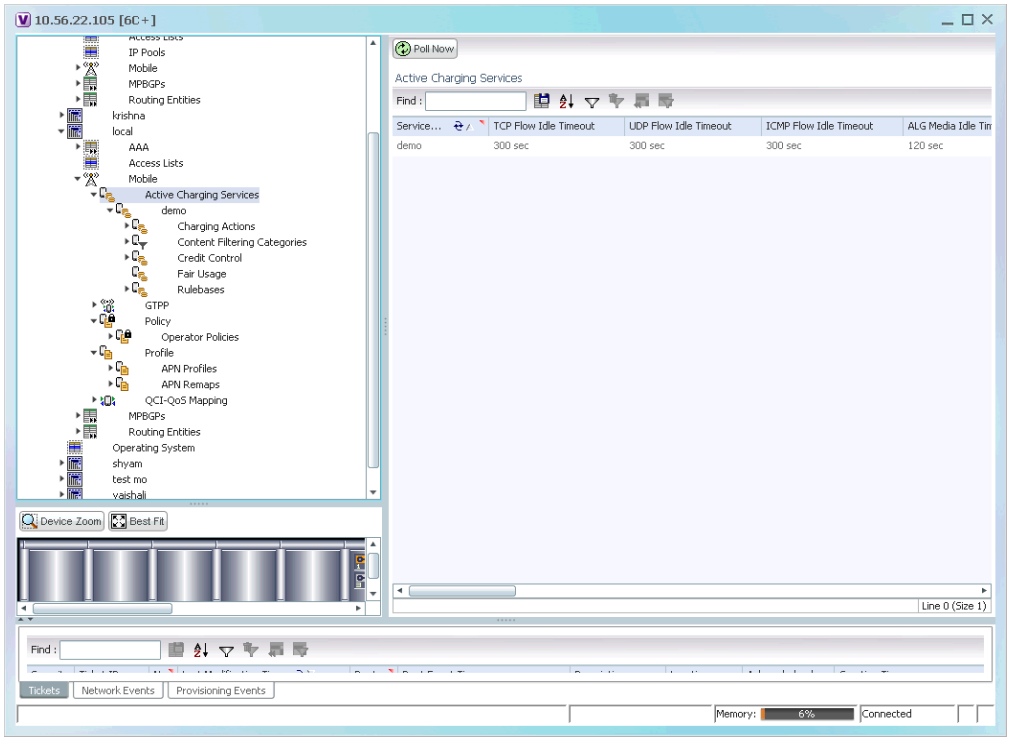
The following topics explain how to work with ACS in the Vision client:

- Viewing Active Charging Services, page 27-204
- ACS Commands, page 27-217

Viewing Active Charging Services

You can view the active charging services in logical inventory as shown in Figure 27-22.

Figure 27-22 Mobile Technology Setup Nodes



Additionally, you can also perform the following for each ACS:

- Viewing Content Filtering Categories, page 27-206
- Viewing Credit Control Properties, page 27-206
- Viewing Charging Action Properties
- Viewing Rule Definitions
- Viewing Rule Base for the Charging Action
- Viewing Bandwidth Policies
- Viewing Fair Usage Properties

To view ACS details in logical inventory:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *local* **> Mobile > Active Charging Services**.

The Vision client displays the list of active charging services configured under the container. You can view the individual ACS details from the table on the right pane or by choosing **Logical Inventory >** *local* **> Mobile > Active Charging Services >** *ACS*.

Table 27-122 describes the details available for each ACS.

Table 27-122 Active Charging Services in Logical Inventory

Field	Description
Service Name	Name of the active charging service.
TCP Flow Idle Timeout	Maximum duration, in seconds, a TCP flow can remain idle.
UDP Flow Idle Timeout	Maximum duration, in seconds, a UDP flow can remain idle.
ICMP Flow Idle Timeout	Maximum duration, in seconds, an Internet Control Message Protocol (ICMP) flow can remain idle.
ALG Media Idle Timeout	Maximum duration, in seconds, an application level gateway (ALG) media flow can remain idle.
TCP Flow Mapping Idle Timeout	The time for which the TCP flow mapping timer holds the resources.
UDP Flow Mapping Idle Timeout	The time for which the UDP flow mapping timer holds the resources.
Deep Packet Inspection	Indicates whether configuration of DPI is enabled or disabled in the mobile video gateway.
Passive Mode	Indicates whether the ACS is in or out of passive mode operation.
CDR Flow Control	Indicates whether flow control is enabled or disabled between the ACS Manager (ACSMGR) and Charging Data Record Module (CDRMOD).
CDR Flow Control Unsent Queue Size	Flow control unsent queue size at ACSMGR level.
Unsent Queue High Watermark	Highest flow control unsent queue size at ACSMGR level.
Unsent Queue Low Watermark	Lowest flow control unsent queue size at ACSMGR level.
Content Filtering	Indicates whether content filtering is enabled or disabled for the ACS.
Dynamic Content Filtering	Indicates whether dynamic content filtering is enabled or disabled for the ACS.
URL Blacklisting	Indicates whether URL blacklisting is enabled or disabled for the ACS.
URL Blacklisting Match Method	Method to look up the URLs in the URL blacklisting database.
Content Filtering Match Method	Method to look up the URLs in the category-based content filtering database.
Interpretation of Charging Rulebase Name	Charging rulebase configured for the ACS.
Selected Charging Rulebase Name for AVP	Charging rulebase name for attribute value pair (AVP) configured for the ACS.

Viewing Content Filtering Categories

To view content filtering categories in logical inventory:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *local* **> Mobile > Active Charging Services >** *ACS* **> Content Filtering Categories**.

The Vision client displays the list of content filtering categories configured under the container. You can view the individual content filtering category details from the table on the right pane or by choosing **Logical Inventory >** *local* **> Mobile > Active Charging Services >** *ACS* **> Content Filtering Categories** > *Content Filtering Category.*

Table 27-123 describes the details available for each content filtering category.

Table 27-123 Content Filtering Categories in Logical Inventory

Field	Description
Policy ID	ID of the content filtering policy.
Failure Action	Action to take for the content filtering analysis result.
EDR File	The EDR file name.
Content Category	Name of the content filtering category.
Content Insert	Content string to insert in place of the message returned from prohibited or restricted site or content server.
Content Priority	Precedence of the category in the content filtering policy.
Content Failure Action	Action to take for the indicated result of the content filtering analysis, which could be one of the following: • allow • content-insert • discard • redirect URL • terminate flow • www-reply-code-and-terminate-flow
Content Redirect	Content string to redirect the subscriber to a specified URL.
Content Reply Code	Reply code to terminate flow.
EDR File Format	Predefined EDR file format.

Viewing Credit Control Properties

In a prepaid environment, the subscribers pay for a service prior to using it. While the subscriber is using the service, credit is deducted from subscriber's account until it is exhausted or the call ends. In prepaid charging, ECS performs the metering function. Credits are deducted in real time from an account balance or quota. A fixed quota is reserved from the account balance and given to the system by a prepaid rating and charging server, which interfaces with an external billing system platform. The system deducts

volume from the quota according to the traffic analysis rules. When the subscriber's quota gets to the threshold level specified by the prepaid rating and charging server, system sends a new access request message to the server and server updates the subscriber's quota. The charging server is also updated at the end of the call.

ECS supports the following credit control applications for prepaid charging:

- RADIUS Credit Control Application—RADIUS is used as the interface between ECS and the prepaid charging server.
- Diameter Credit Control Application—The Diameter Credit Control Application (DCCA) is used to implement real-time credit control for a variety of services, such as networks access, messaging services, and download services.

To view credit control properties in logical inventory:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory > *local* > Mobile > Active Charging Services > *ACS* > Credit Control**.

The Vision client displays the list of credit control groups configured under the container. You can view the individual credit control group details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Active Charging Services > *ACS* > Credit Control** > *Credit Control Group*.

You can also view the following details by clicking the respective node under the credit control group:

- Diameter
- Failure Handling
- Pending Traffic Treatment
- Quota
- Server Unreachable Failure Handling

Table 27-124 describes the details available for each credit control group.

Table 27-124 Credit Control Properties in Logical Inventory

Field	Description
Group	Name of the credit control group for the subscriber.
Mode	Prepaid charging application mode, which could be Diameter or Radius.
APN Name to be Included	Type of APN name sent in the credit control application (CCA) message.
Trigger Type	Condition based on which credit reauthorization is triggered from the server.
Diameter MSCC Final Unit Action Terminate	Indicates whether to terminate a PDP session immediately when the Final-Unit-Action (FUA) in a particular multi service credit control (MSCC) is set as Terminate and the quota is exhausted for that service, or to terminate the session after all MSCCs (categories) have used their available quota.
Diameter Peer Select table	
Peer	Primary hostname.
Realm	Realm for the primary host.
Secondary Peer	Secondary hostname.
Secondary Realm	Realm for the secondary host.
IMSI Range Mode	Mode of peer selection based on IMSI prefix or suffix.
IMSI Start Value	Starting value of the IMSI range for peer selection.
IMSI End Value	Ending value of the IMSI range for peer selection.
Diameter	
End Point Name	Name of the diameter endpoint.
End Point Realm	Realm of the diameter endpoint.
Pending Timeout	Maximum time to wait for response from a diameter peer.
Session Failover	Indicates whether diameter session failover is enabled or not.
Dictionary	Diameter credit control dictionary for the ACS.
Failure Handling	
Initial Request	Failure handling behavior, if failure takes place during initial session establishment. Value could be continue, retry-and-terminate, and terminate.
Update Request	Failure handling behavior, if failure takes place during update request. Value could be continue, retry-and-terminate, and terminate.
Terminate Request	Failure handling behavior, if failure takes place during terminate request. Value could be continue, retry-and-terminate, and terminate.
Pending Traffic Treatment	
Trigger	Indicates whether to allow or drop a trigger while waiting for the credit information from the server. Value could be pass or drop.
Forced Reauth	Indicates whether to allow or drop reauthorization while waiting for the credit information from the server. Value could be pass or drop.
NoQuota	Indicates whether to allow or drop traffic, if there is no quota present. Value could be pass, drop, or buffer.
Quota Exhausted	Indicates whether to allow or drop traffic, if quota is exhausted. Value could be pass, drop, or buffer.

Table 27-124 Credit Control Properties in Logical Inventory (continued)

Field	Description
Validity Expired	Indicates whether to allow or drop traffic, if quota validity is expired. Value could be pass or drop.
Quota	
Request Trigger	Action taken on the packet that triggers the credit control application to request quota. Value could be exclude-packet-causing-trigger or include-packet-causing-trigger.
Holding Time	Duration for which ECS can hold the quota before returning to the credit control server.
Validity Time	Lifetime for which subscriber quota retrieved from the billing server is valid.
Time Threshold	Time threshold limit for subscriber quota in the prepaid credit control service.
Units Threshold	Unit threshold limit for subscriber quota in the prepaid credit control service.
Volume Threshold	Volume threshold limit for subscriber quota in the prepaid credit control service.
Server Unreachable Failure Handling	
Initial Request	Failure handling behavior if server is unreachable during initial session establishment. Value could be continue or terminate.
Update Request	Failure handling behavior if server is unreachable during update request. Value could be continue or terminate.

Viewing Charging Action Properties

Charging Action is an action taken on the incoming data packets once the data packets are treated by the routing and charging rule components. User can configure independent actions such as allow, forward, and block traffic, and bind these actions with other routing and charging rule components.

To view charging action properties in logical inventory:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *local* **> Mobile > Active Charging Services >** *ACS* **> Charging Action**.

The Vision client displays the list of charging actions configured under the container as shown. You can view the individual charging action details from the table on the right pane or by choosing **Logical Inventory >** *local* **> Mobile > Active Charging Services >** *ACS* **> Charging Action** > *Charging Action.*

You can also view the following details by clicking the respective node under the Charging Action node:

- Allocation Retention Priority
- Bandwidth
- Flow Action
- QoS

- Video
- Billing Action

Table 27-125 describes the details available for each charging action record.

Table 27-125 Charging Action Properties in Logical Inventory

Field	Description
Name	Name of the charging action.
Content ID	Content ID to use in the generated billing records as well the AVP used by the credit control application.
Service ID	Configured service ID used to associate the charging action in rule definitions configuration.
Charging EDR Name	Name of the EDR format for the billing action in the ACS.
EGCDRs	Indicates whether eG-CDRs must be generated when the subscriber session ends or an interim trigger condition occurs.
Rf	Indicates whether Rf accounting is enabled or not.
UDRs	Indicates whether UDRs must be generated based on the UDR format declared in the rule base.
Flow Idle Timeout	Maximum duration a flow can remain idle after which the system automatically terminates the flow.
Limit for Flow Type State	Indicates whether the limit for flow type is configured or not.
Limit for Flow Type Value	Maximum number of flows of a particular type.
Limit for Flow Type Action	Action to be taken, if the number of flows exceeds the maximum limit.
IP Type of Service	IP Type of Service (ToS) octets used in the charging action.
Retransmission Count	Indicates whether to count the number of packet retransmissions when the charging action is applied on the incoming data packets.
Content Filtering	Indicates whether content filtering must be applied on the incoming packets or not.
Credit Control	Indicates whether to apply credit control or not.
Credit Rating Group	Coupon ID used in prepaid charging as rating group.
Charge Volume	Method used for charge volume calculation based on the protocol and packet.
Next Hop Forwarding Address	Next hop forwarding address for a charging action.
VLAN ID	VLAN ID configured for the subscriber
Flow Mapping Idle Timeout	Maximum duration, in seconds, a flow can remain idle after which the system automatically terminates the flow.
Allocation Retention Priority	
Priority Level	Priority value that indicates whether to accept or reject a request for establishment or modification of a bearer in a limited resource condition.

Table 27-125 Charging Action Properties in Logical Inventory (continued)

Field	Description
Priority Vulnerability Indicator	Defines whether an active bearer can be preempted by a preemption-capable high priority bearer.
Priority Capability Indicator	Defines whether the bearer request can preempt the resources from the Low Priority Pre-empatable Active Bearers.
Bandwidth	
Bandwidth ID	The bandwidth policy ID for the ACS.
Uplink	Indicates whether uplink flow limit is configured for the subscriber or not.
Downlink	Indicates whether downlink flow limit is configured for the subscriber or not.
Charging Action Bandwidth Direction	
Direction	Direction of the packet flow: Uplink or Downlink
Peak Data Rate	Peak data rate configured for the uplink or downlink packet flow.
Peak Burst Size	Peak burst size allowed for the uplink or downlink packets.
Committed Data Rate	Committed data rate for the uplink or downlink packet flow.
Committed Burst Size	Committed burst size allowed for the uplink or downlink packets.
Exceed Action	Action to take on packets that exceed committed data rate but do not violate the peak data rate.
Violate Action	Action to take on packets that exceed both committed and peak data rates.
Bandwidth Limiting ID	Identifier for bandwidth limiting.
Flow Action	
Redirect URL	Indicates whether packets matched to the rule definition must be redirected to a specified URL or not.
Clear Quota Retry Timer	Indicates whether to reset the CCA quota retry timer for a specific subscriber upon redirection of data packets.
Conditional Redirect	Indicates whether packets matching to a configured user agent must be conditionally redirected to a specified URL.
Discard	Discards packets associated with the charging action.
Random Drop	Indicates whether to degrade voice quality and specify the time interval in seconds at which the voice packets will be dropped.
Readdress	Redirects unknown gateway traffic based on the destination IP address of the packets to known or trusted gateways.
Terminate Flow	Indicates whether to terminate the flow by terminating the TCP connection gracefully between the subscriber and external server.
Terminate Session	Indicates whether to terminate the session.
QoS	
Traffic Class	QoS traffic class for the charging action, which could be background, conversational, interactive, or streaming.
Class Identifier	The QCI value.
Video	

Table 27-125 Charging Action Properties in Logical Inventory (continued)

Field	Description
Bit Rate	Bits per second, at which the TCP video flow must be paced during video pacing.
CAE Readdressing	Indicates whether Content Adaptation Engine (CAE) readdressing is enabled, allowing video traffic to be fetched from the CAEs in the CAE group.
Transrating	Indicates whether transrating is enabled or not. Transrating is a mobile video feature that reduces the encoded bit rates by adjusting video encoding.
Target Rate Reduction	Percentage of the input bit rate of a video flow.
Billing Action	
EDR	Name of the EDR format for the billing action in the ACS.
EGCDR	Indicates whether eG-CDRs must be generated when the subscriber session ends or an interim trigger condition occurs.
Rf	Indicates whether Rf accounting is enabled or not.
UDRs	Indicates whether UDRs must be generated based on the UDR format declared in the rule base.
Radius Accounting Record	Indicates whether radius accounting is enabled or not.

Viewing Rule Definitions

Rule definitions are user-defined expressions, based on protocol fields and protocol states, which define what actions to take when specific field values are true. Each rule definition configuration consists of multiple expressions applicable to any of the fields or states supported by the respective analyzers.

Rule definitions are of the following types:

- Routing—Used to route packets to content analyzers. Routing rule definitions determine which content analyzer to route the packet to when the protocol fields and/or protocol states in the rule definition expression are true. Up to 256 rule definitions can be configured for routing.
- Charging—Used to specify what action to take based on the analysis done by the content analyzers. Actions can include redirection, charge value, and billing record emission. Up to 2048 charging rule definitions can be configured in the system.
- Post-processing—Used for post-processing purposes. Enables processing of packets even if the rule matching for them has been disabled.
- TPO—Used for Traffic Performance Optimization (TPO) in-line service match-rule and match advertisement features.

To view rule definitions in logical inventory:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *local* **> Mobile > Active Charging Services >** *ACS* **> Rule Definitions**.

The Vision client displays the list of rule definitions configured under the container. You can view the individual rule definition details from the table on the right pane or by choosing **Logical Inventory >** *local* **> Mobile > Active Charging Services >** *ACS* **> Rule Definitions** > *Rule Definition.*

Table 27-126 describes the details available for each rule definition.

Table 27-126 Rule Definition Group Properties in Logical Inventory

Field	Description
Name	Name of the rule definition group.
Application Type	Purpose of the rule definition, which could be charging, routing, post-processing, or Traffic Performance Optimization (TPO).
Copy Packet To Log	Indicates whether to copy every packet that matches the rule to a log file.
Tethered Flow Check	Indicates whether tethered flow check if enabled or not. Tethering detection flow check feature enables detection of subscriber data traffic flow originating from PC devices tethered to mobile smart phones, and also provides effective reporting to enable service providers take business decisions on how to manage such usage and to bill subscribers accordingly.
Multiline OR	Indicates whether to apply the OR operator to all 5.3 in a rule definition. This allows a single rule definition to specify multiple URL expressions.
Protocol Configuration	
Protocol	The protocol that this rule definition is applied on.
Fields	Particular protocol field, which is applied on the data packets for inspection. Value could be, host, payload, or domain.
Operator	Logical operator that indicates how to logically match the value in the field analyzed based on the data type.
Value	Value of a particular protocol in a rule definition which has to be applied on the incoming data packets for inspection.

Viewing Rule Definition Groups

A rule definition group enables grouping the rule definitions into categories. A rule definition group may contain optimizable rule definitions. Whether a group is optimized or not is decided on whether all the rule definitions in the group can be optimized. When a new rule definition is added, it is checked if it is included in any rule definition group and whether it needs to be optimized or not.

To view rule definition groups in logical inventory:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *local* **> Mobile > Active Charging Services >** *ACS* **> Group of Rule Definitions**.

The Vision client displays the list of rule definition groups configured under the container. You can view the individual rule definition group details from the table on the right pane or by choosing **Logical Inventory >** *local* **> Mobile > Active Charging Services >** *ACS* **> Group of Rule Definitions** > *Rule Definition Group.*

Table 27-127 describes the details available for each rule definition group.

Table 27-127 Rule Definition Group Properties in Logical Inventory

Field	Description
Name	Name of the rule definition group.
Application Type	Purpose of the rule definition group, which could be charging, routing, content filtering, post-processing, or Traffic Performance Optimization (TPO).
Dynamic Command Content Filtering Policy ID	Content filtering policy ID to add or remove dynamic commands from the rule definition group.

Rule Definition Group Commands

The following RuleDef commands can be launched from the inventory by right-clicking a rule definition group and choosing **Commands > Configuration** or **Commands > Show.** Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-128 Rule Definition Group Commands

Command Type	Command	Inputs Required and Notes
Configuration	**Delete Group of RuleDefs**	Delete the rule definition group.
Show	**Show Group of RuleDefs**	Display the group of rule definitions.

Viewing Rule Base for the Charging Action

A rule base is a collection of rule definitions and their associated billing policy. The rule base determines the action to be taken when a rule is matched. A maximum of 512 rule bases can be specified in the ECS service. It is possible to define a rule definition with different actions.

Rule bases can also be used to apply the same rule definitions for several subscribers, which eliminate the need to have unique rule definition for each subscriber. We can set priority, default bandwidth policy, type of billing for subscriber sessions, for a rule definition/ group of rule definitions in the rule base. Additionally we can configure content based billing and firewall/NAT constituent to rule base.

To view a rule base in logical inventory:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory >** *local* **> Mobile > Active Charging Services >** *ACS* **> Rulebase Container**.

The Vision client displays the list of rule bases configured under the container. You can view the individual rule base details from the table on the right pane or by choosing **Logical Inventory >** *local* **> Mobile > Active Charging Services >** *ACS* **> Rulebase Container** > *Rule Base.* Table 27-129 describes the details available for each rule base record.

Table 27-129 Rule Base Properties in Logical Inventory

Field	Description
Rulebase Name	Name of the rule base.
Flow Any Error Charging Action	Charging action to be used for packets dropped due to any error conditions after data session is created.
Limit for Total Flows	Maximum number of simultaneous uplink and downlink packet flows.
Limit for TCP Flows	Maximum number simultaneous TCP packet flows per subscriber or APN allowed for a rulebase.
Limit for Non TCP Flows	Maximum number simultaneous non-TCP packet flows per subscriber or APN allowed for a rulebase.
Charging Rule Optimization	Internal optimization level to use, for improved performance, when evaluating each instance of the action.
QoS Renegotiation Timeout	Timeout value after which QoS renegotiation is performed.
RTP Dynamic Routing	Indicates whether the Real Time Streaming Protocol (RTSP) and SDP analyzers are enabled to detect the start/stop of RTP (a Transport Protocol for Real-Time Applications) and RTP Control Protocol (RCP) flows.
Ignore Port Number In Application Header	Indicates whether to consider or ignore the port number embedded in the application.
Delayed Charging	Indicates how to charge for the control traffic associated with an application.
XHeader Certificate Name	Name of the encryption certificate to be used for x-header encryption.
XHeader Reencryption Period	Indicates how often to regenerate the encryption key for x-header encryption.
Default Bandwidth Policy	Name of the default bandwidth policy per subscriber.
P2P Dynamic Routing	Indicates whether P2P analyzer is enabled to detect the P2P applications flow configured in ACS.
Fair Usage Waiver Percentage	Waiver percent on top of the average available memory credits per session for the Fair Usage feature of active charging.
URL Blacklisting Action	Configured URL blacklisting action to take when the URL matches ones of the blacklisted URLs.
URL Blacklisting Content ID	Specific content ID for which URL blacklisting is enabled in the rulebase.
Charging Action Priorities tab	Charging rule definitions and their priorities in the rulebase.
Routing Action Priorities tab	Routing actions and their priorities in the rulebase.
Post Processing Action Priorities	Post-processing actions and their priorities in the rulebase.

Viewing Bandwidth Policies

Bandwidth policies are helpful in applying rate limit to potentially bandwidth intensive and service disruptive applications. Using this policy, the operator can police and prioritize subscribers' traffic to ensure that no single or group of subscribers' traffic negatively impacts another subscribers' traffic. Each policy will be identified by a unique ID, which will be associated to a particular group. Bandwidth policies are used to control the direction (uplink/downlink) of bandwidth, peak data rate, and peak burst size, and the actions that need to be taken on violation, if the bandwidth exceeds the burst size and data rate.

To view bandwidth policy in logical inventory:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory > *local* > Mobile > Active Charging Services > *ACS* > Bandwidth Policy Container**.

The Vision client displays the list of bandwidth policies configured under the container. You can view the individual bandwidth policy details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Active Charging Services > *ACS* > Bandwidth Policy Container** > *Bandwidth Policy.*

Table 27-130 describes the details available for each bandwidth policy.

Table 27-130 Bandwidth Policy Properties in Logical Inventory

Field	Description
Name	Name of the bandwidth policy configured.
Total Bandwidth ID Configured	Total number of bandwidth IDs configured.
Total Group Limit Configured	Total number of bandwidth group limits configured.
Flow Limit for Bandwidth ID and Group ID Associations and Group ID tables	Holds all bandwidth IDs and group IDs of the bandwidth policy.

Viewing Fair Usage Properties

To view fair usage properties configured for the ACS:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory > *local* > Mobile > Active Charging Services > *ACS* > Fair Usage**.

The Vision client displays the details on the content pane.

Table 27-131 describes the fair usage properties.

Table 27-131 Fair Usage Properties in Logical Inventory

Field	Description
CPU Threshold Percent	Percentage of system CPU resources that the dynamic inline transrating feature is allowed to use.
Threshold Percent	Percentage of system resources that the dynamic inline transrating feature is allowed to use.
Deactivate Margin Percent	Fair usage deactivate margin, below which monitor action is disabled.

ACS Commands

The following ACS commands can be launched from the inventory by right-clicking an ACS and choosing **Commands > Configuration** or **Commands > Show.** Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-132 Active Charging Services Configuration Commands

Command	Navigation	Description
Create Ruledef	*Expand Active Charging Services node* > *Right-click ACS service* > **Commands** > **Configuration**	Rule definitions (Ruledefs) are user-defined expressions, based on protocol fields and/or protocol-states, which define what actions to take when specific field values are true. Use this command to create a new rule definition for the selected ACS service.
Create group of Ruledefs	*Expand Active Charging Services node* > *Right-click ACS service* > **Commands** > **Configuration**	Group-of-Ruledefs enable grouping ruledefs into categories. When a group-of-ruledefs is configured in a rulebase, if any of the ruledefs within the group matches, the specified charging-action is performed, any more action instances are not. Use this command to create a new group of rule definitions for the selected ACS service.
Create Rulebase	*Expand Active Charging Services node* > *Right-click ACS service* > **Commands** > **Configuration**	A rulebase is a collection of ruledefs and their associated billing policy. The rulebase determines the action to be taken when a rule is matched. Use this command to create a new rule base for the selected ACS service.

Table 27-132 Active Charging Services Configuration Commands (continued)

Command	Navigation	Description
Modify Active Charging Service **Delete Active Charging Service**	*Expand Active Charging Services node* > *Right-click ACS service* > **Commands** > **Configuration**	Use these commands to modify/delete an Active Charging service created for the selected context.
Create Access Ruledef **Delete Access Ruledef**	*Expand Active Charging Services node* > *Right-click ACS service* > **Commands** > **Configuration** > **Access Ruledef**	Use these commands to create/delete an access rule definition for the selected ACS service.
Show Access Ruledef	*Expand Active Charging Services node* > *Right-click ACS service* > **Commands** > **Show**	Use this command to view and confirm the access rule definitions configured for the service.
Create Host Pool **Modify Host Pool** **Delete Host Pool**	*Expand Active Charging Services node* > *Right-click ACS service* > **Commands** > **Configuration** > **Host Pool**	Host pools allow operators to group a set of host or IP addresses that share similar characteristics together. Access rule definitions (ruledefs) can be configured with host pools. Up to ten sets of IP addresses can be configured in each host pool. Use these commands to create/modify/delete a host pool for the selected ACS service.
Create Charging Action	*Expand Active Charging Services node* > *Right-click ACS service* > **Commands** > **Configuration**	Charging Action is an action taken on the incoming data packets once the data packets are treated by the routing and charging rule components. You can configure independent actions such as allow, forward, and block traffic, and bind these actions with other routing and charging rule components. Use this command to configure a charging action for a service.
Modify charging Action **Delete Charging Action**	*Expand Active Charging Services node* > *ACS service* > **Charging Actions** > *Right-click an charging action* > **Commands** > **Configuration**	Use these commands to modify/delete a charging action for a service.
Show Charging Action	*Expand Active Charging Services node* > *Right-click ACS service* > **Commands** > **Show**	Use this command to view and confirm the charging action configuration details.

Mobile Technologies Commands: Summary

The following table provides a summary of the commands you can use to configure and view mobile technologies under a particular context in the Vision client. Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients, page B-1). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-133 Mobile Technologies Configuration Commands

Command	Navigation	Description
Add DNS	Right-click the *context* > **Commands** > **Configuration** > **Others** > **Add DNS**	Creates Domain Name System (DNS).
Remove DNS	Right-click the *context* > **Commands** > **Configuration** > **Others** > **Remove DNS**	Removes a Domain Name System (DNS).
Add NTP	Right-click the *context* > **Commands** > **Configuration** > **Others** > **Add NTP**	Creates a Network Time Protocol (NTP).
Add SNMP	*Right-click the context* > **Commands** > **Configuration** > **Others** > **Add SNMP**	Creates a Simple Network Management Protocol (SNMP).
Configure BFD	*Right-click the context* > **Commands** > **Configuration** > **Others** > **Configure BFD**	Creates Bidirectional Forwarding Detection (BFD) protocol.
Create AAA Group	*Right-click the Context* > **Commands** > **Configuration** > **Mobility** > **Create AAA Group**	AAA refers to Authentication, Authorization, and Accounting, which is a security architecture for distributed systems that determines the access given to users for specific services and the amount of resources they have used. Use this command to create a new AAA group.
Create APN	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create APN**	APN is the access point name that is configured in the GGSN configurations. Use this command to create a new APN service.
Create Access List	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create Access List**	Creates access lists.

Table 27-133 Mobile Technologies Configuration Commands (continued)

Command	Navigation	Description
Create Active Charging Service	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create Active Charging Service**	Enhanced Charging Service (ECS), also known as Active Charging Service (ACS), is an in-line service, which is integrated within the platform and provides mobile operators the ability to offer tiered, detailed, and itemized billing to subscribers. Use this command to create a new ACS service.
Create EGTP	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create EGTP**	Evolved GPRS Tunneling Protocol (EGTP) formulates the primary bearer plane protocol within an LTE / EPC architecture. It provides support for tunnel management including handover procedures within and across LTE networks. Use this command to create an EGTP service.
Create FA	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create FA**	Use this command to create FA.
Create GGSN	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create GGSN**	Gateway GPRS Support Node (GGSM) is the gateway between the GPRS wireless data network and other external packet data networks such as radio networks, IP networks, or private networks. GGSN provides network access to external hosts wishing to communicate with mobile subscribers (MS). Use this command to create a GGSN service.
Create MME	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create MME**	Mobility Management Entity (MME) is the key control-node for an LTE access network, which works in conjunction with NodeB(eNodeB), Serving Gateway, or the LTE/SAW core network. It is responsible for initiating paging and authentication of mobile devices. Use this command to create a GGSN service.
Create SGSN	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create SGSN**	The Serving GPRS Support Node (SGSN) handles the delivery of data from and to the mobile nodes within its geographical service area, such as packet routing and transfer, mobility management, and authentication of users. Use this command to create a SGSN service.
Create GTPP	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create GTPP**	GPRS Tunneling Protocol Prime (GTPP) is used for communicating accounting messages to CGs. Use this command to create a GTPP service.

Table 27-133 Mobile Technologies Configuration Commands (continued)

Command	Navigation	Description
Create IP Pool	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create IP Pool**	An IP pool is a sequential range of IP addresses within a certain network. Use this command to create an IP Pool.
Create GTPU	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create GTPU**	GTPU carries user data within the GPRS core network and between the radio access network and the core network. The user data transported can be packets in any of IPv4, IPv6, or PPP formats. Use this command to create a GTPU service.
Create HSGW	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create HSGW**	Use this command to create a new HSGW service.
Create MAG	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create MAG**	Use this command to create a new Mobile Access Gateway (MAG) service for the selected context.
Create P-GW	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create P-GW**	PDN Gateway (P-GW) is the node that terminates the SGi interface towards the PDN. If a UE is accessing multiple PDNs, there may be more than one P-GW for that UE. Use this command to create a P-GW.
Create QCI-QOS Mapping	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create QCI-QOS Mapping**	The QoS Class Index (QCI) to QoS mapping configuration mode is used to map QCIs to enforceable QoS parameters. Use this command to create a QCI-QOS Mapping.
Create S-GW	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create S-GW**	A Serving Gateway (S-GW) acts as a demarcation point between the Radio Access Network (RAN) and core network, and manages user plane mobility. Use this command to create a S-GW.
Create PDSN	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create PDSN**	Use this command to create a new PDSN service for the selected context.
Create Profile-QCI Mapping	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create Profile-QCI Mapping**	Use this command to create Profile-QCI Mapping

Table 27-133 Mobile Technologies Configuration Commands (continued)

Command	Navigation	Description
Create SAE GW	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create SAE GW**	Use this command to create SAE GW.
Create SGSN	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create SGSN**	Use this command to create an SGSN.
Create VRF	*Right-click the Context* > **Commands** > **Configuration** > **Others** > **Create VRF**	Use this command to create VRF. Virtual routing and forwarding (VRF) is a technology included in IP (Internet Protocol) network routers that allows multiple instances of a routing table to exist in a router and work simultaneously.
Create EPDG	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create EPDG**	Use this command to create a new EPDG service
Create IUPS	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create IUPS**	Use this command to create a new IU PS service.
Delete Context	Right-click the *Context* > **Commands** > **Configuration** > **Others** > **Delete Context**	Use this command to delete a context
Create CGW	Right-click the *Context* > **Commands** > **Configuration** > **Small Cell** > **Create CGW**	Use this command to create CGW
Create HNB GW	Right-click the *Context* > **Commands** > **Configuration** > **Small Cell** > **Create HNB GW**	Use this command to create a new HNB Gateway service.
Create HeNB Access	Right-click the *Context* > **Commands** > **Configuration** > **Small Cell** > **Create HeNB Access**	Use this command to create HeNB access. **Note** You can configure only one HeNB access for a device.
Create HeNB Network	Right-click the *Context* > **Commands** > **Configuration** > **Small Cell** > **Create HeNB Network**	Use this command to create a new HeNB network. **Note** You can configure only one HeNB network for a device.
Create MRME	Right-click the *Context* > **Commands** > **Configuration** > **Small Cell** > **Create MRME**	Use this command to create MRME
Create Crypto Map	Right-click the *Context* > **Commands** > **Configuration** > **SEC GW** > **Create Crypto Map**	Use this command to create Crypto Map.

Table 27-133 Mobile Technologies Configuration Commands (continued)

Command	Navigation	Description
Create Crypto Template	Right-click the *Context* > **Commands** > **Configuration** > **SEC GW** > **Create Crypto Template**	Use this command to create Crypto template.
Create IKEv2 Transform Set	Right-click the *Context* > **Commands** > **Configuration** > **SEC GW** > **Create IKEv2 Transform Set**	Use this command to create a new IKEv2 transform set.
Create IPSec Transform Set	Right-click the *Context* > **Commands** > **Configuration** > **SEC GW** > **Create IPSec Transform Set**	Use this command to create an IPSec Transform Set.
Create SEC GW	Right-click the *Context* > **Commands** > **Configuration** > **SEC GW** > **Create SEC GW**	Use this command to create a new security gateway.
Create SaMOG	Right-click the *Context* > **Commands** > **Configuration** > **Small Cell** > **Create SaMOG**	Use this command to create SaMOG
Delete Context	Right-click the *Context* > **Commands** > **Configuration** > **Others** > **Delete Context**	Use this command to delete a context under the Logical Inventory node.
Modify License	Right-click the *ASR5k* device > **Commands** > **Configuration** > **Modify License**	Use this command to modify the license information.
Create DHCP	Right-click the *Context* > **Commands** > **DHCPv4** > **Configuration** > **Create DHCP** —Or— Right-click the *Context* > **Commands** > **DHCPv6** > **Configuration** > **Create DHCPv6**	DHCP is used to automate host configuration by assigning IP addresses, delegating prefixes (in IPv6), and providing extensive configuration information to network computers. Use this command to create a DHCP service.
Delete DHCP	Right-click the *Context* > **Commands** > **DHCPv4** > **Configuration** > **Delete DHCP** —Or— Right-click the *Context* > **Commands** > **DHCPv6** > **Configuration** > **Delete DHCPv6**	Use this command to delete a DHCP service.

Table 27-133 Mobile Technologies Configuration Commands (continued)

Command	Navigation	Description
Modify DHCP	Right-click the *Context* > **Commands** > **DHCPv4** > **Configuration** > **Modify DHCP** —Or— Right-click the *Context* > **Commands** > **DHCPv6** > **Configuration** > **Modify DHCPv6**	Use this command to modify the configuration details of a DHCP service.
Create HA SPI List	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **HA SPI List** > **Create HA SPI List**	Use this command to create the Security Parameter Index (SPI) between the HA service and the FA.
Delete HA SPI List	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **HA SPI List** > **Delete HA SPI List**	Use this command to delete the HA SPI List.
Modify HA SPI List	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **HA SPI List** > **Modify HA SPI List**	Use this command to modify the HA SPI List configuration details.
Create HA	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Create HA**	Use this command to create a new Home Agent service.
Delete HA	Expand the node **Mobile** > HA > right-click the HA Service > **Commands** > **Configuration** > **Delete HA**	Use this command to delete a HA Service.
Modify HA	Expand the node Mobile > HA > right-click the HA service > **Commands** > **Configuration** > **Modify HA**	Use this command to modify the configuration details of a HA service.
Create Network Requested PDP Context	Right-click the *Context* > **Commands** > **Configuration** > **Others** > **PDP Context** > **Create Network Requested PDP Context**	Packet Data Protocol (PDP) context is the connection or link between a mobile device and a network server that allows them to communicate with each other. A PDP context lasts only for the duration of a specific connection. Use this command to create a network requested PDP context.
Delete Network Requested PDP Context	Right-click the *Context* > **Commands** > **Configuration** > **Others** > **PDP Context** > **Delete Network Requested PDP Context**	Use this command to delete a network requested PDP context.

Table 27-133 Mobile Technologies Configuration Commands (continued)

Command	Navigation	Description
Create Proxy DNS	Right-click the *Context* > **Commands** > **Configuration** > **Others** > **Proxy DNS**	The proxy DNS listens for incoming DNS requests on the local interface and resolves remote hosts using an external PHP script, through http proxy requests. Use this command to create a proxy DNS.
Delete Proxy DNS	Right-click the *Context* > **Commands** > **Configuration** > **Others** > **Proxy DNS**	Use this command to delete a proxy DNS.
Modify Proxy DNS	Right-click the *Context* > **Commands** > **Configuration** > **Others** > **Proxy DNS**	Use this command to modify the proxy DNS configuration details.
Create Route Access List	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Route Map and Route Access List** > **Create Route Access List**	Access lists are a set of rules, organized in a rule table and are used to filter and identify traffic. Use this command to create a new access list.
Create Route Map	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Route Map and Route Access List** > **Create Route Map**	Route maps are similar to access lists; they both have criteria for matching the details of certain packets and an action of permitting or denying those packets. Unlike access lists, though, route maps can add to each "match" criterion a "set" criterion that actually changes the packet in a specified manner, or changes route information in a specified manner. Use this command to create a route map.
Delete Route Access List	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Route Map and Route Access List** > **Delete Route Access List**	Use this command to delete a route access list.
Delete Route Map	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Route Map and Route Access List** > **Delete Route Map**	Use this command to delete a route map.
Modify Route Access List	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Route Map and Route Access List** > **Modify Route Access List**	Use this command to modify a route access list.
Modify Route Map	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Route Map and Route Access List** > Modify **Route Map**	Use this command to modify a route map.

Table 27-133 Mobile Technologies Configuration Commands (continued)

Command	Navigation	Description
Create Subscribers	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Subscriber** > **Create Subscriber**	Use this command to create a new subscriber.
Delete Subscriber	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Subscriber** > **Delete Subscriber**	Use this command to delete a subscriber.
Modify Subscriber	Right-click the *Context* > **Commands** > **Configuration** > **Mobility** > **Subscriber** > **Modify Subscriber**	Use this command to modify subscriber details.
Show APN	Right-click the *Context* > **Commands** > **Show** > **Show APN**	Use this command to view and confirm the APN configuration details.
Show DHCP	Right-click the *Context* > **Commands** > **DHCPv4** > **Show** > **Show DHCP** Right-click the *Context* > **Commands** > **DHCPv6** > **Show** > **Show DHCPv6**	Use this command to view and confirm the DHCP configuration details.
Show EGTP	*Context* > **Mobile** > **EGTP** > right-click the **ETP** service **Commands** > **Show** > **Show EGTP**	Use this command to view and confirm the EGTP configuration details.
Show HA SPI List	Right-click the *Context* > **Commands** > **Show** > **Show HA SPI List**	Use this command to view and confirm the HA SPI List details.
Show HA	*Context* > **Mobile** > **HA** > right-click the HA service > **Commands** > **Show** > **Show HA**	Use this command to view and confirm the home agent service details.
Show IP Pool	Right-click the *Context* > **Commands** > **Show** > **Show IP Pool**	Use this command to view and confirm the IP Pool configuration details.
Show License	Right-click the Device > **Commands** > **Show** > **Show License**	Use this command to view and confirm the License details.
Show Route Access List	Right-click the *Context* > **Commands** > **Show** > **Show Route Access List**	Use this command to view and confirm the Access list details.
Show Route Map	Right-click the *Context* > **Commands** > **Show** > **Show Route Map**	Use this command to view and confirm the Route Map details.

Table 27-133 Mobile Technologies Configuration Commands (continued)

Command	Navigation	Description
Show Subscriber	Right-click the *Context* > **Commands** > **Show** > **Show Subscriber**	Use this command to view and confirm the Subscriber details.
Create Policy Accounting	Right-click the *context* > **Commands** > **Configuration** > **Others** > **Policy Accounting**	Use this command to create a new accounting policy.
Modify Policy Accounting	Right-click the *context* > **Commands** > **Configuration** > **Others** > **Policy Accounting**	Use this command to modify an accounting policy.
Delete Policy Accounting	Right-click the *context* > **Commands** > **Configuration** > **Others** > **Policy Accounting**	Use this command to delete an accounting policy.

Monitoring the Mobility Management Entity

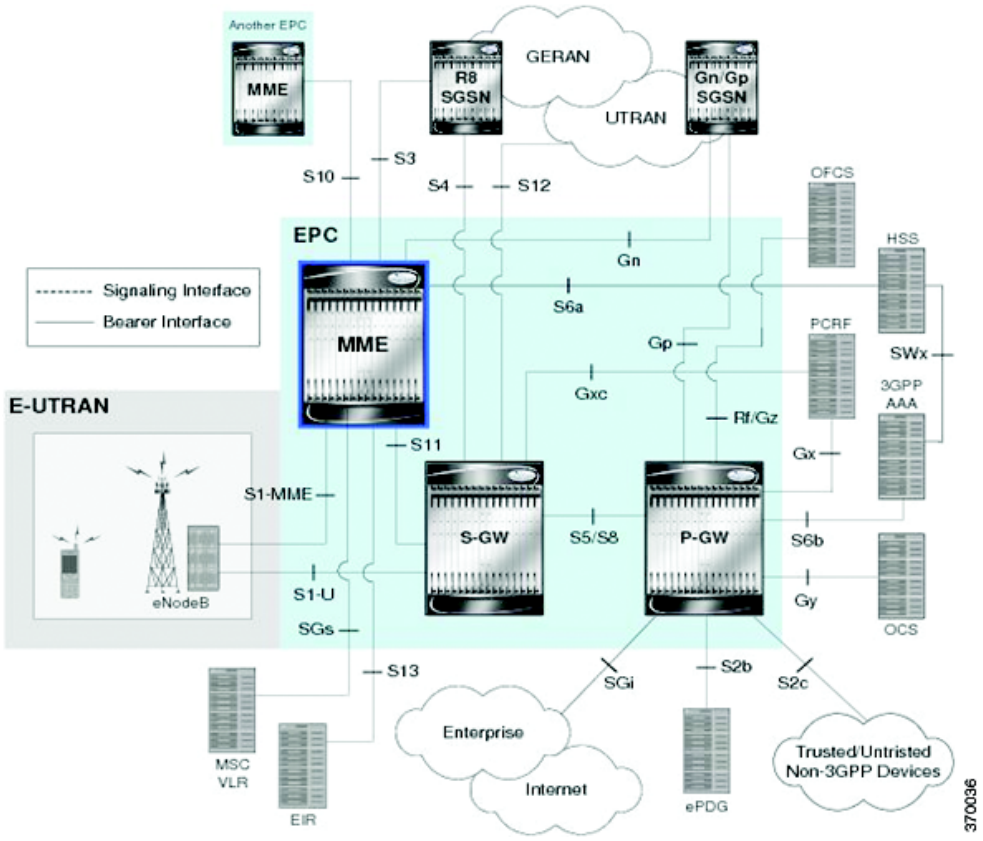
Mobility Management Entity (MME) is the key control-node for an LTE access network, which works in conjunction with NodeB(eNodeB), Serving Gateway, or the LTE/SAW core network. It is responsible for initiating paging and authentication of mobile devices. It keeps location information at the Tracking Area Level for each user and chooses the right gateway during the initial registration process.

The MME uses the SSI-MME interface to connect to an eNode and uses the S11interface to connect to a S-GW. In case there is an increase in the signaling load in the network, you can group multiple MMEs in a pool to meet this load. It is also the termination point in the network for ciphering/integrity protection for NAS signaling.

MME supports lawful interception of signaling and provides the control plane function for mobility between LTE and 2G/3G access networks with the S3 interface terminating at the MME from the SGSN. It also terminates the S6a interface towards the home HSS for roaming UEs.

Figure 27-23 depicts the topology of the LTE network along with MME:

Figure 27-23 MME Topology



The different features of the MME are listed below:

- Involved in bearer activation/deactivation
- Provides P-GW selection to the subscriber to connect to PDN
- Tracks the UE for idle mode and paging procedures, including transmissions
- Chooses the S-GW for a UE during initial attach and also at the time of intra-LTE handover involving Core Network node relocation
- Authenticates the user (by interacting with the HSS)
- Works as a termination point for Non-Access Stratum (NAS) signaling
- Generates and allocates temporary identities to the UEs
- Checks whether the UE is authorized to camp on the service provider's Public Land Mobile Network (PLMN)
- Enforces UE roaming restrictions
- Handles security key management
- Communicates with other MMEs in the same or different PLMN

There are many different MME interfaces, which are listed below:

- S1-MME Interface—The interface used by MME to communicate with eNodeBs on the same PLMN. This interface is the reference point for the control plane protocol between eNodeB and MME, this interface uses the S1 Application Protocol (SI-AP) instead of the Stream Control Transmission Protocol (SCTP) as the transport layer protocol for guaranteed delivery of signaling messages between MME and eNodeB. It serves as a path for establishing and maintaining subscriber UE contexts and supports IPv4, IPv6, IPSec, and multi-homing.
- S3 Interface—The interface used by MME to communicate with S4-SGSNs on the same PLMN for interworking between GPRS/UMTS and LTE network technologies. This interface serves as a signaling path for establishing and maintaining subscriber UE contexts. The MME communicates with SGSNs on the PLMN using the GPRS Tunneling Protocol (GTP). The signaling or control aspect of this protocol is referred to as the GTP Control Plane (GTPC) while the encapsulated user data traffic is referred to as the GTP User Plane (GTPU). One or more S3 interfaces can be configured per system context.
- S6a Interface—The interface used by MME to communicate with Home Subscriber Server (HSS) on PLMN using the diameter protocol. This interface is responsible for transfer of subscription and authenticating or authorizing user access and UE context.
- S10 Interface—The interface used by the MME to communicate with another MME on the same or a different PLMN using the GTPv2 protocol. This interface is also used for MME relocation and MME-to-MME information transfer or handoff.
- S11 Interface—The interface used by the MME to communicate with Serving Gateways (S-GW) for transfer of information, using the GTPv2 protocol.
- S13 Interface—The interface used by the MME to communicate with the Equipment Identity Register (EIR).
- SGs Interface—The interface used to connect the databases in the VLR and MME to support circuit switch fallback scenarios.
- Sv Interface—The interface used by the MME to connect to the Mobile Switching Center to support exchange of messages during a handover procedure for the Single Radio Voice Call Continuity (SRVCC) feature.
- Gn Interface—The interface used to facilitate user mobility between 2G and 3G 3GPP networks. This interface is used for intra-PLMN handovers.
- SLg Interface—The interface used by MME to communicate with the Gateway Mobile Location Center (GMLC) using the diameter protocol. This interface is used for the Location Services (LCS), which enables the system to determine and report location information of the connected UEs.

Viewing the MME Configuration Details

To view the MME configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory > *Context* > Mobile > MME.** The list of MME services configured in Prime Network is displayed in the content pane.

Step 3 From the **MME** node, choose an MME service. The MME service details are displayed in the content pane as shown in Figure 27-24.

Figure 27-24 MME Configuration Details

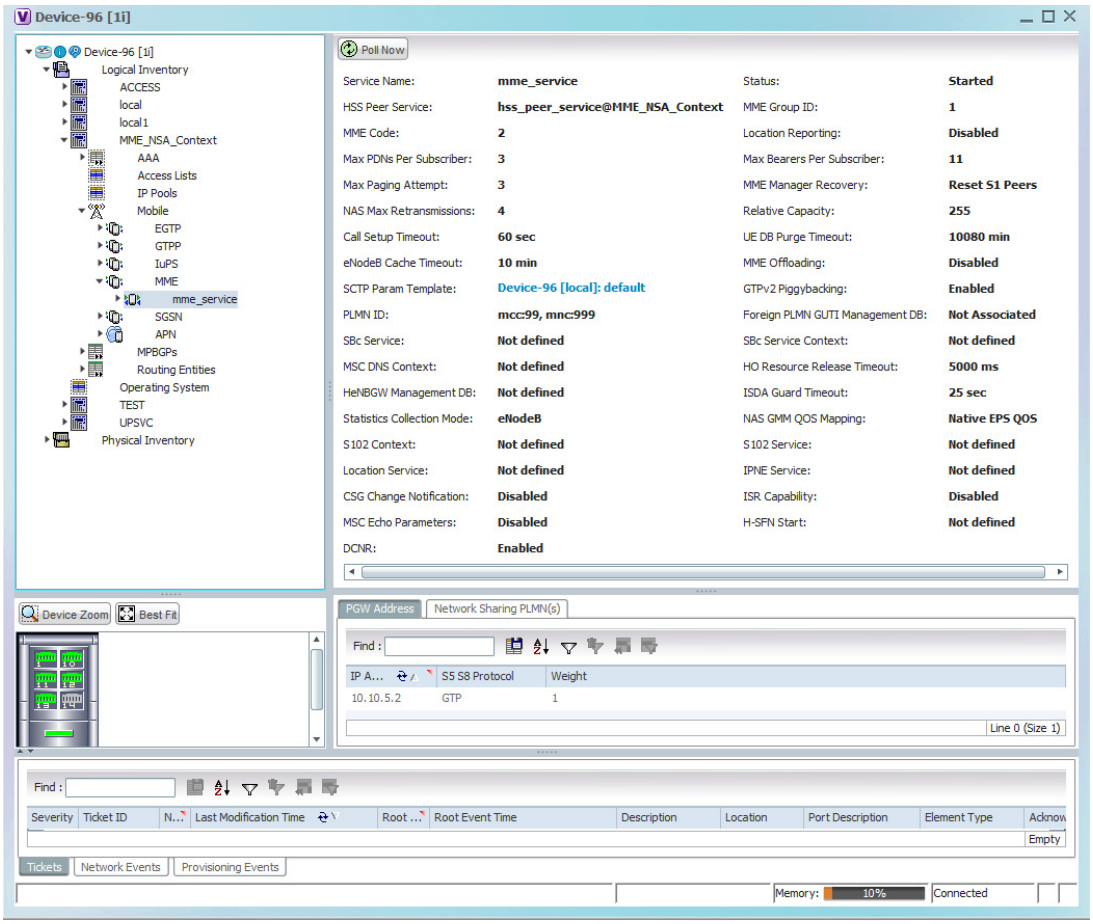


Table 27-134 displays the MME service details.

Table 27-134 MME Service Details

Field	Description
Service Name	The unique name of the MME service.
Status	The status of the MME service, which can be any one of the following: • Unknown • Initiated • Running • Down • Started • Not Started
MME Group ID	The unique ID of the group to which the MME service belongs to.
MME Code	The unique code for the MME service.
EGTP Service	The name of the EGTP peer service associated with the MME service, which is pre-configured for the selected context.
HSS Peer Service	The name of the HSS peer service associated with the MME service, which is pre-configured for the selected context.
SGTPC Service	The name of the SGTPC peer service associated with the MME service, which is pre-configured for the selected context.
SGS Service	The name of the SGS peer service associated with the MME service, which is pre-configured for the selected context.
Peer MME DNS Context	The DNS client service that is used to query and select a peer MME. The peer MME is then associated with the MME service to be used for inter-MME handovers.
Peer SGSN DNS Context	The DNS client service that is used to query and select a peer SGSN. The peer SGSN is then associated with the MME service to be used for inter-RAT handovers.
PGW DNS Context	The DNS client that is used to query and select a P-GW to be associated with the MME service.
SGW DNS Context	The DNS client that is used to query and select a S-GW to be associated with the MME service.
LTE Emergency Profile	The LTE emergency profile for the MME service. This profile helps the MME service to create an emergency session for a subscriber who is not part of the network. A maximum of four such profiles can be created.
Subscriber Map	The unique name of the subscriber map that is pre-configured for the MME service.
SGW Pool	The Serving Gateway (SGW) Pool that is communicating with the MME service. This pool is configured by associating the Tracking Area Identity (TAI) Management Database to the MME service.
MSC IP Address	The IP address of the Mobile Switching Center (MSC) that is linked to the MME service.
MSC Port	The unique MSC port for the MME service.

Table 27-134 MME Service Details (continued)

Field	Description
New Call Policy	Indicates whether the new call policy feature is enabled. The new call policy is executed when duplicate sessions with the same IP address request is received.
Location Reporting	Indicates whether the UE location reporting feature is enabled for the MME service.
Max PDNs Per Subscriber	The maximum number of PDNs that can be accessed by a subscriber simultaneously using the MME service.
Max Bearer Per Subscriber	The maximum number of EPS bearers that can be used by a subscriber simultaneously to access the MME service.
Max Paging Attempt	The maximum number of times a subscriber can attempt to create network requested service, after failure at the first attempt.
NAS Max Retransmission	The maximum number of times NAS messages can be retransmitted for the MME service.
Relative Capacity	The relative capacity variable that is sent to the eNodeB to select an MME in order to load balance the pool.
Call Setup Timeout	The timeout duration (in seconds) for setting up MME calls in the MME service.
UE DB Purge Timeout	The amount of time (in minutes) after which the User Equipment is attached to the MME service and reuses the previously established security parameters. **Note** The UE database is maintained by the MME as a cache of the EPS context for each UE. This cache is maintained in each session manager where the UE was attached first.
eNodeB Cache Timeout	The timeout duration (in minutes) for the eNodeB Cache. This field defaults to 10.
MME Offloading	Indicates whether the MME offloading feature is enabled. **Note** You must configure the load balancing parameters beforehand. For example, if you want to remove all existing subscribers from the MME and route new entrants to the pool area, then you must specify the weight as zero.
Global MMEID MgmtDB	The global MME ID management database for the MME service.
GTPv2 Piggy Bagging	Indicates whether the GTPv2 piggy backing feature is enabled. **Note** The MME service sends a piggy backing flag to a P-GW to determine if the dedicated bearer creation is piggy backed onto the message.
DCNR	Enables Dual Connectivity with New Radio (DCNR) to support 5G Non-Standalone (NSA).

Table 27-134 MME Service Details (continued)

Field	Description
NRI tab	
PLMN Id	The PLMN ID of the MME service. **Note** This code contains the Mobile Country Code (MCC) and Mobile Network Code (MNC). You can configure a maximum of 16 PLMN IDs for an MME service.
Length (bits)	The number of bits in the Packet domain Temporary Mobile Subscriber Identity (P-TMSI) to be used as the Network Resource Identifier (NRI).
PGW Address tab	
IP Address	The IP address of the PDN Gateway (P-GW). **Note** The P-GW address is used to configure P-GW discovery and it uses TP/P-MIP protocol for S5 and S8 interface and other parameters with MME service.
S5 S8 Protocol	The P-MIP protocol type to be used for S5 and S8 interfaces. By default, the GTP protocol is used for these interfaces.
Weight	The weightage assigned to a P-GW address, which indicates the address that must be used as the preferred P-GW. This weight can be any value between 1 and 100 and the address with the lowest values indicates the least preferred address.
Peer MME GUMMEI tab	
MME ID	The unique MME ID of the peer MME.
PLMN ID	The PLMN ID of the peer MME service.
Group ID	The unique ID of the group to which the peer MME services belongs to.
IP Address	The IPv4 address of the peer MME.
Peer MME TAI tab	
MME ID	The unique MME ID of the peer MME.
PLMN ID	The PLMN ID of the peer MME service.
TAC	The Tracking Area Code (TAC) of the peer MME service.
IP Address	The IPv4 address of the peer MME.
Peer SGSN RAI tab	
PLMN ID	The PLMN ID of the peer MME service.
NRI	The Network Resource Identifier (NRI) code used to identify Peer SGSN for support of 3G to 4G handover capability.
RAC	The Routing Area Code (RAC) of the peer SGSN service.
LAC	The Location Area Code (LAC) of the peer SGSN service.
IP Address	The IPv4 address of the peer SGSN service.
Gn Interface	Indicates whether the peer SGSN service is allowed to communicate over the Gn Interface.

Table 27-134 MME Service Details (continued)

Field	Description
Gp Interface	Indicates whether the peer SGSN service is allowed to communicate over the Gp Interface.
S16 Interface	Indicates whether the peer SGSN service is allowed to communicate over the S16 Interface.
S3 Interface	Indicates whether the peer SGSN service is allowed to communicate over the S3 Interface.
Peer SGSN RNC	
PLMN ID	The PLMN ID of the peer MME service.
RNC	The Radio Network Controller (RNC) of the peer SGSN service.
IP Address	The IPv4 to IPv6 address of the peer SGSN service.
Gn Interface	Indicates whether the peer SGSN service is allowed to communicate over the Gn Interface.
Gp Interface	Indicates whether the peer SGSN service is allowed to communicate over the Gp Interface.
S16 Interface	Indicates whether the peer SGSN service is allowed to communicate over the S16 Interface.
S3 Interface	Indicates whether the peer SGSN service is allowed to communicate over the S3 Interface.
Network Sharing PLMN(s)	
PLMN ID	The PLMN identifier, which consists of the Mobile Country Code (MCC) and the Mobile Network Code (MNC).
Group ID	The identifier for the group to which an MME belong to. Id must be an integer value from 0 through 65535.
MME Code	The unique code for an MME service. Code must be an integer value from 0 through 255.
H-SFN Start	Specifies the Extended Discontinuous Reception H-SFN start time. When EDRX is enabled for a UE, the UE is reachable for paging in specific Paging Hyperframes (PH), which is a specific set of H-SFN values. **Note** The PH computation is a formula that is a function of the EDRX cycle, and a UE specific identifier. This value can be computed at all UEs and MMEs without need for signaling.
ISDA Location Validity Time	Displays a timer value with which the location information of the UE is sent immediately through the IDA message.
Reject Attach With Non-3PP Char APN	Specifies that sessions requesting APN containing non-3GPP characters is for rejection.
Reject PDN Connect With Non-3PP Char APN	Specifies that policy applies to additional PDN connectivity procedure, and sessions requesting APN containing non-3GPP characters is for rejection.

Table 27-134 MME Service Details (continued)

Field	Description
IMEI Check	Enables the MME to send additional Mobile Identity check Requests (MICR) towards the EIR over the S13 interface. Choose at least one triggering UE procedure.
SGW Blacklist Params	The MME blacklists un-accessible or un-responsive SGWs for a configured time. **Note** SGW Blacklisting is supported for both Static and Dynamic IP addresses.

MME Configuration Commands

The following MME configuration commands can be launched from the logical inventory by right-clicking a MME service and choosing **Commands > Configuration.** Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-135 MME Configuration Commands

Command	Navigation	Description
Create NRI	Right-click the *MME service* > **Commands** > **Configuration**	Use this command to create NRI.
Create PGW Address		Use this command to create PGW Address.
Create Peer MME GUMMEI		Use this command to create Peer MME GUMMEI.
Modify MME		Use this command to modify a MME service.
Delete MME		Use this command to delete a MME service.
Create Peer SGSN RAI	Right-click the *MME service* > **Commands** > **Configuration**	Use this command to create Peer SGSN RAI.
Create Peer SGSN RNC		Use this command to create Peer SGSN RNC.
Create Peer MME TAI		Use this command to create Peer MME TAI
Show MME		Use this command to view MME service details.
Modify NRI	**MME service** > **NRI Tab** > Right-click the *NRI Table* > **Commands** > **Configuration**	Use this command to modify the NRI details.
Delete NRI		Use this command to delete the NRI details.

Table 27-135 MME Configuration Commands

Command	Navigation	Description
Modify PGW Address	**MME service** > **PGW Address Tab** > Right-click the *PGW Address Table* > **Commands** > **Configuration**	Use this command to modify the PGW Address details.
Delete PGW Address		Use this command to delete the PGW Address details.
Modify Peer MME GUMMEI	**MME service** > **Peer MME GUMMEI Tab** > Right-click the *Peer MME GUMMEI Table* > **Commands** > **Configuration**	Use this command to modify the Peer MME GUMMEI details.
Delete Peer MME GUMMEI		Use this command to delete the Peer MME GUMMEI details.
Modify Peer SGSN RAI	**MME service** > **Peer SGSN RAI Tab** > Right-click *the Peer SGSN RAI Table* > **Commands** > **Configuration**	Use this command to modify the Peer SGSN RAI details.
Delete Peer SGSN RAI		Use this command to delete the Peer SGSN RAI details.
Modify Peer SGSN RNC	**MME service** > **Peer SGSN RNC Tab** > Right-click the *Peer SGSN RNC Table* > **Commands** > **Configuration**	Use this command to modify the Peer SGSN RNC details.
Delete Peer SGSN RNC		Use this command to delete the Peer SGSN RNC details.
Modify Peer MME TAI	**MME service** > **Peer MME TAI Tab** > Right-click the *Peer MME TAI Table* > **Commands** > **Configuration**	Use this command to modify the Peer MME TAI details.
Delete Peer MME TAI		Use this command to delete the Peer MME TAI details.

You can also view the following configurations for a MME service:

- EMM Timeouts—EPS Mobility Management (EMM) is used to support the mobility of a user equipment. For example, it informs the network of the UEs current location and provides user identity confidentiality. Apart from these services, it also provides connection management services to the session management sublayer and defines timer parameters such as timeout durations for retransmission of NAS messages.
- ESM Timeouts—EPS Session Management (ESM) is used to provide subscriber session management for bearer context activation, deactivation, modification and update procedures.
- LTE Security Procedures—The LTE integrity and encryption algorithms used for security procedures for the MME service, which are enabled by default.
- Policy—The session management policies for LTE subscribers of the MME service.
- S1 Interface—Transfer of signaling messages between the MME service and the eNodeB. S1 MME uses the S1 Application Protocol (S1-AP) over the Steam Control Transmission Protocol (SCTP). This interface also serves as a path for establishing and maintaining subscriber EPS bearer context.

Viewing the EMM Configuration Details

To view the EMM configuration details for a MME service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > **MME** > *MME service* > **EMM**. The EMM configuration details are displayed in the content pane.

Table 27-136 displays the EMM configuration details.

Table 27-136 EMM Configuration Details

Field	Description
Implicit Detach Timeouts	The timeout duration (in seconds) after which the subscriber will be detached from the network in case there is no activity. This time can be any value between 1 and 12000, and defaults to 5640.
Mobile Reachable Timeout	The timeout duration (in seconds) after which the attempt to reach the network is discarded and the reattempt procedure starts. This time can be any value between 1 and 12000, and defaults to 5640.
T3412 Timeout	The timeout duration (in seconds) for the T3412 timer, which is used for periodic tracking area update (P-TAU). This time can be any value between 1 and 11160, and defaults to 5400. When this timer expires, the periodic tracking area update procedure starts and the timer is reset for the next start.
T3413 Timeout	The timeout duration (in seconds) for the T3413 timer, which starts when the MME service initiates the EPS paging procedure and requests the lower layer to start paging. When the UE responds to the procedure, then the timer stops the paging procedure. This time can be any value between 1 and 20, and defaults to 10.
T3422 Timeout	The timeout duration (in seconds) for the T3422 timer, which starts when the MME initiates the detach procedure (by sending a Detach Request message) to the UE. On receipt of a Detach Accept message from the UE, the timer stops. This time can be any value between 1 and 20, and defaults to 10.
T3423 Timeout	The timeout duration (in seconds) for the T3423 timer, which starts when the UE is in the **EMM-Deregistered** state or enters the **EMM-Connected** mode. This timer stops when the UE gets back to the **EMM-Registered** state. This time can be any value between 1 and 11160, and defaults to 5400.
T3450 Timeout	The timeout duration (in seconds) for the T3450 timer, which starts when the MME initiates the Globally Unique Temporary Identifier (GUTI) reallocation procedure by sending the **GUTI-Reallocation Command** message to the UE. The timer stops when the **GUTI-Reallocation Complete** message is received. This time can be any value between 1 and 20, and defaults to 6.
T3460 Timeout	The timeout duration (in seconds) for the T3460 timer, which starts when the network initiates the authentication procedure by sending the **Authentication Request** to the UE. The timer stops on receipt of a **Authentication Response** message from the UE. This time can be any value between 1 and 20, and defaults to 6.
T3470 Timeout	The timeout duration (in seconds) for the T3470 timer, which starts when the network initiates the identification procedure by sending an **Identity Request** message to the UE. This timer stops on receipt of a Identity **Response message** from the UE. This time can be any value between 1 and 20, and defaults to 6.

EMM Timeouts Commands

The following EMM Timeout commands can be launched from the logical inventory by right-clicking EMM timeouts of a MME service and choosing **Commands > Configuration.** Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-137 EMM Timeouts Commands

Command	Navigation	Description
Modify EMM Timeouts	**MME** service > Right-click the *EMM Timeouts* > **Commands** > **Configuration**	Use this command to modify EMM Timeout details.

Viewing the ESM Configuration Details

To view the ESM configuration details for a MME service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > **MME** > *MME service* > **ESM**. The ESM configuration details are displayed in the content pane.

Table 27-138 displays the ESM configuration details.

Table 27-138 ESM Configuration Details

Field	Description
T3485 Timeout	The timeout duration (in seconds) for the T3485 timer, which is used to activate the default EPS Bearer context. The timer starts when the MME sends the **Activate Default EPS Bearer Context Request** message to the UE. The timer stops when it receives the either the **Activate Default EPS Bearer Context Accept** or **Activate Default EPS Bearer Context Reject** message. This time can be any value between 1 and 60, and defaults to 6.
T3486 Timeout	The timeout duration (in seconds) for the T3485 timer, which is used to modify the default EPS Bearer context. The timer starts when the MME sends the **Modify EPS Bearer Context Request** message to the UE. The timer stops when it receives the either the **Modify EPS Bearer Context Accept** or **Modify EPS Bearer Context Reject** message. This time can be any value between 1 and 60, and defaults to 6.
T3489 Timeout	The timeout duration (in seconds) for the T3489 timer, which is used to deactivate the default EPS Bearer context. The timer starts when the MME sends the **ESM Information Request** message to the UE. The timer stops when it receives the **ESM Information Response** message. This time can be any value between 1 and 60, and defaults to 4.
T3495 Timeout	The timeout duration (in seconds) for the T3495 timer, which is used to deactivate the default EPS Bearer context. The timer starts when the MME sends the **Deactivate EPS Bearer Context Request** message to the UE. The timer stops when it receives the either the **Deactivate EPS Bearer Context Accept** or **Deactivate EPS Bearer Context Reject** message. This time can be any value between 1 and 60, and defaults to 6.

ESM Timeouts Commands

The following ESM Timeout commands can be launched from the logical inventory by right-clicking ESM timeouts of a MME service and choosing **Commands > Configuration.** Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-139 ESM Timeouts Commands

Command	Navigation	Description
Modify ESM Timeouts	**MME** *service* > Right-click the *ESM Timeouts* > **Commands** > **Configuration**	Use this command to modify ESM Timeout details.

Viewing the LTE Security Procedure Configuration Details

To view the LTE security procedure configuration details for a MME service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > **MME** > *MME service* > **LTE Security Procedure**. The configuration details are displayed in the content pane.

Table 27-140 displays the LTE security procedure configuration details.

Table 27-140 LTE Security Procedure Configuration Details

Field	Description
Encryption Algorithm Priority 1	The encryption algorithm that must be treated as the first priority for security procedures on the MME service, which can be any one of the following values: • 128-eea0—Null Ciphering Algorithm • 128-eea1—SNOW 3G synchronous stream ciphering algorithm • 128-eea2—Advance Encryption Standard (AES) ciphering algorithm
Encryption Algorithm Priority 2	The encryption algorithm that must be treated as the second priority for security procedures on the MME service, which can be any one of the following values: • 128-eea0—Null Ciphering Algorithm • 128-eea1—SNOW 3G synchronous stream ciphering algorithm • 128-eea2—Advance Encryption Standard (AES) ciphering algorithm
Encryption Algorithm Priority 3	The encryption algorithm that must be treated as the third priority for security procedures on the MME service, which can be any one of the following values: • 128-eea0—Null Ciphering Algorithm • 128-eea1—SNOW 3G synchronous stream ciphering algorithm • 128-eea2—Advance Encryption Standard (AES) ciphering algorithm
Integrity Algorithm Priority 1	The integrity algorithm that must be treated as the first priority for security procedures on the MME service, which can be any one of the following values: • 128-eia1—SNOW 3G synchronous stream ciphering algorithm • 128-eia2—Advance Encryption Standard
Integrity Algorithm Priority 2	The integrity algorithm that must be treated as the second priority for security procedures on the MME service, which can be any one of the following values: • 128-eia1—SNOW 3G synchronous stream ciphering algorithm • 128-eia2—Advance Encryption Standard

LTE Security Procedures Commands

The following LTE Security Procedures commands can be launched from the logical inventory by right-clicking LTE Security Procedures of a MME service and choosing **Commands > Configuration.** Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-141 ESM Timeouts Commands

Command	Navigation	Description
Modify LTE Security Procedures	**MME** *service* > Right-click the *LTE Security Procedures* > **Commands** > **Configuration**	Use this command to modify LTE Security Procedures.

Viewing the MME Policy Configuration Details

To view the policy configuration details for a MME service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > **MME** > *MME service* > **Policy** > **Attach**. The policy configuration details are displayed in the content pane.

Table 27-142 displays the Policy configuration details.

Table 27-142 Policy Configuration Details

Field	Description
IMEI Query type	The type of IMEI query use for attaching the user equipment and tracking area update procedure, which can be any one of the following: • imei (International Mobile Equipment Identity) • imei-sv (International Mobile Equipment Identity-Software Version)
Set UE Time	Indicates whether the MME service must set the time in the UE during the attach or tracking area update procedure.
Deny Grey Listed	Indicates whether the MME service must deny the grey listed equipment. In other words, it specifies whether the identification of the UE must be performed by the Equipment Identity Register (EIR) over the S13 interface.
Deny Unknown	Indicates whether the MME service must deny service to an unknown equipment.
Verify Emergency	Indicates whether the MME service must verify the equipment for emergency calls.
Allow On ECA Timeout	Indicates whether the MME service must allow service of equipments that timeout on the ECA.
Initial Context Setup Failure Tau	Indicates policy, which applies to Tracking Area Update procedure when initial context setup failure is received.
Initial Context Setup Failure Service Request	Indicates policy that applies to a service request procedure.
Policy NAS-NON-DELIVERY	Shows that handling for NAS-NON-DELIVERY message is Enabled.
Policy NAS-NOS-DELIVERY Modify Procedure Timer	Shows the timer value in seconds for the modify procedure.
MSC Echo Parameters	Displays EGTPC echo parameters for MSC Fallback. The msc-echo-params configuration overrides any echo parameter that is configured in the egtp-service configuration for the corresponding SV service.
IPNE Service	Associates an IPNE service with a MME service.
CSG Change Notification	Enables or disables the Closed Subscriber Group (CSG) Information reporting (notification) mechanism on the MME. When enabled, the MME includes the CSG Information Reporting Action IE with the appropriate Action field for subscribers.
ISR Capability	Enables or disables the Idle-mode Signaling Reduction (ISR) feature on the MME service.
Location Service	Associates a location service with a specified MME service. Only one location service should be associated with an MME Service.
Trap S1 Path Establishment	Specifies that the SNMP trap for the S1 path establishment is to be enabled or disabled.
EIR Query Type	Indicates whether querying of EIR is enabled or disabled.

MME Policy Configuration Commands

The following MME policy configuration commands can be launched from the logical inventory by right-clicking a MME policy and choosing **Commands > Configuration.** Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-143 MME Policy Configuration Commands

Command	Navigation	Description
Modify Policy	**Logical Inventory** > **Context** > **Mobile** > **MME** > **MME service** > Right-click the **Policy** > **Commands** > **Configuration**	Use this command to modify the MME policy.
Modify Attach	**Logical Inventory** > **Context** > **Mobile** > **MME** > **MME service** > **Policy** > Right-click the **Attach** > **Commands** > **Configuration**	Use this command to modify the MME Attach details.
Modify TAU	**Logical Inventory** > **Context** > **Mobile** > **MME** > **MME service** > **Policy** > Right-click the **TAU** > **Commands** > **Configuration**	Use this command to modify the MME TAU details.

Viewing the S1 Interface Configuration Details

To view the S1 Interface configuration details for a MME service:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > **MME** > *MME service* > **S1 Interface**. The interface configuration details are displayed in the content pane.

Table 27-144 displays the S1 Interface configuration details.

Table 27-144 S1 Interface Configuration Details

Field	Description
Primary IP Address	The IP address (IPv4 or IPv6) of the interface configured as an S1-MME interface.
Secondary IP Address	The optional IP address (IPv4 or IPv6) of the interface configured as an S1-MME interface.
SCTP Port	The source SCTP port used for binding the SCTP socket to communicate with the eNodeB. This port can be any value between 1 and 65535, and defaults to 699.
Max Subscribers	The maximum number of subscribers that can access the MME service on the interface. This number can be any value between 0 and 4,000,000.
QoS DSCP	The Quality of Service (QoS) Differentiated Service Code Point (DSCP) used when sending data packets (of a particular 3GPP QoS class) over the S1-MME interface. This can be any one of the following values: • af11 • af12 • af13 • af21 • af22 • af23 • af31 • af32 • af33 • af41 • af42 • af43 • be • ef
Crypto Template	The name of the crypto template that is used when implementing IP Security on the S1-MME interface.
S1 Interface Connected Trap	Indicates whether the SNMP trap for the S1 interface connection equipment is enabled.

S1 MME Interface Commands

The following S1 MME interface commands can be launched from the logical inventory by right-clicking an S1 MME interface and choosing **Commands > Configuration.** Your permissions determine whether you can run these commands (see Permissions Required to Perform Tasks Using the Prime Network Clients). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Table 27-145 S1 MME Interface Commands

Command	Navigation	Description
Modify S1 MME	**Logical Inventory** > **Context** > **Mobile** > **MME** > **MME service** > Right-click the *S1 Interface* > **Commands** > **Configuration**	Use this command to modify a S1 MME interface.

Enabling DCNR in MME Service

Follow these steps to enable DCNR to support 5G NSA:

Note Prime Network supports NSA from StarOS 21.11 onwards.

Step 1 Install NSA license on the ASR 5500 device for which you want to enable 5G NSA:

```
20000 5G NSA feature Set 100k Sess VPCSW Active
```

Step 2 Once the license is enabled, the **DCNR** option is available in **mme-service** configuration mode. Enable **DCNR** option from the device.

Step 3 The **DCNR** field is now visible in the Vision GUI. See MME Configuration Details

Viewing the Stream Control Transmission Protocol

The Stream Control Transmission Protocol (SCTP) is a message oriented, reliable transport protocol with direct support for multi-homing that runs on top of Internet Protocol (IPv4/IPv6). Like TCP, SCTP provides reliable, connection-oriented data delivery with congestion control, path MTU discovery and message fragmentation.

Its role is similar to the roles of popular protocols such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). It provides some of the same service features of both: it is message-oriented like UDP and ensures reliable, in-sequence transport of messages with congestion control like TCP.

SCTP offers the following services to the users:

- Acknowledged error-free non-duplicated transfer of user data
- Data fragmentation to conform to discovered path MTU size
- Sequenced delivery of user messages within multiple streams, with an option for order-of-arrival delivery of individual user messages
- Optional bundling of multiple user messages into a single SCTP packet
- Network-level fault tolerance through supporting of multi-homing at either or both ends of an association

The SCTP application submits data to be transmitted in messages to the SCTP transport layer. The messages and control information is separated and placed in chunks (data and control chunks), each identified by a chunk header. A message can be fragmented over a number of data chunks, but each data chunk contains data from only one user message. SCTP bundles the chunks into SCTP packets, which are then submitted to the Internet Protocol. The SCTP packet consists of a packet header, SCTP control chuck (if required) and SCTP data chunks (if available).

The primary distinguishing features of this new protocol are:

- multi-homing—The ability of an association to support multiple IP addresses or interfaces at a given endpoint. Currently, SCTP does not do load-sharing, but with the multi-homing facility, SCTP has greater potential to survive a session in case of network failures. Using more than one address allows re-routing of packets in event of failure and also provides an alternate path for retransmissions. Endpoints can exchange lists of addresses during initiation of the association. One address is designated as the primary address to receive data. A single port number is used across the entire address list at an endpoint for a specific session. Heartbeat chunks are used to monitor availability of alternate paths with thresholds set to determine failure of alternate and primary paths.

Note An “association here refers to the connection between two endpoints in this context.

- multi-streaming—Each stream represents a sequence of messages within a single association. These messages may be long or short, which include flags for control of segmentation and reassembly. Stream Identifiers and Stream Sequence numbers are included in the data packet to allow sequencing of messages on a per-stream basis. This ensures that unnecessary head-of-line blocking between independent streams of messages is avoided in case of loss in one stream.

SCTP also provides a mechanism for designating order-of-arrival delivery as opposed to ordered delivery. The design of SCTP includes appropriate congestion avoidance behavior and resistance to flooding and masquerade attacks.

For devices such as the Cisco ASR 5000 series, SCTP carries signaling traffic that flows through IPSec tunnel over LTE S1-MME interface.

To view the SCTP configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Profile** > **SCTP Template**. A list of SCTP templates is displayed in the content pane.

Step 3 In the **Logical Inventory** window, select a template from the **SCTP Template** node. The SCTP template details are displayed in the content pane as shown in Figure 27-25.

Figure 27-25 SCTP Template Details

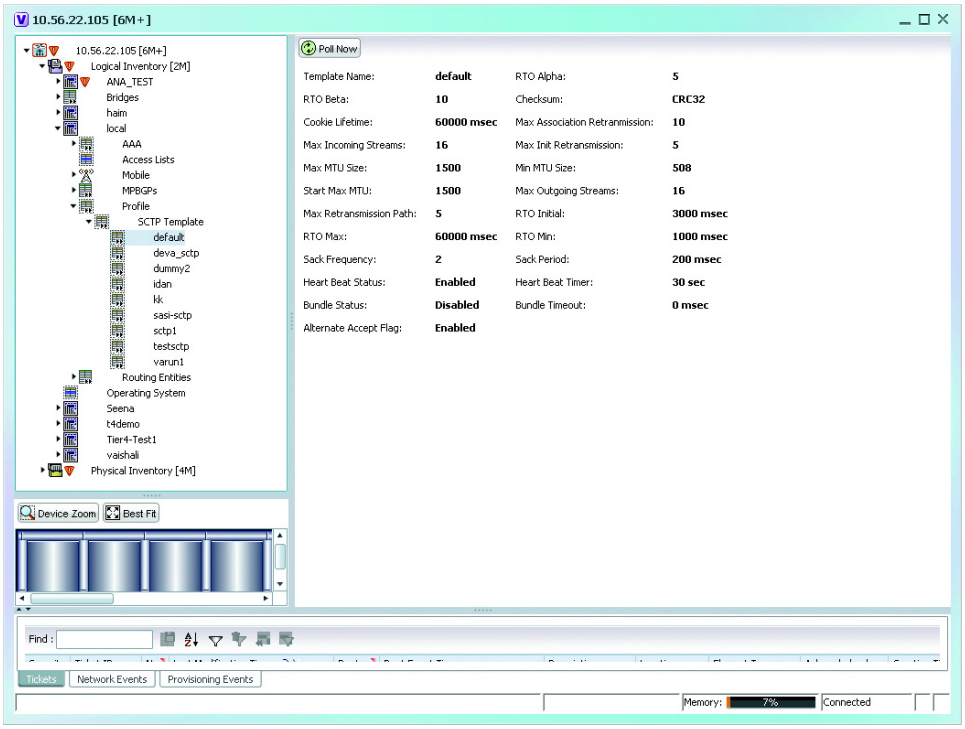


Table 27-146 describes the SCTP Template details.

Table 27-146 SCTP Template Details

Field	Description
Template Name	The unique name of the SCTP template. **Note** Each template can be configured with different values and associated to different services such as the MME service, diameter endpoint and so on.
RTO Alpha	The Retransmission Timeout (RTO) alpha (smoothing factor) value that is used to calculate Smooth Round Trip Time (SRTT) and the Round Trip Time Variation (RTTVAR) for new Round Trip Time (RTT) measurements. **Note** RTO refers to the amount of time to wait before transmitting a package from the retransmission queue to the neighbor. SRTT refers to the amount of time (in milliseconds) it takes for a packet to be sent to the neighbor and for the local router to receive an acknowledgment for the packet.
RTO Beta	The Retransmission Timeout (RTO) beta (delay variance factor) value that is used to calculate Smooth Round Trip Time (SRTT) and the Round Trip Time Variation (RTTVAR) for new Round Trip Time (RTT) measurements.

Table 27-146 SCTP Template Details (continued)

Field	Description
Checksum	The type of checksum that is used to increase data integrity of the SCTP packets, which can be any one of the following: • adler32—the Adler-32 checksum algorithm is used • crc32—the 32 bit cyclic redundancy check algorithm is used.
Cookie Lifetime	The lifetime (in milliseconds) of the SCTP cookie.
Max Association Retransmission	The maximum number of retransmissions allowed by this template for the SCTP associations.
Max Incoming Streams	The maximum number of incoming SCTP streams.
Max Init Retransmissions	The maximum number of SCTP initiation retransmissions.
Max MTU Size	The maximum size (in bytes) of the Maximum Transmission Unit (MTU) for SCTP streams.
Min MTU Size	The minimum size (in bytes) of the MTU for SCTP streams.
Start Max MTU	The starting size (in bytes) of the MTU for SCTP streams.
Max Outgoing Streams	The maximum number of outgoing SCTP streams.
Max Retransmissions Path	The maximum number of retransmissions of the SCTP paths.
RTO Initial	The initial time (in milliseconds) for retransmission of SCTP packets.
RTO Max	The maximum time (in milliseconds) for retransmission of SCTP packets.
RTO Min	The minimum time (in milliseconds) for transmission of SCTP packets.
SACK Frequency	The frequency of the Selective Acknowledgment (SACK) of the SCTP packets.
SACK Period	The period (in milliseconds) of selective acknowledgment of the SCTP packets.
Heart Beat Status	Indicates whether the option to send traffic over an alternate path, in case of a path failure, is enabled. **Note** The Heartbeat message is sent to a peer endpoint to probe the reachability of a particular destination transport address defined in the present association. If the address is not reachable, the traffic is sent over an alternate address. If this option is enabled, then the failover recovery is not even known to the user.
Heart Beat Timer	The amount of time (in seconds) to wait before a peer is considered unreachable. When a Heartbeat request is sent and if an acknowledgment is not received before this timer, then subsequent heartbeat requests are not sent and the peer is considered unreachable.
Bundle Status	Indicates whether the data chunks must be bundled into packets before submitting to the IP. If this option is disabled, then the packets are sent without bundling.

Table 27-146 SCTP Template Details (continued)

Field	Description
Bundle Timeout	The amount of time (in seconds) after which the chunks of SCTP packets are bundled and committed for transmission.
Alternate Accept Flag	Indicates whether the alternate accept flag that denotes additional lifetime for the association, is enabled.

Monitoring Control and User Plane Separation (CUPS)

Long Term Evolution (LTE) is a wireless broadband technology designed to support roaming Internet access through mobile phones and handheld devices. Because LTE offers significant improvements over older mobile communication standards, this sometimes referred as a 4G (fourth generation) technology along with WiMax. With its architecture based on Internet Protocol (IP) unlike many other cellular Internet protocols, Long Term Evolution supports browsing Web sites, VoIP and other IP-based services.

The Evolved Packet Core (EPC) network is evolving and moving towards Control User Plane Separation (CUPS) based architecture where User-Plane and Control-Plane are separate node for P-GW, S-GW, and TDF products. The User Plane and Control Plane combined together provide functionality of a node for other elements in the EPC network. When the control plane and user plane is available as separate nodes it allows numerous advantages. For example it supports different scaling for Control-Plane and User-Plane, supports more capacity on each session level in User-Plane and so on.

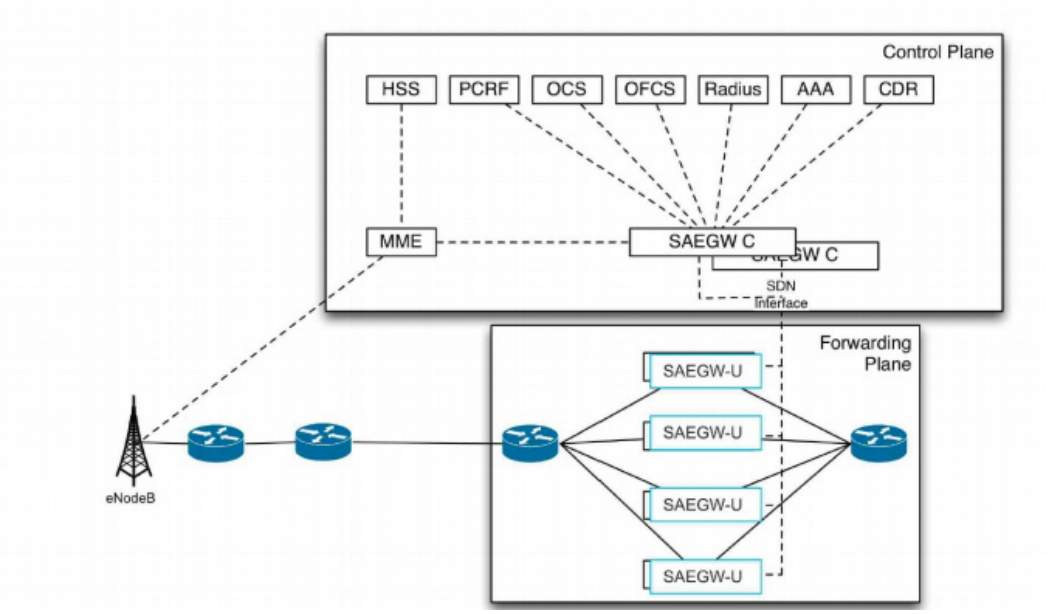
Cisco enhanced the operation of the EPC through the separation of Control and User Plane functions in accordance with 3GPP Standard architectural enhancements. As part of CUPS, Packet Gateway application is split into independent components; Control Plane and User plane. Cisco CUPS solution advantages the SAEGW, which is an optimized combination of S-GW and P-GW. The SAEGW-C is the Cisco UPC CUPS Control Plane (CP) and SAEGW-U is the Cisco UPC CUPS User Plane (UP).

Cisco CUPS solution is designed in such a way that CUPS CP SAEGW-C and CUPS UP SAEGW-U are independent VNFs/products in itself and can be independently scaled up and down. SAEGW-C can control multiple User Planes irrespective of where they are located and what platform they are hosted on. SAEGW-U can be collocated with SAEGW-C in the same data center or could be located remotely in a different data center.

Prime Network 5.3 supports CUPS from star-OS 21.8 onwards. The control plane and user plane nodes are separately deployed in the architecture. You can view two services namely SX-service and User plane-service on the ASR 5500, SI and PI devices. Also, you can identify if a node is a control-plane or a user-plane node based on SX services.

Note Separate feature license is required to use CUPS feature. To check if CUPS is enabled on your device, see "SAE-GW Properties in Logical Inventory".

CUPS Architecture



Cisco UPC CUPS solution uses SAEGW, which is an optimized and combined S-GW+P-GW. SAEGW-C is the CUPS Control Plane (CP) and SAEGW-U is the CUPS User Plane (UP). SAEGW-C and SAEGW-U can anchor any combination of following type of sessions:

- Pure S-GW— When a UE is using S-GW part of SAEGW and a PDN connection, which is terminating at an external P-GW and not part of SAEGW.
- Pure P-GW— When a UE is using an external S-GW, which is not part of SAEGW and a PDN connection is terminating within P-GW part of SAEGW.
- Combined S-GW + P-GW — When a UE is using both S-GW and P-GW, which is part of same SAEGW service.

You can deploy Cisco CUPS SAEGW-C and SAEGW-U either as:

- P-GW only
- S-GW only
- SAEGW

You can deploy Cisco USP CUPS in the following ways:

- Co-Located CUPS
- Hybrid-CUPS
- Remote CUPS

CUPS Services

The following two CUPS services are supported on ASR5000 devices.

1. Sx-Service

2. User-Plane-Service

Sx-Services

The Sx Service provides an interface mentioned as the following reference points:

- Sxa: Reference point between SGW-C and SGW-U.
- Sxb: Reference point between PGW-C and PGW-U.
- Sxc: Reference point between Traffic Detection Function-C (TDF-C) and TDF-U.
- Sxab: Reference point between SAEGW-C and SAEGW-U

The Sx service is agnostic of the interface it supports. A single Sx service instance is capable of running on Sxa, Sxb, and Sxb interfaces. The Sx service runs in two different modes:

- Sx-Control Plane instance
- Sx-User Plane instance

The Sx service is associated with the SAEGW service at the Control-Plane and User-Plane service at the User-Plane. There is one-to-one mapping of the Sx service with the Control-Plane and Data Plane.

User Plane services

Some important points that describe User plane service are:

- User plane can be programmed from Control plane.
- Single User plane service can serve both SGW-U and P-GW-U type sessions.
- Two or more separate User plane services can be defined for each node type, SGW-U and PGW-U, respectively.
- User plane service is associated with Sx service for the Control Plane interface, and GTP-U service for receiving GTP-U packets. Currently, each User Plane Service is associated with only single Sx service to interface with Control Plane.
- User plane service can be associated with four GTP-U services.
- Multiple peers of Control Plane services use single User Plane service

Sx-Services

Sx services can be configured on each context except the local context on the StarOS.

Viewing Sx-Control Plane Services

The Vision client displays the Sx Control plane container under the Mobile node in the logical inventory. The icon used for representing Sx Control plane in the logical inventory is explained in NE Logical Inventory Icons, page A-7.

To view Sx Control plane properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**. For example, Double-click an SI device.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > *Sx Control Plane Container* > *Sx Control Plane*.

The Vision client displays the list of Sx Control plane services configured under the container.

Table 27-147 describes the properties available for Sx Control plane.

Table 27-147 Sx-Control Plane Properties

Field	Description
Service Name	Name of the Sx control plane service.
Service ID	ID of the Sx control plane service.
Status	Status of the Sx control plance service.
Instance Type	Displays the instance type of the Sx-service.
Bind IPV4address	Shows the ipv4 address of the Sx-service to be sent to the peer.
Bind IPV6address	Shows the ipv6 address of the Sx-service to be sent to the peer.
Recovery Timestamp	Shows the recovery timestamp
SXAB	
Retransmission Timeout	Displays the configured retransmission timeout of SXA in milli-seconds.
Maximum Request Retransmissions	Displays the configured the maximum number of request retransmission of SXA.
HB Interval	Shows the heart beat interval in milli-seconds.
HB Retransmission Timeout	Shows the heart beat re-transmission timeout in milli-seconds.
HB Max Retransmission	Shows the Maximum number of request retransmission of Sx service heartbeat.
Control msg Recovery timestamp Counter Changes	Displays Control message recovery time stamp control changes to true or false
Heartbeat req or resp Recovery timestamp Change	Displays either heartbeat request or response recovery time stamp changes to true or false.
Heartbeat Timeout	Displays heart beat Time out to true or false.

Configuring, Monitoring, and Troubleshooting Sx Services

You can use the following commands to configure, monitor, and troubleshoot Sx services. The devices that support these commands are listed in the *Addendum: Additional VNE Support for Cisco Prime Network 5.2*. Whether you can run these commands depends on your permissions. See Vision Client Permissions, page B-1.

Table 27-148 Sx-Interface Commands

Command	Navigation	Description
Show sx-service all	Logical Inventory > Mobile > Sx Control Plane /Data Plane> sx-servuce all	Displays the Sx- control plane services along with attributes listed in Table 27-147.
Show sx-service *name*	Logical Inventory >Mobile > Sx Control Plane/Data Plane > <sx-service name>	The output of this command displays the properties for the specified sx-service.

Table 27-148 Sx-Interface Commands

Command	Navigation	Description
bind { ipv4-address *ipv4_address* | **ipv6-address** *ipv6_address* **}**	Logical Inventory >Mobile > Sx Control Plane/Data Plane > <sx-service name>	Binds the specified Sx service to an IP address.
sxa { max-retransmissions *number* | **retransmissions-timeout-ms** *number***}**	Logical Inventory >Mobile > Sx Control Plane/Data Plane > <sx-service name>	Modifies the Sxa parameters for the S-GW. **max-retransmissions**: Configures the maximum retries for Sx control packets on the S-GW. Enter an integer. The valid values range from 0 to 15. The default value is 4. **retransmissions-timeout-ms**: Configures the retransmission timeout for Sx control packets (on the S-GW), in milliseconds. Enter a value in multiples of 100. The valid values range from 1000 to 20000. The default value is 5000. By default, this command is disabled.
sxab { max-retransmissions *number* | **retransmissions-timeout-ms** *number***}**	Logical Inventory >Mobile > Sx Control Plane/Data Plane > <sx-service name>	Modifies the Sxab parameters for the S-GW and P-GW. **max-retransmissions**: Configures the maximum retries for Sx control packets on the S-GW and P-GW. Enter an integer. The valid values range from 0 to 15. The default value is 4. **retransmissions-timeout-ms**: Configures the retransmission timeout for Sx control packets (on the S-GW), in milliseconds. Enter a value in multiples of 100. The valid values range from 1000 to 20000. The default value is 5000. By default, this command is disabled.

Table 27-148 Sx-Interface Commands

Command	Navigation	Description
sxb {max-retransmissions *number* | **retransmissions-timeout-ms** *number*}	Logical Inventory >Mobile > Sx Control Plane/Data Plane > <sx-service name>	Modifies the Sxb parameters for the P-GW. **max-retransmissions**: Configures the maximum retries for Sx control packets on the P-GW. Enter an integer. The valid values range from 0 to 15. The default value is 4. **retransmissions-timeout-ms**: Configures the retransmission timeout for Sx control packets (on the S-GW), in milliseconds. Enter a value in multiples of 100. The valid values range from 1000 to 20000. The default value is 5000. By default, this command is disabled.
Show saegw-service all	Logical Inventory >Mobile > SAE-GW > saegw-service all	The saegw-service displays details of the sx-services associated with an SAEGW service.
Show saegw-service *name*	Logical Inventory >Mobile > SAE-GW > <service name>	The output of this command displays the field for the specified saegw-service name.
associate sx-service *name*	Logical Inventory >Mobile > SAE-GW > <service name>	Associates an SAEGW service to an existing Sx service within this context
associate sx-service *name*	Logical Inventory >Mobile > User Plane > <sx-service name>	Associate User-Plane service to an existing Sx service within this context.
associate gtpu-service *gtpu_service_name* **up-tunnel**	Logical Inventory >Mobile > SAE-GW > <service name>	Associates an existing GTP-U service to an existing Control Plane function under SAEGW Service Configuration Mode.
associate gtpu-service *gtpu_service_name* **cp-tunnel**	Logical Inventory >Mobile > User Plane > <sx-service name>	Associates an existing GTP-U service to an existing User Plane function under User Plane Configuration Mode.

Table 27-148 Sx-Interface Commands

Command	Navigation	Description
`Show saegw-service statistics`		
`Show sx-service statistics all`		The output of this command is visible only in CLI. You can view the new fields and statistics in support of the Sx service.

User-Plane Services

The following minimum and critical parameters must be configured to start the User Plane service:

- One Sx-Service.
- Three GTP-U Services of interface type P-GW ingress, S-GW-ingress, and S-GW-egress.
- Removal or change of any critical parameters from User Plane service results in the User Plane service getting stopped.
- The services that are associated with the User Plane service should be in running mode. Else, stopping any associated service triggers stopping of the User Plane service.

Viewing User-Plane Services

To view Sx User plane properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > *Sx User plane Container* > *Sx User plane.*

The Vision client displays the list of Sx User plane services configured under the container.

Table 27-149 describes the details available for each user-plane service.

Table 27-149 Sx User Plane Properties in Logical Inventory

Field	Description
Service Name	Name of the Sx User plane service.
Service ID	ID of the Sx user plane service.
Status	Status of the Sx user plane service.
PGW Ingress GTPU Service	Displays the PGW ingress GTPU service of the ASR5K device.
SGW Ingress GTPU Service	Displays the SGW ingress GTPU service of the ASR5K device.
SGW Egress GTPU Service	Displays the SW Egress GTPU service of the ASR5K device.
Control Plane Tunnel GTPU Service	The associated control plane tunnel GTPU service.

Table 27-149 Sx User Plane Properties in Logical Inventory (continued)

Field	Description
Sx Service	Displays its associated Sx service.
Control Plane Group	The group to which the control plane is associated.

Configuring, Monitoring, and Troubleshooting Sx User-Plane Services

You can use the following CLI commands to configure, monitor, and troubleshoot Sx User plane services in CUPS. The devices that support these commands are listed in the *Addendum: Additional VNE Support for Cisco Prime Network 5.2*. Whether you can run these commands depends on your permissions. See Vision Client Permissions, page B-1 :

Table 27-150 User-Plane Services Commands

Command	Navigation	Description
Show user-plane service all	Logical Inventory > Mobile > User Plane Services	Displays the user-plane services along with attributes listed in Table 27-149.
Show user-plane-service *name*	Logical Inventory > Mobile > User Plane Services ><service name>	The output of this command displays the fields for the specified user-plane-service name.
associate gtpu-service *gtpu_service_name* **{ pgw-ingress | sgw-ingress | sgw-egress }**	Logical Inventory > Mobile > User Plane Services ><service name>	Associates the GTPU service with the User Plane service.
associate sx-service *service_name*	Logical Inventory > Mobile > User Plane Services ><service name>	Associates an Sx service with User Plane service. This is a mandatory parameter.
Show service all		Displays the user-plane services. The output of this command includes the fields shown in
Show saegw-service all	Logical Inventory >Mobile > SAE-GW > saegw-service all	The saegw-service displays details of the sx-services associated with an SAEGW service.
Show saegw-service *name*	Logical Inventory >Mobile > SAE-GW > <service name>	The output of this command displays the field for the specified saegw-service name.
Show user-plane-service statistics all		The output of this command is visible only in CLI. You can view the new fields and statistics in support of the user-plane service.

Global SX Peers

Global SX Peers shows all the peer nodes of SX Service.

Viewing Global SX Peers

To view Global SX Peer:

Step 1 Right-click the required device in the Vision client and choose **Inventory**. For example, Double-click an SI device.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory > SX Peers**.

The Vision client displays the list of SX Peers.

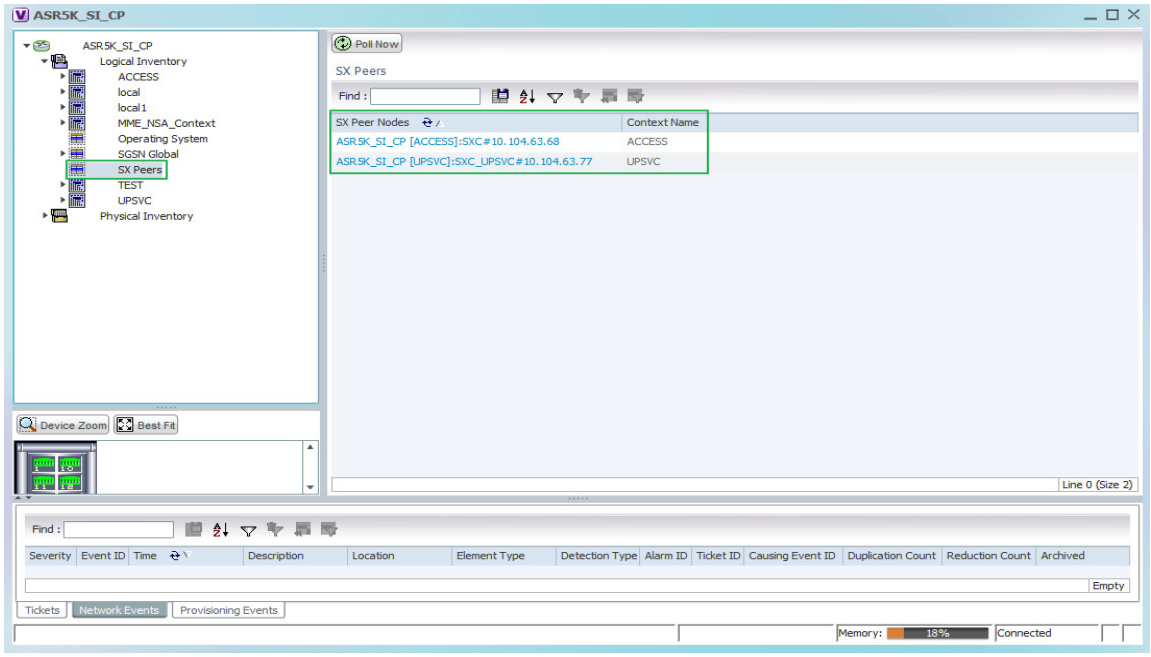
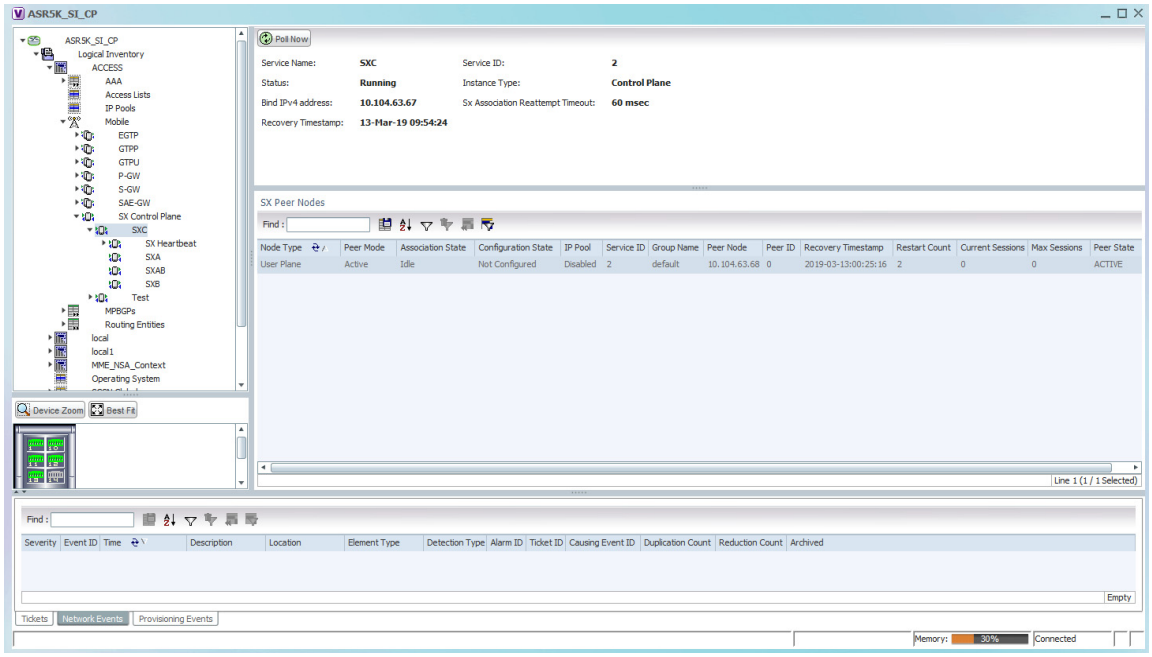


Table 27-151 describes the attributes available for SX Peers.

Table 27-151 SX Peers Attributes

Field	Description
SX Peer Nodes	Displays the peer node information (device name, SX Service name, and IP address).
Context Name	Displays the corresponding context of sx peer.

Step 3 Clicking on an SX Peer Node navigates to the respective SX Peer Node as shown below:



SX Peers neighborship between Control Plane and User Plane services

The Vision client allows you to view neighborship information between the Control Plane and User Plane services.

Note This feature is supported from StarOS 21.9 onwards.

Viewing peer node properties in Control Plane

To view SX Peer Nodes properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**. For example, Double-click an SI device.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > *Sx Control Plane Container* > *Control_Plane_Service*.

The Vision client displays the list of Sx Peer nodes and their properties.

Table 27-152 describes the properties available for Sx Peer Nodes.

Table 27-152 Control Plane Sx Peer Node Properties

Field	Description
Node Type	Type of the peer node (Control Plane/User Plane).
Peer Mode	Mode of the peer node (Active/Standby).
Association State	Association state of the peer node (Idle/Initiated/Associated/Releasing).
Configuration State	Configuration state of the peer node (Configured/Not Configured).
IP Pool	Shows if the IP Pool is enabled/disabled for the peer node.

Table 27-152 Control Plane Sx Peer Node Properties

Field	Description
Service ID	ID of the associated Sx Service.
Group Name	Group Name of the SX Service.
Peer Node	IP address of the peer node.
Peer ID	ID of the peer node.
Recovery Timestamp	Shows the recovery timestamp.
Restart Count	Shows the Restart Count of Sx peer device.
Current Sessions	Shows the Current Sessions count of sx peer device.
Max Sessions	Shows the Max Session count of sx peer device.
Peer State	State of the peer node.

Viewing peer node properties in User Plane

To view SX Peer Nodes properties:

Step 1 Right-click the required device in the Vision client and choose **Inventory**. For example, Double-click an SI device.

Step 2 In the **Logical Inventory** window, choose **Logical Inventory** > *Context* > **Mobile** > *Sx User Plane Container* > *User_Plane_Service*.

The Vision client displays the list of Sx Peer nodes and their properties.

Table 27-153 describes the properties available for Sx Peer Nodes.

Table 27-153 User Plane Sx Peer Node Properties

Field	Description
Node Type	Type of the peer node (Control Plane/User Plane).
Peer Mode	Mode of the peer node (Active/Standby).
Association State	Association state of the peer node (Idle/Initiated/Associated/Releasing).
Configuration State	Configuration state of the peer node (Configured/Not Configured).
IP Pool	Shows if the IP Pool is enabled/disabled for the peer node.
Service ID	ID of the associated Sx Service.
Group Name	Group Name of the SX Service.
Peer Node	IP address of the peer node.
Peer ID	ID of the peer node.
Recovery Timestamp	Shows the recovery timestamp.
Restart Count	Shows the Restart Count of Sx peer device.
Current Sessions	Shows the Current Sessions count of sx peer device.
Max Sessions	Shows the Max Session count of sx peer device
Peer State	State of the peer node.

Monitoring peer nodes

You can use the following CLI command to monitor the Sx peers in CUPS. The devices that support this command are listed in the *Addendum: Additional VNE Support for Cisco Prime Network 5.2*. Whether you can run these commands depends on your permissions. See Vision Client Permissions, page B-1 :

Table 27-154 Sx Peers Commands

Command	Navigation	Description
`Show sx peers`		Displays the attributes listed in Table 27-152 and Table 27-153 for all the Sx peers.

Managing Data Center Networks

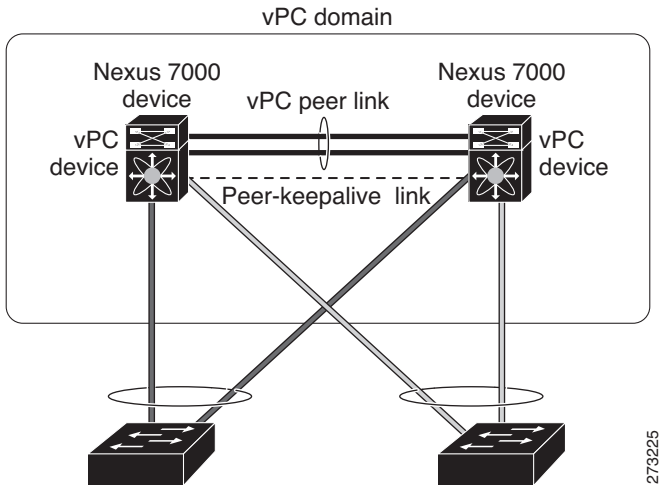
Data Center is a centralized repository, either physical or virtual for the storage, management, dissemination of data and information organized around a particular manner. In other words, it is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communication connections, environmental controls such as air conditioning or fire suppression, and security devices.

Prime Network supports the following technologies as part of data center. If you cannot perform an operation that is described in these topics, you may not have sufficient permissions; see Permissions for Managing Data Center Networks, page B-26.

Viewing Virtual Port Channel (vPC) Configurations

A Virtual Port Channel (vPC) allows links that are physically connected to two different Cisco Nexus 7000 or Cisco Nexus 5000 series network elements to appear as a single port channel by a third device as shown in Figure 28-1. The third device can be a switch, server, or any other networking device that supports port channels. A vPC can provide Layer 2 multipathing, which allows you to create redundancy and increase bisectional bandwidth by enabling multiple parallel paths between nodes and allowing load balancing traffic. You can use only Layer 2 port channels in the vPC.

Figure 28-1 vPC Architecture



A vPC consists of the following components:

- Two vPC peer switches, among which one is primary and one is secondary. The system formed by the two peer switches is referred to as a vPC domain.
- A peer link, also known as multichassis EtherChannel trunk (MCT), which connects the vPC peer switches. A peer link is a redundant 10 Gigabit Ethernet Port Channel,which is used to carry traffic from one system to the other when needed and to synchronize forwarding tables.
- vPC member ports that form the PortChannel and are split between the vPC peers.
- A routed link, called as a vPC peer-keepalive or fault-tolerant link is a Layer 3 Gigabit Ethernet link, used to resolve dual-active scenarios where the peer link connectivity is lost.

A vPC domain is associated to a single Virtual Device Context (VDC), so all vPC interfaces belonging to a given vPC domain must be defined in the same VDC. You must have a separate vPC peer link and peer keepalive link infrastructure for each VDC deployed. Consolidating a vPC pair (two vPC peer devices of the same domain) in two VDCs of the same physical device is not supported. The vPC peer link must use 10-Gigabit Ethernet ports for both ends of the link; otherwise, the link will not be formed.

A vPC provides the following benefits:

- Allows a single device to use a port channel across two upstream devices
- Eliminates STP blocked ports
- Provides a loop-free topology
- Uses all available uplink bandwidth
- Provides fast convergence in case of link or a device failure
- Provides link level resiliency
- Assures high availability

Prime Network supports vPC on Cisco Nexus 5000 series and Cisco Nexus 7000 series network elements.

To view the vPC configuration details in Prime Network Vision:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the Inventory window, choose **Logical Inventory** > **VPC Domain**. The vPC domain details are displayed in the content pane as shown in Figure 28-2.

Figure 28-2 vPC Domain in Logical Inventory

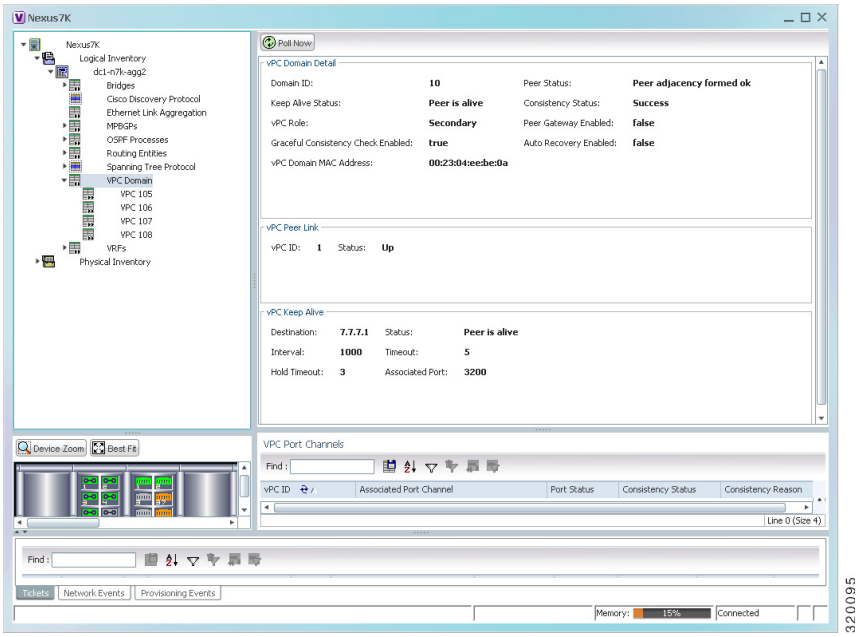


Table 28-1 describes the vPC domain details.

Table 28-1 vPC Domain Properties

Field Name	Description
Domain ID	Unique ID that is used to identify the vPC peer links and ports connected to the vPC downstream devices.
Peer Status	Status of the peer link.
Keep Alive Status	Status of the keep alive link, which could be Alive or Down.
Consistency Status	Consistency status of the vPC, which could be Success or Failed.
vPC Role	Role of the vPC, which could be Primary or Secondary.
Peer Gateway Enabled	Status of the peer gateway, which could be Enabled or Disabled.
Graceful Consistency Check Enabled	Indicates whether graceful consistency check is enabled or disabled. This consistency check helps in preventing traffic drops.
Auto Recovery Enabled	Indicates whether auto recovery is enabled or disabled.
vPC Domain Mac Address	MAC address of the vPC domain.
FabricPath Switch ID	ID of the FabricPath switch connected to the vPC.
vPC Peer Link	
vPC ID	Unique ID for vPC peer link.
Status	Status of the port channel used for communication, which could be Up or Down.
Port Channel	vPC used as the port channel for communication. Click the hyperlink, to view the relevant Ethernet link aggregation node in the physical inventory.
vPC Keep Alive	
Destination	Destination IP address of the peer switch.
Status	Status of the keep alive link, which could be Alive or Down.
Interval	Interval time required to check whether the peer switch is active or inactive.
Timeout	Time taken by the peer switch to respond.
Hold Timeout	Amount of time during which the peer switch information is stored.
Port	Interface used for the communication.
VPC Port Channel	
vPC ID	Unique virtual Port Channel ID.
Port Channel	Ethernet link used as the port channel for communication. Click the hyperlink, to view the relevant Ethernet link aggregation node in the physical inventory.
Port Status	Status of the vPC, which could be Up or Down.
Consistency Status	Consistency status of the vPC, which could be Success or Failed.
Consistency Reason	Reason for the consistency status.

The following VPC commands can be launched from the inventory by right-clicking **VPC Domain** and choosing **Commands > Show.** Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Navigation	Description
Show Port Channel Capacity	*Right-click on the VPC node* > **Commands** > **Show**	Use this command to view and confirm the port channel capacity details.
Show vPC		Use this command to view the vPCs available for the selected domain.
Show vPC Consistency Parameters		Use this command to view the vPC consistency parameters.

Viewing Cisco FabricPath Configurations

Cisco FabricPath is an innovation in Cisco NX-OS software that brings the stability and scalability of routing to Layer 2. It provides a foundation to build a scalable fabric—a network that itself looks like a single virtual switch from the perspective of its users. The switched domain does not have to be segmented anymore, providing data center–wide workload mobility. Because traffic is no longer forwarded along a spanning tree, the bisectional bandwidth of the network is not limited, and massive scalability is possible.

Cisco FabricPath introduces an entirely new Layer 2 data plane by encapsulating the frames entering the fabric with a header that consists of routable source and destination addresses. These addresses are the address of the switch on which the frame was received and the address of the destination switch to which the frame is heading. From there, the frame is routed until it is reaches the remote switch, where it is de-encapsulated and delivered in its original Ethernet format.

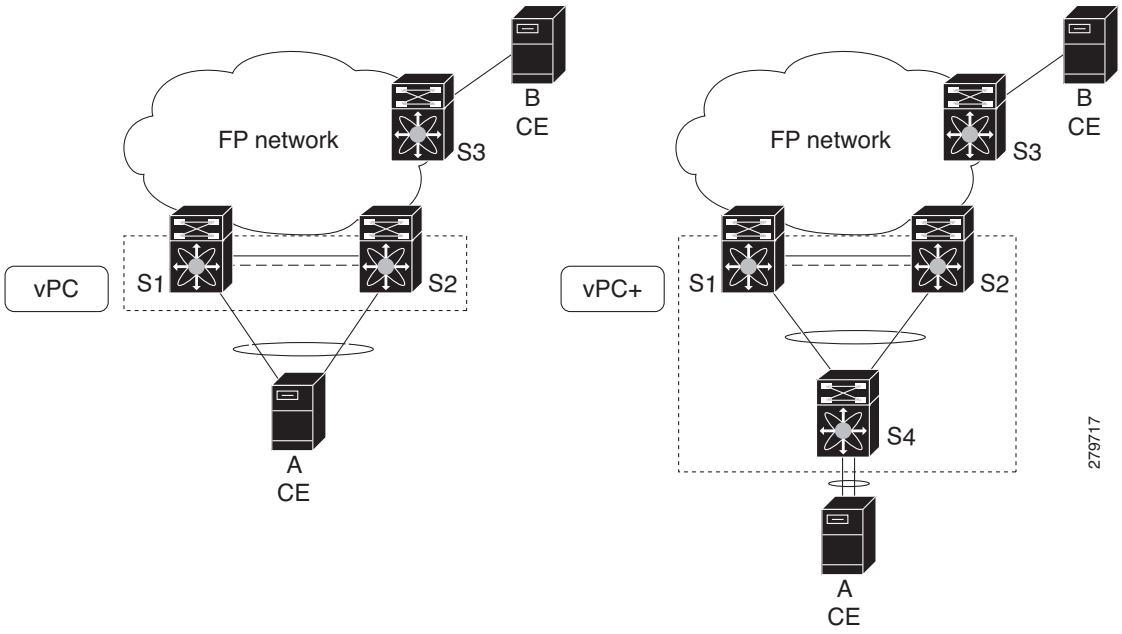
Cisco FabricPath provides the following features:

- Allows Layer 2 multipathing in the FabricPath network.
- Provides built-in loop prevention and mitigation with no need to use the Spanning Tree Protocol (STP).
- Provides a single control plane for unknown unicast, broadcast, and multicast traffic.
- Enhances mobility and virtualization in the FabricPath network.

The system randomly assigns a unique switch ID to each device that is enabled with FabricPath. After you enable FabricPath on the devices, you can configure an Ethernet interface or a port channel interface as a FabricPath interface. If one member of the port channel is in FabricPath mode, then all the other members will also be in FabricPath mode. After you configure the interface as a FabricPath interface, it automatically becomes a trunk port, capable of carrying traffic for multiple Virtual Local Area Networks (VLANs).

Prime Network supports Cisco FabricPath on Cisco Nexus 5000 series and Cisco Nexus 7000 series network elements. Figure 28-3 shows a Cisco FabricPath architecture.

Figure 28-3 Cisco FabricPath Architecture



To view the FabricPath configuration in Prime Network Vision:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the Inventory window, choose **Logical Inventory** > **FabricPath**. The FabricPath configuration details are displayed in the content pane as shown in Figure 28-4. You can also view the properties, by right-clicking the FabricPath node and choosing **Properties**.

Figure 28-4 Cisco FabricPath Node in Logical Inventory

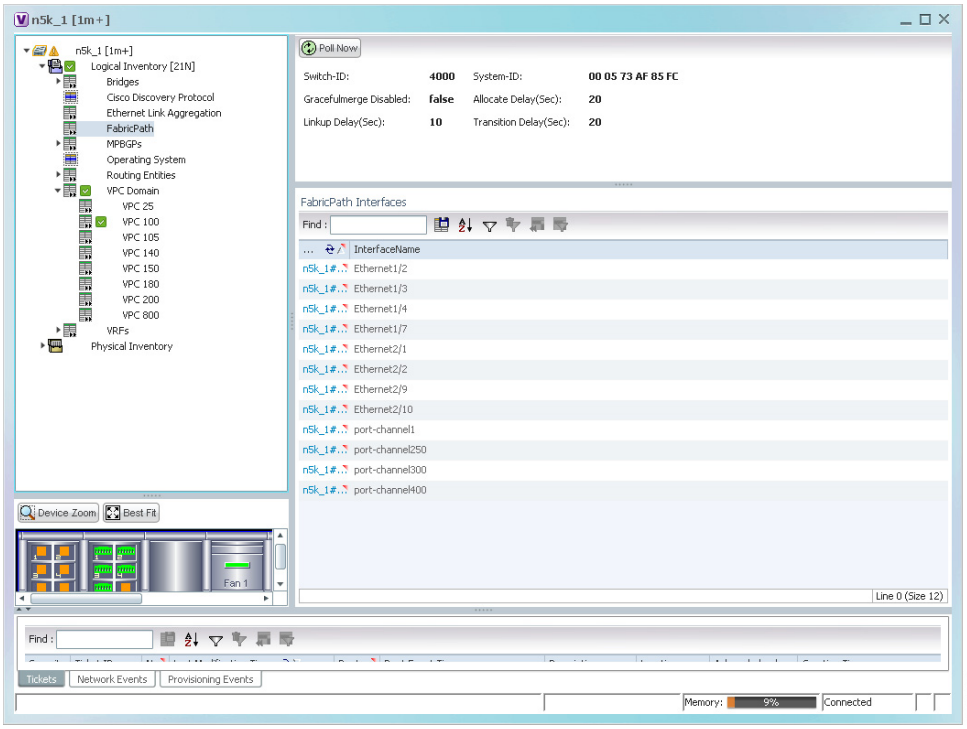


Table 28-2 describes the FabricPath configuration details.

Table 28-2 Cisco FabricPath Configuration

Field Name	Description
Switch ID	Unique ID of the Cisco FabricPath virtual switch.
System-ID	System MAC address of the Cisco FabricPath.
Gracefulmerge Disabled	Indicates whether graceful merge feature is enabled are not. Value could be **True** or **False**. If this feature is enabled, the switch would be effectively linked to the Cisco FabricPath network. If disabled, you may experience traffic drops.
Allocate Delay (sec)	Time delay during new resource propagation.
Linkup Delay (sec)	Time delay for detecting conflicts during linkup sessions.
Transition Delay (sec)	Time delay during transition of value propagation.
FabricPath Interfaces	
Port	Ethernet link, which is configured as a Cisco FabricPath. Click the hyperlink to view the interface link in physical inventory.
Interface Name	Name of the interface for which switch port mode is configured as a Cisco FabricPath.

The following FabricPath commands can be launched from the inventory by right-clicking **FabricPath** and choosing **Commands > Show.** Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Navigation	Description
FabricPath Conflict	*Right-click on the FabricPath node* > **Commands** > **Show**	Use this command to view the Cisco FabricPath conflicts.
MAC Address-Table Learning Mode		Use this command to view the MAC address-table learning mode.

Viewing the Virtual Device Context and Port Allocation

The Virtual Device Context (VDC) partitions a single physical device into multiple logical devices that provide fault isolation, management isolation, address allocation isolation, service differentiation domains, and adaptive resource management. You can manage a VDC instance within a physical device independently. Each VDC appears as a unique device to the connected users. A VDC runs as a separate logical entity within the physical device, maintains its own unique set of running software processes, has its own configuration, and can be managed by a separate administrator.

In Prime Network, you can view the VDC context and port allocation details for a Nexus 7000 device. Each context will contain a list of allocated ports.

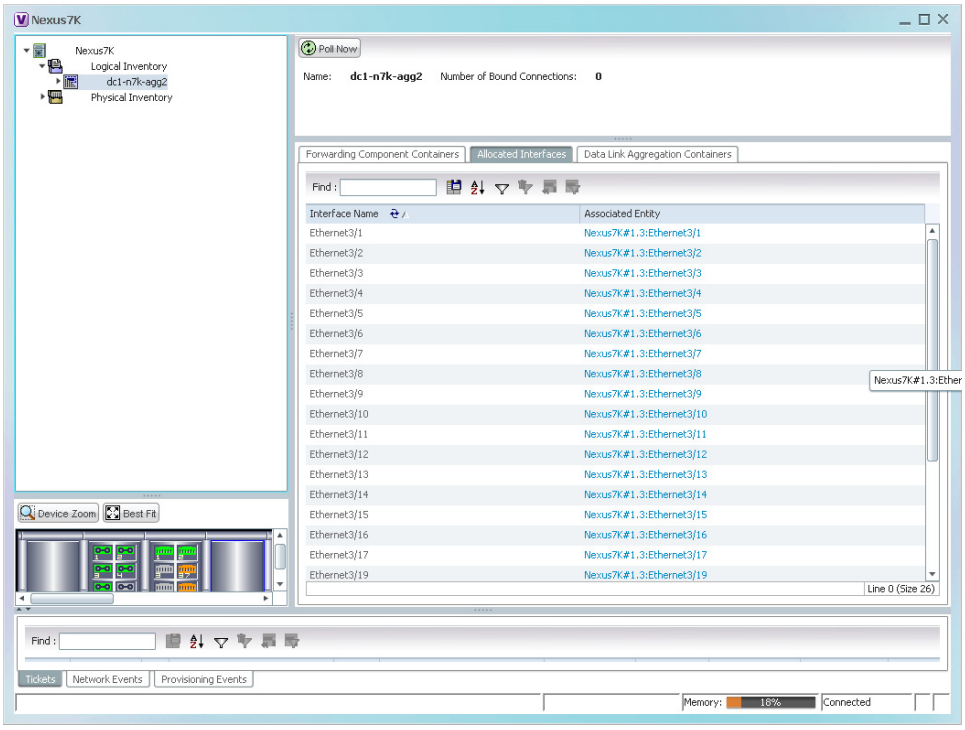
To view the VDC context details:

Step 1 Right-click on the Nexus 7000 device and choose the **Inventory** option.

Step 2 In the Inventory window, choose **Logical Inventory** > *Context*.

Step 3 In the content pane, click the **Allocated Interfaces** tab. The VDC context details are displayed in the content pane as shown in Figure 28-5. The **Interface Name** and the related **Associated Entity** are displayed in the content pane.

Figure 28-5 Allocated Interfaces tab



Step 4 Click the link in the **Associated Entity** field and you will be able to view the related interface node details under the Physical Inventory.

Configuring Prompts and Messages for Unconfigured VDC for a Nexus Device

You can configure prompts and messages of unconfigured Virtual Device Context (VDC) for a Cisco Nexus device by using runRegTool.

Prime Network reads these prompts at the time of switching to unconfigured VDC to avoid collectors from blocking the expected prompt. When the prompts are completely read, Prime network receives the interactive mode response from the device, say Cisco Nexus device. Prime Network detects the situation by comparing the device response with the configured messages of unconfigured VDC in the Registry. After the situation is detected, Prime Network avoids configuring the unconfigured VDC by aborting the switchto command. As soon as the current command result is marked as Valid, you can proceed with inventory discovery.

If either Unconfigured VDC is configured or Suspended VDC is activated, click **Poll Now** to view the updated inventory details.

Note Ensure that prompts and messages must be defined with a unique name and full description.

To configure new prompts, run the below command:

```
runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/ciscovdc-cisco-nexus70xx-product/cisco-catalyst/nexus70xx/product/software
versions/default
version/ip_default/protocols/telnet/unconfigured_vdc_context/expected_prompts/<pro
mptentry>"  <promptvalue>
```

Example: runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/ciscovdc-cisco-nexus70xx-product/cisco-catalyst/nexus70xx/product/software
versions/default
version/ip_default/protocols/telnet/unconfigured_vdc_context/expected_prompts/prom
pt1" "[n]:"

To configure messages, run the below command:

```
runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/ciscovdc-cisco-nexus70xx-product/cisco-catalyst/nexus70xx/product/software
versions/default
version/ip_default/protocols/telnet/unconfigured_vdc_context/expected_messages/<me
ssageentry>" <messagevalue>
```

Example: runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/ciscovdc-cisco-nexus70xx-product/cisco-catalyst/nexus70xx/product/software
versions/default
version/ip_default/protocols/telnet/unconfigured_vdc_context/expected_messages/mes
sage0" "Admin Secure Password".

Viewing Virtualized Resources

Virtualization is a concept of creating a virtual version of any resource, such as hardware platform, operating system, storage device, or network resources, as shown in Figure 28-6. It provides a layer of abstraction between computing, storage and networking hardware, and the applications running on it. Virtual infrastructure gives administrators the advantage of managing pooled resources across the enterprise, allowing IT managers to be more responsive to dynamic organizational needs and to better leverage infrastructure investments.

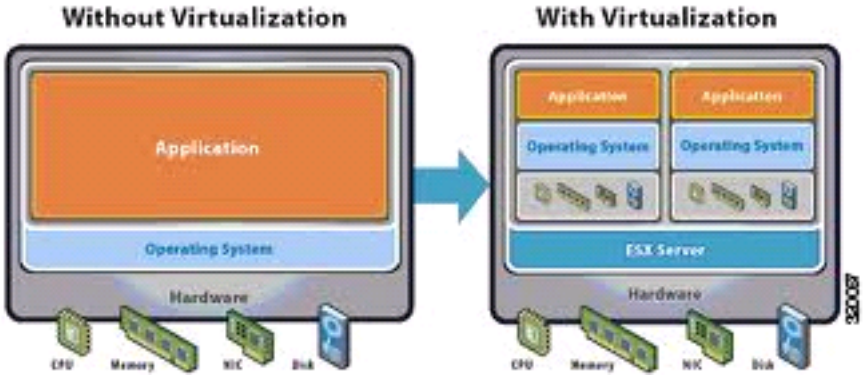
The VMware vCenter Server provides centralized management of virtualized hosts and virtual machines from a single console. With VMware vCenter Server, virtual environments are easier to manage: a single administrator can manage hundreds of workloads, more than doubling typical productivity in managing physical infrastructure.

In Prime Network, VCenter is modelled as a VNE.

Note VCenter is created as a separate VNE using the Administration client. For more information about creating a new VNE, see the *Cisco Prime Network 5.3 Administrator Guide*. You must specify the http credentials for VCenter. However the SNMP credentials are optional, and the SSH credentials are not required.

Note .

Figure 28-6 Virtualization Concept



The various components of virtualization are:

Hypervisor (Host Server)

A hypervisor, also called a blade server, a virtual machine manager, or a host server, is a program that allows multiple operating systems to share a single hardware host. Each operating system appears to have the host's processor, memory, and other resources all to itself. However, the hypervisor is actually controlling the host processor and resources, allocating what is needed to each operating system in turn and making sure that the guest operating systems (called virtual machines) do not disrupt each other.

Virtual Machine

A virtual representation of a real machine using software that provides an operating environment, which can run or host a guest operating system.

Guest Operating System

An operating system running in a virtual machine environment that would otherwise run directly on a separate physical system.

Data Store

A data store represents a storage location for virtual machine files. It can be a Virtual Machine File System (VMFS) volume, a directory on Network Attached Storage, or a local file system path.

Data Center

Data Center serves as a container for hosts, virtual machines, networks, and data stores.

Cluster

A cluster is a collection of servers that operate as if it is a single machine. The primary purpose of these clusters is to provide uninterrupted access to data, even if a server loses network or storage connectivity, or fails completely, or if the application running on the server fails.

Resource Pool

A resource pool is a logical abstraction for flexible management of resources. Resource pools can be grouped into hierarchies and used to hierarchically partition available CPU and memory resources.It is the foundation of virtual data centers, virtual desktops, high availability and other options on virtual servers. Resource pools aggregate CPU processing power and memory, along with any other relevant components, then share these hardware resources among virtual machines (VMs).

The following topics explain how to view and monitor virtual data center properties in Prime Network Vision:

Viewing Virtual Data Centers

To view the virtual data centers in the logical inventory:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the Inventory window, choose **Logical Inventory** > **Compute Virtualization**. The virtual data centers are listed in the content pane.

Table 28-3 describes the virtual data center properties.

Table 28-3 Virtual Data Center Properties

Field Name	Description
Name	Name of the data center.
IP Address	IP address of the vCenter, which manages the virtual data center.
DNS name	The DNS name of the data center.

Step 3 Right-click the data center and choose **Properties** to view more details.

Viewing the Data Stores of a Data Center

To view the details of data stores available for a data center:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the Inventory window, choose **Logical Inventory** > **Compute Virtualization >** *Data Center* > **All Data Stores**. The available data stores are displayed in the content pane. You can view the data store properties from the table or by right-clicking the required data store and choosing **Properties**.

Table 28-4 describes the data store properties.

Table 28-4 Data Store Properties

Field Name	Description
Name	Name of the data store.
Storage Type	Type of data storage for the data store.
Capacity	Capacity of the data store, in GB.
Free Space	Free space of the data store, in GB.
Provisioned Space	The amount of provisioned space available for the data store.
Accessible	Indicates whether the data store is accessible or not. Value could be True or False.
Multi Host Access	Indicates whether the data store supports multi host access. Value could be True or False.
Storage Location	The location of the data store.
Uuid	The unique ID of the data store.
Associated storage device	The storage device associated to the data store.
Connected Hosts	
Host Name	The name of the host connected to the data store.
Associated Host	The link to the associated host, which when clicked will take you to the relevant host node.

Viewing the Host Servers of a Data Center

To view the host centers of a data center:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the Inventory window, choose **Logical Inventory** > **Compute Virtualization >** *Data Center* > **All Host Servers**. Choose a host server and the details are displayed in the content pane as shown in Figure 28-7.

Figure 28-7 Host Server Details

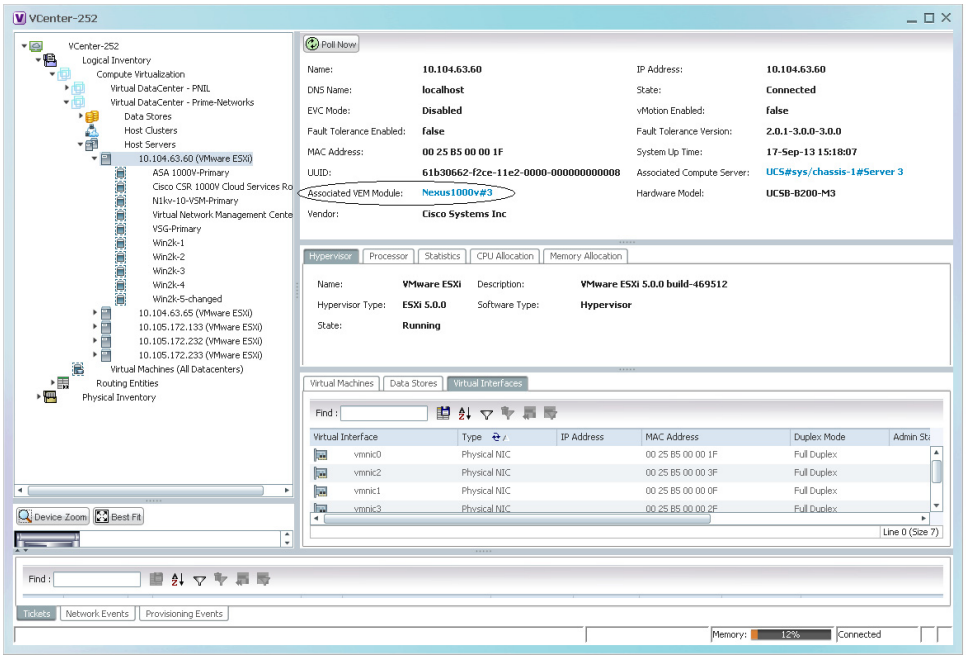


Table 28-5 describes the host server details.

Table 28-5 Host Servers of a Data Center

Field Name	Description
Name	Name of the host server.
IP Address	The IP address of the host server.
DNS Name	The domain name of the host sever.
State	Management state of the host server.
EVC Mode	Enhanced vMotion Capability (Evc) of the host server.
VMotion Enabled	Indicates whether vMotion service is enabled or not. vMotion service helps in migrating the virtual machines from one host server to another, when a particular host server is down.
Fault Tolerance Enabled	Indicates whether fault tolerance service is enabled or not. This service provides continuous availability by protecting the primary virtual machine with a secondary virtual machine that runs simultaneously on a separate host.
Fault Tolerance Version	The fault tolerance version of the host server.
MAC Address	MAC address of the host server.
UUID	The unique ID of the host server.
Hardware Model	The hardware model of the server.
Vendor	The name of the vendor of the host server.
Associated Compute Server	The compute server associated to the host server.
Associated VEM Module	The Virtual Ethernet Module (VEM) associated to the host server. Clicking this link will take you to the related UCS blade server node under the physical inventory.
Associated Cluster	The cluster associated to the host server.
System Up Time	The date and time when the router was last restarted.
Hypervisor tab	
Name	Name of the hypervisor running on the host server.
Description	Description of the hypervisor.
Hypervisor Type	Type of the hypervisor.
Software Type	Type of software used by the hypervisor.
State	State of the hypervisor, which could be Running, Runnable, Waiting, Exiting, or Other.
Processor tab	
Name	Name of the processor used by the host server.
Description	Description of the processor used by the host server.
CPU	Number of central processing units (CPUs) available for the host server.
Cores per CPU	Number of cores per CPU available for the host server.
Rated Speed	Rated speed of the processor, in GHz.
Used Speed	Actual used speed of the processor, in GHz.

Table 28-5 Host Servers of a Data Center (continued)

Field Name	Description
Hyper Threading Enabled	Indicates whether hyper threading is enabled for the host server or not. Hyper threading helps to improve parallelization of computations.
RAM Size	RAM size of the processor, in GB.
Statistics tab	
CPU Usage	CPU usage by the host server, in GHz.
Memory Usage	Memory usage by the host server, in GB.
Disk Usage	Amount of disk space used by the host server, in GB.
CPU Allocation tab	
Resource Type	The type of resource, which in this instance is CPU.
Allocatable	Maximum CPU allocation for the host center, in GHz.
Reserved	The CPU allocation reserved for the host center, in GHz.
Unallocated	The unallocated CPU allocation for the host center, in GHz.
Overhead	The overhead CPU allocation for the host center, in GHz.
Unlimited Provision	Indicates whether the unlimited CPU provision is available for the host center.
Share	Relative importance of the host server for CPU allocation, which could be High, Normal, or Low.
Custom Share Weight	The custom share weight assigned to the host server.
Unreserved	The unreserved CPU allocation for the host center, in GHz.
Memory Allocation tab	
Resource Type	The type of resource.
Allocatable	Maximum memory allocation for the host center, in GHz.
Reserved	The memory allocation reserved for the host center, in GHz.
Unallocated	The unallocated memory allocation for the host center, in GHz.
Overhead	The overhead memory allocation for the host center, in GHz.
Unlimited Provision	Indicates whether the unlimited memory provision is available for the host center.
Share	Relative importance of the host server for memory allocation, which could be High, Normal, or Low.
Custom Share Weight	The custom share weight assigned to the host server.
Unreserved	The unreserved memory allocation for the host center, in GHz.
Data Stores tab	
Data Store Name	Name of the data store associated with the host server.
Associated Data Store	Click the hyperlink to view the associated data store under the **All Data Stores** node.
Virtual Interfaces tab	
Name	Name of the network endpoint of the virtual entity.
Type	Type of the virtual entity network endpoint.

Table 28-5 Host Servers of a Data Center (continued)

Field Name	Description
IP Address	Primary IP address of the virtual entity network endpoint.
MAC Address	MAC address of the virtual entity network endpoint.
Duplex Mode	Communication mode, which could be one of the following: • Half—Transmit data in one direction at a time. • Full—Transmit data in both the directions at the same time.
Compute Resource Pool	
Provider Name	The compute resource pool name.
Description	The description of the compute resource pool.
Status	The status of the compute resource pool.
Root Pool	Indicates whether the compute resource pool is the root pool.

Viewing all the Virtual Machines managed by vCenter

To view a list of all the virtual machines managed by a data center:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the Inventory window, choose **Logical Inventory** > **Compute Virtualization** > *Data Center* > **All Virtual Machines**. A list of virtual machines is displayed in the content pane as shown in Figure 28-7.

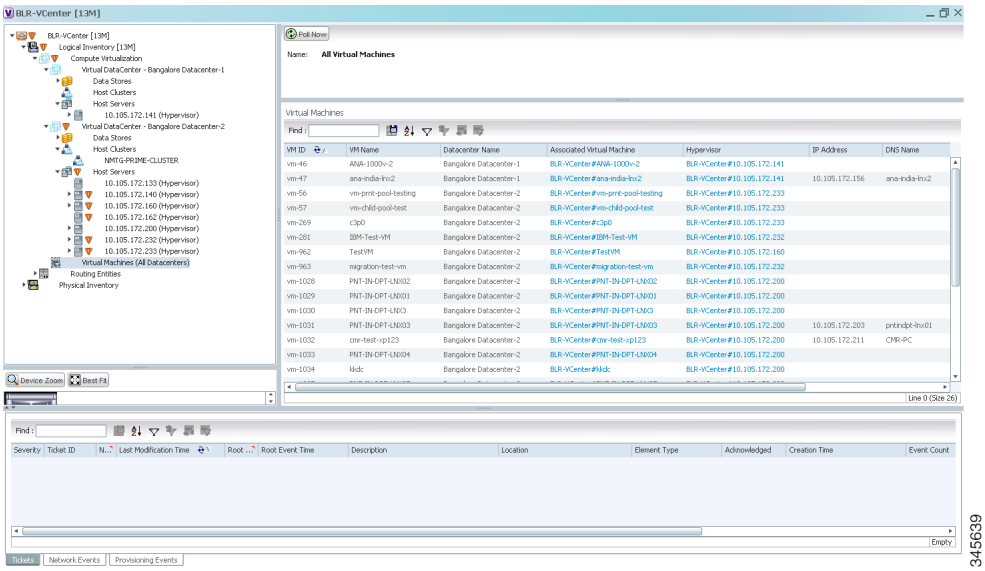


Table 28-6 describes the virtual machine details available in the list.

Table 28-6 Virtual Machines

Field Name	Description
Name	Name of the associated data center.
Virtual Machines	
VM ID	The unique identification code for the virtual machine.
VM Name	The name of the virtual machine.
Data Center Name	The name of the data center associated to the virtual machine.
Associated VM Entity	The associated virtual machine entity.
Hypervisor	The hypervisor associated tot he virtual machine.
DNS Name	The DNS name of the virtual machine.
IP Address	The IP address of the virtual machine.
MAC Address	The MAC address of the virtual machine.

Viewing the Virtual Machines of a Data Center

To view the virtual machines for a data center:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the Inventory window, choose **Logical Inventory** > **Compute Virtualization >** *Data Center* > **All Host** > **Virtual Machine**. A list of virtual machines is displayed in the content pane.

Step 3 Click the hyperlinked virtual machine name to view more details about the virtual machine. Prime Network Vision takes you to the virtual machine node under the mapped host server in the logical inventory. You can view the virtual machine properties on the content pane or by right-clicking the virtual machine and choosing **Properties**.

Table 28-7 describes the properties of the virtual machine.

Table 28-7 Virtual Machine Properties

Field Name	Description
VM ID	The unique identification code of the virtual machine.
Name	Name of the virtual machine.
IP Address	IP address of the virtual machine.
DNS Name	Domain name of the virtual machine.
MAC Address	MAC Address of the virtual machine.
State	Execution state of the virtual machine, which could be Powered On, Powered Off, or Suspended.
VM Version	Hardware version of the virtual machine.
Virtual CPU	Number of virtual CPUs configured for the virtual machine on the host server.
Minimum Required EVC Mode	Minimum required EvC of the virtual machine.
VM Template	The virtual machine template.
Management Address	The management address configured for the virtual machine.
Host Name	The host name of the virtual machine.
Virtual Data Center Name	The virtual data center name associated to the virtual machine.
Fault Tolerance Enabled	Indicates whether fault tolerance service is enabled or not. This service provides continuous availability by protecting the primary virtual machine with a secondary virtual machine that runs simultaneously on a separate host.
Software Type	Type of the software used by the virtual machine.
Source Resource Pool	The source resource pool associated to the virtual machine.
System Uptime	The date and time when the virtual machine was last booted up.
Statistics tab	
CPU Usage	CPU usage by the virtual machine, in GHz.
Memory Usage	Memory usage by the virtual machine, in GB.
Disk Usage	Amount of disk space used by the virtual machine, in GB.
Active Guest Memory Usage	Active guest memory used by the virtual machine, in GB.
CPU Allocation tab	
Resource Type	The type of resource, which in this instance is CPU.
Maximum Allocation	Maximum CPU allocation for the virtual machine, in GHz.
Startup Allocation	The startup CPU allocation for the virtual machine, in GHz.
Guaranteed Allocation	The guaranteed CPU allocation for the virtual machine, in GHz.
Overhead Allocation	The overhead CPU allocation for the virtual machine, in GHz.
Unlimited Maximum Allocation	Unlimited maximum allocation capacity availability check for the virtual machine. Value could be true or false.

Table 28-7 Virtual Machine Properties (continued)

Field Name	Description
Expandable Allocation	Expandable allocation availability for the virtual machine. Value could be true or false.
Share	Relative importance of the virtual machine for CPU allocation, which could be High, Normal, or Low.
Custom Share Weight	Custom share weight assigned to the virtual machine.
Memory Allocation tab	
Resource Type	The type of resource.
Startup Allocation	The startup memory allocation for the virtual machine, in GB.
Guaranteed Allocation	The guaranteed memory allocation for the virtual machine, in GB.
Maximum Allocation	Maximum memory allocation for the virtual machine, in GB.
Overhead Allocation	Overhead memory allocation for the virtual machine, in GB.
Unlimited Maximum Allocation	Unlimited maximum allocation capacity availability check for the virtual machine. Value could be true or false.
Expandable Allocation	Expandable allocation availability for the virtual machine. Value could be true or false.
Share	Relative importance of the virtual machine for memory allocation, which could be High, Normal, or Low.
Custom Share Weight	Custom share weight assigned to the virtual machine.
Disk Allocation tab	
Resource Type	The type of resource, which in this instance is Disk.
Startup Allocation	The startup disk allocation for the virtual machine, in GB.
Guaranteed Allocation	Guaranteed resource allocation for the virtual machine, in GB.
Maximum Allocation	Maximum disk allocation for the virtual machine, in GB.
Overhead Allocation	Overhead disk allocation for the virtual machine, in GB.
Unlimited Maximum Allocation	Unlimited maximum allocation capacity availability check for the virtual machine. Value could be true or false.
Expandable Allocation	Expandable allocation availability for the virtual machine. Value could be true or false.
Share	Relative importance of the virtual machine for memory allocation, which could be High, Normal, or Low.
Custom Share Weight	Custom share weight assigned to the virtual machine.
Data Stores tab	
Data Stores Name	Name of the data store associated with the virtual machine.
Associated Data Sore	Click the hyperlink to view the associated data store under the **All Data Stores** node.
Virtual Interfaces tab	
Name	Name of the network endpoint of the virtual entity.
Type	Type of the virtual entity network endpoint.
IP Address	Primary IP address of the virtual entity network endpoint.

Table 28-7 Virtual Machine Properties (continued)

Field Name	Description
MAC Address	MAC address of the virtual entity network endpoint.
Duplex Mode	Communication mode, which could be one of the following: • Half—Transmit data in one direction at a time. • Full—Transmit data in both the directions at the same time.
Operational Status	The operational status of the virtual machine.
Administrative Status	The administrative status of the virtual machine.
Speed	The speed of the processor in the virtual machine.
MTU	The maximum number of transmission units (in bytes) for the virtual machine.
Secondary Address	The secondary IP address of the virtual machine.

Viewing the Host Cluster Details

To view the host cluster details:

Step 1 In the Vision client, right-click on the required device and select the **Inventory** option.

Step 2 In the Inventory menu, expand the **Logical Inventory** node.

Step 3 Select **Compute Virtualization** > *Data Center* > **Host Clusters** > *Host cluster*. The host cluster details are displayed in the content pane as shown in Figure 28-8.

Figure 28-8 Host Cluster Details

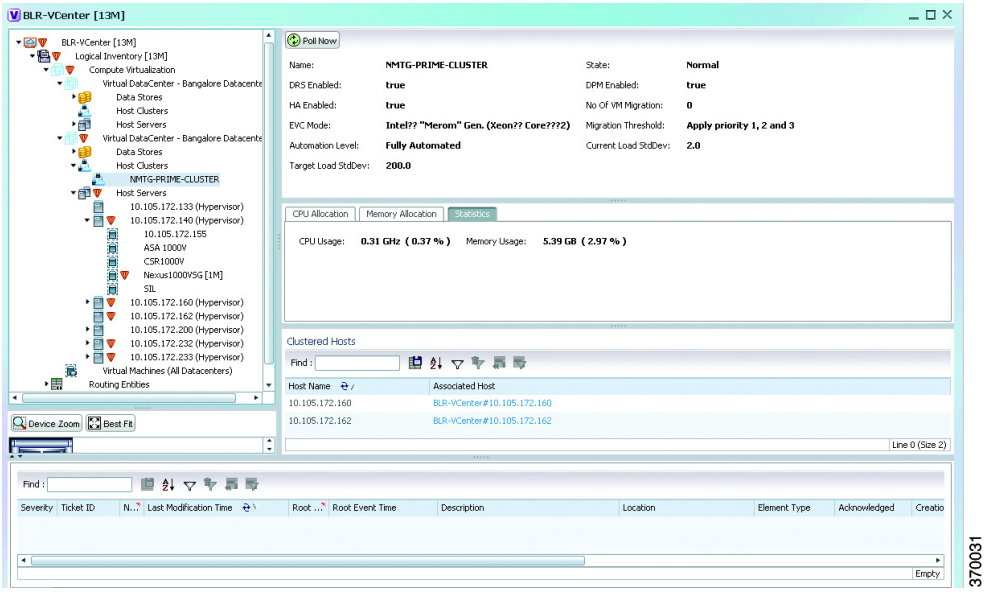


Table 28-8 describes the Host Cluster details.

Table 28-8 Host Cluster Details

Field Name	Description
Name	The name of the host cluster.
Data Center Name	The name of the associated data center.
Description	The description of the host cluster.
State	The status of the host cluster, which can be any one of the following: • Unknown • Normal • Warning • Alert
DRS Enabled	Indicates whether the VMware Distributed Resource Scheduler (DRS) feature is enabled for the host cluster.
DPM Enabled	Indicates whether the VMware Distributed Power Management (DPM) feature is enabled for the host cluster.
HA Enabled	Indicates whether the VMware High Availability (HA) feature is enabled for the host cluster.
No. of VM Migration	The number of virtual machines that have been migrated from one server to another within the same cluster.
EVC Mode	The Enhanced vMotion Compatibility (EVC) mode of the host cluster.
Migration Threshold	The migration threshold for the host cluster.
Automation Level	Indicates that the placement and migration recommendations run automatically for the host cluster.
Current Load Std dev	The current host load standard deviation for the host cluster.
Target Load Std dev	The target hot load standard deviation for the host cluster.
CPU Allocation	
Allocatable	The maximum CPU allocation for the virtual machine, in GHz.
Reserved	The CPU allocation reserved for the virtual machine, in GHz.
Unreserved	The unreserved CPU allocation for the virtual machine, in GHz.
Unlimited Provision	Indicates whether the unlimited CPU provision is available for the virtual machine.
Share	Relative importance of the virtual machine for CPU allocation, which could be High, Normal, or Low.
Custom Share Weight	The custom share weight assigned to the virtual machine.
Memory Allocation	
Allocatable	The maximum memory allocation for the virtual machine, in GB.
Reserved	The memory allocation reserved for the virtual machine, in GB.
Unreserved	The unreserved memory allocation for the virtual machine, in GB.
Unlimited Provision	Indicates whether unlimited memory allocation provision is available for the virtual machine.

Table 28-8 Host Cluster Details (continued)

Field Name	Description
Share	The relative importance of the virtual machine for memory allocation, which could be High, Normal, or Low.
Custom Share Weight	The custom share weight assigned to the virtual machine.
Statistics tab	
CPU Usage	CPU usage by the virtual machine, in GHz.
Memory Usage	Memory usage by the virtual machine, in GB.
Disk Usage	Amount of disk space used by the virtual machine, in GB.
Active Guest Memory Usage	Active guest memory used by the virtual machine, in GB.
Clustered Hosts	
Host Name	The name of the host server in the clustered host.
Associated Host	The link to the associated host, which when clicked will take you to the relevant host server.
Compute Resource Pool	
Provider Name	The compute resource pool name.
Description	The description of the compute resource pool.
Status	The status of the compute resource pool.
Root Pool	Indicates whether the compute resource pool is the root pool.

Viewing the Resource Pool Details

To view the resource pool details:

Step 1 In the Vision client, right-click on the required device and select the **Inventory** option.

Step 2 In the Inventory menu, expand the **Logical Inventory** node.

Step 3 Select **Compute Virtualization** > *Data Center* > **Host Clusters** > *Host cluster*. The host cluster details are displayed in the content pane.

Note Alternatively, you can also view the host cluster details by selecting **Compute Virtualization** > *Data Center* > **All Host** > **Host**.

Step 4 In the Compute Resource Pools tab in the content pane, click on a resource pool link in the **Resource Pool** field. The **Compute Resource Pool Properties** window is displayed.In

Table 28-10 describes the resource pool details.

Table 28-9 Resource Pool Properties

Field Name	Description
Name	The compute resource pool name.
Provider Name	The description of the compute resource pool.
Status	The status of the compute resource pool.
Root Pool	Indicates whether the compute resource pool is the root pool.
CPU Allocation tab	
Resource Type	The type of resource, which in this instance is CPU.
Allocatable	The maximum CPU allocation for the virtual machine, in GHz.
Reserved	The CPU allocation reserved for the virtual machine, in GHz.
Unreserved	The unreserved CPU allocation for the virtual machine, in GB.
Unlimited Provision	Indicates whether unlimited CPU allocation provision is available for the virtual machine.
Share	The relative importance of the virtual machine for CPU allocation, which could be High, Normal, or Low.
Configured Reservation	The CPU reservation configured for the virtual machine.
Available Reservation	The CPU reservation available for the virtual machine.
Overhead	The overhead CPU allocation for the virtual machine, in GHz.
Custom Share Weight	The custom share weight assigned to the virtual machine.
Memory Allocation tab	
Resource Type	The type of resource.
Allocatable	The maximum memory allocation for the virtual machine, in GHz.
Reserved	The memory allocation reserved for the virtual machine, in GHz.
Unallocated	The memory not allocated for the virtual machine.
Overhead	The overhead memory allocation for the host center, in GHz.
Unlimited Provision	Indicates whether unlimited memory allocation provision is available for the virtual machine.
Unreserved	The unreserved memory allocation for the virtual machine, in GB.
Share	The CPU reservation configured for the virtual machine.
Custom Share Weight	The CPU reservation available for the virtual machine.
Configured Reservation	The memory reservation configured for the virtual machine.
Available Reservation	The memory reservation available for the virtual machine.

Viewing the Map Node for an UCS Network Element

Using the Vision client, you can view the physical layout and topology among the multi-chassis devices on the map. The multi-chassis devices have more than one physical chassis, but they are represented as a single entity in Prime Network. In a map, this device is shown as an aggregation of all the device chassis. For more information on viewing multi-chassis devices, see Viewing Multi-Chassis Devices, page 8-5.

For a Cisco Unified Computing Service (UCS) device, you can view its chassis along with the other elements relevant to the UCS device, such as Blade Server and IO Modules.

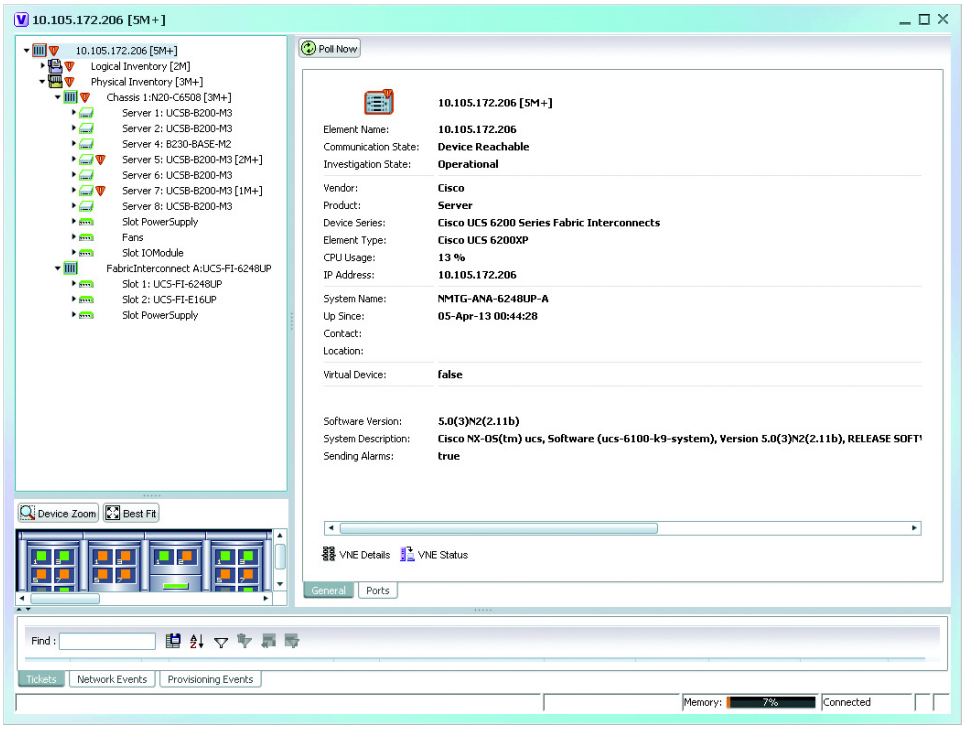
Another important component of the UCS is the Fabric InterConnect. The Fabric InterConnect is a core part of the UCS device. It provides both network connectivity and management capabilities to all attached blades and chassis. All chassis, and therefore all blades, attached to the interconnects become part of a single, highly available management domain.

To view the physical inventory of a UCS:

Step 1 Right-click on the UCS device and choose the **Inventory** option.

Step 2 In the Inventory window, expand the **Physical Inventory** node. The Chassis and Fabric Interconnect chassis are displayed below the node as shown in Figure 28-9.

Figure 28-9 Physical Inventory Node for a UCS Device



Step 3 Expand the **Chassis** node. The Blade servers, Fans, and the IO Modules that make up the Chassis are displayed under this node.

Step 4 Expand the **Fabric InterConnect** node.The slots and the power supply are available here. You can click on each individual node under these nodes to view more details.

Step 5 Close the inventory window.

Each of these parts, i.e. the blade servers, Fabric InterConnect chassis, and IO Modules, can be connected to each other internally. For example, an IO Module can be connected to a blade server or there could also be a link between the IO Module and Fabric InterConnect chassis.

The Ethernet links between the different components of a UCS can be categorized as:

- Backplane links—The links that connect a chassis to a backplane port via the IO Module.
- Fabric links—The links that connect a chassis to a Fabric InterConnect port via the IO Module.

You can also view this link in a map that contains a separate map node for each of the following elements:

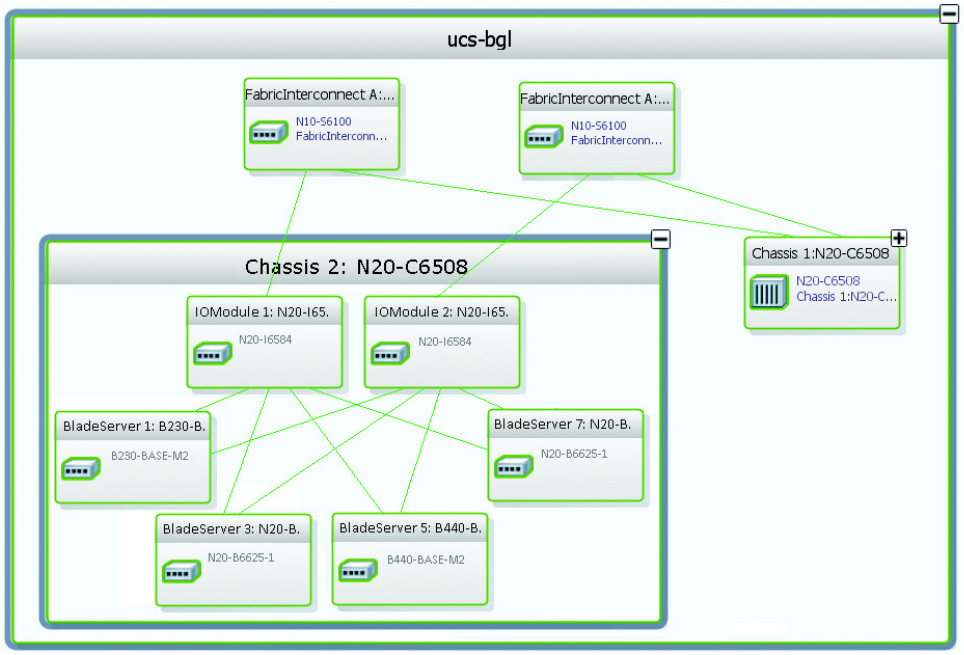
- Fabric Interconnect Chassis
- Blade Server Chassis
- Cisco Blade Server
- IO Module

The blade server chassis is shown as an aggregation that also contains the IO Module.

To view the map for a UCS device:

Step 1 In the Vision client, open a map with a UCS device. The UCS device is displayed with a plus (+) sign. Click on the + sign. The map containing the links between each element in the UCS device is shown in the window as shown in Figure 28-10.

Figure 28-10 UCS Map Node with Aggregation Links



Note Sub-nodes are available for the chassis that have blade servers under them. You can expand/contract these sub-nodes to view more details. However, the elements under the Fabric InterConnect chassis will not be displayed in the map.You can also view the inventory for an element by double-clicking on a node in the map. The inventory window will open with the selected node.

Step 2 Hover your mouse cursor over the required link in a map. A link tooltip is displayed. The tooltip displays the link endpoints identified by the element or service name and the number of links represented by the line on the map.

Step 3 To view additional link information, click the tooltip. The link quick view window is displayed. Alternatively, you can also double-click the link to view the link quick view window.

Note You can view links belonging to a specific type by clicking the Filter icon in the navigation pane and selecting the relevant check box. Open the link again and only the selected type of link is displayed. For more information about filtering a map, see Using Link Filters to Find Links, page 7-21.

Step 4 Close the window.

Step 5 In the map, double-click an element icon to open the Physical inventory and view the ports under it. For example, if you double-click on an IO Module element, the Inventory window is displayed along with the Backplane and Fabric ports under the IO Module node.

Step 6 In the map, double click on a link to view it's properties such as the link type, port alias, and port location. For more information on link properties, see Viewing Link Status and Detailed Link Properties, page 7-25.

Note The links between the UCS components can also be viewed in the Cisco Unified Computing System Manager application.

Discovering the UCS Devices by Network Discovery

The Network Discovery feature automatically discovers network devices by traversing the network. The required information is an IP address for a seed device, and the SNMPv 2 or SNMPv 3 credentials. This information is added to a discovery profile that specifies the IP and SNMP information, along with any additional protocols or filters you want Prime Network to use.

You can also discover the UCS devices by Network Discovery. To manage a UCS device, the CLI and http credentials are required. However, the existing network discovery does not support http.

Since the CLI and http credentials are identical most of the times, the CLI credentials will be copied into http. You need to create a new discovery profile (using telnet or SSH credentials) for the UCS device and execute it. For more information about adding devices using Network Discovery, see the *Cisco Prime Network 5.3 Administrator Guide*.

Viewing the Virtual Network Devices of a Data Center

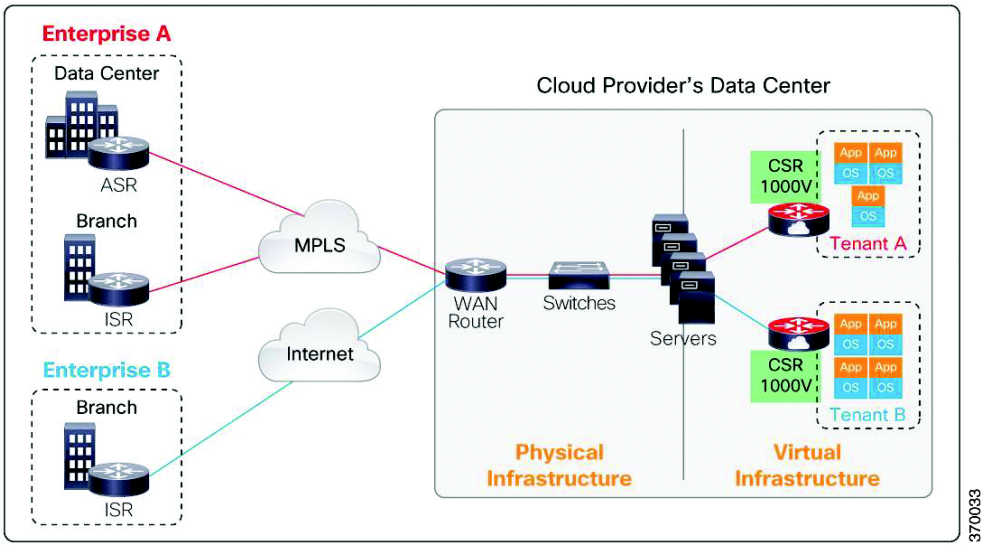
Prime Network supports the following virtual network devices of a data center:

- Cisco Cloud Service Router (CSR) 1000v
- Cisco Nexus 1000V
- Virtual Security Gateway

Viewing the CSR 1000v Properties

The Cisco Cloud Services Router (CSR) 1000V is a single-tenant router in virtual form-factor that delivers comprehensive WAN gateway functionality to multi-tenant provider-hosted clouds. It is a software router that an enterprise or a cloud provider can deploy as a virtual machine (VM) in a provider-hosted cloud.The Cisco CSR 1000V provides selected Cisco IOS XE features on a virtualization platform. It also provides secure connectivity from the enterprise premise (such as a branch office or data center) to the public or private cloud. Figure 28-11 depicts the deployment of CSR 1000v on a provider hosted cloud:

Figure 28-11 Deployment of CSR 1000v on a Provider Hosted Cloud



The Cisco CSR 1000V serves primarily as a router per tenant. In other words, since the CSR 1000v is situated on the tenant's side, each tenant gets its dedicated routing instance and services (along with its own VPN connections, firewall policies, QoS rules, access control, and so on).

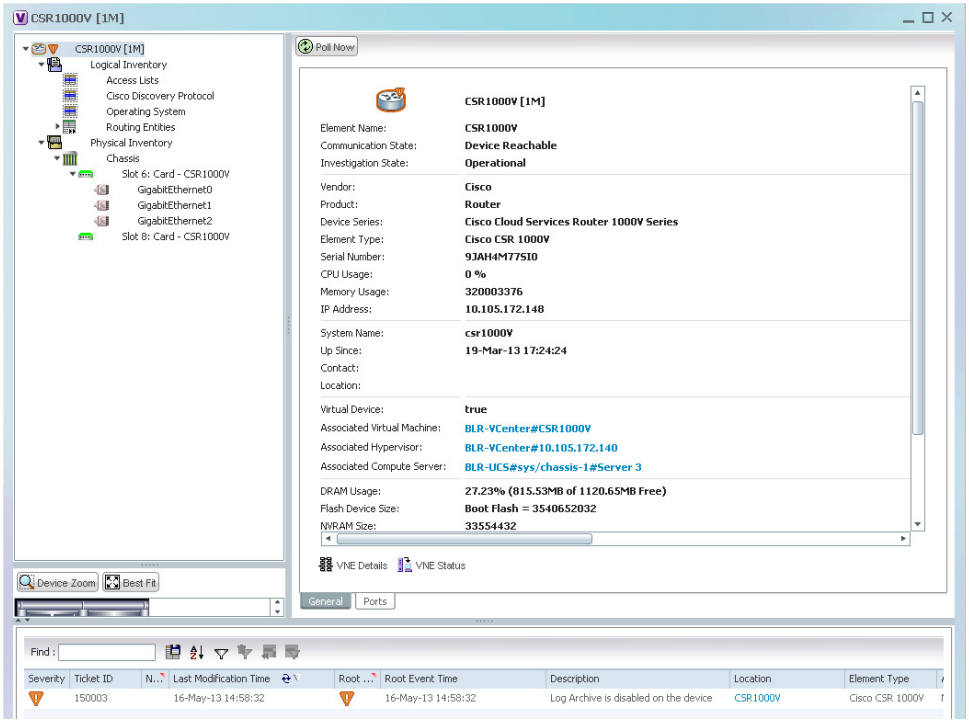
To view the CSR 1000v properties:

Step 1 In the Vision client, open a map that contains the CSR 1000v device.

Step 2 Right-click and choose the **Inventory** option to open the Inventory window.

Step 3 In the **Inventory** window, click the device name to view the Element properties as shown in Figure 28-12. For more information about the properties window, see Drilling Down into the Properties of a Network Element, page 8-2.

Figure 28-12 Element Properties Window



Note The CSR 1000v device is associated with a hypervisor and physically available on a blade server. The links to the hypervisor and blade server are displayed in the Properties window.

Step 4 Under the **Logical Inventory** node, you can view the Access Lists, Cisco Discovery Protocol, Operating System requirements, and Routing Entities. For more information about the logical inventory properties, see Viewing the Logical Properties of a Device (Traffic, Routing, Information, Tunnels, Data Link Aggregations, Processes), page 8-21.

Step 5 Under the **Physical Inventory** node, you can view the two slots under the Chassis node.

Note The first slot contains the Route Processor with three interface ports—one for management and the other two for data traffic. The second slot contains the Embedded Services Processor.

Viewing the Nexus 1000V Properties

The Cisco Nexus 1000V device is a a distributed virtual switch solution that is fully integrated within VMware Virtual Infrastructure, including VMware vCenter for the virtualization administrator. This solution off loads the configuration of the virtual switch and port groups to the network administrator to enforce a consistent datacenter network policy. It manages a data center defined by a VirtualCenter. Each server in the data center is represented as a module and can be managed as if it were a module in a physical Cisco switch.

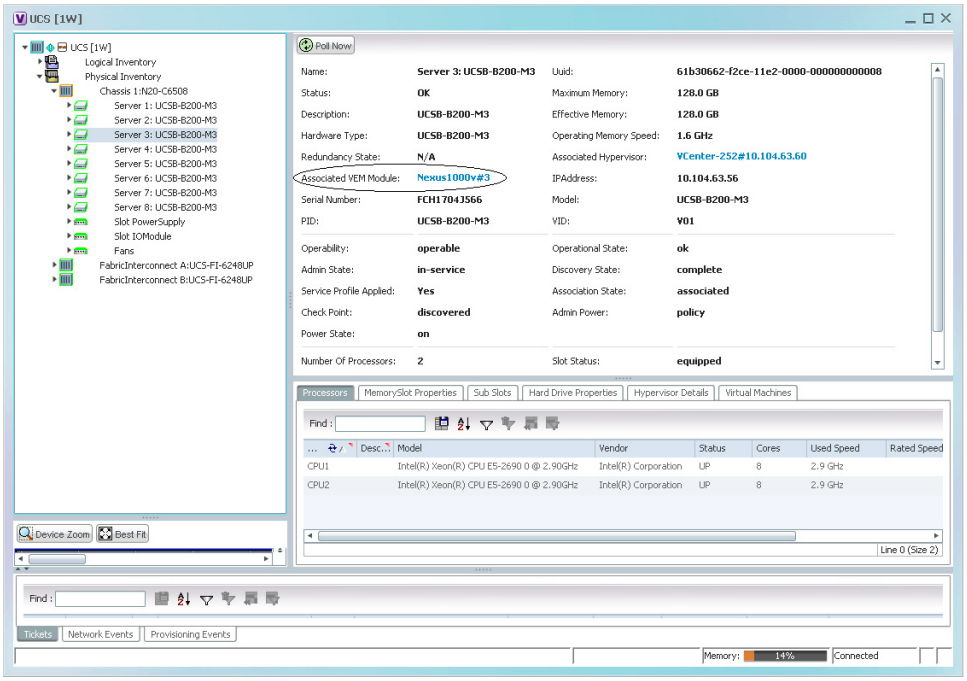
The Cisco Nexus 1000V has the following components that can virtually emulate a 66-slot modular Ethernet switch with redundant supervisor functions:

- Virtual Ethernet module (VEM)—The Virtual Ethernet Module (VEM) is one part of the Cisco Nexus 1000V device that actually switches data traffic. Several VEMs are controlled by one VSM. All the VEMs that form a switch domain should be in the same virtual Data Center as defined by VMware VirtualCenter.
- Virtual supervisor module (VSM)—The VSM is a standalone, external, physical or virtual appliance that performs the following functions for the Cisco Nexus 1000V system (that is, the combination of the VSM itself and all VEMs it controls):
  - Configuration.
  - Management
  - Monitoring.
  - Diagnostics.
  - Integration with VMware vCenter

In the Cisco Nexus 1000V, traffic is switched between virtual machines locally at each VEM instance. Each VEM also interconnects the local virtual machine with the rest of the network through the upstream access-layer network switch (blade, top-of-rack, end-of-row, and so forth). The VSM runs the control plane protocols and configures the state of each VEM accordingly, but it never forwards packets.

In Prime Network, you can view the connectivity between the Nexus 1000V device and the host and blade server as shown in Figure 28-13.

Figure 28-13 Connectivity between Nexus 1000V and host/blade server



In other words, you can view the hosts under vCenter to which the device provides switching support and the underlying blade servers that are connected to the device.

To view the connectivity:

Step 1 Right-click on the vCenter device and choose the **Inventory** option.

Step 2 In the Inventory window, choose **Logical Inventory > Compute Virtualization** > **Virtual Data Center** > **Host Servers** > *Host Server.*

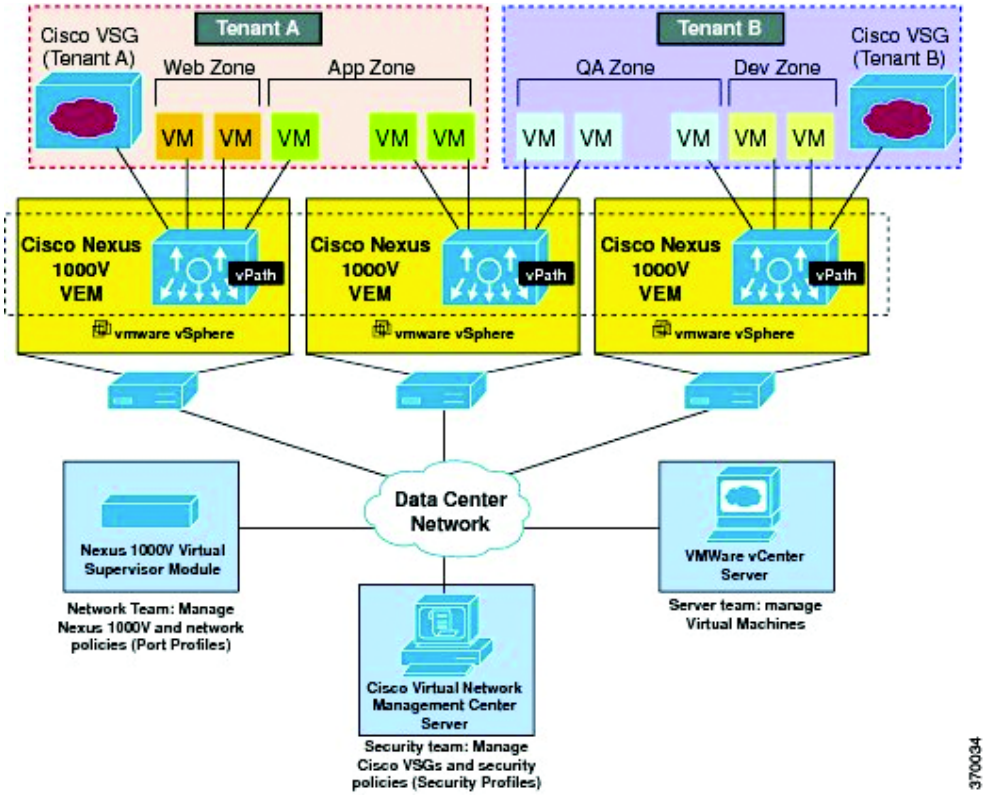
Step 3 In the content pane, click the link in the **Associated VEM Module** field. You can view the details of the UCS blade server of the Nexus 1000v device to which the vCenter is connected to.

Viewing the VSG Properties

The Cisco Virtual Security Gateway (VSG) is a virtual firewall appliance that provides trusted access to virtual data center and cloud environments. The Cisco VSG enables a broad set of multi tenant workloads that have varied security profiles to share a common compute infrastructure in a virtual data center private cloud or in a public cloud. By associating one or more virtual machines (VMs) into distinct trust zones, the Cisco VSG ensures that access to trust zones is controlled and monitored through established security policies.

Figure 28-14 depicts the deployment of VSG:

Figure 28-14 Deployment of VSG



The Cisco VSG operates with the Cisco Nexus 1000V in the VMware vSphere hypervisor, and the Cisco VSG leverages the virtual network service datapath (vPath) that is embedded in the Nexus 1000V Virtual Ethernet Module (VEM). A VEM can be associated to a Cisco VSG.

To view the VSG Properties:

Step 1 In the Vision client, open a map that contains the VSG device.

Step 2 Right-click and choose the **Inventory** option to open the Inventory window.

Step 3 In the **Inventory** window, click the device name to view the Element properties. For more information about the properties window, see Drilling Down into the Properties of a Network Element, page 8-2

Note The VSG device is associated with a hypervisor and physically available on a blade server. The links to the hypervisor and blade server are displayed in the Properties window.

Step 4 Under the **Logical Inventory** node, you can view the Access Lists, Cisco Discovery Protocol, Operating System requirements, and Routing Entities. For more information about the logical inventory properties, see Viewing the Logical Properties of a Device (Traffic, Routing, Information, Tunnels, Data Link Aggregations, Processes), page 8-21.

Step 5 Under the **Physical Inventory** node, you can view only one slot.

Viewing the Compute Server Support Details

Prime Network provides support for the following compute servers:

- UCS B-Series Servers—The Cisco UCS B-Series Blade Servers are crucial building blocks of the Cisco Unified Computing System and are designed to increase performance, energy efficiency, and flexibility for demanding virtualized and non virtualized applications. Each Cisco UCS B-Series Blade Server uses converged network adapters (CNAs) for access to the unified fabric. This design reduces the number of adapters, cables, and access-layer switches while still allowing traditional LAN and SAN connectivity.
- UCS C-Series Servers—Cisco UCS C-Series Rack Servers deliver unified computing in an industry-standard form factor to reduce total cost of ownership and increase agility
- Third party or Non-Cisco servers—Includes support for non-UCS servers such as HP, Dell or IBM.

In Prime Network, the UCS B-Series and UCS C-Series servers are modelled as part of the UCS VNE. The UCS C-Series (standalone) and non-Cisco servers are modelled as individual VNEs.

Note For a Cisco UCS device, you can also view the physical inventory, which includes the blade server, Fabric InterConnect and IO Modules. You can also view the physical layout and topology for the UCS device on the map. For more information, see Viewing the Map Node for an UCS Network Element, page 28-25.

Note There is also a direct correlation between the blade server and its associated virtual entities. For instance, if the blade server is shut down, then the associated entities such as the virtual machines and hypervisor will also be shut down.

To view the UCS server details:

Step 1 In the Vision client, right-click a UCS device and choose the **Inventory** option.

Step 2 In the Inventory window, expand the **Physical Inventory** node.

Step 3 Select *Chassis* > *Blade Server*. The blade server configuration details are displayed in the content pane as shown in Figure 28-15.

Figure 28-15 Blade Server Configuration Details

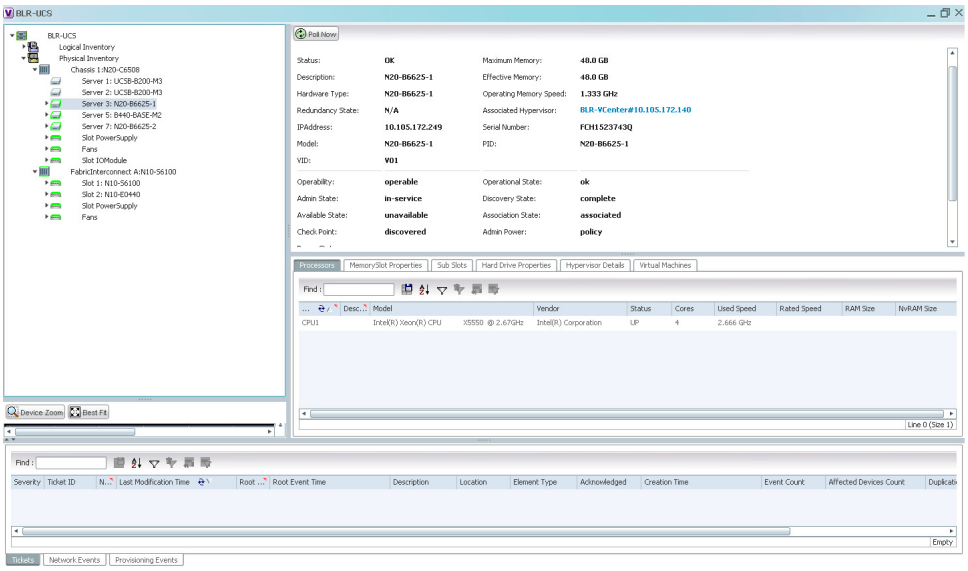


Table 28-10 describes the configuration details of a blade server.

Table 28-10 Blade Server Configuration Details

Field Name	Description
Name	The name of the blade server.
Uuid	The unique ID of the blade server.
Status	The status of the server.
Maximum Memory	The total amount of memory (in gigabytes) available on the server.
Description	The description of the server.
Effective Memory	The amount of memory (in gigabytes) currently available to the server.
IP Address	The IP address of the blade server.
Operating Memory Speed	The speed (in GHz) at which the operating memory can be accessed.
Redundancy State	The redundancy state of the server, which can be Online or Offline.
Associated Hypervisor	The hypervisor associated to the blade server. Click this link to view the hypervisor details.
Associated VEM Module	The Virtual Ethernet Module (VEM) associated to the server.
Sub Slots tab	
Equipment	The name of the equipment.
Type	The type of equipment.
Processors tab	
Name	The name of the processor used by the blade server.

Table 28-10 Blade Server Configuration Details (continued)

Field Name	Description
Description	The description of the processor used by the blade server.
Model	The processor model used by the blade server.
Vendor	The vendor of the processor.
Status	The status of the processor.
Cores	The number of cores used by the blade server.
Used Speed	The actual used speed of the processor, in GHz.
Rated Speed	The rated speed of the processor, in GHz.
RAM Size	The RAM size of the processor, in GB.
NvRAM Size	The NvRAM Size of the processor, in GB.
Memory Slot Properties tab	
Slot Name	The name of the memory slot.
Speed	The memory slot speed, in GHz.
Memory Capacity	The maximum memory capacity of the hard drive, in GB.
Serial Number	The serial number of the memory slot.
Status	The status of the memory slot.
Hard Drive Properties	
Model Name	The model name of the hard drive.
Storage Capacity	The total storage capacity of the hard drive, in GB.
Free Space	The total space available for usage in the hard drive.
isFRU	Indicates whether the hard drive is removable.
Drive Type	The type of hard drive, which can be any one of the following: • Fixed Disk • RAM Disk • Flash Memory • Network Disk • Removable Disk
Status	The status of the hard drive.
Hypervisor tab	
Fault Tolerance Version	The fault tolerance version of the hypervisor.
Uuid	The unique ID of the hypervisor.
Model	The model of the hypervisor.
EvcMode	The Enhanced vMotion Capability (Evc) mode of the hypervisor.
Virtual Data Center Name	The name of the virtual data center of the hypervisor.
Isv Motion Enabled	Indicates whether the Lsv motion is enabled.
MAC Address	The MAC address of the hypervisor.

Table 28-10 Blade Server Configuration Details (continued)

Field Name	Description
Fault Tolerance Enabled	Indicates whether fault tolerance service is enabled or not. This service provides continuous availability by protecting the primary virtual machine with a secondary virtual machine that runs simultaneously on a separate host.
Software Type	The type of software used by the hypervisor.
IP Address	The IP address of the hypervisor.
Name	The name of the hypervisor.
State	The status of the hypervisor, which could be Running, Runnable, Waiting, Exiting, or Other.
Vendor	The name of the vendor for the hypervisor.
Virtual Machines tab	
Virtual Machine	The name of the virtual machine associated with the blade server. The severity of the blade server is also displayed along with the name.
IP Address	The IP address of the virtual machine.
DNS Name	The domain name of the virtual machine.
MAC Address	The MAC address of the virtual machine.
State	The status of the virtual machine, which could be Powered On, Powered Off, or Suspended.
VM Version	The hardware version of the virtual machine.
Virtual CPU	The number of virtual CPUs configured for the virtual machine on the virtual machine.
Fault Tolerance Enabled	Indicates whether fault tolerance service is enabled or not.

Note The Hypervisor and Virtual Machine tabs will be displayed only if the compute server is managed by a VMware VCenter, which is monitored by the same instance of Prime Network.

Viewing the Non Cisco Server Details

In Prime Network, non Cisco servers such as IBM, HP, and Dell are modeled as individual VNEs. These servers are modeled based on the operating system installed on them, and not on the native hardware pr management applications (except Supported Management Applications) running on these hardware.

The following operating systems are supported for modeling:

- Windows
- Linux
- VMWare ESXi
- Any other operating system that supports MIB2, RFC-1213-MIB, HOST-RESOURCE-MIB

Supported Management Applications

Prime Network supports only the following Linux-based management applications as individual VNEs:

- Cisco Prime Access Registrar (CPAR)
- Cisco Prime Network Registrar (CPNR)

Note When ESXi is modeled on VMWare, ensure that SSH is also modeled along with it.

To view the non Cisco server details:

Step 1 In the Vision client, right-click Non-Cisco device and choose the **Inventory** option.

Step 2 In the Inventory window, expand the **Physical Inventory** node.

Step 3 Select the **Server** node. The server configuration details are displayed in the content pane along with the details of the operating system available in the server. The following tabs are also available:

- Ports
- Processors
- Hard Drive Properties
- Memory Slot Properties
- Hypervisor Details

Viewing the Mapping between the Compute Server and Hypervisor

The Cisco and non Cisco servers also support hypervisory functions to support various operating systems. Prime Network allows you to view the mapping details between the compute server and the hypervisor.

To view the mapping between the compute server and hypervisor:

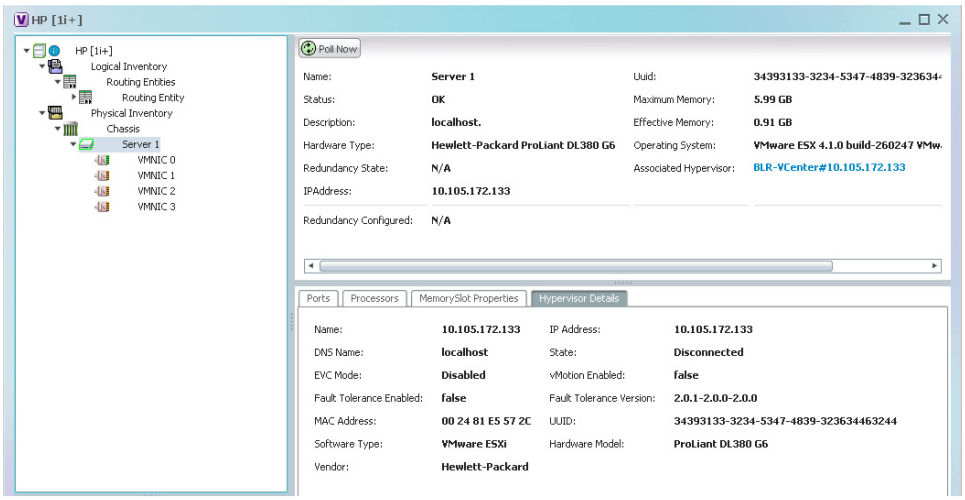
Step 1 In the Vision client, right-click a UCS device and choose the **Inventory** option.

Step 2 In the Inventory window, expand the **Physical Inventory** node.

Step 3 Select **Chassis** > *Blade Server*. The blade server configuration details are displayed in the content pane.

Step 4 Click the link in the **Associated Hypervisor** field to go to the relevant hypervisor under the vCenter node. The details of the hypervisor are displayed in the content pane, which also includes the **Associated Compute Server** field that contains a link to the relevant compute server.

Each blade server under the Chassis in the Physical inventory will link to the associated hypervisor. This is also applicable to the third party servers. In other words, the third party server also contains a link to the associated hypervisor.



Viewing the Storage Area Network Support Details

A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to make storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network by other devices.

A virtual storage area network (VSAN) is a collection of ports from a set of connected Fibre Channel switches, that form a virtual fabric. Ports within a single switch can be partitioned into multiple VSANs, despite sharing hardware resources. Conversely, multiple switches can join a number of ports to form a single VSAN.

Most storage networks use the SCSI protocol for communication between servers and disk drive devices. A mapping layer to other protocols is used to form a network.

In Prime Network, the following technologies are used for storage area networks:

- Fibre Channel (FC)—Fibre Channel is a high-speed network technology (commonly running at 2-, 4-, 8- and 16-gigabit speeds) primarily used for storage networking. It was primarily used in the supercomputer field, but has now become the standard connection type for storage area networks (SAN) in enterprise storage. Fibre Channel can help with design of large-scale, storage-intensive systems. It can also provide a solution that allows rapid storage and retrieval of information, while simplifying the interconnection of different components in the system
- Fibre Channel over Ethernet (FCoE)—Fibre Channel over Ethernet is an encapsulation of Fibre Channel frames over Ethernet networks. This allows Fibre Channel to use 10 Gigabit Ethernet networks (or higher speeds) while preserving the Fibre Channel protocol. It drastically reduces the number of I/O adapters, cables, and switches in the data center, while providing a wire-once, agile infrastructure. Based on lossless, reliable 10 Gigabit Ethernet, FCoE networks combine LAN and multiple storage protocols on a single converged network.

For information on the devices that support VSAN, refer to *Cisco Prime Network 4.1 Supported VNEs*.

Note The Cisco Fabric InterConnect UCS devices only supports the Fibre Channel over Ethernet technology.

Viewing the Storage Area Network Configuration Details

To view the VSAN configuration details:

Step 1 In the Vision client, right-click the required device and choose the **Inventory** option.

Step 2 In the Inventory window, expand the **Logical Inventory** node.

Step 3 Select **VSANs >** *VSAN service*. The VSAN configuration details are displayed in the content pane as shown in the Figure 28-16.

Figure 28-16 VSAN Configuration Details

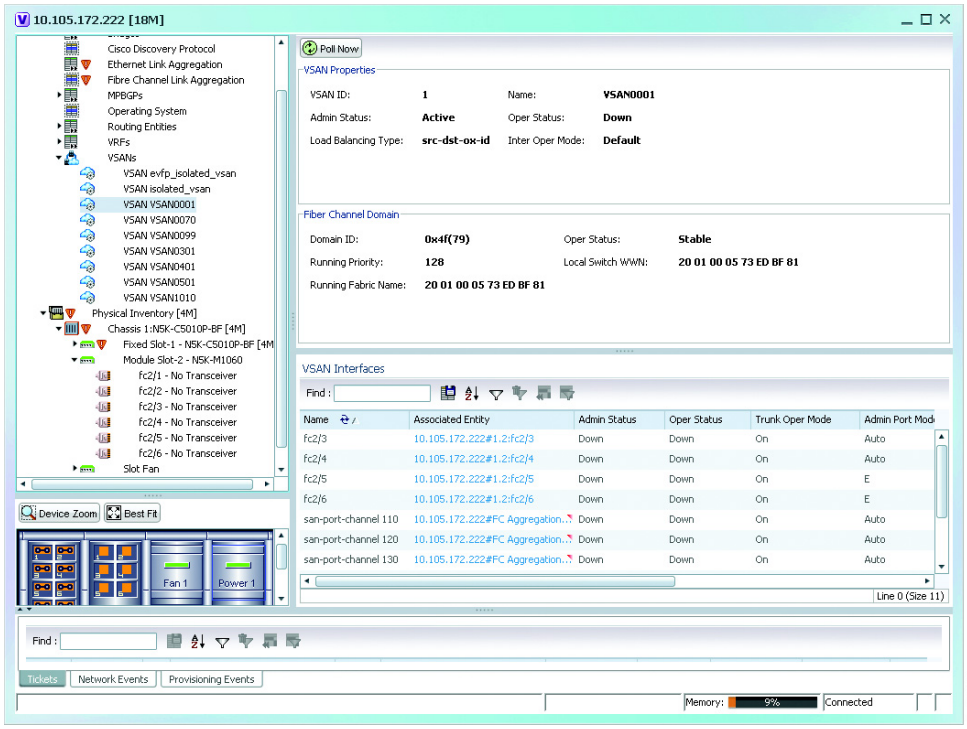


Table 28-10 describes the VSAN configuration details.

VSAN Configuration Details

Field Name	Description
VSAN ID	The unique identification code of the VSAN.
Name	The name of the VSAN.
Admin Status	The administrative status of the VSAN, which can be any one of the following: • Active—Indicates that the VSAN is configured and enabled and that you can activate the services of the VSAN. • Suspended—Indicates that the VSAN is configured, but not enabled. Any port configured in this VSAN will also be disabled.
Oper Status	The operational status of the VSAN, which can be any one of the following: • Up • Down
Load Balancing Type	The method used for load balancing path selection in the VSAN, which can be any one of the following: • Source destination ID • Originator Exchange OX ID
Inter Oper Mode	The inter operations mode.
Associated VLAN	The name of the VLAN associated to the VSAN.
In Order Delivery	The in order delivery of the VSAN.
MTU	The maximum number of transmission units (in bytes) of the VSAN.
Fibre Channel Domain	
Domain ID	The domain ID of the Fibre Channel domain.
Oper Status	The operational status of the Fibre Channel domain, which can be any one of the following: • Stable • Enable • Disable
Running Priority	The assigned priority of the switch. This field defaults to 128.
Local Switch WWN	The local switch World Wide Name (WWN) for the Fibre Channel, which is a unique identifier in the SAN.
Running Fabric Name	The WWN number of the Fabric to which the switch belongs.
VSAN Interfaces	
Name	The name of the VSAN technology interface.
Associated Entity	The associated Fibre Channel interface, which when clicked will take you to the relevant Fibre channel node under the Chassis node.

VSAN Configuration Details (continued)

Field Name	Description
Admin Status	The administrative status of the interface, which can be any one of the following: • Up • Down
Oper Status	The operational status of the interface, which can be any one of the following: • Up • Down • Trunking
Trunk Oper Mode	The operational status of the trunk mode for a VSAN interface, which can be any one of the following: • On • Off • Auto
Trunk Admin Mode	The status of the trunk administrative mode.
Admin Port Mode	The administrative port mode of the interface, which can be any one of the following: • E—Expansion port, where the interface functions as a fabric expansion port. This port may be connected to another E port to create an Inter-Switch Link (ISL) between two switches. • F—Fabric port, where an interface functions as a fabric port. This port may be connected to a peripheral device (host or disk) operating as an N port. • NP—When the switch is operating in NPV mode, the interfaces that connect the switch to the core network switch are configured as NP ports. • TE—Trunking E port, where the interface functions as a trunking expansion port. It may be connected to another TE port to create an extended ISL (EISL) between two switches. • TF—Trunking fabric port, where an F port with trunk mode enabled becomes operational. • TNP—Trunking NP port, where an NP port with trunk mode enabled becomes operational. • SD—SPAN Destination port, where the interface functions as a switched port analyzer. • FX—An interface configured as FX port can operate in either F port or FL port mode. • Auto—An interface configured in auto mode can operate in F port, E port, or TE port, which is determined during interface initialization.

VSAN Configuration Details (continued)

Field Name	Description
Oper Port Mode	The operational port mode of the port.
Allowed VSANs	The VSANs that are active and allowed to receive data for the specified VSAN range. The port will allow traffic for the VSANs specified here.
Native VSAN	The VSAN ID to which the FC port belongs.
Virtual Interface	The VFC ID, which is displayed only if the VFC is configured to a port and the port is bound to a VF.
Fibre Channel	The fibre channel associated to the VSAN.
FCS Database Entries tab	
Local Interface Name	The name of the local interface for VSAN.
Local Connected Interface	The local interface connected to the VSAN.
Local Port	The name of the local port for the VSAN.
Remote Port	The name of the remote port for the VSAN.
Remote Node	The remote node for the VSAN.
Remote Permanent Port	The name of the remote permanent port.
Remote Node IP Address	The IP address of the remote node.
Remote Port Name	The name of the remote port.

Note For more information about the alarms relating to FC and FCoE, see the *Cisco Prime Network 5.3 Supported Service Alarms*.

Viewing the FC Interface Details

To view the FC Interface details:

Step 1 In the Vision client, right-click the required device and choose the **Inventory** option.

Step 2 In the Inventory window, expand the **Physical Inventory** node.

Step 3 Select **Chassis** > *Module Slot* > *Fibre channel interface*. The FC interface details are displayed in the content pane.

Table 28-11 describes the FC configuration details.

Table 28-11 FC Configuration Details

Field Name	Description
Location Information	
Type	The type of fibre interface, which can be any one of the following: • Fibre Channel
Location	The location of the FC/FCoE interface.
Sending Alarms	Indicates whether the port is sending all alarms correctly.
Port Alias	The port alias of the interface.
Managed	The managed status.
Status	The status of the FC/FCoE interface.
Pluggable Transceiver	
Connector Type	The type of connector used for the interface.
Pluggable Port State	The status of the pluggable port in the interface.
VSAN Interface	
Name	The name of the VSAN technology interface.
Admin Status	The administrative status of the interface, which can be any one of the following: • Up • Down
Oper Status	The operational status of the interface, which can be any one of the following: • Up • Down • Trunking
Trunk Oper Mode	The operational status of the trunk mode for a VSAN interface, which can be any one of the following: • On • Off • Auto
Admin Port Mode	The administrative port mode of the interface.
Native VSAN	The VSAN ID to which the FC port belongs.
Fibre Channel	
Name	The name of the fibre channel.
TxB2B Credit	The Transmit Buffer to Buffer Credit value for the fibre channel. **Note** Buffer to Buffer credit is a flow control mechanism that ensure that fibre channel switches do not run out of buffers so that the switches do not drop frames.

Table 28-11 FC Configuration Details (continued)

Field Name	Description
RxB2B Credit	The Receive Buffer to Buffer Credit value for the fibre channel. This value is configured for each interface.
Admin Status	The administrative status of the fibre channel, which can be any one of the following: • Up • Down
Oper Status	The operational status of the fibre channel, which can be any one of the following: • Up • Down
Port WWN	The World Wide Name (WWN) of the port for the Fibre Channel.

Viewing the FCoE Interface Details

To view the FCoE Interface details:

Step 1 In the Vision client, right-click the required device and choose the **Inventory** option.

Step 2 In the Inventory window, expand the **Physical Inventory** node.

Step 3 Select **Chassis** > *Fixed Slot* > *FCoE interface*. The FCoE interface details are displayed in the content pane. The following information is displayed in the content pane:

Table 28-12 describes the FCoE configuration details.

Table 28-12 FCoE Configuration Details

Field Name	Description
VLAN Interface tab	
Mode	The VLAN interface configuration mode, which can be any one of the following: • Unknown • Access • Dynamic Auto • Dynamic Desirable • Trunk • Dot 1Q Tunnel
VLAN Type	The VLAN interface type, such as Layer 2 VLAN.
Native VLAN ID	VLAN Identifier (VID) associated with this VLAN. The range of the VLAN ID is 1 to 4067.

Table 28-12 FCoE Configuration Details (continued)

Field Name	Description
Allowed VLANs	The list of the VLANs allowed on this VLAN interface.
TenGigabit Ethernet	
MAC Address	The MAC address.
Ethernet LMI Enabled	Indicates whether the Ethernet Local Management Interface (LMI) is enabled.
Discovery Protocols	
Discovery Protocol Type	The type of discovery protocol, which can be CDP or LLDP.
Info	Displays more information about the protocol type, which can be any one of the following: • for CDP—Up or Down • for LLDP—Tx (Enabled/Disabled) or Rx (Enabled/Disabled)
Ethernet CSMA/CD	
Admin Status	The administrative status of the Ethernet Carrier sense multiple access with collision detection (CSMA/CD).
Oper Status	The operational status of Ethernet CSMA/CD.
Port Type	The type of port.
Last Changed	The date and time when the ethernet status was last changed.
Maximum Speed	The maximum bandwidth.
Port Description	The description of the port as defined by the user.
MTU	The size of the Maximum Transmission Unit (MTU) for the interface.
Internal Port	Indicates whether an internal port is available.

Note For more information about the other sections in this window, see Table 28-11.

Viewing the Fibre Channel Link Aggregation

To view the Fiber Channel Link Aggregation details:

Step 1 In the Vision client, right-click the required device and choose the **Inventory** option.

Step 2 In the Inventory window, expand the **Logical Inventory** node.

Step 3 Select the **Fibre Channel Link Aggregation** option. The list of aggregations are displayed in the content pane.

Step 4 Double-click on an aggregation. The **Fibre Channel Link Aggregation Properties** window is displayed as shown in Figure 28-17.

Figure 28-17 Fibre Channel Link Aggregation

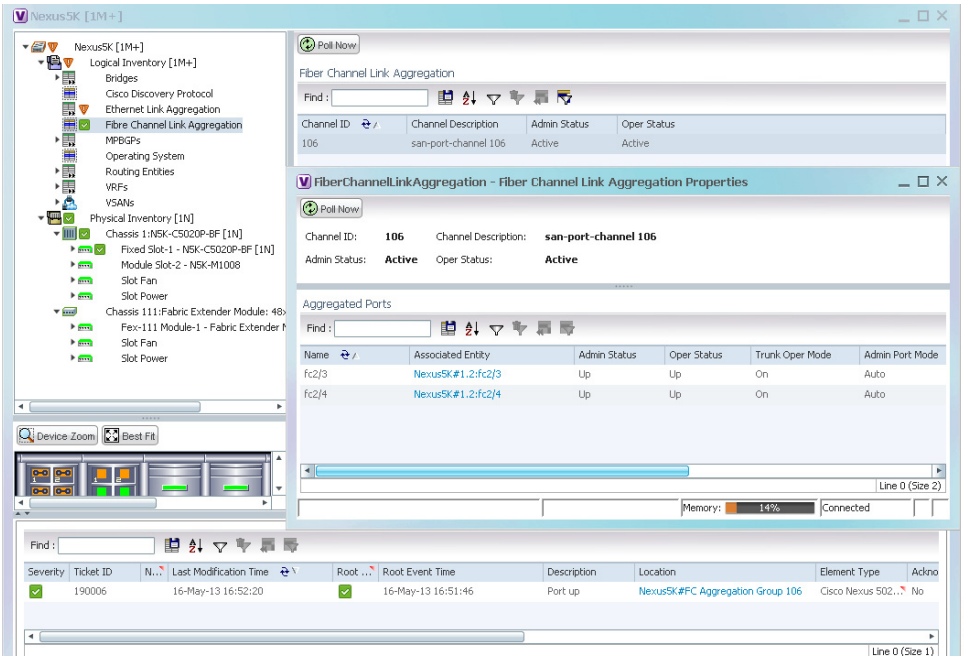


Table 28-13 describes the Fibre Channel Link Aggregation Properties.

Table 28-13 Fibre Channel Link Aggregation Properties

Field Name	Description
Channel ID	The unique identification code for the aggregation.
Channel Description	The description of the aggregation.
Admin Status	The administrative status of the aggregation.
Oper Status	The operational status of the aggregation.
Aggregated Ports	
Name	The name of the port that is included in the aggregation.
Associated Entity	The associated port, which when clicked will take you to the relevant FC or FCoE port.
Admin Status	The administrative status of the associated port.
Oper Status	The operational status of the associated port.
Trunk Oper Status	The Trunk operational status of the associated port.
Admin Port Mode	The administrative port mode of the associated port.
Oper Port Mode	The operational port mode of the associated port.
Allowed VSANs	The number of VSANs that are active and allowed to receive data.
Native VSAN	The number of native VSANs.
Virtual Interface	The name of the virtual interface for the VSAN.

Viewing Fibre Channel Links Between Devices in a Map

To view the FC links between devices in a map:

Step 1 In the Vision client, open the map that contains the Fibre Channel links.

Step 2 Click on the Filter icon in the navigation menu and select only the **Fibre Channel** check box. Click **OK**. The map that you have opened only displays the Fibre Channel links between devices. For more information about viewing these link properties, see Viewing the Map Node for an UCS Network Element, page 28-25.

Searching for Compute Services

The Compute Services Search feature in Prime Network allows you to search for the following entities:

- Virtual Machines (can be found in the VCenter device)
- Hypervisors (can be found in the VCenter device)
- Bare Metal (For example, the blade servers, which can be found in a UCS device)

To use the Compute services search feature:

Step 1 In the Vision client, select **Network Inventory** > **Compute Services**.

Step 2 In the **Compute Services** window, select the **Search** radio button.

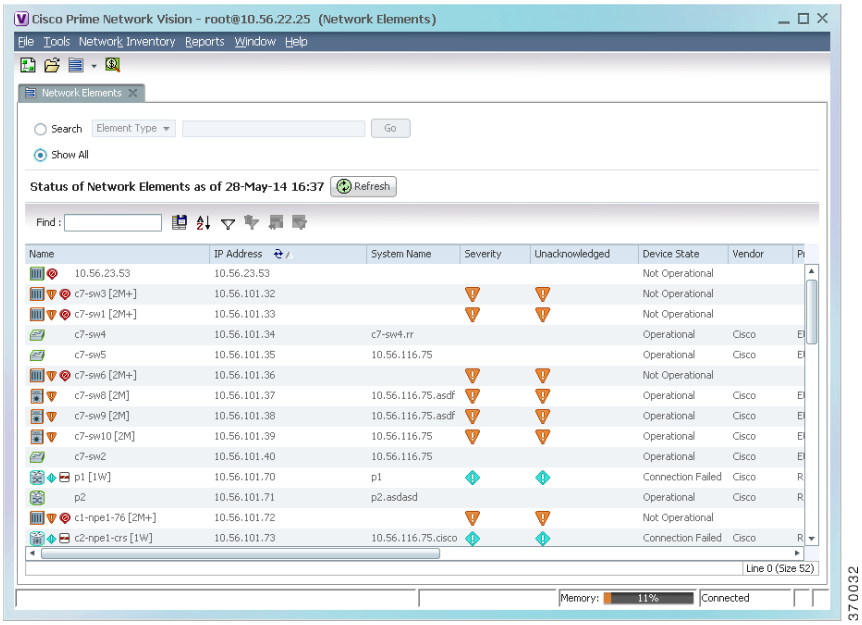
Step 3 From the Search drop down box, select any one of the following options:

- DNS Name
- IP Address
- Name

Step 4 In the text box available, enter the name based on the option selected in the Search drop-down box.

Step 5 Click **Go**. The entity details are displayed in the table below as shown in Figure 28-18.

Figure 28-18 Compute Service Search



Note You can also click the **Show All** radio button to view a list of devices with hypervisors, blade servers, and virtual machines.

Table 28-14 describes the compute services search results.

Table 28-14 Compute Services Search Result

Field Name	Description
Severity	The severity of the device.
Name	The name of the device.
Service Type	The service type, which can be Virtual Machine, Hypervisor, or Bare Metal.
IP Address	The IP address of the device.
DNS Name	The DNS name of the device.
State	The status of the device.
Host	The host server associated to the device, which when clicked will take you to the relevant host node.
Compute Server	The compute server associated to the device, which when clicked will take you to the relevant node.
Compute System	The device where the blade server is available, which when clicked will take you to the relevant node.

Monitoring Virtualized Service Module

Virtualized Service Module (VSM)

The Cisco ASR 9000 VSM Card is a service card built specifically for the Cisco ASR9000 platform. The Cisco ASR 9000 VSM Card is supported on any slot on the Cisco ASR 9000 Series Aggregation Services Router (ASR90xx and ASR99xx). The Cisco ASR 9000 VSM Card has the capability to run a hypervisor on it. The hypervisor (example KVM) can host a single VM.

Service Enablement

Service Enablement provides the ability to install and uninstall a service without impacting the other services running on the Cisco ASR 9000 VSM Card. Service enablement allows you to instantiate a service instance by specifying the name and location of the service image package and the target of the service.

For more information on virtual service package and its installation, refer Configuring Virtual Services on the Cisco ASR 9000 Series Router.

Viewing VSM Properties in Physical Inventory

To view VSM properties in the physical inventory:

Step 1 In the Vision client, double-click the device in which the VSM card is configured.

Step 2 In the inventory window, expand the Physical Inventory node.

Step 3 Choose **Chassis** > **Server <Number>: Card A9K-VSM-500**. The server configuration details are displayed in the content pane.

Table 28-15 describes configuration details of the server configured with ASR 9000 series VSM service information.

Table 28-15 Server Configuration Details with ASR 9000 series VSM Service

Field Name	Description
Name	The name of the server.
Uuid	The unique ID of the server.
Status	The status of the server.
Maximum Memory	The total amount of memory (in gigabytes) available on the server.
Description	Description of the VSM card. For example, ASR9000 series Virtualized Services Module.
Effective Memory	The amount of memory (in gigabytes) currently available to the server.
Hardware Type	Hardware type of the VSM card. For example, cevModuleA9KVSM500.
Hardware Version	Hardware version of the VSM card. For example,V00.

Table 28-15 Server Configuration Details with ASR 9000 series VSM Service (continued)

Field Name	Description
Software Version	Operating system software version.
Redundancy State	The redundancy state of the server: • Online • Offline • N/A—Redundancy state is not supported.
Serial Number	The serial number of the ASR 9000 series VSM card.
Cores	The number of cores used by the server.
Redundancy Configured	Redundancy configured on the server: • Working—Redundancy is configured and enabled. • None—Redundancy is not configured • N/A—Redundancy is not supported
Associated Host	The Kernal Virtual Machine (KVM) associated to the server. Click this link to view the related KVM host server node under the logical inventory.
Processors tab	
Name	The name of the KVM associated server.
Description	The description of the processor used by the server.
Model	The processor model used by the server.
Vendor	The vendor of the processor.
Status	The status of the processor.
Cores	The number of cores used by the server.
Used Speed	The actual used speed of the processor, in GHz.
Rated Speed	The rated speed of the processor, in GHz.
RAM Size	The RAM size of the processor, in GB.
NvRAM Size	The NvRAM Size of the processor, in GB.
Memory Slot Properties tab	
Slot Name	The name of the memory slot.
Speed	The memory slot speed, in GHz
Memory Capacity	The maximum memory capacity of the hard drive, in MB.
Serial Number	The serial number of the memory slot.
Status	The status of the memory slot.
Sub Slots tab	
Equipment	The name of the equipment in the sub slot.
Type	The type of equipment in the sub slot.
Hardware Type	Name of the sub slot hardware card.
Hard Drive Properties tab	

Table 28-15 Server Configuration Details with ASR 9000 series VSM Service (continued)

Field Name	Description
Model Name	The model name of the hard drive.
Storage Capacity	The total storage capacity of the hard drive, in GB.
Free Space	The total space available for usage in the hard drive.
FRU	Indicates whether the hard drive is removable.
Drive Type	N/A—Drive Type is not supported.
Status	The status of the hard drive.

Step 4 Choose **Server <Number>: Card A9K-VSM-500** > **Subslot <Number>: Subcard – A9K-MODULEv**. The slot details configured with VSM card is displayed in the content pane.

Table 28-16 describes slot configuration details with ASR 9000 series VSM service information.

Table 28-16 Slot Configuration Details

Field Name	Description
Name	The name of the slot configured in the server.
Status	The status of slot in the server.
Description	The description for the slot configured in the server. For example, Virtual Module.
Hardware Type	Hardware type of the VSM card. For example, cevModuleA9KVSM500.
Hardware Version	None.
Software Version	None.
Redundancy State	N/A—Redundancy state is not supported.
Serial Number	N/A—Serial number is not supported.
Redundancy Configured	N/A—Redundancy configured property is not supported.
Ports	
Location	Location of the port in the device, using the format slot.module/port, such as 2.0TenGigE0/2/1/0.
Type	Port type. For example, fiber optic port.
Sending Alarms	Whether or not the element is configured for sending alarms (True or False)
Pluggable Transceiver	For the Pluggable port type, indicates that the port can hold a pluggable transceiver.
Port Alias	Name used in the device CLI for the port.

Table 28-16 Slot Configuration Details (continued)

Field Name	Description
Managed	Whether or not the port is managed: True or False.
Status	Port status: OK or one of the following: • Major—Port is operationally down • Disabled—Port is administratively down (someone purposely shut the port down) • Out—Port has been physically removed

Step 5 Choose **Server No: Card A9K-VSM-500** > **Subslot <Number>: Subcard – A9K-MODULEv** > **Interface Name**. The port details configured with VSM card is displayed in the content pane.

You can view the information displayed for the interface in the physical inventory.

The following information is displayed, depending on the interface and its configuration:

- Location information that includes the physical interface port number with status.
- TenGigabit Ethernet details.
- Discovery Protocols details.
- Ethernet CSMA/CD that includes the port description with ASR 9000 series VSM card information.
- DWDM properties.

Viewing VSM Properties in Logical Inventory

To view VSM properties in the logical inventory:

Step 1 In the Vision client, double-click the device in which the VSM card is configured.

Step 2 In the inventory window, expand the Logical Inventory node.

Step 3 Choose **Compute Virtualization**> **Virtual DataCenter - Default** > **Host Servers** > **Host server (KVM)**. The configuration details of KVM host server are displayed in the content pane.

Table 28-17 describes KVM host configuration details.

Table 28-17 KVM Host Configuration Details

Field	Description
Uuid	The unique ID of the KVM host server.
Model	The model name of the KVM host server. For example, A9K-VSM-500.
Isv Motion Enabled	Indicates whether the Isv motion is enabled.
Software Version	Software version used by KVM host server.

Table 28-17 KVM Host Configuration Details (continued)

Field	Description
Fault Tolerance Enabled	True or False. Indicates whether the fault tolerance service is enabled or not. This service provides continuous availability by protecting the primary virtual machine with a secondary virtual machine that runs simultaneously on a separate host.
Host Description	The description of the KVM host server.
Name	The name of the KVM host server.
State	The status of the hypervisor that can be Running, Runnable, Waiting, Exiting, Connected, or Disconnected.
Vendor	The name of the vendor for the KVM host server.
Associated Compute Server	The compute server associated to the KVM host server. Click this link to view the related host server node configured with the Cisco ASR 9000 series VSM service information under the physical inventory.
Hypervisor tab	
Name	Name of the hypervisor running on the host server.
Hypervisor Type	Type of the hypervisor.
Software Type	Type of software used by the hypervisor.
State	State of the hypervisor that can be Running, Runnable, Waiting, Exiting, or Other.
Version	Software version running on KVM host server.
Processors tab	
Name	The name of the KVM associated server.
CPU	Number of CPUs running in the hypervisor.
Cores Per CPU	Number of threads running in the processor.
Hyper Threading Enabled	Whether the processor uses Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following: • False—The processor does not permit hyperthreading. • True—The processor allows for the parallel execution of multiple threads.
Statistics Tab	
CPU Usage	CPU usage of the virtual machine, in GHz.
Memory Usage	Memory usage of the virtual machine, in MB.

Table 28-17 KVM Host Configuration Details (continued)

Field	Description
CPU Allocation tab	
Allocatable	Maximum CPU allocation for the virtual machine, in GHz.
Reserved	The overhead CPU allocation for the virtual machine, in GHz.
Unlimited Provision	Unlimited maximum allocation capacity availability check for the virtual machine. The value is either true or false.
Memory Allocation tab	
Allocatable	Memory allocation for the virtual machine, in MB.
Unallocated	Memory unallocated for the virtual machine, in MB.
Reserved	The overhead memory allocation for the virtual machine, in MB.
Unlimited Provision	Unlimited maximum allocation capacity availability check for the virtual machine. The value is either true or false.
Interfaces tab	
Name	Interface name.
Physical Termination Point	Associated link to the physical interface.
Virtual Machine tab	
Name	The name of the virtual machine.
State	Execution state of the virtual machine, which could be Powered On, Powered Off, or Suspended.
VM Version	Hardware version of the virtual machine.
Virtual CPU	Number of virtual CPUs configured for the virtual machine on the host server.
Fault Tolerance Enabled	Indicates whether fault tolerance service is enabled or not. This service provides continuous availability by protecting the primary virtual machine with a secondary virtual machine that runs simultaneously on a separate host.
Software Type	Type of the software used by the virtual machine.
UUID	The unique ID of the virtual machine.
VM ID	The unique identification code for the virtual machine.
Profile Name	The name of the profile created for monitoring the virtual service gateway configuration. This property is not supported.

Step 4 Choose **Compute Virtualization** > **Virtual DataCenter - Default** > **Host Servers** > **Host server (KVM)** > **WSG**. The configuration details of virtual service gateway such as Wireless Security Gateway (WSG) are displayed in the content pane.

Table 28-18 describes virtual service gateway configuration details.

Table 28-18 Virtual Service Gateway Configuration Details

Field	Description
Name	The name of the virtual service gateway.
State	Execution state of the virtual machine that can be Powered On, Powered Off, or Suspended.
VM Version	Hardware version of the virtual machine.
Virtual CPU	Number of virtual CPUs configured for the virtual machine on the host server.
Fault Tolerance Enabled	True or False. Indicates whether fault tolerance service is enabled or not. This service provides continuous availability by protecting the primary virtual machine with a secondary virtual machine that runs simultaneously on a separate host.
Software Type	Type of the software used by the virtual machine. For example, StarOS Security Gateway.
UUID	The unique identification of the virtual service gateway.
VM ID	The unique identification code of the virtual machine.
Profile Name	The name of the profile created for monitoring the virtual service gateway configuration.This property is not supported.
Manage Virtual Entity	The associated link to service inventory (WSG). Click this link to open the wireless service gateway instance inventory window. In this window, there are associated links for host service, virtual machine, hypervisor, and physical inventory of the VSM card. Using these associated links, you can navigate between virtual instance and VSM card.
Statistics tab	
CPU Usage	CPU usage by the virtual machine, in GHz.
Memory Usage	Memory usage by the virtual machine, in MB.
Disk	Amount of disk space used by the virtual machine, in MB.
CPU Allocation tab	
Maximum Allocation	Maximum CPU allocation for the virtual machine, in GHz.

Table 28-18 Virtual Service Gateway Configuration Details (continued)

Field	Description
Overhead Allocation	The overhead CPU allocation for the virtual machine, in GHz.
Unlimited Allocation	Unlimited maximum allocation capacity availability check for the virtual machine. The value is either true or false.
Expandable Allocation	Expandable allocation availability for the virtual machine. The value is either true or false.
Memory Allocation tab	
Maximum Allocation	Maximum memory allocation for the virtual machine, in MB.
Overhead Allocation	The overhead memory allocation for the virtual machine, in MB.
Unlimited Allocation	Unlimited maximum allocation capacity availability check for the virtual machine. The value is either true or false.
Expandable Allocation	Expandable allocation availability for the virtual machine. The value is either true or false.
Disk Allocation tab	
Maximum Allocation	Maximum disk allocation for the virtual machine, in MB.
Overhead Allocation	The overhead disk allocation for the virtual machine, in MB.
Unlimited Allocation	Unlimited maximum allocation capacity availability check for the virtual machine. The value is either true or false.
Expandable Allocation	Expandable allocation availability for the virtual machine. The value is either true or false.
Interfaces	
Interfaces	Interfaces associated to virtual machine are listed. Click the associated interface link to view the KVM page. From there the link takes you to actual physical interface.

Step 5 Choose **Compute Virtualization**> **Virtual Machines (All Datacenters)**. The virtual machine details are displayed in the content pane.

Table 28-19 Virtual Machine Details

Field	Description
VM ID	The name of the KVM host server.
VM Name	The name of the virtual service gateway.

Table 28-19 Virtual Machine Details

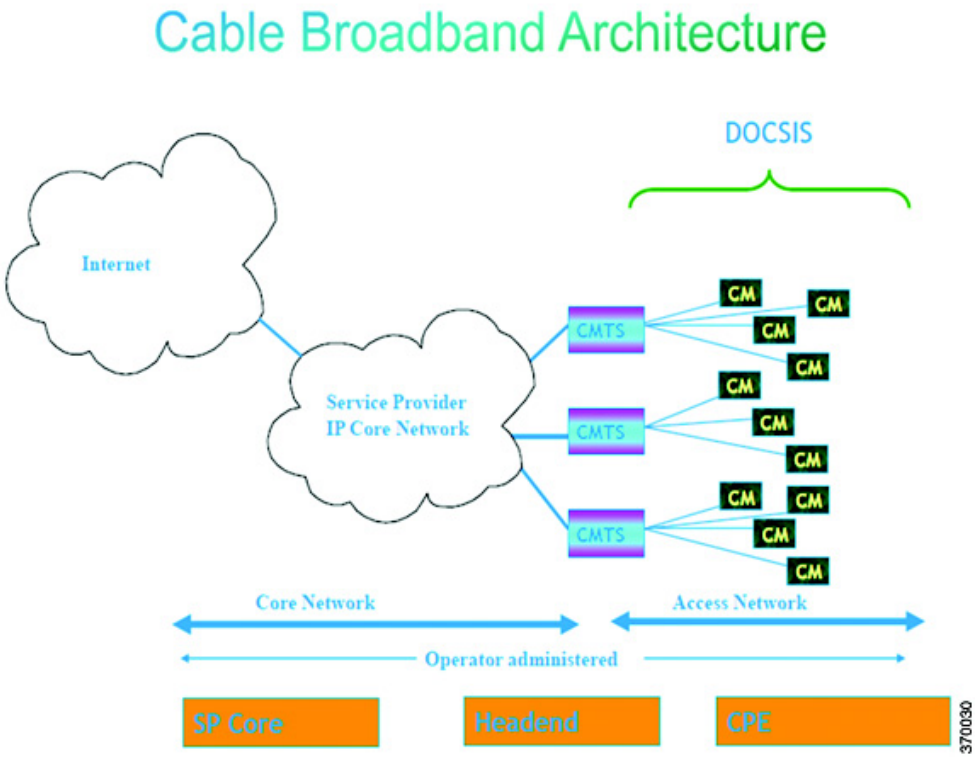
Field	Description
Datacenter Name	The virtual data center name associated to the virtual machine.
Associated Virtual Machine	Associated link to wireless service gateway virtual instance.
Hypervisor	Associated link to KVM host server.
IP Address	The IP address of the virtual machine.
DNS Name	The DNS name of the virtual machine. This property is not supported.
MAC Address	The MAC address of the virtual machine. This property is not supported.

CHAPTER 29

Monitoring Cable Technologies

Cable broadband communication operates in compliance with the Data Over Cable Service Interface Specification (DOCSIS) standard which prescribes multivendor interoperability and promotes a retail model for the consumer's direct purchase of a cable modem (CM) of choice. Figure 29-1 depicts the architecture of the cable broadband in compliance with this standard:

Figure 29-1 Cable Broadband Architecture



DOCSIS defines two key devices necessary for broadband cable communication:

- Cable Modem Termination System (CMTS) is a piece of equipment typically located in a cable company's headend or hubsite, and used to provide high speed data services, such as cable Internet or voice over Internet Protocol, to cable subscribers. A CMTS provides many of the same functions provided by the DSLAM in a DSL system. In order to provide these high speed data services, a cable company will connect its headend to the Internet via very high capacity data links to a network

service provider. On the subscriber side of the headend, the CMTS enables the communication with subscribers' cable modems. A single CMTS can accommodate thousands of cable modems, and provides the connection point to the Internet backbone.

- Cable Modem (CM) is a type of network bridge and modem that provides bi-directional data communication via radio frequency channels on a hybrid fiber-coaxial (HFC) and RFoG infrastructure. Cable modems are primarily used to deliver broadband Internet access in the form of cable Internet, taking advantage of the high bandwidth of a HFC and RFoG network. Usually located at the customer premises, terminates the cable line, and modulates/demodulates signals to and from the CMTS.

Data flowing from the CMTS to the Cable Modem is deemed downstream traffic. Data from the Cable Modem to the CMTS is upstream traffic. A DOCSIS binary configuration file provides the appropriate ISP parameters for cable modems to connect to the network.

There are two types of CMTS systems, which are explained below:

- Integrated CMTS (I-CMTS)—In this type of CMTS, the contents of the downstream channel are directly modulated and transmitted by the Downstream RF Port.
- Modular CMTS (M-CMTS)—In this type of CMTS, the contents of the downstream channel are encapsulated into a DEPI tunnel for transmission.

Cisco Systems offers a complete portfolio of standards-based cable products, solutions, and network management systems that enable integration of data, voice, and video services on a single multiservice cable IP network. For information on supported CMTS systems, refer to *Cisco Prime Network 5.0 Supported VNEs*.

These topics describe how to use the Vision client to manage cable networks. If you cannot perform an operation that is described in these topics, you may not have sufficient permissions; see Permissions for Managing Cable Technologies, page B-27.

Viewing the Cable Broadband Configuration Details

You can view the following Cable technology configurations:

- DTI Client—The DOCSIS Timing Interface (DTI) client collects DTI server master clock, DOCSIS timestamp, and Time of Day information from the DTI Server. It interfaces with the DTI Server to provide Time, Frequency and Management interfaces to the Modular Cable Modem Termination System (M-CMTS) device.
- QAM Domain—Quadrature Amplitude Modulation (QAM) domain
- MAC Domain—A MAC domain is a logical subcomponent of a Cisco CMTS router and is responsible for implementing all DOCSIS functions on a set of downstream and upstream channels. The CMTS MAC domain typically includes one or more downstream paths and one or more upstream paths. Depending on the CMTS configuration, the CMTS MAC domain can be defined to have its downstream on one cable interface line card with its upstreams on another card, or one or more CMTS MAC domains per cable interface line card.

- Narrowband Channels—A Narrowband Channel is a logical representation of a non-bonded channel that is a standard DOCSIS 1.x/2.0 protocol downstream channel that contains one RF channel. The wideband protocol utilizes the existing narrowband downstream channel for carrying the MAC management and signaling messages and the associated narrowband upstream for return data traffic and signaling.
- Wideband Channels—A Wideband Channel or Bonded Group (BG) is a logical grouping of one or more physical RF channels over which MPEG-TS packets are carried. Wideband channel carries DOCSIS bonded packets encapsulated in MPEG-TS packets from a WCMTS to one or more WCMs. The wideband channel, comprising of one or more RF channels on the EQAM device, is used for DS data traffic. The US channels on interface line cards—such as the Cisco uBR-MC3GX60V or Cisco uBR10-MC5X20—are used for US traffic.
- Fiber Node—A Fiber Node allows the Multiple Server Operator (MSO) or service provider to configure the CMTS to be more intelligent by making Cisco IOS aware of how the cable plant is wired. The downstream channels of the cable plant must be accurately configured in the CMTS fiber nodes. This allows the CMTS to accurately signal the wideband modems on which the wideband channels are available to the modem.

Viewing the DTI Client Configuration Details

To view the DTI Client configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory** > **DTI Client**. The DTI Client details are displayed in the content pane.

Table 29-1 describes the DTI Client configuration details.

Table 29-1 DTI Client Configuration Details

Field	Description
DTI Server Details	
Server Status	The status of the server, which can be any one of the following: • Free Run • Warm Up • Fast Tracking • Normal • Hold Over • Client Stable • Test
Root Server Clock Type	The clock type of the DTI Server, which can be any one of the following: • ITU Type 1 • ITU Type 2 • ITU Type 3 • ITU STRATUM 3

Table 29-1 DTI Client Configuration Details (continued)

Field	Description
Root Server Source	The clock source of the DTI server, which can be any one of the following: • Internal • External • GPS • None
Server Type	The type of DTI Server, which can be any one of the following: • Root • User Time • NTPV 4 • GPS
Client Performance Stable	Indicates the stability of the performance of the DTI client.
Client Cable Advance Valid	Indicates the cable advance status of the DTI Server Frame.
TOD Setting Mode	The output of the Time of Day Setting mode (User time, NTP, GPS), which can be any one of the following: • Short • Verbose **Note** The output is based on the TOD message sent by the DTI Server.
Time of Day	The date and time of the clock.
DTI Client Port Status	
DTI Client	The name of the DTI client, which when clicked will take you to the relevant slot under the Physical Inventory node.
DTI Client Status	The status of the DTI client, which can be any of the following: • Active • Standby
Connected	Indicates whether the DTI Server is active in the DTI client port.

Viewing the QAM Domain Configuration Details

To view the QAM domain configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory** > **QAM Domain** > *QAM Domain name*. The QAM Domain details are displayed north content pane.

Table 29-2 describes the QAM Domain configuration details.

Table 29-2 QAM Domain Configuration Details

Field	Description
QAM Domain ID	The unique identification code of the QAM domain.
QAM Domain	
QAM Domain ID	The unique identification code of the QAM domain.
UDP Start Range	The starting port in the range of UDP ports for the video route.
UDP End Range	The ending port in the range of UDP ports for the video route.
QAM Block	The QAM block ID for the video route.

Viewing the MAC Domain Configuration Details

To view the MAC domain configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory** > **MAC Domains** > *MAC Domain name*. The MAC Domain configuration details are displayed in the content pane.

Table 29-3 describes the MAC Domain configuration details.

Table 29-3 MAC Domain Configuration Details

Field	Description
MAC Domain Name	The name of the MAC domain.
Domain Status	The status of the MAC domain, which can be any one of the following: • Up • Down • Administrative Up • Administrative Down • Unknown
Bundle	The bundle address associated with the MAC domain.
Active Remote DS	The downstream channel associated with the MAC domain.
Upstream Channels	
US Channel ID	The unique identification code of the Upstream channel.

Table 29-3 MAC Domain Configuration Details (continued)

Field	Description
Status	The status of the upstream channel, which can be any one of the following: • Up • Down • Administrative Up • Administrative Down • Unknown
Port	The port to which the upstream channel is associated with.
Frequency	The frequency of the upstream channel.
Channel width	The width of the upstream channel.
Modulation	The modulation value of the upstream channel.
Backoff End	The backoff end time of the upstream channel.
Backoff Start	The backoff start time of the upstream channel.
Downstream Channels	
DS Channel ID	The unique identification code of the Downstream Channel.
Associated Narrowband	The name of the narrowband channel that is associated to the downstream channel.
Port	The port to which the downstream channel is associated with.
Status	The status of the downstream channel, which can be any one of the following: • Up • Down • Administrative Up • Administrative Down • Unknown
Frequency	The frequency of the downstream channel.
Bandwidth	The bandwidth of the downstream channel.
Total Modem	The total number of modem for the downstream channel.
Modem Active	The number of modems active for the downstream channel.
Network Delay	The network delay (in terms of bits per second) in the downstream channel.

Viewing the Narrowband Channels Configuration Details

To view the Narrowband channels configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory** > **Narrowband Channels** > *Narrowband channel cable*. The Narrowband channels configuration details are displayed in the content pane.

Table 29-4 describes the Narrowband channels configuration details.

Table 29-4 Narrowband Channels Configuration Details

Field	Description
Name	The name of the narrowband channel.
Channel Status	The status of the narrowband channel, which can be any one of the following: • Up • Down • Unknown
DS ID	The identification code of the downstream channel associated with the narrowband channel.
RF Channel ID	The identification code of the Radio Frequency (RF) channel associated with the narrowband channel.
Bandwidth	The percentage of bandwidth available for the narrowband channel.
Downstream ID	The link to the downstream channel that is associated to the narrowband channel.
Wideband Associations	
Associated Entity	The wideband channel that is associated to the narrowband channel, which when clicked will take you to the relevant wideband channel configuration under the **Wideband Channels** node.
Bandwidth	The percentage of bandwidth available for the wideband channel.

Viewing the Wideband Channels Configuration Details

To view the Wideband channels configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory** > **Wideband Channels** > *Wideband cable*. The Wideband channels configuration details are displayed in the content pane.

Table 29-5 describes the Wideband channels configuration details.

Table 29-5 Wideband Channels Configuration Details

Field	Description
Wideband Name	The name of the wideband channel.
Status	The status of the wideband channel, which can be any one of the following: • Up • Down • Administrative Up • Administrative Down • Unknown
Bonding Group ID	The unique identification code of the bonding group. **Note** A bonding group is a logical grouping of one or more physical radio frequency (RF) channels over which wideband MPEG-TS packets are carried. By aggregating or "channel bonding" multiple RF channels, the wideband channel is capable of greater bandwidth capacity for downstream data traffic than a single narrowband channel.
Bundle	The bundle address associated with the wideband.
NB Channel Interface	The Narrowband (NB) channel interface associated with the wideband channel.
Reserved CIR	The Committed Information Rate (CIR) reserved for the wideband channel.
Total CIR	The total Committed Information Rate (CIR) associated to the Wideband channel available.
Multicasting Reserved CIR	Indicates the Reserved Committed Information Rate associated to the multicasting group of the Wideband channel.
Multicasting Total CIR	Indicates the Total Committed Information Rate associated to the multicasting group of the Wideband channel.
RF Channels	
RF Channel ID	The unique identification code of the RF channel.
Port	The port to which the RF channel is associated with.
Bandwidth	The percentage of bandwidth available for the RF channel.
Channel Type	The type of the RF channel, which can be any one of the following: • Primary • Non-Primary
Frequency	The frequency (in terms of Mhz) allocated to the RF channel.
Modulation	The modulation (in terms of QAM) allocated to the RF channel.
Annex	The annexure that is allocated to the RF channel.
IP Address	The IP address that is assigned to the RF channel for downstream data transmission.

Table 29-5 Wideband Channels Configuration Details (continued)

Field	Description
MAC Address	The MAC address that is assigned to the RF channel for downstream data transmission.
DEPI Remote ID	The Downstream External PHY Interface (DEPI) remote session ID that is assigned to the RF channel.

Viewing the Fiber Node Configuration Details

To view the Fiber Node configuration details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory** > **Fiber NOde**. The Fiber Node configuration details are displayed in the content pane.

Table 29-6 describes the Fiber Node configuration details.

Table 29-6 Fiber Node Configuration Details

Field	Description
Fiber Node Number	The unique number assigned to the Fiber node.
Total DS Channels	The total number of downstream channels associated to the fiber node.
Total US Channels	The total number of upstream channels associated to the fiber node.
Status	The status of the fiber node, which can be any one of the following: • Valid • Invalid

Configure Cable Ports and Interfaces

These cable port and interface commands can be launched from the Vision client. Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Configure Cable Ports

Command	Navigation	Description
Modify Port	**Physical Inventory** > *Ethernet Slot* > *Navigate to Ethernet port* > **Commands** > **Configuration > Port**	Controls a variety of RFGW port characteristics (status of port, IP address type and so forth).
Modify Cable Port	**Physical Inventory > Chassis >** *Slot* **>** *Subslot* **>** *Cable* **> Commands > Configuration > Port**	Controls a variety of CMTS device port characteristics (status of port, bundle ID and so forth).
Configure Downstream Port	**Physical Inventory > Chassis >** *Slot* **>** *Subslot* **>** *Cable* **> Commands > Configuration > Downstream**	Configure and enable the downstream ports on the CMTS card (such as the Cisco uBR 10000 card). Configure parameters like modulation rate, downstream interleave depth in number of rows of code words, and so on.
Create Upstream Port **Modify Upstream Port**	**Physical Inventory > Chassis >** *Slot* **>** *Subslot* **>** *Cable or Ethernet port* **> Commands > Configuration > Upstream**	Create or modify an upstream port.

Configure Cable Interfaces

Command	Navigation	Description
Create IP Interface	**Logical Inventory** > **Routing Entities** > **Routing Entity** > **Commands** > **Configuration**	Configure IP interface as part of the routing entity for the selected device.
Modify IP Interface **Delete IP Interface**	**Logical Inventory** > **Routing Entities** > **Routing Entity** > *Select an interface* > **Commands** > **Configuration**	Changes or removes descriptive information that is displayed in GUI clients when the interface is selected.

View Upstream and Downstream Configuration for Cable

Use the following command to view the cable upstream and downstream configuration. Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Command	Navigation	Description
Show > Upstream **Show > Downstream**	**Physical Inventory** > *Ethernet Slot* > *Navigate to Ethernet port* > **Commands** > **Configuration > Port**	View the configured upstream and downstream rate for the selected cable.

Configure and View QAM

The following commands configure the Quadrature Amplitude Modulation (QAM) domain for the RF channel. Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Configure RF and Frequency Profiles

Command	Navigation	Description
Create RF Profile **Modify RF Profile** **Delete RF Profile**	*NE* > **Commands > Configuration > RF Profile**	Configures a combination of RF attributes to be used across all line cards in the chassis.
Delete Frequency Profile **Create Lane** **Create Block**	*NE* > **Commands > Configuration > Frequency Profile**	Configure the frequency profile at the port level. These user-defined frequency scheme provides flexibility to define each lane and block start frequencies. These frequency profiles can then be applied to the port in this scheme.

Configure QAM Port and Channel

Command	Navigation	Description
Modify QAM Port **Modify QAM Channel**	**Physical Inventory** > **Chassis** > *Slot* > *QAM* > **Commands** > **Configuration**	Modify the QAM port and channel.

View QAM Configurations

Command	Navigation	Description
Show > **RF Profile** **Show** > **Frequency Profile**	*NE* > **Commands**	Display RF and Frequency profiles created on the device.
Show > **QAM Port** **Show** > **QAM Channel**	**Physical Inventory** > **Chassis** > *Slot* > *QAM* > **Commands**	Displays cable information configured on the QAM channel and port.

Configure DEPI and L2TP

These commands configure the Downstream External PHY Interface (DEPI) and Layer 2 Tunnel Protocol (L2TP). The table below lists the navigation of each of these commands. Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the *Cisco Prime Network 5.3 Supported Cisco VNEs*.

Configure DEPI Class and Tunnel

Command	Navigation	Description
Create DEPI Class **Delete DEPI Class** **Create DEPI Tunnel** **Modify DEPI Tunnel** **Delete DEPI Tunnel**	*NE* > **Commands > Configuration > DEPI**	Configures template of DEPI control plane and tunnel configuration settings.

Configure L2TP Class

Command	Navigation	Description
Create L2TP Class **Modify L2TP Class** **Delete L2TP Class**	*NE* > **Commands > Configuration > L2TP**	Configures a template of Layer 2 Tunnel Protocol (L2TP) control plane configuration settings.

View DEPI Tunnel, DEPI Session, and L2TP Class

Command	Navigation	Description
Show > L2TP Class	*NE* > **Commands** > **Configuration**	Displays Layer 2 Tunnel Protocol control plane configuration settings.
Show > DEPI Tunnel		Displays DEPI tunnel configuration settings.
Show > DEPI Session		Displays DEPI session information and DEPI sessions configured on the line card.
Show > Cable DEPI Session		

Monitoring ADSL2+ and VDSL2 Technologies

This chapter discusses the following technology enhancements in Prime Network:

- ADSL2+
- VDSL2
- Bonding Group

These topics describe how to use the Vision client to manage these technologies. If you cannot perform an operation that is described in these topics, you may not have sufficient permissions; see Permissions for Managing DSL2+ and VDSL2, page B-28.

Viewing the ADSL2+/VDSL2 Configuration Details

Asymmetric digital subscriber line (ADSL) is a type of digital subscriber line (DSL) technology, a data communications technology that enables faster data transmission over copper telephone 5.3 than a conventional voiceband modem can provide. It does this by utilizing frequencies that are not used by a voice telephone call.

ADSL2+ extends the capability of basic ADSL by doubling the number of downstream channels. The data rates can be as high as 24 Mbit/s downstream and up to 1.4 Mbit/s upstream depending on the distance from the DSLAM to the customer's premises. It is capable of doubling the frequency band of typical ADSL connections from 1.1 MHz to 2.2 MHz. This doubles the downstream data rates of the previous ADSL2 standard (which was up to 12 Mbit/s), and like the previous standards will degrade from its peak bitrate after a certain distance.

Very-high-bit-rate digital subscriber line (VDSL or VHDSL) is a digital subscriber line (DSL) technology providing data transmission faster than ADSL over a single flat untwisted or twisted pair of copper wires (up to 52 Mbit/s downstream and 16 Mbit/s upstream), and on coaxial cable (up to 85 Mbit/s down- and upstream); using the frequency band from 25 kHz to 12 MHz. These rates mean that VDSL is capable of supporting applications such as high-definition television, as well as telephone services (voice over IP) and general Internet access, over a single connection.

Very-high-bit-rate digital subscriber line 2 (VDSL2) is an access technology that exploits the existing infrastructure of copper wires that were originally deployed for traditional telephone service as a way of delivering very high speed internet access. The main high-speed link (e.g. a fibre optic connection) terminates at a hub near the customers' location. The existing copper wire infrastructure is then used to

carry the high speed connection for the short remaining distance to the customers. It can be deployed from central offices, from fiber-optic connected cabinets located near the customer premises, or within buildings.

In Prime Network, the ADSL2+ and VDSL2 technologies are grouped under the XDSL Traffic Descriptors node.

To view the XDSL Traffic Descriptors Details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 Expand the **Logical Inventory** node and choose **XDSL Traffic Descriptors**. The relevant details are displayed in the content pane as shown in Figure 30-1.

Figure 30-1 XDSL Traffic Descriptor Details

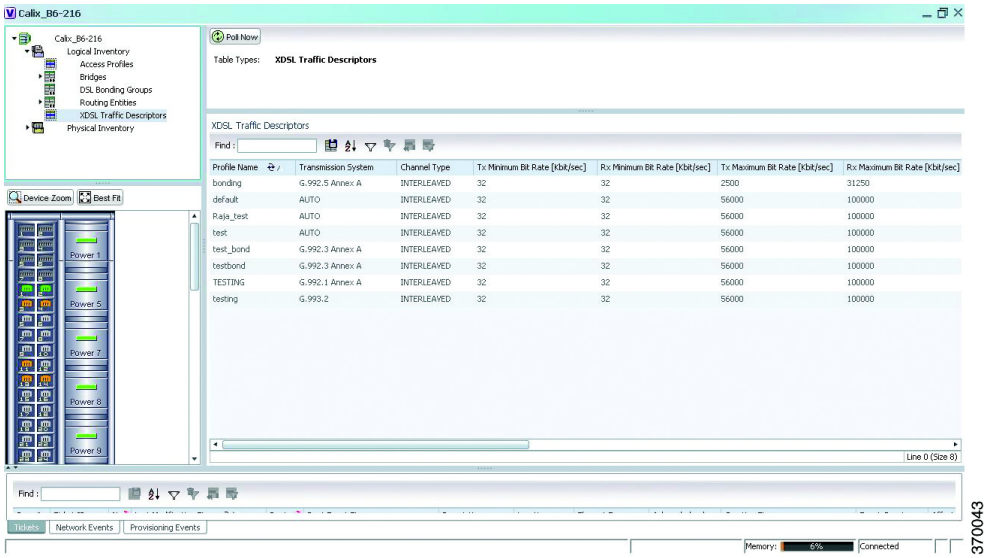


Table 30-1 describes the XDSL Traffic Descriptor details.

Table 30-1 XDSL Traffic Descriptor Details

Field	Description
XDSL Traffic Descriptors	
Profile Name	The name of the ADSL2+/VDSL2 profile.
Transmission System	The operating mode of the transmission system.
Channel Type	The type of physical channel, which can be any one of the following: • Fast • Interleaved
Tx Minimum Bit Rate [Kbit/sec]	The minimum bit rate (in terms of kilobits per second) transmitted for adaptive bit rate.
Rx Minimum Bit Rate [Kbit/sec]	The minimum bit rate (in terms of kilobits per second) received for adaptive bit rate.
Tx Maximum Bit Rate [Kbit/sec]	The maximum bit rate (in terms of kilobits per second) transmitted for adaptive bit rate.

Table 30-1 XDSL Traffic Descriptor Details

Field	Description
Rx Maximum Bit Rate [Kbit/sec]	The maximum bit rate (in terms of kilobits per second) received for adaptive bit rate.
Tx Target Noise Margin [dB]	The target amount of noise (in decibel) transmitted by XDSL TU-C/TU-R.
Rx Target Noise Margin [dB]	The target amount of noise (in decibel) received by XDSL TU-C/TU-R.
Tx Minimum Noise Margin [dB]	The minimum amount of noise (in decibel) transmitted by XDSL TU-C/TU-R.
Rx Minimum Noise Margin [dB]	The minimum amount of noise (in decibel) received by XDSL TU-C/TU-R.
Tx Maximum Noise Margin [dB]	The maximum amount of noise (in decibel) transmitted by XDSL TU-C/TU-R.
Rx Maximum Noise Margin [dB]	The maximum amount of noise (in decibel) received by XDSL TU-C/TU-R.
Transmission System	The operating mode of the transmission system.
XDSL2 Line Profile	The XDSL2 line profile that must be used. **Note** This field is applicable only for VDSL2 technology.
Upstream Band 0 Mask	The XDSL2 upstream band 0 mask. **Note** This field is applicable only for VDSL2 technology.

Viewing the ADSL2+/VDSL2 Details for a Device

The physical inventory details for a device displays the location information as well as the XDSL support details for ADSL2+ and VDSL2 devices,

To view the physical inventory details for a device:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 Expand the **Physical Inventory** node.

Step 3 Choose the port and the following details are displayed in the content pane:

- Location Details—This section displays the Device Type, Location, Port Alias, and Status of the device. It also indicates whether alarms must be sent for any event or alarm.
- ATM on port—This section displays the Asynchronous Transfer Mode details for the port.
- PTM on port—This section displays the Packet Transfer Mode (PTM) details for the port. The PTM section displays the following information:

  - Encapsulation Type
  - TPS-TC Admin Mode—Will be displayed only for VDSL line cards.
  - TPS-TC Oper Mode—Will be displayed only for VDSL line cards.

Note The ATM on Port and PTM on Port sections will not be displayed if the port is bonded to a DSL group or if the **TPS-TC Admin Mode** is specified as **Auto** and the **TPS-TC Oper Mode** is specified as **Unknown.**

- XDSL/ADSL2/2+—This section displays the XDSL support details. These support details include the Administrative and Operating statuses, Operating Mode, Aggregation Group, the various Bit rates and Noise margins.

  The **Operating Mode** indicates whether the device is an ADSL2 or VDSL 2 device. The **Aggregation Group** indicates whether the port is associated to a DSL bonding group. This is a link, which when clicked will take you to the relevant bonding group in the **DSL Bonding Group** node.For more information about the attributes in this section, refer to Table 30-1.

Note The name of this section changes based on the value in the **Operating Mode** field. If the value in the **Operating Mode** field is **None**, then this section is titled **XDSL**. If the value in this field refers to a ADSL device (for example **G.992.5 Annex A**), then this section is titled **ADSL Ver 2/2+**. If the value in this field refers to a VDSL device (for example **G.993.2**), then this section is titled **VDSL Ver2**.

Viewing the DSL Bonding Group Configuration Details

Channel bonding is a computer networking arrangement in which two or more network interfaces on a host computer are combined for redundancy or increased throughput. Similarly, multiple DSL 5.3 can be bonded to give higher bandwidth.

A bonded DSL uses multiple DSL connections and aggregates the bandwidth together to increase the speed of upload and download process.

To view the DSL bonding group details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 Expand the **Logical Inventory** node and choose **DSL Bonding Groups**. The relevant details are displayed in the content pane as shown in Figure 30-2.

Figure 30-2 DSL Bonding Group Node

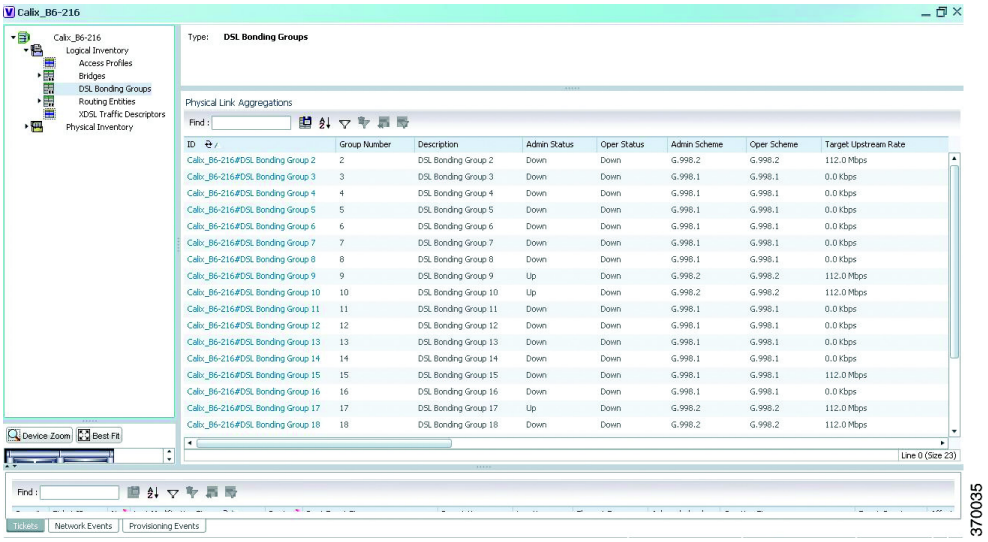


Table 30-2 describes the DSL Bonding Group details.

Table 30-2 DSL Bonding Group Details

Field	Description
Physical Link Aggregations	
ID	The unique identification code of the DSL bonding group.
Group Number	The group number for the DSL bonding group.
Description	The description of the DSL bonding group.
Containing TPs	The termination points associated with the DSL bonding group.
Admin Status	The administrative status of the DSL bonding group, which can be any one of the following: • Up • Down
Oper Status	The operative status of the DSL bonding group, which can be any one of the following: • Up • Down
Admin Scheme	The administrative scheme of the DSL bonding group, which can be any one of the following: • G998.1 • G998.2 • Unknown

Table 30-2 DSL Bonding Group Details

Field	Description
Oper Scheme	The operative scheme of the DSL bonding group, which can be any one of the following: • G998.1 • G998.2 • Unknown
Target Upstream Rate	The target upstream rate (in kbps or mbps) of the DSL bonding group.
Target Downstream Rate	The target downstream rate (in kbps or mbps) of the DSL bonding group.
Upstream Rate	The current upstream rate (in kbps or mbps) of the DSL bonding group.
Downstream Rate	The current downstream rate (in kbps or mbps) of the DSL bonding group.
Minimum Upstream Rate	The minimum upstream rate (in kbps or mbps) of the DSL bonding group.
Minimum Downstream Rate	The minimum downstream rate (in kbps or mbps) of the DSL bonding group.
Number of Aggregated Ports	The number of aggregated ports that is configured in the DSL bonding group.
Maximum Aggregated Ports	The maximum number of aggregated ports that can be configured in the DSL bonding group.
Peer Admin Scheme	The peer administrative scheme of the DSL bonding group, which can be any one of the following: • G998.1 • G998.2 • Unknown
Peer Oper Scheme	The peer operational scheme of the DSL bonding group, which can be any one of the following: • G998.1 • G998.2 • Unknown
Designated End Point	The designated end point of the DSL bonding group.
Maximum Peer Aggregated Ports	The maximum number of peer aggregated ports that is configured in the DSL bonding group.
Discovery Code	The unique 6-octet-long code that is used by the Discovery function of the Generic Bonding Sub-layer port.
G988.2 Properties	

Table 30-2 DSL Bonding Group Details

Field	Description
Control Protocol Type	The type of control protocol currently operating on the G.bond port, which can be any one of the following: • BACP • G.HS This field defaults to G.HS. **Note** This field is available only if the **Oper Scheme** for the DSL bonding group is specified as **G.988.2**.
PTM Encapsulation Type	The Packet Transfer Mode-Transport Convergence Layer (PTM-TC) encapsulation type supported by the G.bond port, which can be any one of the following: • 64/65-octet • HDLC **Note** This field is available only if the **Oper Scheme** for the DSL bonding group is specified as **G.988.2**.
Is BACP Supported	Indicates whether the Bonding Aggregation Control Protocol (BACP) is supported y the G.bond port. **Note** This field is available only if the **Oper Scheme** for the DSL bonding group is specified as **G.988.2**.

Viewing Transport Models Supported by ADSL2+ and VDSL2

In Prime Network, the following transport models are supported in the ADSL2+ and VDSL2 technologies:

- N-to-One—In this most commonly used model, a Service VLAN tag (S-Vid) is assigned to a service throughout the network. The destination is determined by the MAC address of the device and the service VLAN at the edge of the network. This transport model is supported on ADSL2+ and VDSL2 line cards.
- One-to-One—In this model, the destination is determined by a pair of VLAN tags, which must be unique throughout the network. This transport model is supported on B6 VDSL2 line cards.

- Transparent LAN Service (TLS) —This model allows transparency to the business customers while transporting business traffic between geographically disperse business endpoints. The traffic that is transported by the infrastructure that interconnects the locations is transparent to the carrier network (including protocols such as STP, unicast and multicast protocols). The traffic can be of any format and often includes VLAN tagged traffic.

Viewing the N-to-One Access Profile

To view the N-to-One access profile:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 Expand the **Logical Inventory** node and choose **N-to-One Access Profiles**. The relevant details are displayed in the content pane as shown in Figure 30-3.

Figure 30-3 N-to-One Access Profile

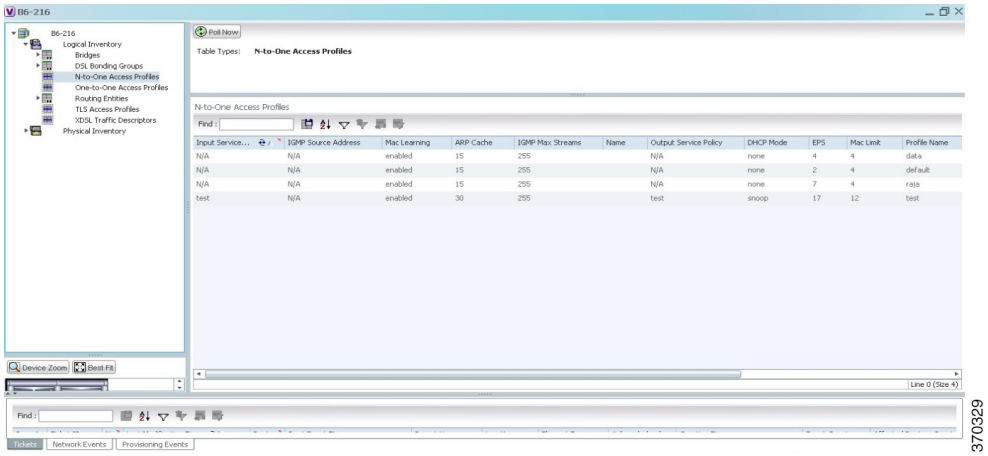


Table 30-3 describes the N-to-One Access Profile details.

Table 30-3 N-to-One Access Profiles

Field	Description
Table Types	The type of access profile, which in this instance is **N-to-One Access Profiles**.
N-to-One Access Profiles	
Input Service	The input service policy applicable to the device.
IGMP Source Address	The Internet Group Management Protocol (IGM) source address.
Mac Learning	Indicates whether the Mac Learning feature is enabled for the device.

Table 30-3 N-to-One Access Profiles

Field	Description
ARP Cache	The Address Resolution Protocol (ARP) cache of the device. **Note** ARP converts an IP address to its corresponding physical network address, which is usually implemented in the device drivers of the network operating systems. When a device wants to send data to another device over ethernet, it must first determine the MAC address of the target device. These IP to MAC address mappings are derived from the ARP cache maintained on each device.
IGMP Max Streams	The maximum Internet Group Management Protocol (IGMP) stream value.
Name	The name of the N-to-One access profile.
Output Service Policy	The output service policy applicable to the device.
DHCP Mode	The Dynamic Host Configuration Protocol (DHCP) mode applicable to the device.
EPS	The Ethernet Protection Switching (EPS) VLAN tag assigned to the device. **Note** The VLAN tag numbers can be any value between 2 and 122 when B6 line cards access rings. When the B6-450 is used on aggregation rings, it supports VLAN tag numbers between 2 and 1000.
Mac Limit	The maximum number of MAC addresses allowed for the service.
Profile Name	The name of the access profile.
Input Service Policy	The name of the service policy that is assigned to the access profile as an input policy. This is a rate-limiting policy that controls and limits all unicast incoming traffic from the B6 card to the subscriber.
Output Service Policy	The name of the service policy that is assigned to the access profile as an output policy. This is a rate-limiting policy that controls and limits all unicast outgoing traffic to the B6 card from the subscriber.

Viewing the One-to-One Access Profile

To view the One-to-One access profile details, expand the logical inventory and choose **One-to-One Access Profiles**.

Figure 30-4 One-to-One Access Profile

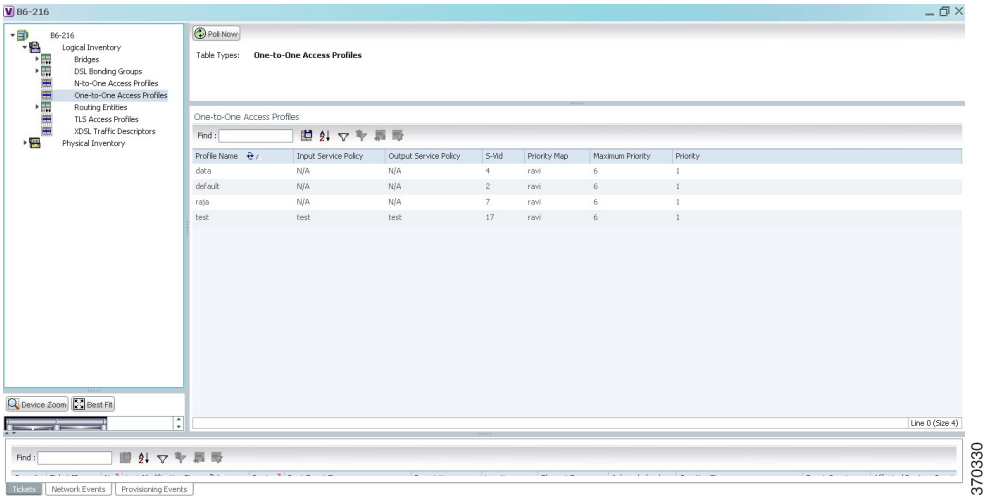


Table 30-4 describes the N-to-One Access Profile details.

Table 30-4 N-to-One Access Profiles

Field	Description
Table Types	The type of access profile, which in this instance is **One-to-One Access Profile**.
One-to-One Access Profiles	
Profile Name	The name of the One-to-one access profile.
Input Service Policy	The name of the service policy that is assigned to the access profile as an input policy. This is a rate-limiting policy that controls and limits all unicast incoming traffic from the B6 card to the subscriber.
Output Service Policy	The name of the service policy that is assigned to the access profile as an output policy. This is a rate-limiting policy that controls and limits all unicast outgoing traffic to the B6 card from the subscriber.
S-Vid	The unique Subscriber VLAN identification code. This code can be any value between 2 and 122.
Priority Map	The name of the 802.1p priority map, which is available in the DSCP-to-DOTP mapping profile.
Maximum Priority	The maximum 802.1 priority level.
Priority	The 802.1 priority level configured and applied to the incoming S-VID packet. This level can be any value between 0 and 6.

Viewing the TLS Access Profile

To view the TLS access profile details:

Step 1 Right-click the required device in the Vision client and choose **Inventory**.

Step 2 Expand the **Logical Inventory** node and choose **TLS Access Profiles**. The relevant details are displayed in the content pane as shown in Figure 30-5.

Figure 30-5 TLS Access Profiles

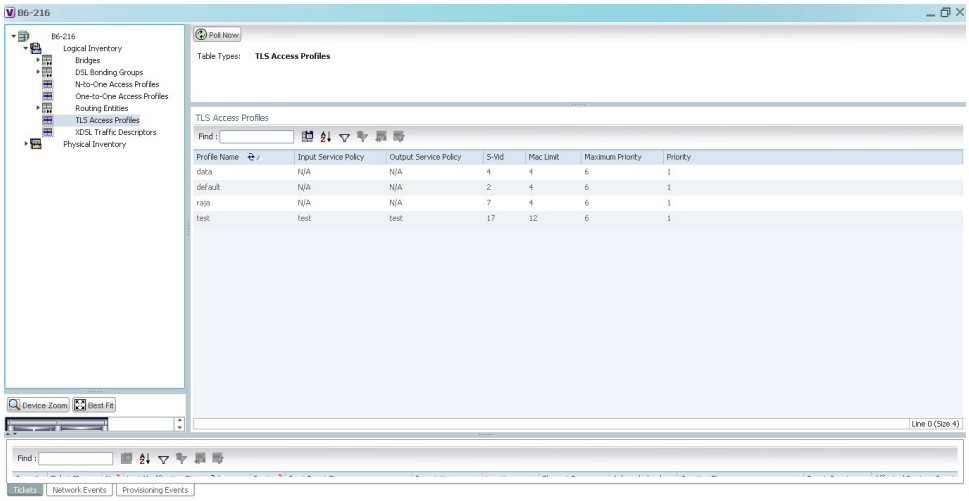


Table 30-5 describes the N-to-One Access Profile details.

Table 30-5 N-to-One Access Profiles

Field	Description
Table Types	The type of access profile, which in this instance is **TLS Access Profile**.
TLS Access Profiles	
Profile Name	The name of the TLS access profile.
Input Service Policy	The name of the service policy that is assigned to the access profile as an input policy. This is a rate-limiting policy that controls and limits all unicast incoming traffic from the B6 card to the subscriber.
Output Service Policy	The name of the service policy that is assigned to the access profile as an output policy. This is a rate-limiting policy that controls and limits all unicast outgoing traffic to the B6 card from the subscriber.
S-Vid	The unique Subscriber VLAN identification code. This code can be any value between 2 and 122.
Mac Limit	The maximum number of MAC addresses allowed for the specific service.
Maximum Priority	The maximum 802.1 priority level.
Priority	The 802.1 priority level configured and applied to the incoming S-VID packet. This level can be any value between 0 and 6.

Monitoring Cisco Virtualized Packet Core

The following topics provide an overview of Cisco Virtualized Packet Core (VPC) and describe the two configurations of VPC.

Overview of Cisco Virtualized Packet Core (VPC)

Cisco VPC is the industry's first hardware platform and hypervisor-independent solution that combines network functions virtualization (NfV) and software-defined networking (SDN). Cisco Virtualized Packet Core (VPC) provides a single solution for all the packet core services (4G, 3G, 2G, Wi-Fi, and small cell networks). As the network functions are provided as virtualized services, VPC enables a user to scale capacity and introduce new services in a faster and cost-effective manner.

Cisco VPC is based on the same proven StarOS software used in Cisco ASR 5000 Series platforms. VPC is mainly designed to distribute and orchestrate packet core functions across physical and virtual resources to enable users to perform the transition from physical to virtualized packet core services, or use both simultaneously.

The configurations supported by VPC:

- SI (Single instance)
- DI (Distributed instance)

VPC–SI

With a single VM per virtual node, the VPC-SI is used as a solution for small to medium instances. Based on the StarOS, each VM deployed on the device supports a single function mapped to it. In general, VPC-SI supports SAE-GW, PGW, SGW, SGSN, and HNBGW services, and all the other mobility services that are supported by Cisco ASR5000.

Identifying VPC–SI VNE

To identify a VPC –SI device, follow the steps provided below:

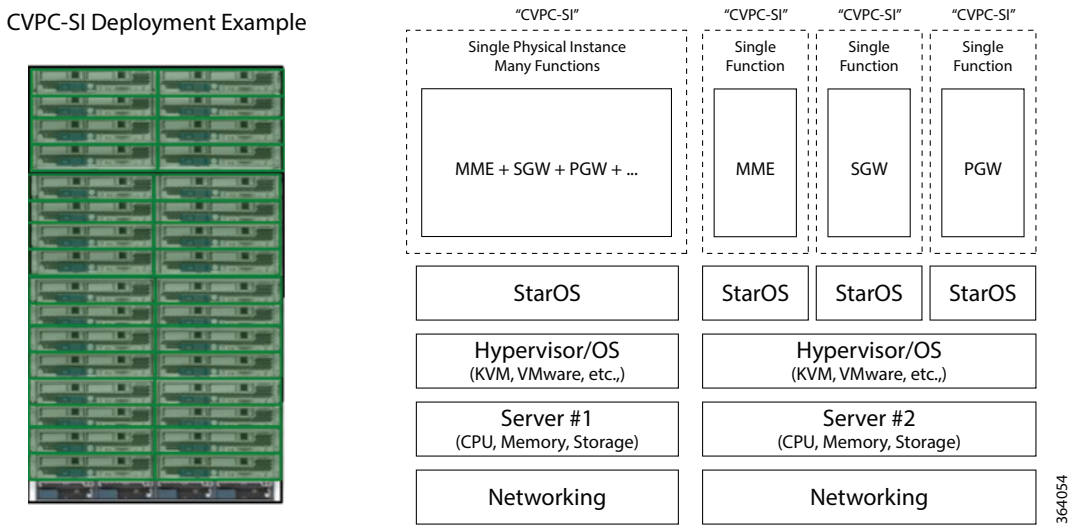
Step 1 Click the VNE.

Step 2 In the **VNE Inventory** window, verify if Device series is **Virtual ASR 5K SI Series Mobile-Gateway**.

Step 3 Verify if the **Element type** is **Virtual ASR 5K SI Mobile-Gateway**.

Step 4 Verify if the **Virtual device property** is set to **True**.

Figure 31-1 Deployment of VPC -SI VNE



VPC–DI

The VPC-DI supports larger instances using multiple VMs. This capability is achieved by creating a distributed infrastructure by combining all the VMs in the virtual node to perform a single or multiple services. However, the VPC-DI is designed in such a way that the VMs have a single point of management. Based on StarOS, the VPC-DI supports distributed services (load balancing) across all VMs using a single service address.

At least one among the VMs is a MIO VM, and one or more VMs act as Fabric VMs and Service VMs. However, with StarOS 17, in the future releases, the fabric VM functionality will be intercoupled within the service VM and will not exist as separate VM.

Identifying VPC–DI VNE

To identify a VPC–DI device, follow the steps provided below:

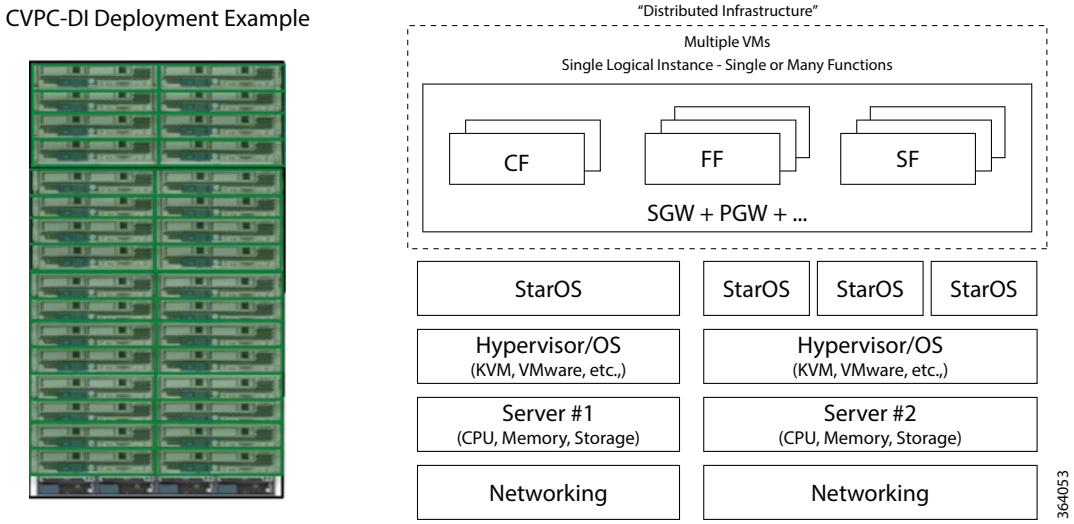
Step 1 Click on the VNE.

Step 2 In the **VNE inventory** window, verify if Device series is **Virtual ASR 5K DI Series Mobile-Gateway**.

Step 3 Verify if the **Element type** is **Virtual ASR 5K DI Mobile-Gateway**.

Step 4 Verify if the **Virtual device property** is set to **True**.

Figure 31-2 Deployment of VPC -DI VNE



UUID Support in Prime Network

In the absence of infrastructure monitoring tools like VCenter, the associations (hyperlinks) between Cisco Virtualized Packet Core (CvPC) VNE and the corresponding VCenter and UCS are not displayed in Prime Network. To identify a VM in the CvPC setup, UUID (a textual representation) is added in the physical inventory at the card level for all the virtual cards.

Viewing UUID Properties in Physical Inventory

To view UUID properties in the physical inventory:

Step 1 In the Vision client, double-click the device in which the CvPC is configured.

Step 2 In the **VNE inventory** window, expand the Physical Inventory node.

Step 3 Choose **Chassis > Server <Number>: Card A9K-VSM-500**. The server configuration details are displayed in the content pane.

Step 4 Choose **Server <Number>: Card A9K-VSM-500 > Subslot <Number>: Subcard -A9K-MODULEv**. The slot details configured with UUID details is displayed in the content pane.

Cisco Virtual Gateway Fault Correlation

The following table describes the fault correlations between CVPC devices and VMs:

Root Cause Alarm	Correlating Alarm
HostShutdown	HostConnectionLostEvent
	HostDisconnectedEvent
	VM out
	VMDisconnectedEvent
	PossiblyVMMigratedEvent
	Card out/Device Unreachable
HostRemoved	HostConnectionLostEvent
	HostDisconnectedEvent
	VM out
	VMDisconnectedEvent
	Card out/Device Unreachable
HostConnectionLostEvent	HostConnectionLostEvent
	VM out
	VMDisconnectedEvent
	PossiblyVMMigratedEvent
	Card out/Device Unreachable

Root Cause Alarm	Correlating Alarm
HostDisconnected	HostDisconnectedEvent
	VM out
	VMDisconnectedEvent
VMPoweredOff	VM out
	VMPoweredOff
	Card out/Device Unreachable

Note The faults correlations described in the above table are applicable only for virtual machines hosted in VMWare.

Monitoring VSS Redundancy System

The following topics provide an overview of Cisco 6500 virtual switching redundancy system.

Cisco 6500 VSS Redundancy System Overview

The Cisco Catalyst 6500 Series Virtual Switching System (VSS) allows the clustering of two chassis units together into a single, logical entity. The two chassis units are connected through a Virtual switch link (VSL) link, where one chassis acts as an active unit and the another chassis acts as a standby unit. If the active chassis fails, then the standby chassis act as the active chassis. The chassis units are selected as the active or standby units based on the priority set.

This clustering of chassis allows enhancements in all areas of network design including high availability, scalability, management, and maintenance.

The VSS redundancy system has the following processors:

- Dual 6500 processor—Each chassis has 1 SUP card.
- Quad processor—Each chassis has 2 SUP cards, one is active and the other one is standby hot (switchover target). The chassis which is in standby hot (switchover target) acts as the next active chassis.

Viewing VSS Redundancy System Properties in Logical Inventory

To view the VSS redundancy system properties in the logical inventory:

Step 1 Double-click the Cat 6500 VSS device to open the **Inventory** window.

Step 2 Choose **Logical Inventory**> **Redundancy Systems**. Click a particular VSS domain ID. The properties of the VSS domain are displayed in the content pane.

Figure 32-1 shows the VSS redundancy system properties in the logical inventory

Figure 32-1 VSS Redundancy System Properties

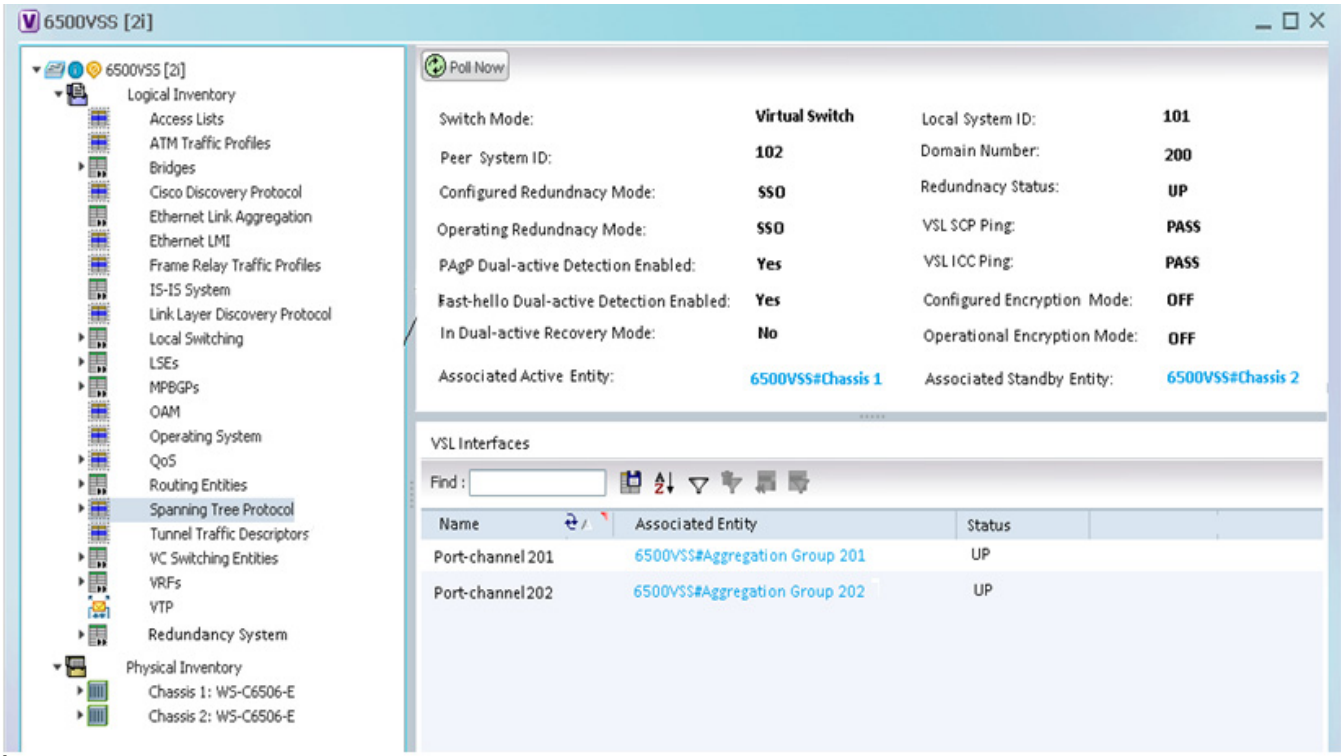


Table 32-1 describes the information that is displayed in the Redundancy System

Table 32-1 Redundancy System Details

Field Name	Description
Switch Mode	The current mode of the switch.
Local System ID	Unique identifier of a local physical chassis in the virtual switch.
Peer System ID	Unique identifier of a peer physical chassis in the virtual switch.
Domain Number	The virtual switch domain number to recognize a virtual switch domain. Only switches with the same domain number can be in the same virtual switch.
Configured Redundancy Mode	The configured redundancy mode.
Redundancy Status	Redundancy state: Up or Down. If the field is empty, it means the data was not collected from the device.
Operating Redundancy Mode	The operational redundancy mode.
VSL SCP Ping	Status of the VSL ISCP ping.
VSL ICC Ping	Status of the VSL ICC ping.
PAgP Dual-active Detection Enabled	Yes or No. Represents whether PAgP messaging over the MEC links to communicate between the two chassis through a neighbor switch is enabled or disabled.

Table 32-1 Redundancy System Details (continued)

Field Name	Description
Fast-hello Dual-active Detection Enabled	Yes or No. Represents whether hello messages over a backup Ethernet connection is enabled or disabled.
In Dual-active Recovery Mode	Yes or No. Represents whether BFD messaging over a backup Ethernet connection is enabled or disabled.
Configured Encryption Mode	ON or OFF. Represents whether the encryption mode is configured or not.
Operational Encryption Mode	ON or OFF. Represents whether the encryption mode is operational or not.
Associated Active Entity	Active chassis name linked to the active chassis.
Associated Standby Entity	Standby chassis name linked to the standby chassis.
VSL Interfaces Table	
Name	Name of the interface on which VSS is configured.
Associated Entity	Associated entity linked to the interface on which LAG and VSS are configured.
Status	Interface status: UP or DOWN

Viewing Switch Virtual Redundancy State in Physical Inventory

To view the virtual switch redundancy state in the physical inventory:

Step 1 In the Vision client, double-click the Cat 6500 VSS device to open the **Inventory** window.

Step 2 In the **Inventory** window, expand the Physical Inventory node.

Step 3 Click **Chassis** and click an SUP card.

Step 4 In the SUP card details window, the VSS redundancy state is displayed.

Figure 32-2 depicts the redundancy states of virtual switching system:

Figure 32-2 Redundancy States of Virtual Switching System

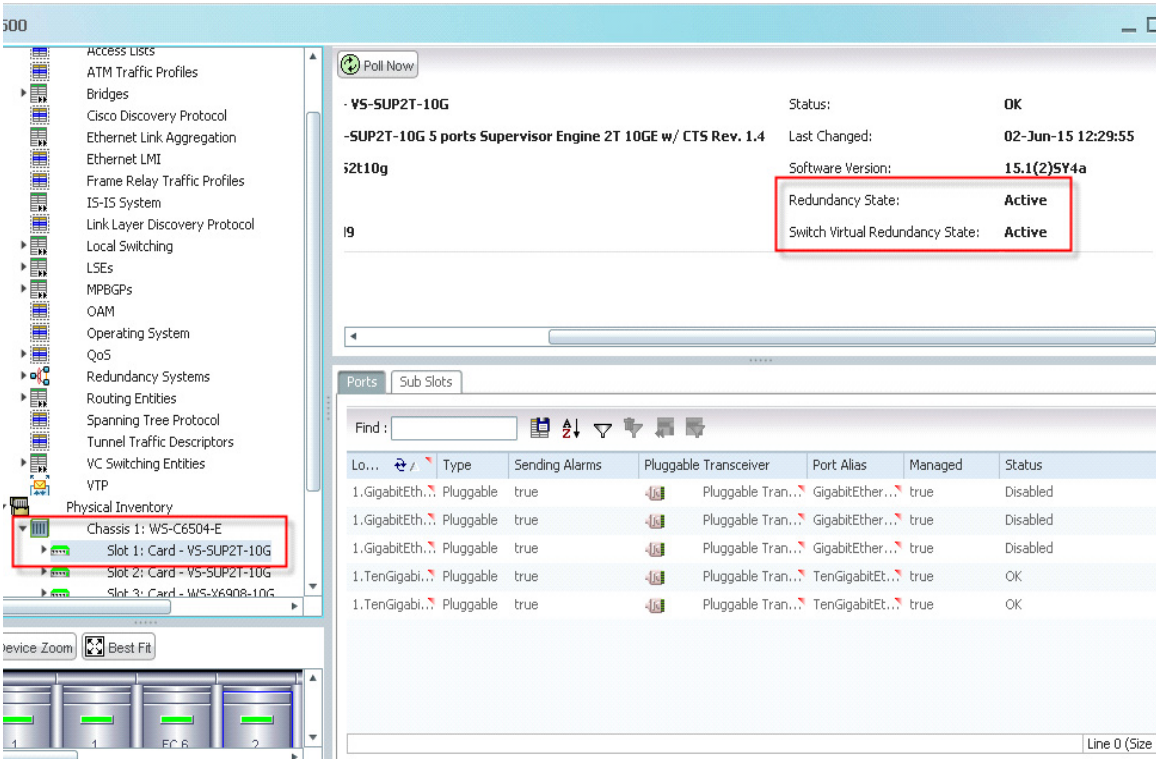


Table 32-2 describes the information displayed for the VSL link:

Table 32-2 Virtual Switch Virtual Redundancy State

Switch Virtual Redundancy State Value	Description
Active	This RP is in active state
Standby HOT (Chassis)	This RP is in standby state for this chassis (not ready to take over)
Standby HOT (Switchover Target)	This RP is in standby state and ready to take over
NA	Not Applicable as the system is not operating in VSS mode

Virtual Switch Link

Any device connected to VSS system, if there is a Virtual switch link (VSL) failure from the device to the first active chassis, then the system internally runs SSO and creates a VSL link with the second active chassis. Hence there is no network failure seen in the device connected to the VSS system.

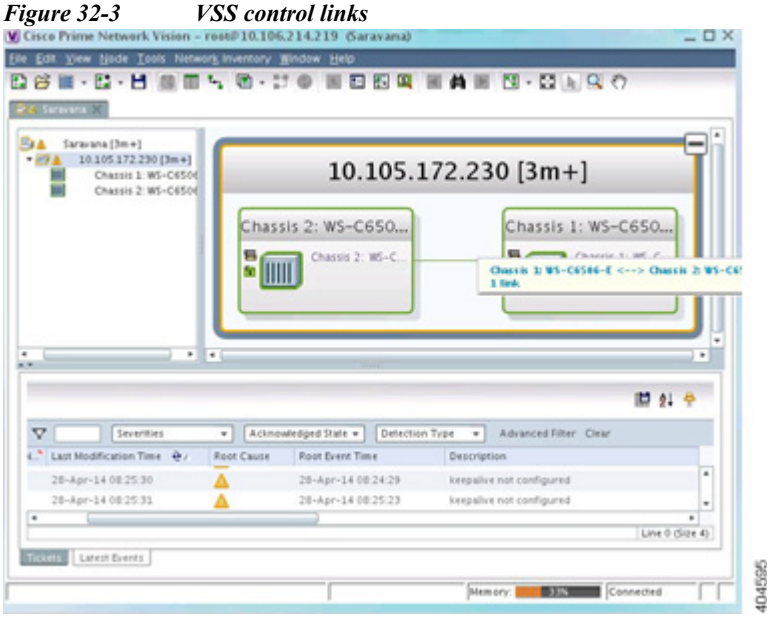
Viewing VSL Link Properties

To view the VSL link properties between two virtual switches:

Step 1 In the Vision client map view, select a link connected between two chassis in Cat 6500 VSS device and open the link quick view window.

Figure 32-3 depicts the VSS control links:

Figure 32-3 VSS control links



Step 2 In the link quick view window, click **Properties**.

Step 3 In the link **properties** window, select the VSL link to display the link properties.

Figure 32-4 depicts the link properties:

Figure 32-4 Link properties

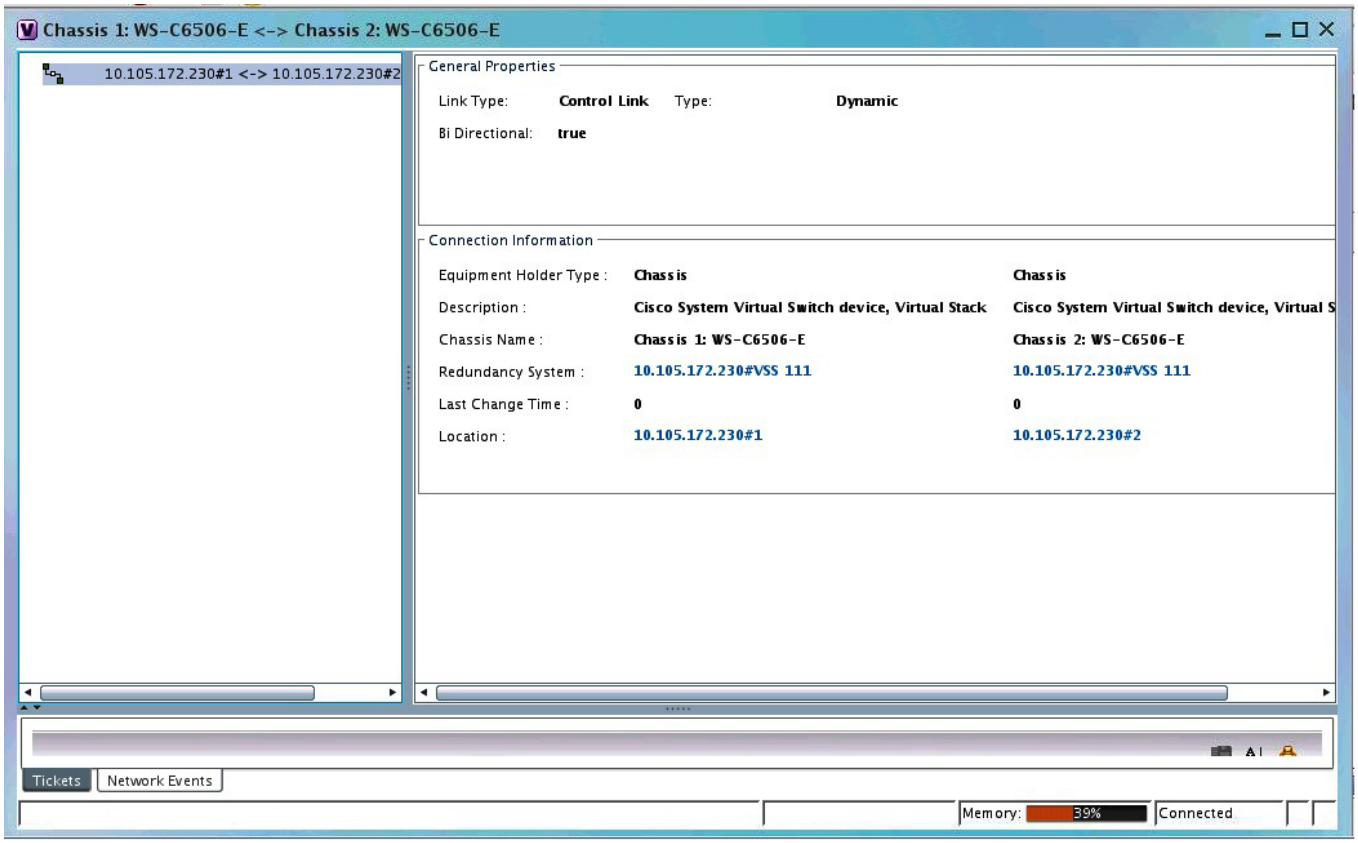


Table 32-3 describes the information that is displayed for the VSL link

Table 32-3 VSL Link Properties

Field Name	Description
General Properties	
Link Type	Link protocol. In this case, Control Link.
Type	Type of link: Dynamic or Static.
Bi Directional	Whether the link is bidirectional: True or False.
Connection Information	
Equipment Holder Type	Chassis
Chassis Name	Chassis names of the two virtual switches.
Description	Cisco System Virtual Switch device, virtual stack.
Redundancy System	Links to the associated redundancy system.
Location	Links to chassis of the associated virtual switches.

vssredundancysystem.html

Icon Reference

The following topics identify the buttons, icons, and badges used in the Vision client and the Events client:

Icons

Icons are categorized into these four classes:

NE Type Icons

When an NE icon changes color, that means it has a ticket, and the ticket has the severity indicated by the color (see Severity Icons and Colors for Events, Tickets, and NEs, page A-15). Depending on the icon size, the following information may also be displayed:

- Element model
- IP address
- Software version
- Inventory button
- Filter Tickets button
- Attach Business Ta g button

Icon	Network Element
	Access pseudowire Router
	Cisco ASA device
	ATM switch
	Basic rate access (BRA)
	Cisco 7600 series router
	Cisco ASR 1000 series router
	Cisco ASR 5000 series router
	Cisco ASR 9000 series router
	Cisco CRS series router
	Cisco IOS XR 12000 series router
	Cisco MWR 3941
	Cisco ME-3800 and Cisco ME-3400 series routers
	Cisco Nexus 1000 series
	Cisco Unified Computing System (UCS) 6100 series
	Cloud

Icon	Network Element
	Digital subscriber line access multiplexer (DSLAM)
	Ethernet switch
	Generic Server
	Generic SNMP device
	Ghost, or unknown device
	ICMP device
	Lock, or security violation; viewable by a user with a higher permission level
	Missing icon, displayed in either of the following situations: • A device has been deleted using the Administration client, but remains in the map. • A unique icon for an element (physical or logical) does not exist.
	Cisco MDS device
	Nexus 5000 Series device
	Nexus 7000 Series device
	Sun Netra server
	PC
	Printer

Icon	Network Element
	RFGW-10 device
	Service control switch
	UBR 10012 device
	UCS C Series device
	vCenter device
	Virtual Security Gateway (VSG) device
	WiFi element

Business Element Icons)

Icon	Business Element	Additional Information That May Be Displayed with Element
	Aggregation or root node	
	Backup pseudowire edge	• Local IP address • Peer IP address • Attach Business Tag button • Inventory button • Properties button
	Business IP interface	
	• Connection termination point (TP) • Ethernet flow point (EFP) • MToP service	Ethernet Flow Points may display: • Type, such as Trunk, Access, Dot1Q Tunnel, and so on • Match criteria

Icon	Business Element	Additional Information That May Be Displayed with Element
	Customer	
	EFP cross-connect	
	Ethernet service	• Number of edge EFPs
	Ethernet virtual connection (EVC)	• Number of instances of domains (VPLS, EoMPLS, bridge, or cross-connect) with a maximum of four 5.3
	Label-Switched Path (LSP) endpoint	• (Applies to both working and protected) • Bandwidth • Attach Business Tag button • Properties button
	LSP midpoint	• Forward bandwidth • Reverse bandwidth • Reverse in and out labels • Attach Business Tag button • Inventory button • Properties button
	Network LSP	
	Network pseudowire	
	Network TP tunnel	MPLS TP tunnel: • Attach Business Tag button • Properties button
	Network VLAN	• Name in card body • Number of switching entities • Number of edge EFPs
	Protected LSP	
	Pseudowire edge	

Icon	Business Element	Additional Information That May Be Displayed with Element
	Pseudowire switching entity	
	Site	
	Subnet	
	Switching entity	
	TP tunnel endpoint	• Tunnel identifier • Attach Business Tag button • Inventory button • Properties button
	Virtual router	
	VPLS forward	• VPN identifier • Number of core pseudowires
	VPLS instance	• Number of access EFPs • Number of access pseudowires • Number of VPLS forwards
	VPN	• Attach Business Tag button • Properties button
	Working LSP	

NE Logical Inventory Icons

Icon	Logical Inventory Item
	Access Lists ATM Traffic Profiles Bidirectional Forwarding Detection (BFD) Cisco Discovery Protocol (CDP) Clock DTI Client Ethernet LMI Fiber Node Frame Relay Traffic Profiles IP SLA IP Pool Dynamic Config Templates QoS Link Layer Discovery Protocol (LLDP) Modular OS Operating System Operations, Administration, and Maintenance (OAM) Resilient Ethernet Protocol (REP) Session Border Controller Spanning Tree Protocol Tunnel Traffic Descriptors BBA Groups Policy Container
	Access Gateway ARP Entity Bridges Ethernet Link Aggregation GRE Tunnels ICCP Redundancy container IMA Groups Local Switching LSEs MLPPP MPBGPs Multicast Multiple Spanning Tree protocol (MST) instance OSPF Processes Pseudowires Routing Entities Traffic Engineering Tunnels VC Switching Entities VRFs VSIs VPC Domain BNG DHCP Service

Icon	Logical Inventory Item
	AAA Group MAC Domain Narrowband Channels QAM Domain Wideband Channels
	Probe
	Y.1731 Probe
	Bridge May also display this information: • Name in card title and body • Number of Ethernet flow points
	Connectivity Fault Management (CFM) Maintenance Association
	CFM Maintenance Domain
	Connectivity Fault Management
	Context, for devices that support multiple virtual contexts
	Cross-VRF
	Encapsulation
	ICCP Redundancy group
	Inverse Multiplexing over ATM (IMA) group
	Label switching
	Layer 2 Tunnel Protocol (TP) peer

Icon	Logical Inventory Item
	Logical inventory
	Virtual Switch Interface (VSI)
	VLAN Trunk Protocol (VTP)
	Mobile node
	GGSN / SAE-GW / P-GW / S-GW / EGTP / GTPP container
	GGSN / SAE-GW / P-GW / S-GW / EGTP / GTPP
	GTPU
	APN container
	APN
	ACS
	Operator policy
	APN profile / APN remap
	Virtual data center
	Data store
	Data stores container

Icon	Logical Inventory Item
	Host server or hypervisor
	Host servers/hypervisor container
	Virtual machine
	Virtual machines container
	VSAN
	Compute Resource Pool

NE Physical Inventory Icons

Icon	Device
	Chassis
	Cluster
	Satellite
	Shelf
	Slot/Subslot
	Port/Logical Port
	Unmanaged Port

Links

The following sections describe link icons and characteristics:

- Link Icons, page A-12
- Link Colors, page A-13
- Link Characteristics, page A-13

Link Icons

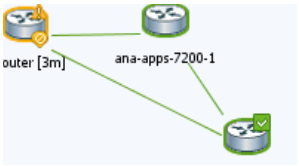
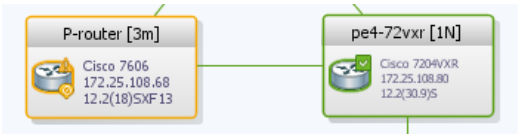
Icon	Description	Icon	Description
	Asynchronous Transfer Mode		Unknown
	Bidirectional Forwarding Detection		Physical layer
	Border Gateway Protocol		Private Network-to-Network Interface
	Business link		Point-to-Point Protocol
	Ethernet		Pseudowire
	Frame Relay		Serial
	Generic Routing Encapsulation		MPLS TE Tunnel
	Internal		MPLS TP Tunnel
	IP		VLAN
	Link aggregation group		IPv6 VPN over IPv4-MPLS
	Multilink Point-to-Point Protocol		VPN
	MPLS		Fiber Channel
	Entity Association		Inter-Control Center Communications Protocol

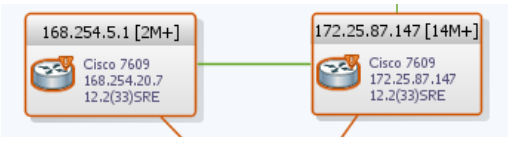
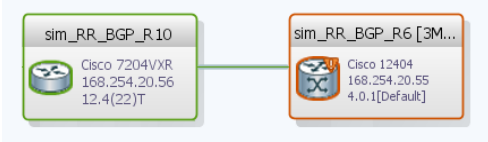
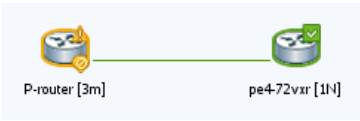
Icon	Description	Icon	Description
	Open Shortest Path First Protocol		Virtual Switching System
	Control Link		

Link Colors

Color	Severity	Description
	Critical	Critical alarm is on the link.
	Major	Major alarm is on the link.
	Minor	Minor alarm is on the link.
	Normal	Link is operating normally.
	Selected	Link is selected.

Link Characteristics

Example	Description
Solid Line vs. Dashed Line	
	Solid line—Physical, topological, or service link, such as a link between two devices.
	Dashed line—Association or *business link* between such elements as EVCs, VPLS service instances, or VPN components.
Link Widths	
	Normal—Contains links of the same group. Available groups are: • Business • GRE • MPLS-TP • Pseudowire • VLAN • All others

Example	Description
	Wide—Aggregated links that contain links of different groups. When viewing a map at a low zoom level, aggregated links cannot be distinguished in the client.
	Tunnel—The center color represents the severity of any alarms on the link.
Arrowhead vs. No Arrowhead	
	No arrowhead—Bidirectional link.
	Arrowhead Unidirectional link, with the flow in the direction of the arrowhead.

Severity Icons and Colors for Events, Tickets, and NEs

Icon	Color	Severity
	Red	Critical
	Orange	Major
	Yellow	Minor
	Light Blue	Warning
	Green	Cleared, Normal, or OK
	Medium Blue	Information
	Dark Blue	Indeterminate

When new tickets are accumulated, a label is displayed in the navigation pane and map, based on the following formula:

n s [+]

where:

Symbol	Description
n	The number of alarms with the highest severity that have the source as the network element and are part of the network element ticket(s).
s	The highest severity level in the new tickets: • C = Critical • M = Major • m = Minor • W = Warning • N = Normal (cleared alarm) • i = Informational
+	Additional, less severe tickets (optional) exist.

For example:

- An object with three critical new alarms, two major alarms, and one warning alarm is labeled 3C+.
- An object with five minor new alarms is labeled 5m.

Buttons (Maps, Tables, Links, Events, Tickets, Reports)

The following topics describe the buttons used in the Vision client:

Prime Network Vision Buttons

Button	Function
	Opens the Network Elements tab.
Map Options	
	Creates a new map in the database.
	Opens a map saved in the database using the Open dialog box.
	Adds a network element to the map or to the subnetwork selected in the navigation pane and displayed in the content pane.
	Saves the current map (the background and the location of devices) to the database.
Viewing Options	
	Displays the map view in the Vision client content pane (the button toggles when selected or deselected).
	Displays the list view in the Vision client content pane (the button toggles when selected or deselected).
	Displays the links view in the Vision client content pane (the button toggles when selected or deselected).
Overlay Tools	
	• Chooses and displays an overlay of a specific type on top of the elements displayed in the content pane in the map view. Ethernet Service • MPLS-TP Tunnel • Network Clock • Pseudowire • VLAN • VPLS • VPN • None—Removes the existing overlays. When an overlay is selected, all the elements and links that are part of the overlay are colored, and those that are not part of the overlay are dimmed.

Button	Function
	Displays or hides a previously defined overlay of a specific type on top of the elements displayed in the content pane in map view. **Note** Overlays do not reflect changes that occur in the selected service. As a result, the information in an overlay can become stale.
	Refreshes the overlay.
Navigation Tools	
	Moves up a level (goes to parent) in the navigation pane and map pane to enable you to view different information.
	Opens the Link Filter dialog box, enabling you to display or hide different types of links in the map and links views. If a link filter is applied to the map, the Link Filter Applied button is displayed instead.
	Indicates a link filter is currently applied to the map and opens the Link Filter dialog box so you can remove or modify the existing link filter. If no link filter is applied to the map, the Link Filter button is displayed instead.
	Opens a window displaying an overview of the network.
Search Tools	
	Finds the previous instance of the search string entered in the Find in Map dialog box.
	Opens the Find in Map dialog box, enabling you to find a device or aggregation in the map by its name or IP address.
	Finds the next instance of the search string entered in the Find in Map dialog box.
	Opens the Find Business Tag dialog box, enabling you to find and detach a business tag according to a name, key, or type.
Map Zoom and Layout Tools	
	Defines the way in which the NES are arranged in the Vision client map view: circular, hierarchical, orthogonal, or symmetric.
	Fits the entire subnetwork or map in the map pane.
	Activates the normal selection mode.

Button	Function
	Activates the zoom selection mode, which enables you to select an area in the map pane to zoom in on by clicking and dragging.
	Activates the pan mode, which enables you to move around in the map pane by clicking and dragging.
Print Preview Options	
	Opens the Printer Setup dialog box so you can specify your print settings.
	Opens the Print dialog box so you can print the displayed network or map to the required printer.
	Zooms in on the network or map.
	Zooms out of the network or map.
	Displays the entire network or map in the Print Preview window.

Table Buttons

Icon	Name	Description
	Find	Searches the current table for the string you enter.
	Export to CSV	Exports the information displayed in the list view. Either the selected rows are exported, or, when nothing is selected, the entire table is exported.
	Sort Table Values	Sorts the information displayed in the list view (for example, according to *element category*).
	Filter	Filters the information displayed in the table by the criteria you specify.
	Clear Filter	Clears the existing filter.
	Show All Rows	Displays all table rows that meet the current filtering criteria.
	Show Only Selected Rows	Displays only the rows that you select.

Link Filtering Buttons

Button	Name	Description
	All Links	Displays the complete list of links for the selected context (map or aggregation). In other words, the list is not filtered and all the links are displayed, including external links.
	External Links	Displays links with only one side of the link in this context (map or aggregation) and the other side either not in the map or outside the selected context.
	Flat Links	Displays the links currently visible on the map for the selected context (map or aggregation), excluding any thumbnails.
	Deep Links	Displays the links for the current aggregation where both endpoints are within the currently selected context.

Events client Buttons

Button	Function
	Displays the previous page of events in the Events client window.
	Displays the next page of events in the Events client window.
	Refreshes the events displayed in the log by querying the database. If a filter is active, the refresh is done according to the filter. The log returns to the beginning of the list, displaying the events in ascending or descending order depending on the order of the current list. Descending order means that the last event is displayed first.
	Displays the Events client Filter dialog box, which enables you to define a filter for the events displayed in the Events client log.
	Toggles automatic refresh of event data on and off. You define the refresh-time period (in seconds) in the Events client Options dialog box. The default is 60 seconds. If a filter is active, the refresh is done according to the filter.
	Displays the properties of the selected event or ticket in the Properties pane.

Ticket Properties Buttons

Icon	Description
	Refreshes the information displayed in the Ticket Properties dialog box.
	Acknowledges that the ticket is being handled. The status of the ticket is displayed as true in the ticket pane and in the Ticket Properties dialog box. If a ticket was acknowledged, and some events were correlated to it afterward, then the ticket is considered to have not been acknowledged. This button is enabled only if the ticket is not acknowledged.
	Requests the relevant Prime Network system to remove the faulty network element from the Prime Network networking inventory. In addition, it sets the ticket to Cleared severity or status (the icon is displayed in green) and automatically changes the acknowledged status of the ticket to true. This button is enabled only if the severity of the alarm is higher than Cleared or Normal.
	Clicking on this ticket will deacknowledge a ticket.
	Saves the notes for the selected ticket. This button is enabled only when text is entered in the Notes field of the Notes tab.

Report Manager Buttons

Table A-1 Report Manager Buttons

Icon	Name	Description
	Define Report of This Type	Enables you to define a report of this type that is suited specifically to your environment.
	Delete	Deletes one or more folders that you created.
	Delete Report	Deletes the selected report.
	Move	Moves one or more folders or reports that you created.
	New Folder	Creates a new folder
	Rename	Renames a folder that you created.
	Run	Generates the selected report
	View	Displays the selected report in HTML format.

Badges

Badges are small icons that appear with other network elements, such as element icons or links. The following topics describe the badges used by the Vision client and the Events client:

- VNE Communication State Badges, page A-23
- VNE Investigation State Badges, page A-23
- Network Element Technology-Related Badges, page A-24

VNE Communication State Badges

Badge	State Name	Description
None	Agent Not Loaded	The VNE is not responding to the gateway because it was stopped, or it was just created. This communication state is the equivalent of the Defined Not Started investigation state.
	VNE/Agent Unreachable	The VNE is not responding to the gateway. This can happen if the unit or AVM is overutilized, the connection between the gateway and unit or AVM was lost, or the VNE is not responding in a timely fashion. (A VNE in this state does not mean the device is down; it might still be processing network traffic.)
None	Connecting	The VNE is starting and the initial connection has not yet been made to the device. This is a momentary state. Because the investigation state decorator (the hourglass) will already be displayed, a special client decorator is not required.
	Device Partially Reachable	The element is not fully reachable because at least one protocol is not operational.
	Device Unreachable	The connection between the VNE and the device id down because all of the protocols are down (though the device might be sending traps or syslogs).
None	Tracking Disabled	The reachability detection process is not enabled for any of the protocols used by the VNE. The VNE will not perform reachability tests nor will Prime Network generate reachability-related events. In some cases this is desirable; for example, tracking for Cloud VNEs should be disabled because Cloud VNEs represent unmanaged network segments.

VNE Investigation State Badges

Badge	State Name	Description
None	Defined Not Started	A new VNE was created (and is starting); or an existing VNE was stopped. In this state, the VNE is managed and is validating support for the device type. (This investigation state is the equivalent of the Agent Not Loaded communication state.) A VNE remains in this state until it is started (or restarted) by a user.
	Unsupported	The device type is either not supported by Prime Network or is misconfigured (it is using the wrong scheme, or is using reduced polling but the device does not support it). To extend Prime Network functionality so that it recognizes unsupported devices, use the VNE Customization Builder. See the *Cisco Prime Network 5.3 Customization Guide*.
	Discovering	The VNE is building the model of the device (the device type was found and is supported by Prime Network). A VNE remains in this state until all device commands are successfully executed at least once, or until there is a discovery timeout.
None	Operational	The VNE has a stable model of the device. Modeling may not be fully complete, but there is enough information to monitor the device and make its data available to other applications, such as activation scripts. A VNE remains in this state unless it is stopped or moved to the maintenance state, or there are device errors.

Badge	State Name	Description
	Currently Unsynchronized	The VNE model is inconsistent with the device. This can be due to a variety of reasons; for a list of these reasons along with troubleshooting tips, see the topic on troubleshooting VNE investigation state issues in the *Cisco Prime Network 5.3 Administrator Guide*.
	Maintenance	VNE polling was suspended because it was manually moved to this state (by right-clicking the VNE and choosing **Actions > Maintenance**). The VNE remains in this state until it is manually restarted. A VNE in the maintenance state has the following characteristics: • Does not poll the device, but handles syslogs and traps. • Maintains the status of any existing links. • Does not fail on VNE reachability requests. • Handles events for correlation flow issues. It does not initiate new service alarms, but does receive events from adjacent VNEs, such as in the case of a Link Down alarm. The VNE is moved to the Stopped state if: it is VNE is moved, the parent AVM is moved or restarted, the parent unit switches to a standby unit, or the gateway is restarted.
	Partially Discovered	The VNE model is inconsistent with the device because a required device command failed, even after repeated retries. A common cause of this state is that the device contains an unsupported module. To extend Prime Network functionality so that it recognizes unsupported modules, use the VNE Customization Builder. See the *Cisco Prime Network 5.3 Customization Guide*.
	Shutting Down	The VNE has been stopped or deleted by the user, and the VNE is terminating its connection to the device.
None	Stopped	The VNE process has terminated; it will immediately move to Defined Not Started.

Network Element Technology-Related Badges

Icon	Name	Description	Related Topics
	Access gateway	An MST or REP access gateway is associated with the element.	Viewing Access Gateway Properties, page 18-14
	Blocking	The element associated with this badge has a REP alternate port.	Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 18-80
	REP primary blocking	The element associated with this badge has a REP primary port that is also blocking.	Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 18-80
	REP primary	The element associated with this badge has a REP primary port.	Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 18-80

Icon	Name	Description	Related Topics
	Clock service	A clocking service is running on the associated element.	Viewing CEM Interfaces, page 26-50
	Lock	The associated network LSP is in lockout state.	Viewing MPLS-TP Tunnel Properties, page 17-9
	Redundancy service	The element associated with this badge is a backup pseudowire or a protected LSP.	• Adding an MPLS-TP Tunnel, page 17-7 • Viewing Pseudowire Redundancy Service Properties, page 18-113
	Multiple links	One or more links is represented by the visual link and at least one of the links contains a badge.	Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 18-80
	Reconciliation	The element with this badge is associated with a network element that does not exist. For example, the device configuration has changed and a network problem exists. Some elements can be deleted only if their components, such as EFPs, VPLS forwards, or VRFs, display the reconciliation icon.	Labelling NEs to Associate Them with Customers (Business Tags), page 4-9
	STP root	The element associated with this badge is a STP root bridge or the root of an STP tree.	Viewing STP Information in VLAN Domain Views and VLAN Overlays, page 18-83

Permissions Required to Perform Tasks Using the Prime Network Clients

Users are allowed to view and manage devices and services depending on how their user account is configured.

- For GUI operations that do not affect network elements, authorization is based on the default permission that is assigned to your user account.
- For NE operations (tasks that do affect elements), authorization is based on whether the element is in one of your assigned *device scopes* and whether you meet the minimum security level for that scope.

For more information on user authorization, see the *Cisco Prime Network 5.3 Administrator Guide*.

These topics provide tables that describe the permissions required to perform tasks in Prime Network.

- Vision Client Permissions, page B-1—Basic operations, map and inventory window operations, Cisco PathTracer, link operations, ticket operations
- Events Client Permissions, page B-7—All operations performed from the Events client.
- Change and Configuration Management (CCM) Permissions, page B-8—Device configuration and software image file management
- Permissions for Business Tags and Business Elements (Vision and Events Clients), page B-10—Labels that are applied to NEs
- Reports Permissions (Vision and Events Clients), page B-10—The native reports feature that is launched from the **Reports** menu
- Technologies and Services Permissions, page B-12—The technologies and services that are managed from the Vision client inventory window

Vision Client Permissions

Permissions for Vision Client Basic Operations

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Start the Prime Network Vision client	X	X	X	X	X
Change a user password in the Vision client	—[1]	—[1]	—[1]	—[1]	X[1]
Set Prime Network Vision client options	X	X	X	X	X
Work with Vision client tables	X	X	X	X	X

1. Each user can change their own password, but only the Administrator role can change another user's password.

Permissions for Vision Client Maps

Vision Client Maps—NEs in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Map-Related Tasks					
Apply a background image	—	—	—	X	X
Create maps	—	—	X	X	X
Define a map layout	X	X	X	X	X
Delete maps	—	—	X	X	X
Open maps	X	X	X	X	X
Preview and print maps	X	X	X	X	X
Rename maps	—	—	X	X	X
Save as a new map	—	—	X	X	X
Save as an image	X	X	X	X	X
Save map appearance	—	—	X	X	X
Select viewing options	X	X	X	X	X
Use Overview window	X	X	X	X	X
View maps	X	X	X	X	X
Element-Related Tasks					
Add elements to a map	—	—	X	X	X
Remove elements from a map	—	—	X	X	X
Resize elements in a map	X	X	X	X	X
Aggregation-Related Tasks					
Group and ungroup aggregations	—	—	X	X	X
Rename aggregations	X	X	X	X	X
View aggregation thumbnails	X	X	X	X	X

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Finding Items in Maps					
Find affected elements	X	X	X	X	X
Find an element or service	X	X	X	X	X
Find and select a link in a map[1]	X	X	X	X	X
Link-Related Task					
Filter links	X	X	X	X	X
Overlay-Related Tasks					
Apply an overlay	X	X	X	X	X
Hide or view an overlay	X	X	X	X	X
Remove an overlay	X	X	X	X	X
Other Tasks					
Open the CPU Usage Graph	—	—	X	X	X
Use Ping and Telnet to communicate with devices	—	—	—	X	X

1. This applies to links within the selected context, and not links identified as network links.

Vision Client Maps—NEs Not in User's Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Map-Related Tasks					
Apply a background image	—	—	—	X	X
Create maps	—	—	X	X	X
Define a map layout	X	X	X	X	X
Delete maps	—	—	X	X	X
Open maps	X	X	X	X	X
Preview and print maps	X	X	X	X	X
Rename maps	—	—	X	X	X
Save as a new map	—	—	X	X	X
Save as an image	X	X	X	X	X
Save map appearance	—	—	X	X	X
Select viewing options	X	X	X	X	X
Use Overview window	X	X	X	X	X
View maps	X	X	X	X	X
Element-Related Tasks					
Add elements to a map	—	—	X	X	X
Remove elements from a map	—	—	X	X	X
Resize elements in a map	X	X	X	X	X

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Aggregation-Related Tasks					
Group and ungroup aggregations	—	—	X	X	X
Rename aggregations	X	X	X	X	X
View aggregation thumbnails	X	X	X	X	X
Finding Items in Maps					
Find affected elements	—	—	—	—	X
Find an element or service	X	X	X	X	X
Find and select a link in a map[1]	X	X	X	X	X
Link-Related Task					
Filter links	X	X	X	X	X
Overlay-Related Tasks					
Apply an overlay	X	X	X	X	X
Hide or view an overlay	X	X	X	X	X
Remove an overlay	X	X	X	X	X
Other Tasks					
Open the CPU Usage Graph	—	—	—	—	X
Use Ping and Telnet to communicate with elements	—	—	—	—	X

1. This applies to links within the selected context, and not links identified as network links.

Permissions for Vision Client NE-Related Operations

Vision Client NE Operations—NEs in User's Device Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View maps	X	X	X	X	X
View network element properties	X	X	X	X	X
View network element properties in logical and physical inventory	X	X	X	X	X
View port status and properties	—	X	X	X	X
View VNE properties	X	X	X	X	X
Launch command (*NE* > **Commands**)	—[1]	—[1]	—[1]	X[1]	X[1]
Open the Port Utilization Graph	X	X	X	X	X
Enable and disable port alarms	—	—	—	X[2]	X[2]
View tickets in inventory window	X	X	X	X	X
View network events in inventory window	X	X	X	X	X
View provisioning events in inventory window	X	X	X	X	X

1. Most commands provided with Prime Network require Configurator privileges. For commands created using Command Manager or Command Builder, the access role is specified when the command is created.
2. To enable and disable port alarms on a device, the Administrator scope level must also be configured for that device.

Vision Client NE Operations—NEs Not in User's Device Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View maps	X	X	X	X	X
View network element properties	—	—	—	—	X
View network element properties in logical and physical inventory	—	—	—	—	X
View port status and properties	—	—	—	—	X
View VNE properties	—	—	—	—	X
Launch command (*NE* > **Commands**)	—[1]	—[1]	—[1]	X[1]	X[1]
Open the Port Utilization Graph	—	—	—	—	X
Enable and disable port alarms	—	—	—	—	X[2]
View tickets in inventory window	—	—	—	—	X
View network events in inventory window	—	—	—	—	X
View provisioning events in inventory window	—	—	—	—	X

1. Most commands provided with Prime Network require Configurator privileges. For commands created using Command Manager or Command Builder, the access role is specified when the command is created.

Permissions for Vision Client Cisco PathTrace

Vision Client PathTrace—NEs in User's Device Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Launch a path trace	—	X	X	X	X
View path information	—	X	X	X	X
Save Cisco PathTracer map files	—	X	X	X	X
Save Cisco PathTracer counter values	—	X	X	X	X
Rerun a path and compare results	—	X	X	X	X

Vision Client PathTrace—NEs Not in User's Device Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
All actions	—	—	—	—	X
View path information	—	—	—	—	X
Save Cisco PathTracer map files	—	—	—	—	X
Save Cisco PathTracer counter values	—	—	—	—	X
Rerun a path and compare results	—	—	—	—	X

Permissions for Vision Client Links

Vision Client Links—NEs in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View link properties in Map view	X	X	X	X	X
View link properties in Links view	X[1]	X[1]	X[1]	X[1]	X
View link properties in the Link Properties window	X	X	X	X	X
View link impact analysis	—	—	—	—	X
Add static links	—	—	—	X	X
Filter links using collection method	X	X	X	X	X
Find and select a link in a map	X	X	X	X	X

1. Link properties are limited in the Links view; not all information is available.

Links: NEs Not in User's Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View link properties in Map view	X[1]	X[1]	X[1]	X[1]	X
View link properties in Links view	X[2]	X[2]	X[2]	X[2]	X
View link properties in the Link Properties window	—	—	—	—	X
View link impact analysis	—	—	—	—	X
Add static links	—	—	—	—	X
Filter links using collection method	X	X	X	X	X
Find and select a link in a map	X	X	X	X	X

1. Link properties are limited in the Map view; not all link information is available.
2. Link properties are limited in the Links view; not all link information is available.

Permissions for Tickets in Vision Client

The following conditions apply when working with tickets in the Vision client:

- If an element that is outside of your scope is the root cause of a ticket that affects an element in your scope, you can view the ticket in the Vision client, but you will not be able to:
  - View inventory by clicking the Location hyperlink.
  - Acknowledge, deacknowledge, clear, add note, or remove the ticket.
- You can acknowledge, deacknowledge, clear, remove, or add notes for a ticket only if you have OperatorPlus or higher permission for the element that holds the root alarm for that ticket.
- If the source or contained sources of the ticket are not in your scope, you cannot view the ticket in the ticket table, view ticket properties, or perform actions on the ticket.
- If the ticket contains a source that is in your scope, but the source is not the root cause, you can view the ticket in the ticket table and view ticket properties, but you cannot perform actions on the ticket.
- If the source of the ticket is in your scope, you can view the ticket in the ticket table, view ticket properties, filter tickets, and perform actions on the ticket.
- By default, users with the Administrator role have access to all managed elements and can perform any action on tickets. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 5.3 Administrator Guide*.

The following table identifies the roles required to perform the high level tasks:

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Acknowledge/deacknowledge tickets	—	—	X[1]	X	X
Add notes to a ticket	—	—	X[1]	X	X
Clear and remove tickets	—	—	X[1]	X	X
Clear tickets	—	—	X[1]	X	X
Filter tickets	X	X	X	X	X
Find affected elements	X	X	X	X	X
Remove tickets	—	—	X[1]	X	X
View ticket properties	X	X	X	X	X
View tickets	X	X	X	X	X

1. In addition, the security level for the device scope must be OperatorPlus or higher for the device that holds the root alarm for a ticket.

Events Client Permissions

This topic identifies the roles that are required to work with the Events client. Prime Network determines whether you are authorized to perform a task as follows:

- For GUI operations that do not affect elements, authorization is based on the default permission that is assigned to your user account.
- For NE operations (tasks that do affect elements), authorization is based on the default permission that is assigned to your account. That is, whether the element is in one of your assigned scopes and whether you meet the minimum security level for that scope.

Change and Configuration Management (CCM) Permissions

Note In CCM, the user role always takes precedence over the device scope security level.

Task	Minimum GUI Access Role	Minimum Device Scope Security Level
Dashboard		
Access top families	Viewer	Viewer
Access configuration sync status	Viewer	Viewer
Access configuration changes in the last week	Viewer	Viewer
Access most recent configuration changes	Viewer	Viewer
Configuration Management		
View configuration archives	Viewer	Viewer
View files in archive	Viewer	N/A
Compare files in archive	Viewer	N/A
Compare the latest configuration in device	Viewer	OperatorPlus
Synchronize configurations	Viewer	Configurator
Back up (copy) files from devices to archive	Viewer	OperatorPlus
Restore files from archive to devices	Configurator	Configurator
Edit configuration files before restoring them to devices	Configurator	Configurator
Edit the edited archive version of configuration files and restore them to devices	Configurator	Configurator
View configuration change logs	Viewer	Viewer
Delete configuration files from archive	Configurator	N/A
Manage labels for archive files[1]	Configurator	N/A
Add and edit comments for archive file	Configurator	N/A
Export configuration files from archive	Configurator	N/A
Edit configuration file from archive	Configurator	N/A
Edit configuration file and restore it to device	Configurator	N/A
Restore the edited archive versions of configuration file to device	Configurator	N/A
Restore configuration files	Viewer	N/A
Image Management		
Upload software image from device to repository	Configurator	OperatorPlus
Distribute images	Configurator	Configurator
Activate and deactivate images	Configurator	Configurator
Commit image changes	Configurator	Configurator

Task	Minimum GUI Access Role	Minimum Device Scope Security Level
Rollback images	Configurator	Configurator
View images in repository	Viewer	N/A
Add package	Configurator	Configurator
Add images to repository	Configurator	N/A
Delete images from repository	Configurator	N/A
Import images from device	Configurator	OperatorPlus
Managing Device Groups		
Create device groups	Configurator	Configurator
Edit device group details	Configurator	Configurator
Delete device groups	Configurator	N/A
Compliance Audit		
Create policies	Configurator	N/A
Create policy profiles	Operator	N/A
Execute audit job	Operator	Operator
View audit job results	Operator	Operator
Execute a Fix job **Note** To execute a fix job, the device-level role of the user must be Configurator or Administrator. The role of the user for a device overrides the role of a user on Prime Network.	Configurator	OperatorPlus
View the fix job results[2]	Configurator	OperatorPlus
Configuration Audit		
Define configuration policies	Configurator	Configurator
Schedule configuration audit	Configurator	Configurator
View configuration audit jobs and audit results	OperatorPlus	OperatorPlus
Global Tasks		
View jobs	Viewer	N/A
Administer jobs (suspend, delete, and so forth)[2]	Configurator	N/A
Change settings	Configurator	N/A

1. Configuration files are filtered according to the device scope of a user.
2. Users with Viewer, Operator, and OperatorPlus roles can view only their own jobs; Users with Configurator role can view and manage their own jobs; Administrators can view and manage all jobs.

If a user role is modified in Prime Network, you need to logout from CCM and then login again for the changes to get effect.

For information on how Prime Network performs user authentication and authorization, including an explanation of user access roles and device scopes, see the *Cisco Prime Network 5.3 Administrator Guide*.

Permissions for Business Tags and Business Elements (Vision and Events Clients)

Business Tags—NEs in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Attach a business tag	—	—	—	Partial[1]	X
Detach a business tag	—	—	—	Partial[1]	X
Search for a business tag	—	—	—	Partial[1]	X
View business tag properties	—	—	—	Partial[1]	X
Rename a business element	X	X	X	X	X
Delete a business element	X	X	X	X	X

1. Configurator user role default permission supports the action for business elements, which do not have scopes. The Configurator user role default permission supports the action for elements only if the elements are in the user's scope.

Business Tags—Devices Not in User's Scope (or Actions Not Related to NEs)

)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Attach a business tag	—	—	—	Partial[1]	X
Detach a business tag	—	—	—	Partial[1]	X
Search for a business tag	—	—	—	Partial[1]	X
View business tag properties	—	—	—	Partial[1]	X
Rename a business element	X	X	X	X	X
Delete a business element	X	X	X	X	X

1. Configurator user role default permission supports the action for business elements, which do not have scopes. The Configurator user role default permission supports the action for elements only if the elements are in the user's scope.

Reports Permissions (Vision and Events Clients)

Reports—NEs in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Generate Events Reports					
• Detailed Network Events Reports[1]	X	X	X	X	X
• Detailed Non-Network Events Reports	—	—	—	Partial[2]	X

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
• All other events reports	X	X	X	X	X
Generate Inventory Reports	X	X	X	X	X
Generate Network Service Reports	X	X	X	X	X

1. Detailed Ticket reports include only those tickets that have a root cause alarm associated with an element in the user's scope.
2. A user with the Configurator role can generate Detailed Provisioning Events reports for elements that are in and outside their scope.

Reports—NEs Not in User's Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Generate Events Reports					
• Detailed Network Events Reports	—	—	—	—	X
• Detailed Non-Network Events Reports	—	—	—	Partial[1]	X
• All other events reports	—	—	—	—	X
Generate Inventory Reports	—	—	—	—	X
Generate Network Service Reports	—	—	—	—	X

1. A user with the Configurator role can generate Detailed Provisioning Events reports for elements that are in and outside their scope.

Reports—Generated by User

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Schedule reports	X	X	X	X	X
Cancel reports	X	X	X	X	X
Delete reports	X	X	X	X	X
Export reports	X	X	X	X	X
Rename reports	X	X	X	X	X
Save reports	X	X	X	X	X
Set report preferences for purging and sharing	—	—	—	—	X
Share/unshare reports	X[1]	X[1]	X[1]	X[1]	X
View report properties	X	X	X	X	X
View reports	X	X	X	X	X

1. You can share or unshare reports only if sharing is enabled in the Administration client.

Reports—Generated by Other

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
All tasks	—	—	—	—	X

Reports—Report Folders

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
All tasks	—	—	—	—	X

Technologies and Services Permissions

These topics provides tables that list the permissions that are required to perform operations on devices that have the technologies or services configured on them.

Permissions for Managing Carrier Ethernet

Carrier Ethernet—NEs in User's Device Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Adding Elements to a Map					
Add associated VLANs to a map	—	—	X	X	X
Add EFP cross-connects	—	—	X	X	X
Add Ethernet services to a map	—	—	X	X	X
Add pseudowires to a map	—	—	X	X	X
Add unassociated bridges	—	—	X	X	X
Add VLANs to a map	—	—	X	X	X
Add VPLS instances to a map	—	—	X	X	X
Viewing Element Properties					
View access gateway properties	X	X	X	X	X
View associated network VLAN service links and VLAN mapping properties	X	X	X	X	X
View CDP properties	X	X	X	X	X
View EFD properties	X	X	X	X	X
View EFP cross-connect properties	X	X	X	X	X
View EFP properties	X	X	X	X	X
View Ethernet flow domains	X	X	X	X	X
View Ethernet LAG properties	X	X	X	X	X
View Ethernet service properties	X	X	X	X	X
View EVC service properties	X	X	X	X	X
View IP SLA responder service properties	X	X	X	X	X
View IS-IS properties	X	X	X	X	X
View Link Layer Discovery Protocol (LLDP) properties	X	X	X	X	X
View mLACP properties	X	X	X	X	X
View OSPF properties	X	X	X	X	X
View Provider Backbone Bridge (PBB) properties	X	X	X	X	X
View pseudowire properties	X	X	X	X	X
View pseudowire redundancy service properties	X	X	X	X	X
Viewing the PW-HE configuration	X	X	X	X	X
View REP properties	X	X	X	X	X
View REP properties for VLAN service links	X	X	X	X	X
View HSRP properties	X	X	X	X	X
View STP properties	X	X	X	X	X
View STP properties for VLAN service links	X	X	X	X	X
View VLAN bridge properties	X	X	X	X	X
View VLAN links between VLAN elements and devices	X	X	X	X	X

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View VLAN mappings	X	X	X	X	X
View VLAN service link properties	X	X	X	X	X
View VLAN trunk group properties	X	X	X	X	X
View VPLS access EFP properties	X	X	X	X	X
View VPLS core or access pseudowire endpoint properties	X	X	X	X	X
View VPLS instance properties	X	X	X	X	X
View VSI properties	X	X	X	X	X
Working with Overlays					
Apply overlays	X	X	X	X	X
Display or hide overlays	X	X	X	X	X
Remove overlays	X	X	X	X	X
View pseudowire tunnel links in VPLS overlays	X	X	X	X	X
View REP information in VLAN domain views and VLAN overlays	X	X	X	X	X
View STP information in VLAN domain views and VLAN overlays	X	X	X	X	X
Other Tasks					
Display pseudowire information	—	—	—	X	X
Ping a pseudowire	—	—	—	X	X
Remove VLANs from a map	—	—	X	X	X
Rename Ethernet flow domains	X	X	X	X	X
Using REP and mLACP Show Commands	—	—	—	X	X
Using Pseudowire Ping and Show Commands	—	—	—	X	X

Carrier Ethernet—NEs Not in User's Device Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Adding Elements to Maps					
Add associated VLANs to a map	—	—	X	X	X
Add EFP cross-connects	—	—	X	X	X
Add Ethernet services to a map	—	—	X	X	X
Add pseudowires to a map	—	—	X	X	X
Add unassociated bridges	—	—	X	X	X
Add VLANs to a map	—	—	X	X	X
Add VPLS instances to a map	—	—	X	X	X
Viewing Element Properties					
View access gateway properties	—	—	—	—	X

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View associated network VLAN service links and VLAN mapping properties	—	—	—	—	X
View CDP properties	—	—	—	—	X
View EFD properties	—	—	—	—	X
View EFP cross-connect properties	Partial[1]	Partial[1]	Partial[1]	Partial[1]	X
View EFP properties	Partial[1]	Partial[1]	Partial[1]	Partial[1]	X
View Ethernet flow domains	X	X	X	X	X
View Ethernet LAG properties	—	—	—	—	X
View Ethernet service properties	X	X	X	X	X
View EVC service properties	—	—	—	—	X
View IP SLA responder service properties	—	—	—	—	X
View IS-IS properties	—	—	—	—	X
View Link Layer Discovery Protocol (LLDP) properties	—	—	—	—	X
View mLACP properties	—	—	—	—	X
View OSPF properties	—	—	—	—	X
View Provider Backbone Bridge (PBB) properties	—	—	—	—	X
View pseudowire properties	Partial[1]	Partial[1]	Partial[1]	Partial[1]	X
View pseudowire redundancy service properties	Partial[2]	Partial[2]	Partial[2]	Partial[2]	
Viewing the PW-HE configuration	—	—	—	—	X
View REP properties	—	—	—	—	X
View REP properties for VLAN service links	—	—	—	—	X
View STP properties	—	—	—	—	X
View STP properties for VLAN service links	—	—	—	—	X
View HSRP properties	—	—	—	—	X
View virtual service instance properties	—	—	—	—	X
View VLAN bridge properties	—	—	—	—	X
View VLAN links between VLAN elements and devices	Partial[3]	Partial[3]	Partial[3]	Partial[3]	X
View VLAN mappings	—	—	—	—	X
View VLAN service link properties	—	—	—	—	X
View VLAN trunk group properties	—	—	—	—	X
View VPLS access EFP properties	—	—	—	—	X
View VPLS core or access pseudowire endpoint properties	—	—	—	—	X
View VPLS instance properties	X	X	X	X	X
Working with Overlays					
Apply overlays	X	X	X	X	X
Display or hide overlays	X	X	X	X	X
Remove overlays	X	X	X	X	X

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View pseudowire tunnel links in VPLS overlays	—	—	—	—	X
View REP information in VLAN domain views and VLAN overlays	—	—	—	—	X
View STP information in VLAN domain views and VLAN overlays	—	—	—	—	X
Other Tasks					
Display pseudowire information	—	—	—	—	X
Ping a pseudowire	—	—	—	—	X
Remove VLANs from a map	—	—	X	X	X
Rename Ethernet flow domains	X	X	X	X	X
Using REP and mLACP Show Commands	—	—	—	X	X
Using Pseudowire Ping and Show Commands	—	—	—	X	X

1. The user can view properties available via **Node > Properties** but not those available via the right-click Properties option or in logical inventory.
2. The user can view the pseudowire redundancy icon in the navigation and map panes, but not the inventory or properties window.
3. The user can view links, but the links are dimmed and do not indicate their status.

Permissions for Managing Carrier Grade NAT

Carrier Grade NAT—NEs in User's Device Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View Carrier Grade NAT properties	X	X	X	X	X
Using CG NAT Configure, Delete, and Show Commands	—	—	—	X	X

Carrier Grade NAT—NEs Not in User's Device Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View Carrier Grade NAT properties	—	—	—	—	X
Using CG NAT Configure, Delete, and Show Commands	—	—	—	X	X

Permissions for Managing DWDM

DWDM—NEs in User's Device Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View DWDM properties	X	X	X	X	X
View G.709 properties	X	X	X	X	X
View performance monitoring configuration information	X	X	X	X	X
Using IPoDWDM Configuration and Show Commands	—	—	—	X	X

DWDM—NEs Not in User's Device Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View DWDM properties	—	—	—	—	X
View G.709 properties	—	—	—	—	X
View performance monitoring configuration information	—	—	—	—	X
Using IPoDWDM Configuration and Show Commands	—	—	—	X	X

Permissions for Using Ethernet OAM Tools

Ethernet OAM Tools—NEs in User's Device Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View CFM properties	X	X	X	X	X
View Ethernet LMI properties	X	X	X	X	X
Use CFM, E-LMI, and L-OAM commands	—	—	—	X	X

Ethernet OAM Tools—NEs Not in User's Device Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View CFM, E-LMI, L-OAM properties	—	—	—	—	X
Use CFM, E-LMI, and L-OAM commands	—	—	—	X	X

Permissions for Managing Y.1731 IPSLA

Y.1731 IPSLA—NEs in User's Device Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View the Y.1731 probe properties	X	X	X	X	X
Configure Y.1731 probes	—	—	—	X	X

Y.1731 IPSLA—NEs Not in User's Device Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View the Y.1731 probe properties	X	X	X	X	X
Configure Y.1731 probes	—	—	—	X	X

Permissions for Managing MPLS Services

MPLS Services—NEs in User's Device Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
VPNs and VRFs					
Add tunnels to VPNs	—	X	X	X	X
Add VPNs to a map	—	—	X	X	X
Create VPNs	—	—	X	X	X
Display VRF egress and ingress adjacents	—	—	—	—	X
Move virtual routers between VPNs	—	X	X	X	X
Remove tunnels from VPNs	X	X	X	X	X
Remove VPNs from a map	—	—	X	X	X
View IPv6 properties	X	X	X	X	X
View VPN properties	X	X	X	X	X
View VPNs	X	X	X	X	X
View VRF properties	—	—	—	—	X
VPN Overlays					
Add VPN overlays	X	X	X	X	X
Display or hide VPN overlays	X	X	X	X	X
Remove VPN overlays	X	X	X	X	X
Routing Entities					
View the ARP table	X	X	X	X	X
View the NDP table	X	X	X	X	X
View rate limit information	X	X	X	X	X
Other					
View 6RD properties	X	X	X	X	X
View BFD properties	X	X	X	X	X
View cross-VRF routing entries	X	X	X	X	X
View LSE properties	X	X	X	X	X
View MP-BGP information	X	X	X	X	X
View MPLS TE tunnel information	X	X	X	X	X

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View MPLS-TP information	X	X	X	X	X
View port configurations	X	X	X	X	X
View pseudowire end-to-end emulation tunnels	X	X	X	X	X

MPLS Services—NEs Not in User's Device Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Working with Elements					
View IPv6 properties	—	—	—	—	X
Add tunnels to VPNs	—	X	X	X	X
Add VPNs to a map	—	—	X	X	X
Create VPNs	—	—	X	X	X
Move virtual routers between VPNs	—	X	X	X	X
Remove tunnels from VPNs	X	X	X	X	X
Remove VPNs from a map	—	—	X	X	X
Viewing Element Properties					
View 6RD properties	—	—	—	—	X
View BFD properties	—	—	—	—	X
View cross-VRF routing entries	—	—	—	—	X
View LSE properties	—	—	—	—	X
View MP-BGP information	—	—	—	—	X
View MPLS TE tunnel information	—	—	—	—	X
View MPLS-TP information	—	—	—	—	X
View port configurations	—	—	—	—	X
View pseudowire end-to-end emulation tunnels	—	—	—	—	X
View rate limit information	—	—	—	—	X
View the ARP table	—	—	—	—	X
View the NDP table	—	—	—	—	X
View VPN properties	X	X	X	X	X
View VPNs	X	X	X	X	X
View VRF egress and ingress adjacents	—	—	—	—	X
View VRF properties	—	—	—	—	X
Working with Overlays					
Add VPN overlays	X	X	X	X	X
Display or hide VPN overlays	X	X	X	X	X
Remove VPN overlays	X	X	X	X	X

Permissions for Managing IP and MPLS Multicast

IP and MPLS Multicast—NEs in User's Device Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View multicast configuration details	X	X	X	X	X
View Multicast Label Switch details	X	X	X	X	X
View Routing entities	X	X	X	X	X
View VRF Properties	X	X	X	X	X

IP and MPLS Multicast—NEs Not in User's Device Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View multicast configuration details	X	X	X	X	X
View Multicast Label Switch details	X	X	X	X	X
View Routing entities	X	X	X	X	X
View VRF Properties	X	X	X	X	X

Permissions for Managing MToP

MToP—NEs in User's Device Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View MToP properties	X	X	X	X	X
Using SONET Configure, Clear, and Show Commands	—	—	—	X	X

MToP—NEs Not in User's Device Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View MToP properties	—	—	—	—	X
Using SONET Configure, Clear, and Show Commands	—	—	—	X	X

Permissions for Managing SBCs

SBC—NEs in User's Device Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing SBC properties	X	X	X	X	X
Using SBC Configuration and Monitoring Commands	—	—	—	X	X
Using SBC Show Commands	—	—	—	X	X

SBC—NEs Not in User's Device Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing SBC properties	—	—	—	—	X
Using SBC Configuration and Monitoring Commands	—	—	—	X	X
Using SBC Show Commands	—	—	—	X	X

Permissions for Managing AAA

AAA—NEs in User's Device Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View AAA group profile	X	X	X	X	X
View dynamic authorization profile	X	X	X	X	X
View RADIUS global configuration details	X	X	X	X	X
View diameter configuration details for AAA group	X	X	X	X	X
View RADIUS configuration details for AAA group	X	X	X	X	X
View RADIUS keepalive and dtect dead server for AAA group	X	X	X	X	X
View RADIUS authentication configuration details for AAA group	X	X	X	X	X
View charging configuration details for AAA group	X	X	X	X	X
View charging trigger configuration details for AAA group	X	X	X	X	X
Use AAA configuration commands	—	—	—	X	X

AAA—NEs Not in User's Device Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View AAA group profile					
View dynamic authorization profile					
View RADIUS global configuration details					

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View diameter configuration details for AAA group					
View RADIUS configuration details for AAA group					
View RADIUS keepalive and detect dead server for AAA group					
View RADIUS authentication configuration details for AAA group					
View charging configuration details for AAA group					
View charging trigger configuration details for AAA group					
Use AAA configuration commands					

Permissions for Managing IP Pools

IP Pools—NEs in User's Device Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View IP pool properties	X	X	X	X	X
Use IP pool configuration commands	X	X	X	X	X

IP Pools—NEs Not in User's Device Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View IP pool properties					
Use IP pool configuration commands					

Permissions for Managing BNG

BNG—NEs in User's Device Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View BBA profiles	X	X	X	X	X
View Subscriber Access Points	X	X	X	X	X
Diagnose Subscriber Access Points	—	—	—	X	X
View DHCP Service Profile	X	X	X	X	X
View IP Subscriber Template	X	X	X	X	X
View PPP Templates	X	X	X	X	X
View Service Templates	X	X	X	X	X
View policy details	X	X	X	X	X

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View QoS profile	X	X	X	X	X
View AAA Group profile	X	X	X	X	X
View Dynamic Authorization profile	X	X	X	X	X
View Radius Global Configuration details	X	X	X	X	X

BNG—NEs Not in User's Device Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View BBA profiles					
View Subscriber Access Points					
Diagnose Subscriber Access Points					
View DHCP Service Profile					
View IP Subscriber Template					
View PPP Templates					
View Service Templates					
View policy details					
View QoS profile					
View AAA Group profile					
View Dynamic Authorization profile					
View Radius Global Configuration details					

Permissions for Managing Mobile Technologies

Mobile Technologies—NEs in User's Device Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing GGSN properties	X	X	X	X	X
Viewing additional characteristics of a GGSN	X	X	X	X	X
Working with GGSN commands	—	—	—	X	X
Viewing the SGSN Configuration Details	X	X	X	X	X
Working with SGSN commands	—	—	—	X	X
Viewing the MME Configuration Details	X	X	X	X	X
Working with MME commands	—	—	—	X	X
Viewing GTPU properties	X	X	X	X	X
Working with GTPU commands	—	—	—	X	X
Viewing APN properties	X	X	X	X	X

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing additional characteristics of an APN	X	X	X	X	X
Working with APN commands	—	—	—	X	X
Viewing SAE-GW properties	X	X	X	X	X
Viewing P-GW properties	X	X	X	X	X
Working with P-GW commands	—	—	—	X	X
Viewing S-GW properties	X	X	X	X	X
Working with S-GW commands	—	—	—	X	X
Viewing SaMOG properties	X	X	X	X	X
Working with SaMOG commands	—	—	—	X	X
Viewing CGW properties	X	X	X	X	X
Working with CGW commands	—	—	—	X	X
Viewing MRME properties	X	X	X	X	X
Working with MRME commands	—	—	—	X	X
Viewing GTPP properties	X	X	X	X	X
Viewing additional characteristics of a GTPP	X	X	X	X	X
Working with GTPP commands	—	—	—	X	X
Viewing EGTP properties	X	X	X	X	X
Working with EGTP commands	—	—	—	X	X
Viewing operator policies	X	X	X	X	X
Viewing APN remaps	X	X	X	X	X
Viewing APN profiles	X	X	X	X	X
Viewing additional characteristics of an APN profiles	X	X	X	X	X
Viewing active charging services (ACS)	X	X	X	X	X
Working with ACS commands	—	—	—	X	X
Viewing QCI-QoS mapping	X	X	X	X	X
Viewing the Layer 2 Tunnel Access Concentrator Configurations	X	X	X	X	X
Viewing the HSGW configuration	X	X	X	X	X
Viewing the Home Agent configuration	X	X	X	X	X
Viewing the Foreign Agent configuration details	X	X	X	X	X
Viewing the ePDG configuration details	X	X	X	X	X
Viewing the PDSN configuration details	X	X	X	X	X
Viewing the Local Mobility Anchor configuration	X	X	X	X	X

Mobile Technologies—NEs Not in User's Device Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing GGSN properties	—	—	—	—	X
Viewing additional characteristics of a GGSN	—	—	—	—	X
Working with GGSN commands	—	—	—	—	X
Viewing the SGSN Configuration Details	—	—	—	—	X
Working with SGSN commands	—	—	—	—	X
Viewing the MME Configuration Details	—	—	—	—	X
Working with MME commands	—	—	—	—	X
Viewing GTPU properties	—	—	—	—	X
Working with GTPU commands	—	—	—	—	X
Viewing APN properties	—	—	—	—	X
Viewing additional characteristics of an APN	—	—	—	—	X
Working with APN commands	—	—	—	—	X
Viewing SAE-GW properties	—	—	—	—	X
Viewing P-GW properties	—	—	—	—	X
Working with P-GW commands	—	—	—	—	X
Viewing S-GW properties	—	—	—	—	X
Working with S-GW commands	—	—	—	—	X
Viewing SaMOG properties	—	—	—	—	X
Working with SaMOG commands	—	—	—	—	X
Viewing CGW properties	—	—	—	—	X
Working with CGW commands	—	—	—	—	X
Viewing MRME properties	—	—	—	—	X
Working with MRME commands	—	—	—	—	X
Viewing GTPP properties	—	—	—	—	X
Viewing additional characteristics of a GTPP	—	—	—	—	X
Working with GTPP commands	—	—	—	—	X
Viewing EGTP properties	—	—	—	—	X
Working with EGTP commands	—	—	—	—	X
Viewing operator policies	—	—	—	—	X
Viewing APN remaps	—	—	—	—	X
Viewing APN profiles	—	—	—	—	X
Viewing additional characteristics of an APN profiles	—	—	—	—	X
Viewing active charging services (ACS)	—	—	—	—	X
Working with ACS commands	—	—	—	—	X
Viewing QCI-QoS mapping	—	—	—	—	X

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing the Layer 2 Tunnel Access Concentrator Configurations	—	—	—	—	X
Viewing the HSGW configuration	—	—	—	—	X
Viewing the Home Agent configuration	—	—	—	—	X
Viewing the Foreign Agent configuration details	—	—	—	—	X
Viewing the ePDG configuration details	—	—	—	—	X
Viewing the PDSN configuration details	—	—	—	—	X
Viewing the Local Mobility Anchor configuration	—	—	—	—	X

Permissions for Managing Data Center Networks

Data Center—NEs in User's Device Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing Virtual Port Channel Configuration	X	X	X	X	X
Viewing vPC Configuration	X	X	X	X	X
Viewing Cisco FabricPath Configuration	X	X	X	X	X
Monitoring Cisco FabricPath Configuration	X	X	X	X	X
Viewing Virtual Data Centers	X	X	X	X	X
Viewing the Data Stores of a Data Center	X	X	X	X	X
Viewing the Host Servers of a Data Center	X[1]	X[1]	X[1]	X[1]	X[1]
Viewing the Virtual Machines of a Data Center	X[1]	X[1]	X[1]	X[1]	X[1]
Viewing Host Cluster Details	X[1]	X[1]	X[1]	X[1]	X[1]
Viewing Resource Pool Details	X[1]	X[1]	X[1]	X[1]	X[1]
Viewing the Map Node for an UCS Network Element	X	X	X	X	X
Viewing the Virtual Network Devices of a Data Center	X[1]	X[1]	X[1]	X[1]	X[1]
Viewing the Compute Server Support Details	X[1]	X[1]	X[1]	X[1]	X[1]
Viewing the Storage Area Network Support Details	X[1]	X[1]	X[1]	X[1]	X[1]
Monitoring the Compute Services Search Capability	X	X	X	X	X

1. For users to be able to view VMs and hypervisors, a user's device scope must include all relevant vCenter VNEs.

Data Center—NEs Not IN User's Device Scope (Or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing Virtual Port Channel Configuration					
Viewing vPC Configuration					

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing Cisco FabricPath Configuration					
Monitoring Cisco FabricPath Configuration					
Viewing Virtual Data Centers					
Viewing the Data Stores of a Data Center					
Viewing the Host Servers of a Data Center					
Viewing the Virtual Machines of a Data Center					
Viewing Host Cluster Details					
Viewing Resource Pool Details					
Viewing the Map Node for an UCS Network Element					
Viewing the Virtual Network Devices of a Data Center					
Viewing the Compute Server Support Details					
Viewing the Storage Area Network Support Details					
Monitoring the Compute Services Search Capability					

Permissions for Managing Cable Technologies

Cable Technologies—NEs in User's Device Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing the Cable Broadband Configuration Details	X	X	X	X	X
Viewing the DTI Configuration Details	X	X	X	X	X
Viewing the QAM Domain Configuration Details	X	X	X	X	X
Viewing the MAC Domain Configuration Details	X	X	X	X	X
Viewing the Narrowband Channels Configuration Details	X	X	X	X	X
Viewing the Wideband Channels Configuration Details	X	X	X	X	X
Viewing the Fiber Node Configuration Details	X	X	X	X	X

Cable Technologies—NEs Not in User's Device Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing the Cable Broadband Configuration Details					
Viewing the DTI Configuration Details					
Viewing the QAM Domain Configuration Details					
Viewing the MAC Domain Configuration Details					
Viewing the Narrowband Channels Configuration Details					

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing the Wideband Channels Configuration Details					
Viewing the Fiber Node Configuration Details					

Permissions for Managing DSL2+ and VDSL2

ADSL2+ and VDSL2—NEs in User's Device Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing the ADSL2+/VDSL2 configuration details	X	X	X	X	X
Viewing the ADSL/ADSL2+ physical inventory details for a device	X	X	X	X	X
Viewing the DSL Bonding Group configuration details	X	X	X	X	X

ADSL2+ and VDSL2—NEs Not in User's Device Scope (or Actions Not Related to NEs)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing the ADSL2+/VDSL2 configuration details					
Viewing the ADSL/ADSL2+ physical inventory details for a device					
Viewing the DSL Bonding Group configuration details					

Permissions for Managing GPON Technology

GPON Technology—NEs in User's Device Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing the Profile Configurations	X	X	X	X	X
Viewing the Class of Service Configuration	X	X	X	X	X
Viewing the Link Aggregation Group Configuration	X	X	X	X	X
Viewing the Firmware Configuration	X	X	X	X	X
Viewing the OLT Services and Bridges Configuration	X	X	X	X	X
Viewing the Physical Inventory of the ONU and OLT	X	X	X	X	X
Viewing the DHCP Relay Agent Configuration for OLT	X	X	X	X	X
Viewing the Routing Entities Configuration for OLT	X	X	X	X	X

Event Correlation Examples

The following topics provide examples of how Prime Network correlates events:

Correlation Scenario Overview

The following scenarios demonstrate Prime Network correlation functionality. Figure C-1 shows the lab setup for the scenarios described in these topics. The lab simulates a service provider (SP) network. The core is based on MPLS and uses OSPF as the Interior Gateway Protocol (IGP).

The P-network is topologically contiguous, whereas the C-network is delineated into a number of sites (contiguous parts of the customer network that are connected in some way other than through the VPN service). Note that a site does not need to be geographically contained.

The devices that link the customer sites to the P-network are called customer edge (CE) devices, whereas the service provider devices to which the CE routers connect are called provider edge (PE) devices. Where the provider manages an Ethernet access network, the CE devices are connected to the PE devices, which are usually LAN switches with Layer 3 capabilities.

The access network can be any Layer 2 technology.

In this lab there are two Layer 2 technologies in the access network:

- Ethernet
- Frame Relay

The access network in the lab is unmanaged (a cloud).

In most cases, the P-network is made up of more than just the PE routers. These other devices are called P-devices (or, if the P-network is implemented with Layer 3 technology, P routers). Similarly, the additional Layer 3 devices at the customer sites that have no direct connectivity to the P-network are called C routers. In this example, C-routers are not part of the lab setup and are not managed by Prime Network.

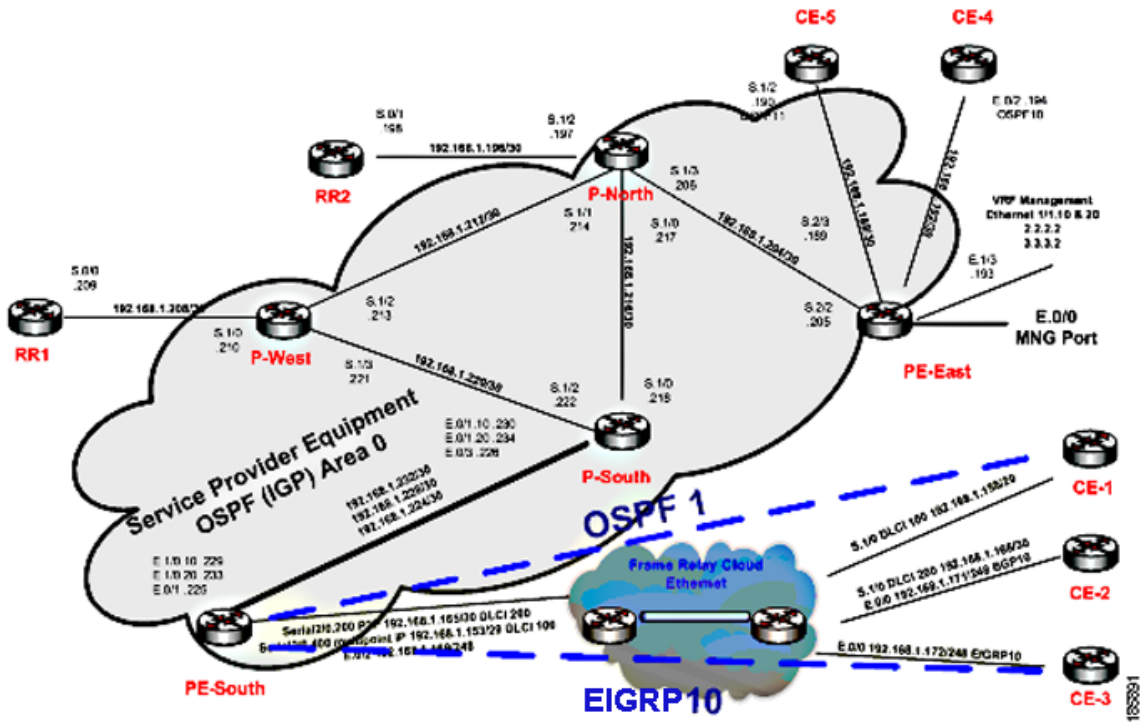
The CE devices are located at the customer site and can be managed by the SP. All other devices (PEs, Ps, and RRs) are located at the SP site. These devices are maintained by the SP.

An end-to-end MPLS VPN solution is, like any other VPN solution, divided into the central P-network to which a large number of customer sites (sites in the C-network) are attached. The customer sites are attached to the PE devices (PE routers) through CE devices (CE routers). Each PE router contains several VRF tables, at least one per VPN customer. These tables are used together with multiprotocol BGP to run between the PE routers to exchange customer routes and to propagate customer datagrams across the MPLS network. The PE routers perform the label imposition (ingress PE router) and removal (egress PE router). The central devices in the MPLS network (P routers) perform simple label switching.

There are BGP processes running on the PE devices, and each PE is a neighbor to both RR devices. This way, the lab has a backup if one RR is down.

All the devices are managed inband. The management access point is Ethernet 0/0 on PE-East. To enable access to the CE devices, a loop was created between two ports on PE-East.

Figure C-1 Correlation Scenarios Lab Setup



Correlation Scenarios

The following topics describe specific alarms that use correlation logic on top of the root cause analysis flow:

- Device Unreachable Correlation Scenarios, page C-3
- Multiroute Correlation Scenarios, page C-11
- BGP Neighbor Loss Correlation Scenarios, page C-14
- EFP Down Correlation Scenarios, page C-29
- HSRP Scenarios, page C-31

Device Unreachable Correlation Scenarios

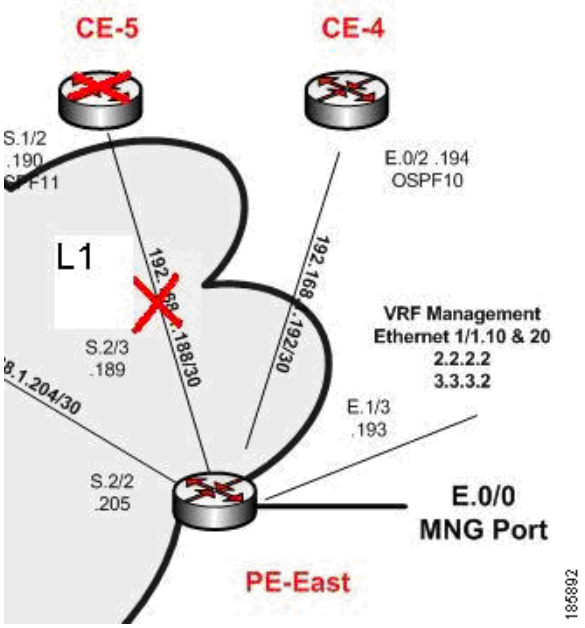
Device reachability is measured by management protocol connectivity. Connectivity tests are used to verify the connection between VNEs and the managed network elements. The connectivity is tested on each protocol a VNE uses to poll a device. Prime Network-supported protocols for connectivity tests are SNMP, Telnet, and ICMP.

The following topics describe the scenarios in which device reachability issues occur:

Device Unreachable on Device Reload or Device Down Event

Figure C-2 illustrates the lab setup for Device Unreachable on Device Down or Device Reload event.

Figure C-2 Lab Setup for Device Unreachable on Device Down or Device Reload Event



Description of Fault Scenario in the Network

CE-5 goes down or is reloaded.

Related Faults

- The port S.1/2 of CE-5 operationally goes down (between CE-5 and PE-East).
- The port S.2/3 of PE-East operationally goes down (between PE-East and CE-5).
- CE-5 is unreachable from the management subnet.

Note Other related faults might occur due to the CE-5 down or reload. Syslogs and traps corresponding to network faults are also reported. Additional faults, other than for the connectivity issue of CE-5 and the Link Down with the PE-East device, might be reported but are not described in this section. This topic relates specifically to Device Unreachable events.

Prime Network Failure Processing

Event Identification

The following service alarms are generated by the system:

- [Device Unreachable, CE-5] event.

  The device unreachability event means that no other information can be collected from this device by the VNE.

- [Link Down on Unreachable, PE-East < > CE-5] event.

  The Link Down event is issued by the PE-East VNE (active) as a result of the link down negotiation process.

Possible Root Cause

1. Prime Network waits two minutes. For more information, see How Prime Network Correlates Incoming Events, page 10-4.
2. After two minutes, the following occurs:
   - The [Device Unreachable, CE-5] event triggers the CE-5 VNE to initiate an IP-based flow to the management IP address:

     Flow Path: CE-5 > PE-East > management subnet
   - The [Link Down on Unreachable, PE-East < > CE-5] event triggers the CE-5 VNE to initiate local correlation.

Root Cause Selection

For the event [Device Unreachable, CE-5]:

- Collected Events: [Link Down on Unreachable, PE-East < > CE-5].

  Note Other possible events are also collected, such as Interface Status Down events.

- Root Cause: There is no root cause (opens a new ticket in the gateway).

Note The root cause selection process activates special filtering for the event [Device Unreachable, CE-5] for which the event [Link Down on Unreachable] cannot be selected as the root cause; therefore, the event [Link Down on Unreachable, PE-East < > CE-5] is not selected as the root cause.

For the event [Link Down on Unreachable, PE-East < > CE-5]:

- Collected Events: [Device Unreachable, CE-5].
- Root Cause: Correlates to [Device Unreachable, CE-5].

Figure C-3 shows how the events are correlated in this scenario.

Figure C-3 Device Unreachable on Device Down

Event Correlation Hierarchy	Location
Device unreachable	ce-5-IOU-161
└Link down on unreachable	PE-East-IOU-161#0:Serial2/3<->ce-5-IOU-161#0:Serial1/2
└OSPF neighbor down syslog	PE-East-IOU-161 VRF vrfB IP:Serial2/3 : 169.254.161.223
└Interface status down	PE-East-IOU-161 VRF vrfB IP:Serial2/3
└Line down syslog	PE-East-IOU-161 VRF vrfB IP:Serial2/3

370855

Clearing Phase

When a down or reloaded device comes up again and starts responding to polling requests made by the corresponding VNE, the device is declared reachable, thus clearing the unreachable alarm. Other related alarms are cleared in turn after the corresponding VNEs verify that the malfunctions have been resolved.

Variation

In a device reload scenario, the following additional events are identified by the system (in addition to the device down scenario):

- Reloading Device syslog.
- Cold Start trap.

For the event [Device Unreachable, CE-5]:

- Additional Collected Event: [Reloading Device syslog, CE-5].
- Root Cause: Correlates to [Reloading Device syslog, CE-5].

Figure C-4 shows how the event are correlated in this scenario.

Figure C-4 Device Unreachable on Device Reload

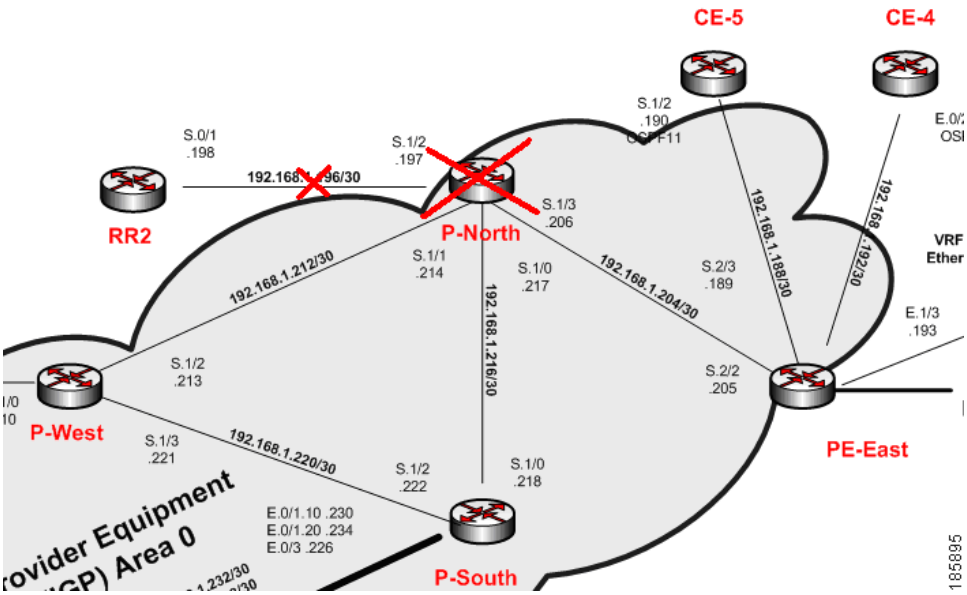
Event Correlation Hierarchy	Location
Reloading device syslog	ce-5-IOU-161
OSPF neighbor down syslog	PE-East-IOU-161 VRF vrfB IP:Serial2/3 : 169.254.161.223
Interface status down	PE-East-IOU-161 VRF vrfB IP:Serial2/3
Line down syslog	PE-East-IOU-161 VRF vrfB IP:Serial2/3
Device unreachable	ce-5-IOU-161
Link down on unreachable	PE-East-IOU-161#0:Serial2/3<->ce-5-IOU-161#0:Serial1/2

370856

Device Unreachable on Another Device Unreachable Event

Figure C-5 illustrates the lab setup for Device Unreachable on another Device Unreachable event.

Figure C-5 Lab Setup for Device Unreachable on Another Device Unreachable Event



Description of Fault Scenario in the Network

P-North device is reloaded.

Related Faults

- P-North is unreachable from the management subnet.
- The links of P-North operationally go down and, as a result, the surrounding devices go down.
- RR2, accessed by the link P-North, RR2 (also known as L3) is unreachable.

Prime Network Failure Processing

Note This scenario is similar to the one described in Device Unreachable on Device Reload or Device Down Event, page C-3, except that in this scenario the L3 Link Down is *not* discovered because both connected devices (RR2 and P-North) are unreachable by Prime Network. Therefore, the VNE is unable to detect the Link Down problem.

Event Identification

The following service alarms are generated by the system:

- [Device Unreachable, P-North] event.

  The device unreachability event means that no other information can be collected from this device by the VNE.

- [Device Unreachable, RR2] event.

Possible Root Cause

1. Prime Network waits two minutes.
2. After two minutes, the following occurs:

- The [Device Unreachable, P-North] event triggers the P-North VNE to initiate an IP-based flow to the management IP subnet:

  Flow Path: P-North > PE-East > management subnet

- The [Device Unreachable, RR2] event triggers the RR2 VNE to initiate an IP-based flow to the management IP.

  Flow Path: RR2 > P-North > PE-East > management subnet

Root Cause Selection

- For the event [Device Unreachable, P-North]:
  - Collected Events: [Reloading Device syslog, P-North].
  - Root Cause: Correlates to [Reloading Device syslog, P-North].
- For the event [Device Unreachable, RR2]:
  - Collected Events: [Device Unreachable, P-North] and [Reloading Device syslog, P-North].
  - Root Cause: Correlates to [Reloading Device syslog, P-North] (as this has a higher weight than the event [Device Unreachable, P-North]).

Figure C-6 displays the events identified by the system in this scenario.

Figure C-6 Device Unreachable on Other Device Unreachable

Event Correlation Hierarchy	Location
Reloading device syslog	P-North-IOU-161
LDP neighbor down	PE-East-IOU-161
LDP neighbor down syslog	PE-East-IOU-161
Interface status down	PE-East-IOU-161 IP:Serial2/2
Line down syslog	PE-East-IOU-161 IP:Serial2/2
BGP neighbor down syslog	PE-East-IOU-161 : 169.254.161.216
BGP neighbour loss	PE-East-IOU-161
BGP neighbor down syslog	PE-East-IOU-161 : 169.254.161.224
Device unreachable	RR1-IOU-161
Device unreachable	P-West-IOU-161
Device unreachable	ce-1-IOU-161
Device unreachable	RR2-IOU-161
Device unreachable	PE-South-IOU-161
Device unreachable	P-South-IOU-161
Device unreachable	P-North-IOU-161
Link down on unreachable	P-North-IOU-161#0:Serial1/3<->PE-East-IOU-161#0:Serial2/2
LDP neighbor down	PE-East-IOU-161
LDP neighbor down syslog	PE-East-IOU-161

370857

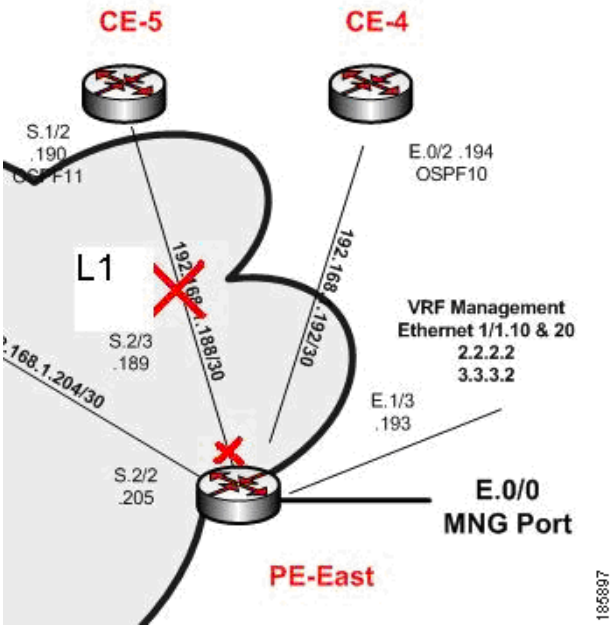
Clearing Phase

When a reloaded device comes up again (along with the L3 link that is vital for the RR2 management), the RR2 starts responding to polling requests from the RR2 VNE. The device is declared as reachable, thus clearing the Device Unreachable alarm.

Device Unreachable on Link Down Event

Figure C-7 illustrates the lab setup for a Device Unreachable on a Link Down event.

Figure C-7 Lab Setup for Device Unreachable on a Link Down Event



Description of Fault Scenario in the Network

The S.2/3 port of PE-East connected to the S.1/2 port of the CE-5 device (also called L1 link) is set to administrative status down. This effectively takes the L1 link down.

Related Faults

The CE-5 device is managed from this link with no backup. With the L1 link down, the CE-5 device is unreachable from the management subnet.

Prime Network Failure Processing

Event Identification

The following service alarms are generated by the system:

- [Device Unreachable, CE-5] event.

  The device unreachability event means that no other information can be collected from this device by the VNE.

- [Link Down Due to Admin Down, PE-East < > CE-5] event.

  The Link Down event is issued by the PE-East VNE (active) as a result of the link down negotiation process.

Noncorrelating Events

The noncorrelating event is:

[Link Down Due to Admin Down, PE-East < > CE-5]

This event opens a new ticket in the gateway.

The L1 Link Down event is configured to not correlate to other events. This is logical because the edge VNEs identify the Link Down events as [Link Down Due to Admin Down] events. This implies that the VNEs know the root cause of the event already, based on the administrator's configurations. The [Link Down Due to Admin Down] events reach the northbound interface immediately after the links' new statuses are discovered by Prime Network and after the link down negotiation methods are completed.

Possible Root Cause

1. Prime Network waits two minutes.
2. After two minutes, the [Device Unreachable, CE-5] event triggers the CE-5 VNE to initiate an IP-based flow to the management subnet:

   Flow Path: CE-5 > PE-East > management subnet

Root Cause Selection

For the event [Device Unreachable, CE-5]:

- Collected Events: [Link Down Due to Admin Down, PE-East < > CE-5].

  Note Other possible events are also collected, such as Interface Status Down events.

- Root Cause: Correlates to [Link Down Due to Admin Down, PE-East < > CE-5].

Figure C-8 displays the events identified by the system in this scenario.

Figure C-8 Device Unreachable on Link Down

Event Correlation Hierarchy	Location
Link down due to admin down	PE-East-IOU-161#0:Ethernet0/3<->ce-5-IOU-161#0:Etherenet0/2
— OSPF neighbor down syslog	PE-East-IOU-161 VRF vfrB IP:Ethernet0/3 : 169.254.161.223
— Interface status down	PE-East-IOU-161 VRF vfrB IP:Ethernet0/3
— Link down syslog	PE-East-IOU-161 VRF vfrB IP:Ethernet0/3
— Line down syslog	PE-East-IOU-161 VRF vfrB IP:Ethernet0/3
— Device unreachable	ce-5-IOU-161

370858

Note In Figure C-8, port E.0/3 should read S.2/3, and E.0/2 should read S.1/2.

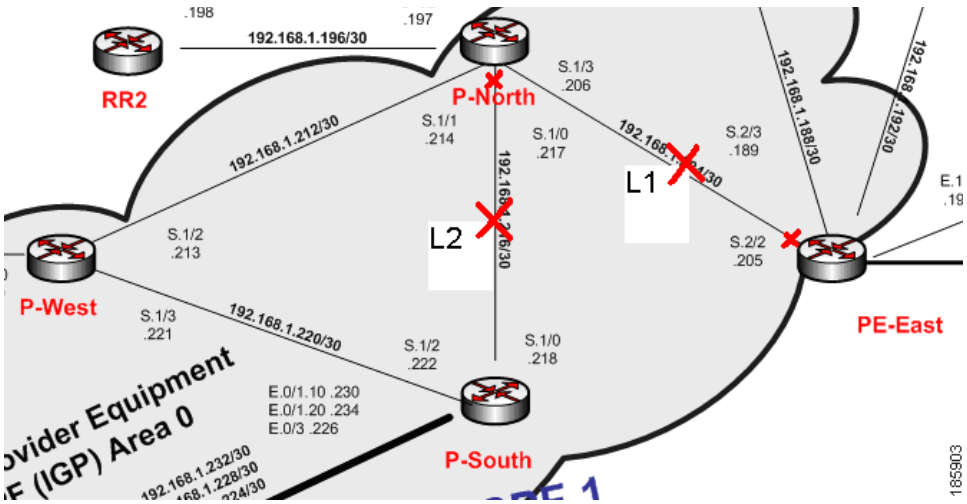
Clearing Phase

When the PE-East port S.2/3 (L1 link) comes up again, the CE-5 reachability from the management subnet also returns. The CE-5 starts responding to polling requests from the CE-5 VNE. The device is declared reachable, thus clearing the Device Unreachable alarm. The L1 Link Down is cleared when the PE-East device indicates that the status of the connected port has changed to up.

Multiroute Correlation Scenarios

Figure C-9 displays the lab multiroute configuration setup between P-South, P-North, and P-West devices. The OSPF cost is the same along the path from P-South and P-North whether or not it goes via P-West; that is, P-South and P-North connect along two paths with equal cost.

Figure C-9 Lab Multiroute Configuration Setup Between P-South, P-North and P-West



Description of a Fault Scenario in the Network

In this example, the P-North, P-South link (also known as L2) goes down in a multiroute segment between P-South and P-North. After approximately one minute, another link, L1 (PE-East, P-North), also goes down. Both links go down administratively, the first from the P-North device and the second from the PE-East devices' ports.

Related Faults

Almost all devices are unreachable from the management subnet. This discussion focuses on CE-1 unreachability (see Figure C-1).

Note Syslogs and traps corresponding to network faults are also reported. Additional related faults might also be reported, but are not described in this topic.

Prime Network Failure Processing

Event Identification

The following service alarms are generated by the system:

- [Device Unreachable, CE-1] event.

  The device unreachability event means that no other information can be collected from this device by the VNE.

- [Link Down Due to Admin Down, P-North < > PE-East] event.

The Link Down event is issued by the PE-East VNE (active) as a result of the link down negotiation process.

- [Link Down Due to Admin Down, P-North < > P-South] event.

  The Link Down event is issued by the P-North VNE as a result of the link down negotiation process.

Noncorrelating Events

- [Link Down Due to Admin Down, P-North < > PE-East] opens a new ticket in the gateway.
- [Link Down Due to Admin Down, P-North < > P-South] opens a new ticket in the gateway.

For more information, see Noncorrelating Events, page C-10.

Possible Root Cause

1. Prime Network waits two minutes.
2. After two minutes, the [Device Unreachable, CE-1] event triggers the CE-1 VNE to initiate an IP-based flow to the management IP subnet:

   Flow Path: CE-1 > Cloud > PE-South > P-South > P-North > PE-East > management subnet

   Flow Path: CE-1 > Cloud > PE-South > P-South > P-West > P-North > PE-East > management subnet

Root Cause Selection

For the event [Device unreachable, CE-1]:

- For the flow path CE-1 > Cloud > PE-South > P-South > P-North > PE-East > management subnet:
  - Collected Events: [Link Down Due to Admin Down, P-North < > PE-East] and [Link Down Due to Admin Down, P-South > P-North].

    Note Other possible events are also collected, such as Interface Status Down events.

  - Root Cause—Correlates to:
    [Link down due to admin down, P-SouthS.1/0 > P-North S.1/0 < > PE-East S.2/2] and
    [Link down due to admin down, P-NorthS.1/3 > PE-East S.2/2]
- For the Flow Path
  CE-1 > Cloud > PE-South > P-South > P-West > P-North > PE-East > management subnet:

  Root Cause: Correlates to [Link Down Due to Admin Down, P-North S.1/0 < > PE-East S.2/2]

Note The CE-1's VNE root cause selection method identifies the Device Unreachable event's root cause on the L1 Link Down event. According to the logic, when two flows split and result in two sets of possible root cause events, sets that are supersets of others (depending on whether both flows end at the same location) are removed. Sets that are not removed are united into one set containing all events. This implies that, in this scenario, the set that includes both links is removed because it is a superset of the set that contains only the L1 link.

Note All devices that are unreachable correlate their unreachability events to the L1 link as expected.

Figure C-10 displays the events identified by the system in this scenario (L1).

Figure C-10 Multiroute Scenario—L1

Event Correlation Hierarchy	Location
Link down due to admin down	P-North-IOU-161#0:Serial1/3<->PE-East-IOU-161#0:Serial2/2
Interface status down	PE-East-IOU-161 IP:Serial2/2
Link down syslog	PE-East-IOU-161 IP:Serial2/2
Line down syslog	PE-East-IOU-161 IP:Serial2/2
LDP neighbor down	PE-East-IOU-161
LDP neighbor down syslog	PE-East-IOU-161
BGP neighbor down syslog	PE-East-IOU-161 : 169.254.161.224
BGP neighbour loss	PE-East-IOU-161
BGP neighbor down syslog	PE-East-IOU-161 : 169.254.161.216
Device unreachable	ce-3-IOU-161
Device unreachable	ce-1-IOU-161
Device unreachable	ce-2-IOU-161
Device unreachable	PE-South-IOU-161
Device unreachable	RR1-IOU-161
Device unreachable	P-West-IOU-161
Device unreachable	P-South-IOU-161
Device unreachable	P-North-IOU-161
Device unreachable	RR2-IOU-161
LDP neighbor down	PE-East-IOU-161
LDP neighbor down syslog	PE-East-IOU-161

370859

Figure C-11 displays the events identified by the system in this scenario (L2).

Figure C-11 Multiroute Scenario—L2

Event Correlation Hierarchy	Location
Link down due to admin down	P-North-IOU-161#0:Serial1/0<->P-South-IOU-161#0:Serial1/0
Interface status down	P-North-IOU-161 IP:Serial1/0
OSPF neighbor down syslog	P-North-IOU-161 IP:Serial1/0 : 169.254.161.214
Link down syslog	P-North-IOU-161 IP:Serial1/0
Line down syslog	P-North-IOU-161 IP:Serial1/0
OSPF neighbor down syslog	P-South-IOU-161 IP:Serial1/0 : 169.254.161.213
Interface status down	P-South-IOU-161 IP:Serial1/0
Line down syslog	P-South-IOU-161 IP:Serial1/0
LDP neighbor down	P-North-IOU-161
LDP neighbor down syslog	P-North-IOU-161
LDP neighbor down	P-South-IOU-161
LDP neighbor down syslog	P-South-IOU-161

370860

Clearing Phase

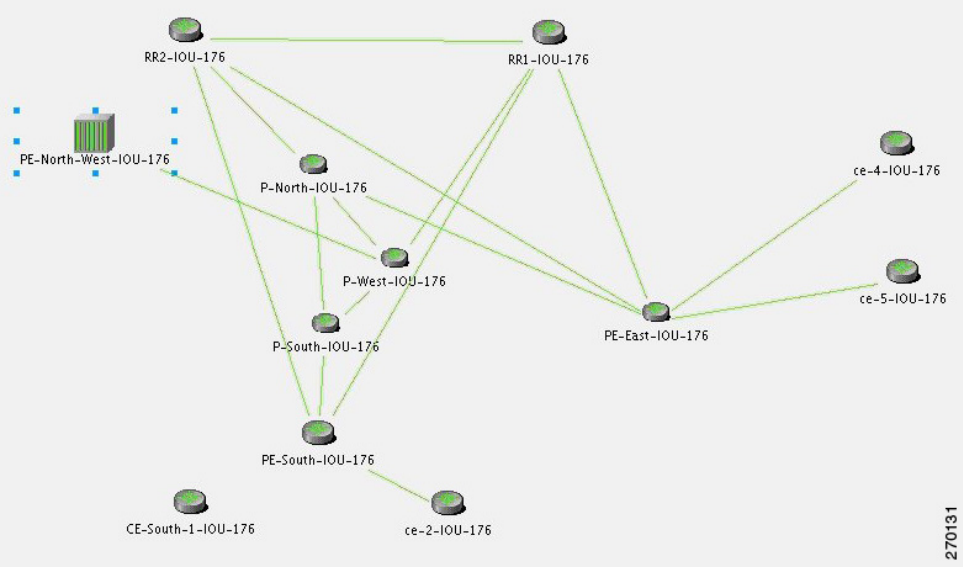
Enabling the L1 link makes the CE-1 device reachable from the management subnet IP address, thereby clearing the Device Unreachable event of the CE-1 device. When the L1 link's new status is discovered by Prime Network, the PE-East device eventually initiates a Link Up event for this link. When the administrator enables the Layer 2 link and Prime Network discovers this change, the Link Down event is cleared by its matching Link Up event.

BGP Neighbor Loss Correlation Scenarios

The VNE models the BGP connection between routers and actively monitors its state. BGP neighbor loss events are generated from both sides of the connection only when connectivity is lost, and when the other side of the link is unmanaged.

The correlation engine identifies various faults that affect the BGP connection and reports them as the root cause for the BGP Neighbor Loss alarm; for example, Link Down, CPU Overutilized, and Link Data Loss.

Figure C-12 Lab Setup for BGP Neighbor Loss Correlation Scenarios



Note In Figure C-12 the link between P-West and PE-North-West is not real and merely emphasizes how PE-North-West is connected in the network.

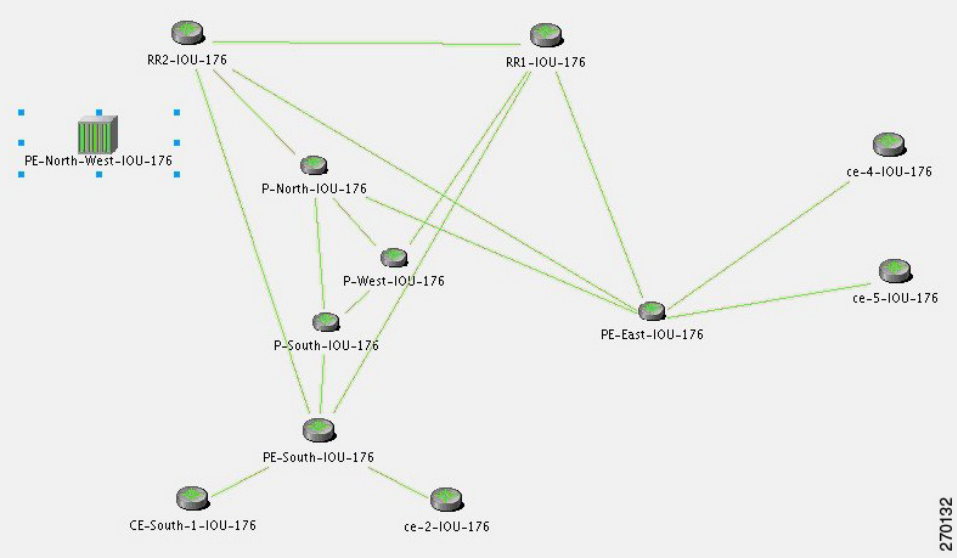
There are two main scenarios that might lead to a BGP neighbor loss event:

- BGP neighbor loss due to a Link Down (or an equivalent port down).
- BGP neighbor loss due to BGP Process Down or device down.

BGP Neighbor Loss Due to Port Down

Figure C-13 displays the BGP neighbor loss due to port down scenario.

Figure C-13 BGP Neighbor Loss Due to Physical Port Down (P-West > PE-North-West)



Description of Fault Scenario in the Network

In Figure C-13 the BGP neighbor loss occurs due to a physical port down (in P-West that connects to PE-North-West). The relevant devices are PE-North-West, RR2, P-North and P-West.

Related Faults

- Port on P-West that is connected to the PE-North-West goes down.
- BGP neighbor, on RR2, to PE-North-West changes state from Established to Idle.

Note Syslogs and traps corresponding to network faults are also reported. Additional related faults might also be reported, but are not included in this discussion.

Prime Network Failure Processing

Event Identification

The following service alarms are generated by the system:

- [BGP Neighbor Loss, RR2] event.

  Since the VNE that monitors each PE or RR holds records of the entire device's BGP information, the change in the BGP table is identified by the VNE and causes it to send this event.

Possible Root Cause

1. Prime Network waits two minutes. For more information, see How Prime Network Correlates Incoming Events, page 10-4.
2. After two minutes, the [BGP Neighbor Loss, RR2] event triggers the VNE to initiate an IP-based flow to the destination IP of its lost BGP neighbor (PE-North-West):

   Flow Path: RR2 > P-North > P-West > P-West port is connected to PE-North-West (which is unmanaged), and is in a down state.

Root Cause Selection

For the event [BGP Neighbor Loss, RR2]:

- Collected Events: [Port Down, P-West].
- Root Cause: Correlates to [Port Down, P-West].

Figure C-14 displays the events identified by the system in this scenario.

Figure C-14 BGP Neighbor Loss Due to Physical Port Down

Event Correlation Hierarchy	Location
Port down	P-West-IOU-176#0:Serial...
OSPF neighbor down syslog	P-West-IOU-176 IP:Serial...
Interface status down	P-West-IOU-176 IP:Serial...
Link down syslog	P-West-IOU-176 IP:Serial...
Line down syslog	P-West-IOU-176 IP:Serial...
Line down trap	P-West-IOU-176 IP:Serial...
LDP neighbor down	P-West-IOU-176
LDP neighbor down syslog	P-West-IOU-176
BGP neighbor down syslog	RR2-IOU-176 : 169.254....
BGP neighbour loss	RR2-IOU-176
BGP neighbor down syslog	RR1-IOU-176 : 169.254....
BGP neighbour loss	RR1-IOU-176

370861

Clearing Phase

When a Port Up event is detected by the system for the same port that was detected as the root cause for the BGP Neighbor Loss event, the alarm is cleared. The ticket is cleared (colored green) when all the alarms in the ticket have been cleared.

Figure C-15 displays the up event that clears all the down events identified by the system.

Figure C-15 BGP Neighbor Up Event that Clears All the Down Events

Event Correlation Hierarchy	Location
Port up	P-West-IOU-176#0:Serial...
OSPF neighbor up syslog	P-West-IOU-176 IP:Serial...
Interface status up	P-West-IOU-176 IP:Serial...
Link up syslog	P-West-IOU-176 IP:Serial...
Line up syslog	P-West-IOU-176 IP:Serial...
Line down trap	P-West-IOU-176 IP:Serial...
LDP neighbor up	P-West-IOU-176
LDP neighbor up syslog	P-West-IOU-176
BGP neighbor up syslog	RR2-IOU-176 : 169.254....
BGP neighbour found	RR2-IOU-176
BGP neighbor up syslog	RR1-IOU-176 : 169.254....
BGP neighbour found	RR1-IOU-176

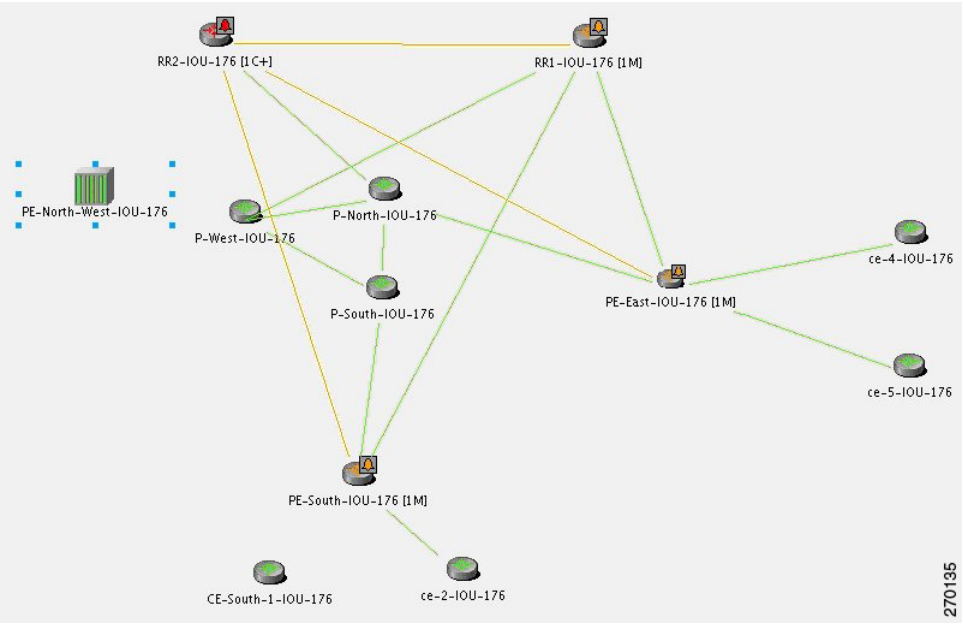
370862

Variation

In a BGP process down scenario, the BGP Process Down event is identified by the system in addition to the BGP Neighbor Loss event.

As illustrated in Figure C-16, the BGP Process Down event causes several events (the BGP Neighbor Loss event cannot be seen). The relevant devices are RR2 (BGP Process Down, marked in red) and PE-North-West (marked as unmanaged).

Figure C-16 BGP Process Down Causes Several Events



For the event [BGP Neighbor Loss, RR2]:

- Additional Collected Events: [BGP Process Down, RR2], [BGP Neighbor Loss, RR2].
- Root cause: Correlates to [BGP Process Down, RR2].

Figure C-17 displays the events identified by the system in this scenario.

Figure C-17 BGP Process Down Correlation

Event Correlation Hierarchy	Location
BGP process down	RR2-IOU-176
— BGP neighbor down syslog	RR2-IOU-176 : 169.254....
— BGP neighbor down syslog	RR2-IOU-176 : 169.254....
— BGP neighbor down syslog	RR1-IOU-176 : 169.254....
— BGP neighbor down syslog	PE-South-IOU-176 :169...
— BGP neighbor down syslog	RR2-IOU-176 : 169.254....
— BGP neighbor down syslog	PE-East-IOU-176 :169.2...
— BGP neighbor down syslog	RR2-IOU-176 : 169.254....
— BGP link down	PE-East-IOU-176<->RR...
— BGP link down	PE-South-IOU-176<->R...
— BGP link down	RR1-IOU-176<->RR2-I...
— BGP neighbour loss	RR2-IOU-176

370863

BGP Link Down Scenarios

Figure C-18 illustrates the lab setup for the BGP Link Down scenarios described in this topic.

Figure C-18 Lab Setup for BGP Link Down Scenarios

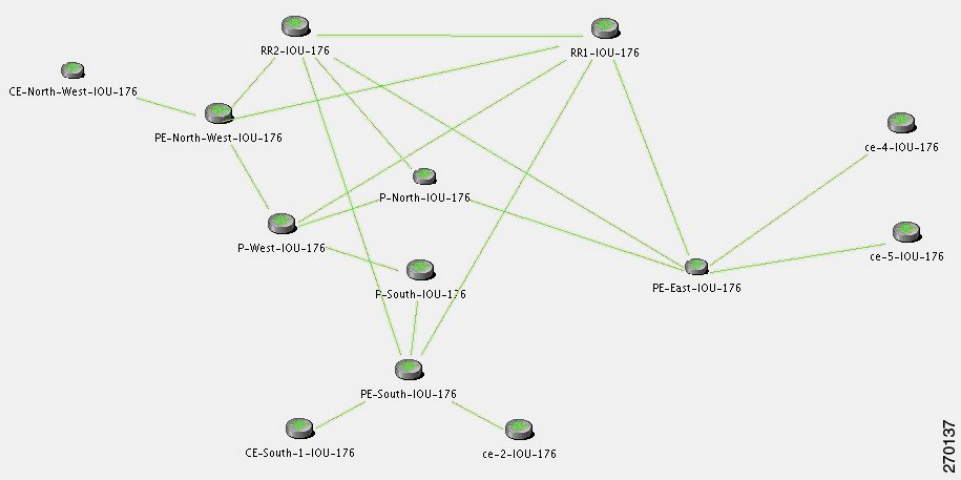
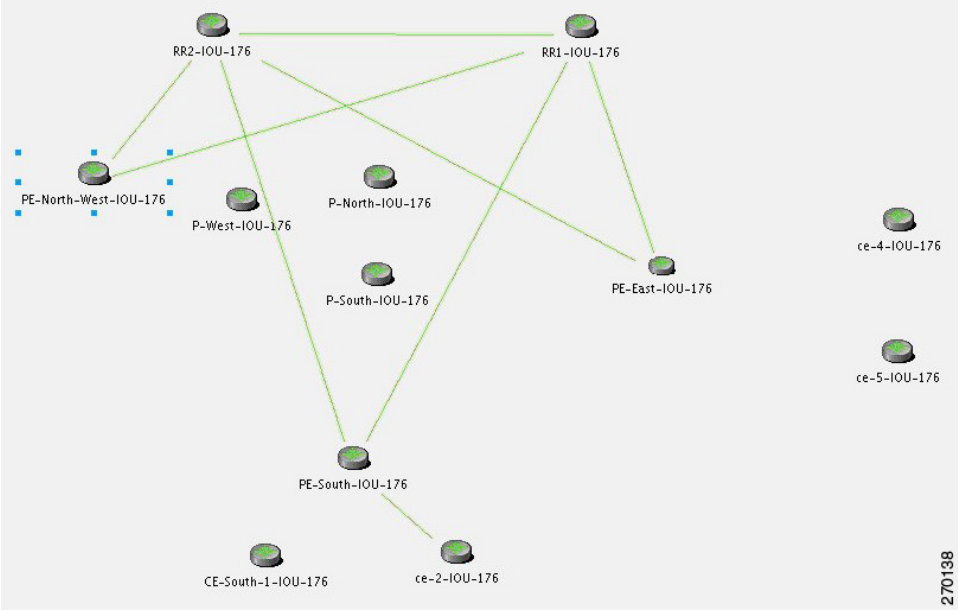


Figure C-19 illustrates the lab setup for the scenarios with only the BGP links displayed.

Figure C-19 Lab Setup for Scenarios with Only the BGP Links Displayed



The VNE models the BGP connection between routers and actively monitors its state. If connectivity is lost and a link between the devices exists in the VNE, a BGP Link Down event is created. A BGP Link Down event is created only if both sides of the link are managed.

A BGP link might be disconnected in the following scenarios:

- The BGP process on a certain device goes down, causing all the BGP links that were connected to that device to disconnect.
- A physical link (path) is disconnected, causing one side of the logical BGP link to become unreachable.
- A device becomes unreachable, due to reload or shutdown. This causes all the links to the device to be lost, including the BGP links.

Description of Fault Scenario in the Network

Due to a physical link down, the BGP connection between PE-North-West and RR2 is lost.

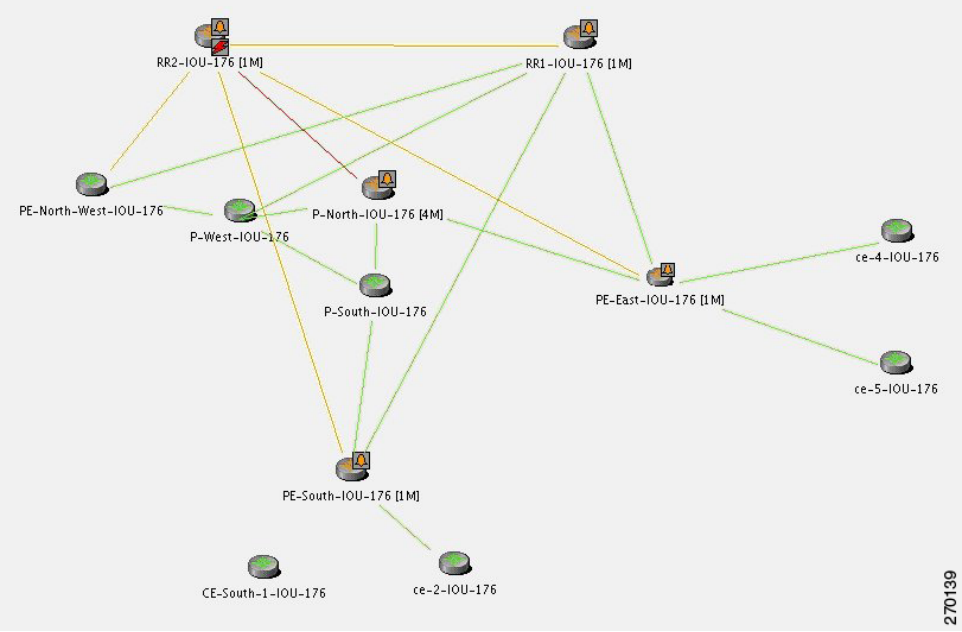
Related Faults

- Port that is connected to the P-North goes down.
- Port that is connected to the RR2 goes down.
- BGP link between RR2 and PE-North-West is disconnected.

Note Syslogs and traps corresponding to network faults are also reported. Additional related faults might also be reported, but are not described in this discussion.

Figure C-20 reflects the BGP Link Down due to physical link down scenario. The relevant devices are RR2, P-north, P-West, and PE-North-West.

Figure C-20 BGP Link Down Due to Physical Link Down



Prime Network Failure Processing

Event Identification

The following service alarms are generated by the system:

- [BGP Link Down, RR2 < > PE-North-West] event. This event might be revealed in one of two ways:
  - After polling, changes are found in the BGP neighbor list in the device.
  - Syslogs suggest that something has changed in the device's BGP neighbors or process.

  This alarm causes an acceleration of the polling for the BGP neighbor data on the device.

Possible Root Cause

1. Prime Network waits two minutes. For more information, see How Prime Network Correlates Incoming Events, page 10-4.
2. After two minutes, the [BGP Link Down, RR2 < > PE-North-West] event triggers the RR2 VNE to initiate two IP-based flows:
   - One from its routing entity to the destination IP address of its lost BGP neighbor, PE-North-West.
   - One from the destination IP address of its lost BGP neighbor back to the RR2.

   Flow Path: RR > P-North > PE-North-West

   Flow Path: RR > PE-North-West > P-North > RR2

Root Cause Selection

For the event [BGP Link Down, RR2 < > PE-North-West]:

- Collected Events: [Link Down, P-North < > RR2] and [BGP Link Down, RR2 < > PE-North-West].
- Root Cause: Correlates to [Link Down, P-North < > RR2].

Figure C-21 displays the events identified by the system in this scenario.

Figure C-21 BGP Link Down Correlation to the Root Cause of Physical Link Down

Event Correlation Hierarchy	Location
Link down due to admin down	P-North-IOU-176#0:Seri...
— OSPF neighbor down syslog	P-North-IOU-176 IP:Seri...
— Interface status down	P-North-IOU-176 IP:Seri...
— — Link down syslog	P-North-IOU-176 IP:Seri...
— — Line down syslog	P-North-IOU-176 IP:Seri...
— — Line down trap	P-North-IOU-176 IP:Seri...
— BGP neighbor down syslog	PE-South-IOU-176 : 169...
— BGP link down	PE-South-IOU-176<->R...
— BGP neighbor down syslog	RR1-IOU-176 : 169.254....
— BGP neighbor down syslog	PE-East-IOU-176 : 169.2...
— BGP link down	PE-East-IOU-176<->RR...
— BGP link down	RR1-IOU-176<->RR2-I...
— Device unreachable	RR2-IOU-176
— BGP link down	PE-North-West-IOU-176...

370864

Clearing Phase

A BGP Link Up event arrives when the root cause event is fixed so that the network is repaired. This clearing event is created after a clearing syslog arrives or after the next polling result reestablishes the BGP connection.

Figure C-22 displays the up event that clears all tickets identified by the system.

Figure C-22 BGP Link Up Clears All the Tickets

Event Correlation Hierarchy	Location
Link up	P-North-IOU-176#0:Seri...
OSPF neighbor up syslog	P-North-IOU-176 IP:Seri...
Interface status up	P-North-IOU-176 IP:Seri...
Link up syslog	P-North-IOU-176 IP:Seri...
Line up syslog	P-North-IOU-176 IP:Seri...
Line down trap	P-North-IOU-176 IP:Seri...
BGP neighbor up syslog	PE-South-IOU-176 : 169...
BGP link up	PE-South-IOU-176<->R...
BGP neighbor up syslog	RR1-IOU-176 : 169.254....
BGP neighbor up syslog	PE-East-IOU-176 : 169.2...
BGP link up	PE-East-IOU-176<->RR...
BGP link up	RR1-IOU-176<->RR2-I...
Device reachable	RR2-IOU-176
BGP link up	PE-North-West-IOU-176...

370865

Variation

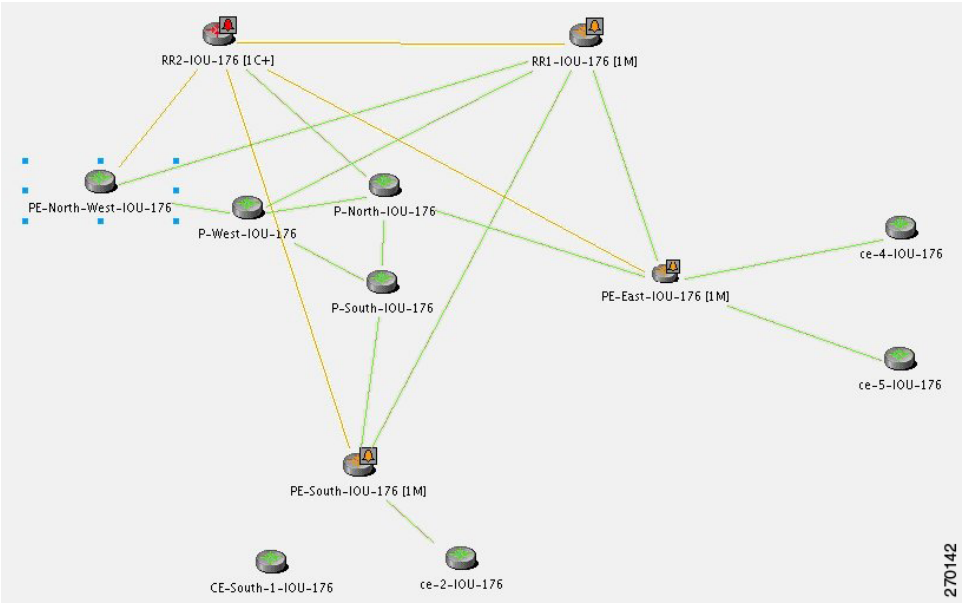
In a managed network, the following events might be identified in addition to the BGP Link Down event:

- BGP Process Down.
- Device Unreachable.

BGP Process Down

Figure C-23 displays the scenario where a BGP Process Down event causes BGP Link Down events.

Figure C-23 BGP Process Down Causes BGP Link Down Events



For the event [BGP Link Down, RR2 < > PE-North-West]:

- Additional Collected Events: [BGP Process Down, RR2].
- Root cause: Correlates to the event [BGP Process Down, RR2].

Figure C-24 displays the events identified by the system in this scenario.

Figure C-24 BGP Process Down Correlation

Event Correlation Hierarchy	Location
BGP process down	RR2-IOU-176
— BGP neighbor down syslog	RR2-IOU-176 : 169.254....
— BGP neighbor down syslog	RR2-IOU-176 : 169.254....
— BGP neighbor down syslog	RR2-IOU-176 : 169.254....
— BGP neighbor down syslog	PE-East-IOU-176 : 169.2...
— BGP neighbor down syslog	RR2-IOU-176 : 169.254....
— BGP link down	PE-East-IOU-176<->RR...
— BGP link down	PE-South-IOU-176<->R...
— BGP link down	RR1-IOU-176<->RR2-I...
— BGP link down	PE-North-West-IOU-176...
— BGP neighbor down syslog	PE-South-IOU-176 : 169...
— BGP neighbor down syslog	RR1-IOU-176 : 169.254....

370866

Device Unreachable

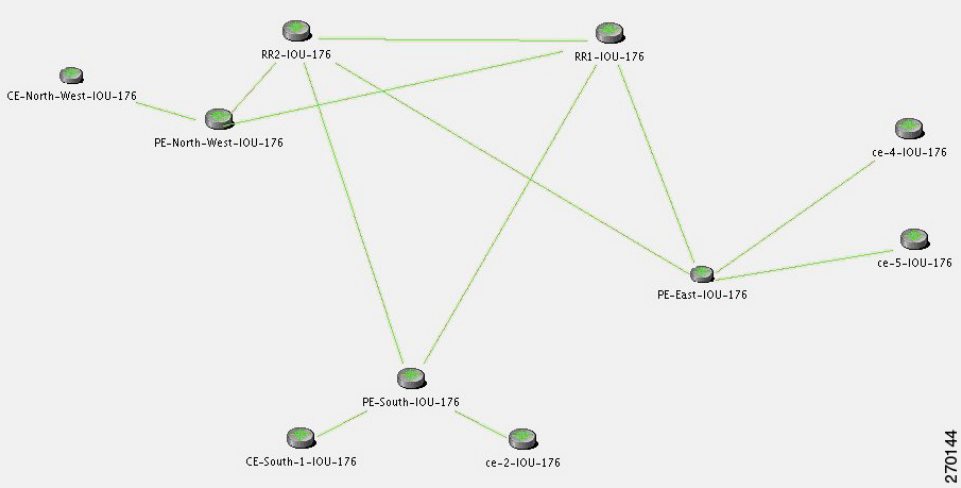
For the event [BGP Link Down, RR2 < > PE-North-West]:

- Additional Collected Events: [Device Unreachable, RR2].
- Root cause: Correlates to [Device Unreachable, RR2].

In an unmanaged network core (as illustrated in Figure C-25), the following events might be identified in addition to the BGP Link Down event:

- BGP Process Down.
- Device Unreachable.

Figure C-25 Lab Setup with Unmanaged Network Core

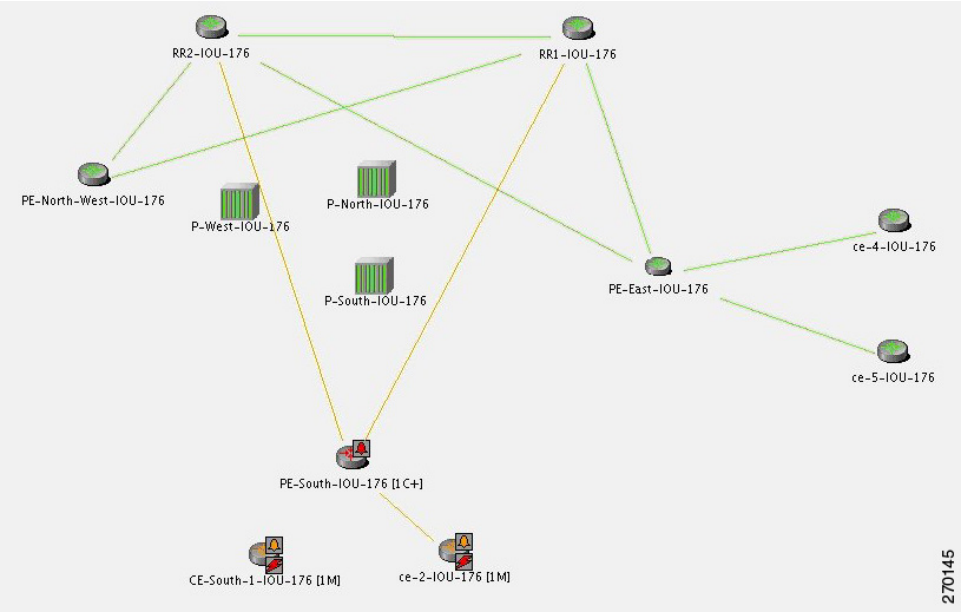


BGP Process Down

Note The BGP Process Down event occurs on the managed PE-South.

In Figure C-26, the BGP Process Down event on PE-South causes BGP Link Down events. The relevant devices are PE-South, RR1, and RR2.

Figure C-26 BGP Process Down on PE-South Causes BGP Link Down Events



For the event [BGP Link Down, PE-South < > RR2]:

- Additional Collected Events: [BGP Process Down, PE-South] and [BGP Link Down, PE-South < > RR1].
- Root cause: Correlates to [BGP Process Down, PE-South].

Figure C-27 displays the events identified by the system in this scenario.

Figure C-27 BGP Process Down Correlation

Event Correlation Hierarchy	Location
BGP process down	PE-South-IOU-176
— BGP neighbor down syslog	PE-South-IOU-176 : 169.254.176.216
— BGP neighbor down syslog	PE-South-IOU-176 : 169.254.176.224
— BGP link down	PE-South-IOU-176<->RR2-IOU-176
— BGP link down vrf	PE-South-IOU-176<->ce-2-IOU-176
— BGP link down	PE-South-IOU-176<->RR1-IOU-176

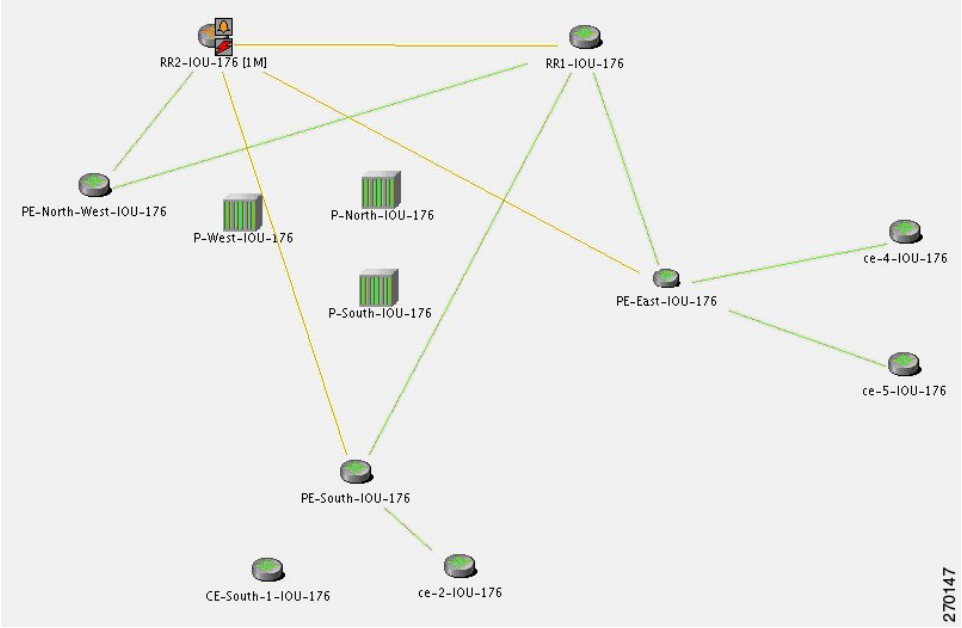
370867

Device Unreachable

For the Device Unreachable event, one or more PEs report on BGP connectivity loss to a neighbor that is unreachable.

In Figure C-28, the Device Unreachable on an unmanaged core causes multiple BGP Link Down events. The relevant devices are RR2 (Device Unreachable), RR1, PE-East, and PE-South.

Figure C-28 Device Unreachable on Unmanaged Core Causes Multiple BGP Link Down Events



For the event [BGP Link Down, RR2 < > PE-South]:

- Additional Collected Events: [Device Unreachable, RR2] and [BGP Link Down, RR2 < > RR1].
- Root cause: Correlates to [Device Unreachable, RR2].

Figure C-29 displays the events identified by the system in this scenario.

Figure C-29 Device Unreachable on Unmanaged Core Correlation

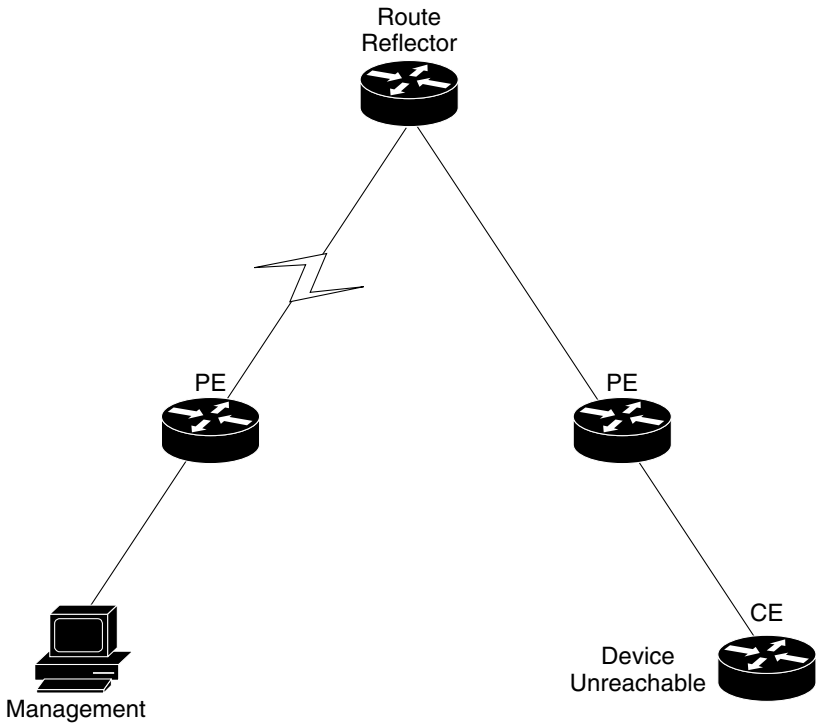
Event Correlation Hierarchy	Location
Device unreachable	RR2-IOU-176
— BGP link down	PE-South-IOU-176<->R...
— BGP link down	PE-East-IOU-176<->RR...
— BGP link down	RR1-IOU-176<->RR2-I...

370868

For the event [Device Unreachable, RR2] (see Figure C-30:

- Additional Collected Events: [BGP Link Down, RR2 < > PE-South].
- Root cause: Correlates to [BGP Link Down, RR2 < > PE-South].

Figure C-30 Device Unreachable on CE



EFP Down Correlation Scenarios

An Ethernet Flow Point (EFP) is a forwarding decision point in the PE switch or router that gives network designers the flexibility to make many Layer 2 flow decisions at the interface level. Many EFPs can be configured on a single physical port. These EFPs can be configured on any Layer 2 traffic port (usually on the UNI port). Each EFP manipulates the frames that enter it in a different manner and makes different forwarding decisions.

EFP Down Correlation Example 1

Figure C-31 provides an example of devices with EFP provisioning.

Figure C-31 EFP Down Example 1

In this example, service instances 900 and 901 are configured on port Gi4/3.

The physical link (Gi0/3 < > Gi4/3) is shut down. The expected alarm hierarchy:

- Link down
  - EFP down
  - Link down syslogs
  - Other related faults

EFP Down Correlation Example 2

Figure C-32 provides an example of devices with EFPs and a pseudowire provisioned.

Figure C-32 EFP Down Example 2

Service instances 900 and 901 are configured on port Gi4/3, and a local pseudowire is configured between Gi4/3 900 and Gi4/3 901 (local switching).

Service instance 900 is shut down. The expected alarm hierarchy:

- EFP down due to administrative down
  - EFP down syslogs
  - Local switching down
  - Other related faults

EFP Down Correlation Example 3

Example 3 also uses Figure C-32. Service instance 900 is configured on port Gi4/3 and connects to a pseudowire through a bridge domain.

Service instance 900 is shut down. The expected alarm hierarchy:

- EFP down due to administrative down
  - EFP syslogs
  - Pseudowire tunnel down
  - Other related faults

EFP Down Correlation Example 4

Example 4 also uses Figure C-32. Service instance 900 is configured on port Gi4/3 and connects to a pseudowire through a bridge domain.

Generate traffic to switch the service instance status to error disabled. The expected alarm hierarchy:

- EFP down due to error disabled
  - EFP syslogs
  - Pseudowire tunnel down
  - Other related faults

HSRP Scenarios

These topics describe scenarios that can generate HSRP alarms:

- HSRP Alarms, page C-31
- HSRP Example, page C-31

HSRP Alarms

When an active Hot Standby Router Protocol (HSRP) group's status changes, a service alarm is generated and a syslog is sent.

Table C-1 HSRP Service Alarms

Alarm	Ticketable?	Correlation allowed?	Correlated to	Severity
Primary HSRP interface is not active/Primary HSRP interface is active	Yes	No	Can be correlated to several other alarms; for example, link down	Major
Secondary HSRP interface is active/Secondary HSRP interface is not active	Yes	No	Can be correlated to several other alarms; for example, link down	Major

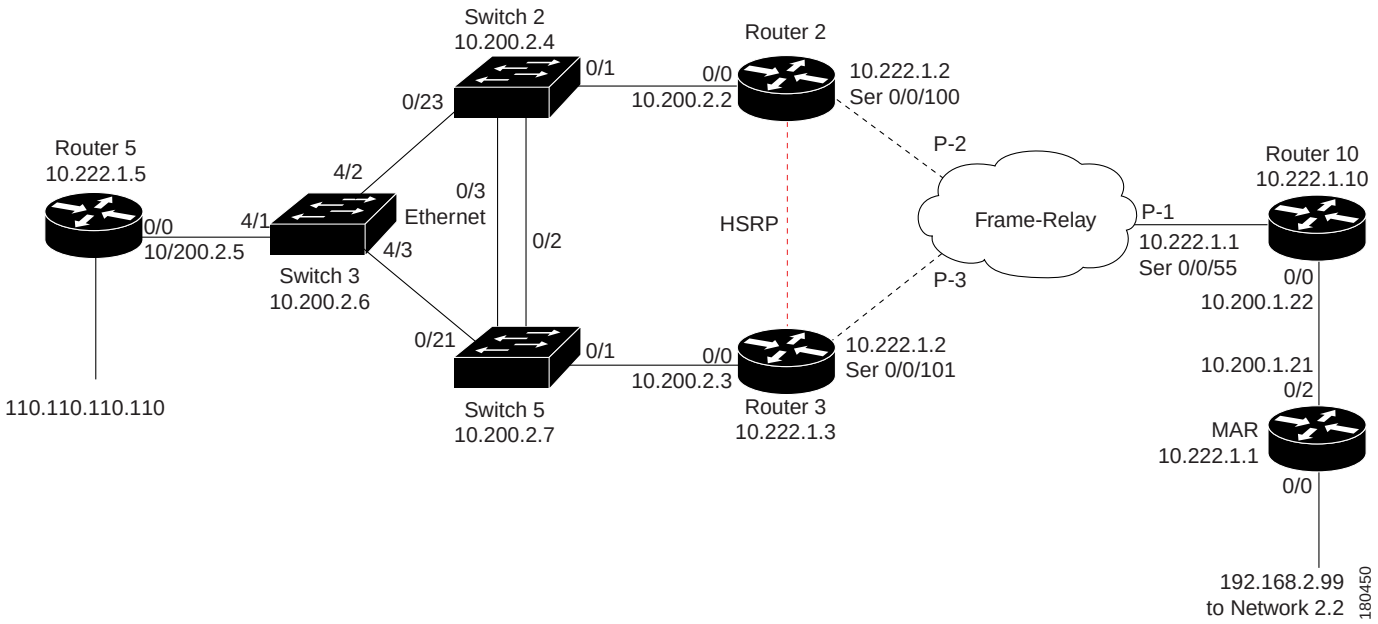
Note HSRP group information can be viewed in the inventory window of Prime Network NetworkVision.

HSRP Example

In Figure C-33, the link between Router 2 and Switch 2 is shut down, causing the HSRP standby group on Router 3 to become active, and a Link Down service alarm to be generated. The primary HSRP group on Router 2 is no longer active. A service alarm is generated and correlated to the Link Down alarm. Router 2 also sends a syslog which is correlated to the Link Down alarm.

The secondary HSRP group configured on Router 3 now changes from standby to active. This network event triggers an IP-based active flow with the destination being the virtual IP address configured in the HSRP group. When the flow reaches its destination, a service alarm is generated and correlated to the Link Down alarm. Router 3 also sends a syslog that is correlated to the Link Down alarm.

Figure C-33 Example



In this case, the system provides the following report:

- Root cause: [Link Down, Router 2 < > Switch 2]
- Correlated events:
  - [Primary HSRP Interface is Not Active, Router 2]

    ```
    %HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Active -> Speak (source:
    Router 2)
    ```

  - [Secondary HSRP Interface is Active, Router 3]

    ```
    %STANDBY-6-STATECHANGE: Ethernet0/0 Group 1 state Standby -> Active (source:
    Router 3)
    ```

IP Interface Failure Scenarios

These topics describe scenarios that can generate IP interface failures:

- Interface Status Down Alarm, page C-32
- All IP Interfaces Down Alarm, page C-34
- IP Interface Failure Examples, page C-34

Interface Status Down Alarm

Alarms related to subinterfaces (for example, a Line Down trap or syslog) are reported on IP interfaces configured above the relevant subinterface. This means that in the system, subinterfaces are represented by the IP interfaces configured above them. All events sourcing from subinterfaces without a configured IP interface are reported on the underlying Layer 1.

An Interface Status Down alarm is generated when the status of an IP interface (whether over an interface or a subinterface) changes from up to down or any other nonoperational state (see Table C-2). All events sourced from the subinterfaces correlate to this alarm. In addition, an All IP Interfaces Status Down alarm is generated when all the IP interfaces above a physical port change state to down.

Table C-2 Interface Status Down Alarm

Name	Description	Ticketable	Correlation allowed	Correlated to	Severity
Interface Status Down/Up	Sent when an IP interface changes operational status to down/up	Yes	Yes	Link Down/Device Unreachable	Major

The alarm's description includes the full name of the IP interface, for example Serial0.2 (including the identifier for the subinterface if it is a subinterface), and the alarm source points to the IP interface (and not to Layer 1).

All syslogs and traps indicating changes in subinterfaces (above which an IP address is configured) correlate to the Interface Status Down alarm. The source of these events is the IP interface. Syslogs and traps that indicate problems in Layer 1 (that do not have a subinterface qualifier in their description) are sourced to Layer 1.

Note If a syslog or trap is received from a subinterface that does not have an IP interface configured above it, the source of the created alarm is the underlying Layer 1.

For example:

- Line Down trap (for subinterface)
- Line Down syslogs (for subinterface)

For events that occur on subinterfaces:

- When sending the information northbound, the system uses the full subinterface name in the interface name in the source field, as described in the ifDesc/ifName OID (for example, Serial0/0.1 and not Serial0/0 DLCI 50).
- The source of the alarm is the IP interface configured above the subinterface.
- If IP is not configured on the interface, the source is the underlying Layer 1.

If the main interface goes down, all related subinterface traps and syslogs are correlated as child tickets to the main interface parent ticket.

The following technologies are supported:

- Frame Relay/HSSI
- ATM
- Ethernet, Fast Ethernet, Gigabit Ethernet
- Packet over SONET (POS)
- Channelized Optical Carrier (CHOC)

Correlation of Syslogs and Traps

Upon receipt of a trap or syslog for the subinterface level, Cisco ANA immediately polls the status of the relevant IP interface and creates a polled parent event (such as Interface Status Down). The trap or syslog is correlated to this alarm.

In a multipoint setup when only some circuits under an IP interface go down do not cause the state of the IP interface to change to down, Cisco ANA does not create an Interface Status Down alarm. All circuit down syslogs correlate by flow to the possible root cause, such as Device Unreachable on a CE device.

All IP Interfaces Down Alarm

- When all IP interfaces configured above a physical interface change their state to down, the All IP Interfaces Down alarm is sent.
- When at least one of the IP interfaces changes its state to up, a clearing (Active IP Interface Found) alarm is sent.
- The Interface Status Down alarm for each of the failed IP interfaces is correlated to the All IP Interfaces Down alarm.

Note If an All IP Interfaces Down alarm is cleared by the Active IP Interfaces Found alarm, but some correlated Interface Status Down alarms still exist for some IP interfaces, the severity of the parent ticket is the highest severity among all the correlated alarms. For example, if an Interface Status Down alarm is uncleared, the severity of the ticket remains major, despite the Active IP Interface Found alarm having a cleared severity.

For more information, see Table C-3.

Table C-3 All IP Interfaces Down

Name	Description	Ticketable	Correlation allowed	Correlated to	Severity
All IP Interfaces Down/Active IP Interfaces Found	Sent when all IP interfaces configured above a physical port change their operational status to down.	Yes	Yes	Link Down	Major

The All IP Interfaces Down alarm is sourced to the Layer 1 component. All alarms from the other side (such as Device Unreachable) correlate to the All IP Interfaces Down alarm.

IP Interface Failure Examples

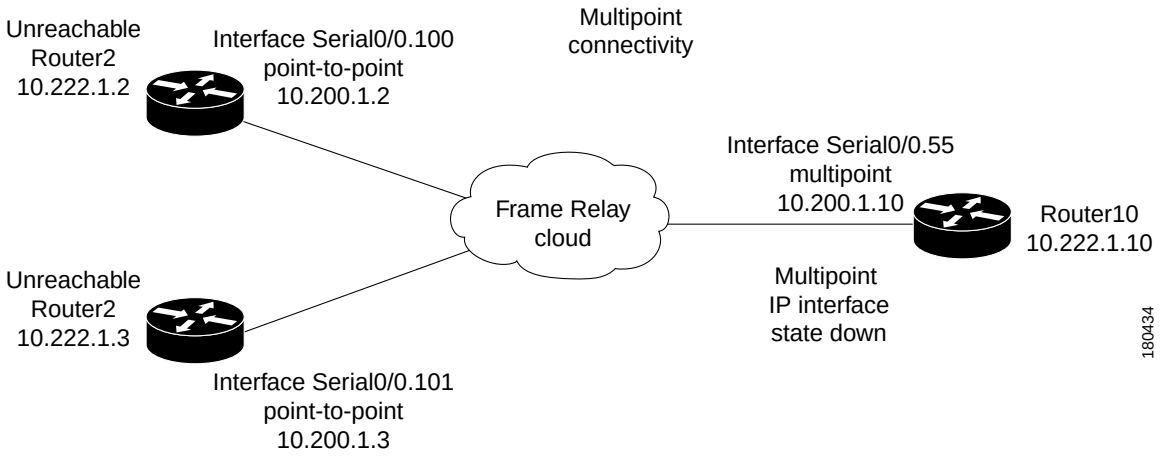
Note In the following examples, it is assumed that the problems that result in the unmanaged cloud, or the problems that occurred on the other side of the cloud (such as an unreachable CE device from a PE device) cause the relevant IP interfaces' state to change to down. This, in turn, causes the Interface Status Down alarm to be sent.

If this is not the case, as in some Ethernet networks, and there is no change to the state of the IP interface, all the events on the subinterfaces that are capable of correlation flow will try to correlate to other possible root causes, including Cloud Problem.

Interface Example 1

Figure C-34 represents an environment with multipoint connectivity between a PE and number of CEs through an unmanaged Frame Relay network. All CEs (Router2 and Router3) have logical connectivity to the PE through a multipoint subinterface on the PE (Router10). The keepalive option is enabled for all circuits. A link is disconnected inside the unmanaged network, causing all CEs to become unreachable.

Figure C-34 Interface Example 1



The following failures are identified in the network:

- A Device Unreachable alarm is generated for each CE.
- An Interface Status Down alarm is generated for the multipoint IP interface on the PE.

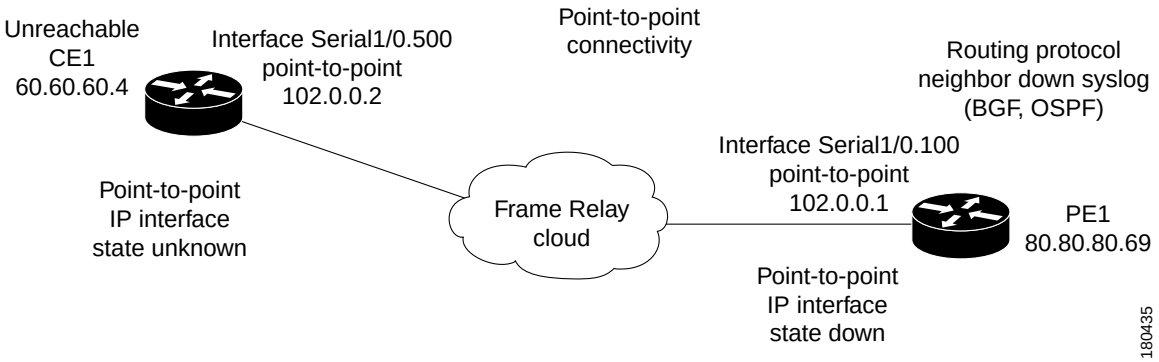
The following correlation information is provided:

- The root cause is Interface Status Down.
- All Device Unreachable alarms are correlated to the Interface Status Down alarm on the PE.

Interface Example 2

Figure C-35 represents an environment with point-to-point connectivity between a PE and a CE through an unmanaged Frame Relay network. CE1 became unreachable, and the status of the IP interface on the other side (on PE1) changed to down. The keepalive option is enabled. The interface is shut down between the unmanaged network and CE1.

Figure C-35 Interface Example 2



The following failures are identified in the network:

- A Device Unreachable alarm is generated on the CE.
- An Interface Status Down alarm is generated on the PE.

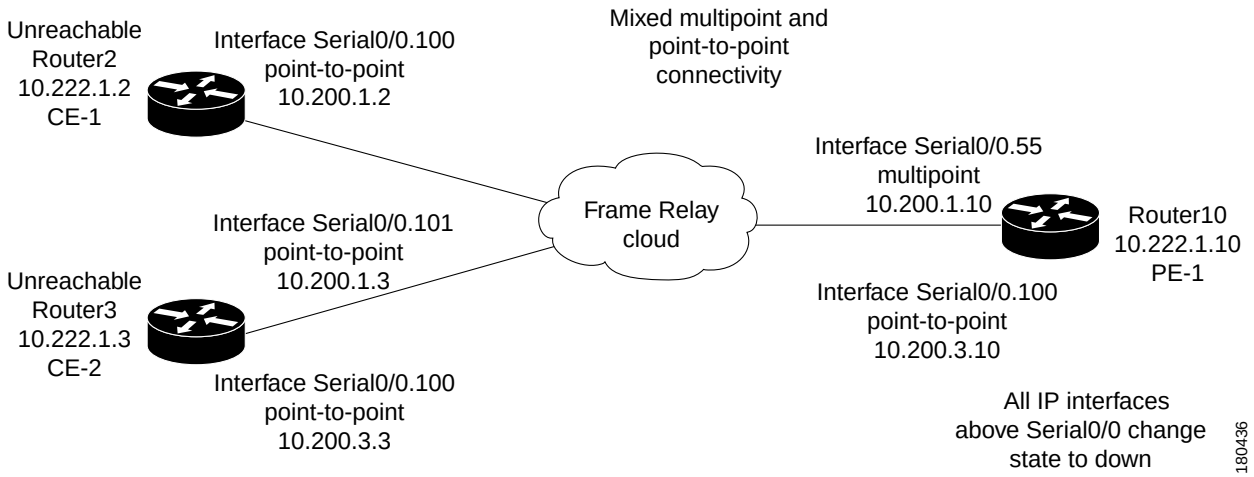
The following correlation information is provided:

- The root cause is Device Unreachable:
  - The Interface Status Down alarm is correlated to the Device Unreachable alarm.
  - The syslogs and traps for the related subinterfaces are correlated to the Interface Status Down alarm.

Interface Example 3

Figure C-36 represents an environment in which the failure of multiple IP interfaces occurs above the same physical port (mixed point-to-point and multipoint Frame Relay connectivity). CE1 (Router2) has a point-to-point connection to PE1 (Router10). CE1 and CE2 (Router3) have multipoint connections to PE1. The IP interfaces on PE1 that are connected to CE1 and CE2 are all configured above Serial0/0. The keepalive option is enabled. A link is disconnected inside the unmanaged network, causing all CEs to become unreachable.

Figure C-36 Interface Example 3



The following failures are identified in the network:

- All the CEs become unreachable.
- An Interface Status Down alarm is generated for each IP interface above Serial0/0 that has failed.

The following correlation information is provided:

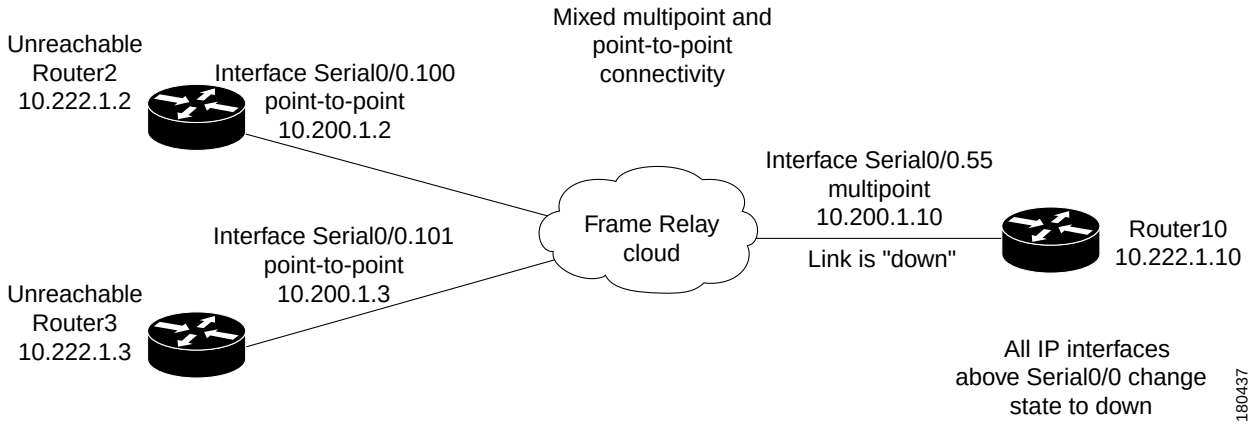
- The root cause is All IP Interfaces Down on Serial0/0 port:
  - The Interface Status Down alarms are correlated to the All IP Interfaces Down alarm.
  - The Device Unreachable alarms are correlated to the All IP Interfaces Down alarm.
  - The syslogs and traps for the related subinterfaces are correlated to the All IP Interfaces Down alarm.

Interface Example 4

Figure C-37 represents an environment in which the failure of multiple IP interfaces occurs above the same physical port (mixed point-to-point and multipoint Frame Relay connectivity). CE1 (Router2) has a point-to-point connection to PE1 (Router10). CE1 and CE2 (Router3) have multipoint connections to PE1. The IP interfaces on PE1 that are connected to CE1 and CE2 are all configured above Serial0/0. The keepalive option is enabled.

A link is disconnected inside the unmanaged network, causing all CEs to become unreachable. When a Link Down occurs, whether or not it involves a cloud, the link failure is considered to be the most probable root cause for any other failure. In this example, a link is disconnected between the unmanaged network and the PE.

Figure C-37 Interface Example 4



The following failures are identified in the network:

- A Link Down alarm is generated on Serial0/0.
- A Device Unreachable alarm is generated for each CE.
- An Interface Status Down alarm is generated for each IP interface above Serial0/0.
- An All IP Interfaces Down alarm is generated on Serial0/0.

The following correlation information is provided:

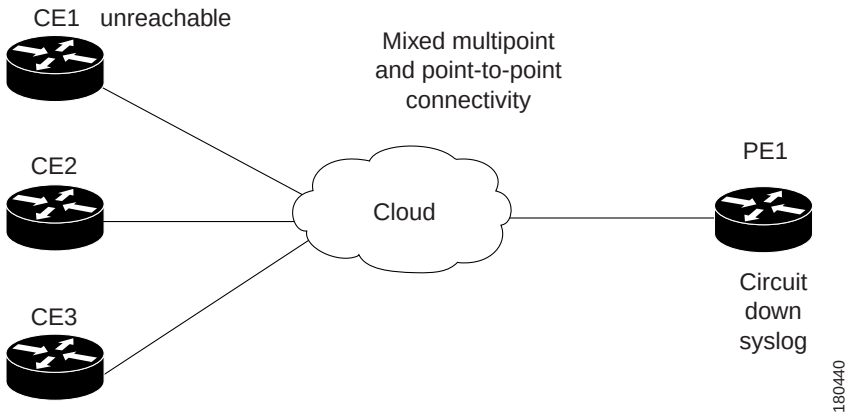
- The Device Unreachable alarms are correlated to the Link Down alarm.
- The Interface Status Down alarm is correlated to the Link Down alarm.

- The All IP Interfaces Down alarm is correlated to the Link Down alarm.
- All the traps and syslogs for the subinterfaces are correlated to the Link Down alarm.

Interface Example 5

Figure C-38 represents an environment in which a PE1 device has multipoint connectivity, one of the circuits under the IP interface has gone down, and the CE1 device has become unreachable. The status of the IP interface has not changed and other circuits are still operational.

Figure C-38 General Interface Example



The following failures are identified in the network:

- A Device Unreachable alarm is generated on CE1.
- A syslog alarm is generated, notifying the user about a circuit down.

The following correlation information is provided:

- Device Unreachable on the CE—The syslog alarm is correlated by flow to the Device Unreachable alarm on CE1.

ATM Failure Examples

Examples involving ATM technology have the same result as the examples in IP Interface Failure Examples, page C-34, assuming that a failure in an unmanaged network causes the status of the IP interface to change to down (ILMI is enabled).

Ethernet, Fast Ethernet, and Gigabit Ethernet Examples

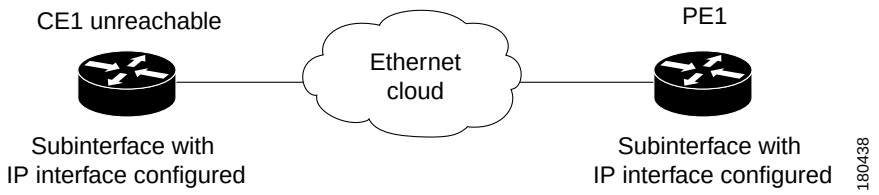
This section includes the following examples:

- A CE becomes unreachable due to a failure in the unmanaged network (see Interface Example 6, page C-39).
- A link down on a PE results in a CE becoming unreachable (see Interface Example 7, page C-39).

Interface Example 6

Figure C-39 shows an unreachable CE due to a failure in the unmanaged network.

Figure C-39 Interface Example 6



The following failures are identified in the network:

- A Device Unreachable alarm is generated on the CE.
- A Cloud Problem alarm is generated.

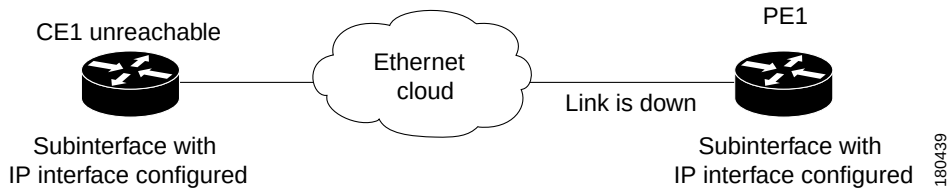
The following correlation information is provided:

- No alarms are generated on a PE for Layer 1, Layer 2, or IP interface layers.
- The Device Unreachable alarm is correlated to the Cloud Problem alarm.

Interface Example 7

Figure C-40 shows a Link Down alarm on a PE that results in a CE becoming unreachable.

Figure C-40 Interface Example 7



The following failures are identified in the network:

- A Link Down alarm is generated on the PE.
- An Interface Status Down alarm is generated on the PE.
- A Device Unreachable alarm is generated on the CE.

The following correlation information is provided:

- Link Down on the PE:
  - The Interface Status Down alarm on the PE is correlated to the Link Down alarm.
  - The Device Unreachable alarm on the CE is correlated to the Link Down alarm on the PE.
  - The traps and syslogs for the subinterface are correlated to the Link Down alarm on the PE.

GRE Tunnel Down/Up

Generic routing encapsulation (GRE) is a tunneling protocol that encapsulates a variety of network layer packets inside IP tunneling packets, creating a virtual point-to-point link to devices at remote points over an IP network. It is used on the Internet to secure VPNs. GRE encapsulates the entire original packet with a standard IP header and GRE header before the IPsec process. GRE can carry multicast and broadcast traffic, making it possible to configure a routing protocol for virtual GRE tunnels. The routing protocol detects loss of connectivity and reroutes packets to the backup GRE tunnel, thus providing high resiliency.

GRE is stateless, meaning that the tunnel endpoints do not monitor the state or availability of other tunnel endpoints. This feature helps service providers support IP tunnels for clients who do not know the service provider's internal tunneling architecture. It gives clients the flexibility of reconfiguring their IP architectures without worrying about connectivity.

GRE Tunnel Down/Up Alarm

When a GRE tunnel link exists, if the status of the IP interface of the GRE tunnel edge changes to down, a GRE Tunnel Down alarm is created. The IP Interface Status Down alarms of both sides of the link correlate to the GRE Tunnel Down alarm. The GRE Tunnel Down alarm initiates an IP-based flow toward the GRE destination. If an alarm is found during the flow, it correlates to it.

Note The GRE Tunnel Down alarm is supported only on GRE tunnels that are configured with keepalive. If keepalive is configured on the GRE tunnel edge and a failure occurs in the GRE tunnel link, both IP interfaces of the GRE tunnel move to the Down state. If keepalive is not configured on the GRE tunnel edge, the GRE Tunnel Down alarm might not be generated because the alarm is generated arbitrarily from one of the tunnel devices when the IP interface changes to the Down state.

When a failure occurs, the GRE tunnel link is marked orange. When the IP interface comes back up, a fixing alarm is sent, and the link is marked green. The GRE Tunnel Down alarm is cleared by a corresponding GRE Tunnel Up alarm.

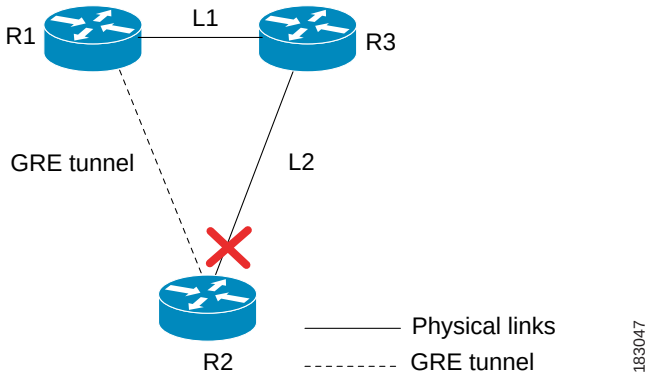
GRE Tunnel Down Correlation Example 1

Figure C-41 illustrates an example of a GRE Tunnel Down correlation for a single GRE tunnel.

In this example:

- Router 1 (R1) is connected to Router 3 (R3) through physical link L1.
- Router 3 is connected to Router 2 through physical link L2.
- Router 1 is connected to Router 2 through a GRE tunnel.

Figure C-41 GRE Tunnel Down Example 1 (Single GRE Tunnel)



When the link down occurs on L2, a Link Down alarm appears. A GRE Tunnel Down alarm is issued as the IP interfaces of the tunnel edge devices go down. The Interface Status Down alarms correlate to the GRE Tunnel Down alarm. The GRE Tunnel Down alarm correlates to the Link Down alarm.

The system provides the following report:

- Root cause—[Link Down: L2 Router 2 < > Router 3]
- Correlated events:

  [GRE Tunnel Down, Router1:tunnel < > Router 2:tunnel]

  – [Interface Status Down, Router 1:tunnel]

  – [Interface Status Down, Router 2:tunnel]

GRE Tunnel Down Correlation Example 2

This example provides a real-world scenario in which multiple GRE tunnels cross through a physical link. When this link is shut down by an administrator, many alarms are generated. All of these alarms are correlated to the root cause ticket, Link Down Due to Admin Down ticket, as illustrated in Figure C-42.

Figure C-42 GRE Tunnel Down Example 2 (Multiple GRE Tunnels)

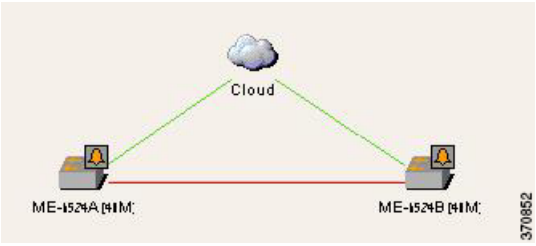


Figure C-43 shows the Correlation tab of the Ticket Properties dialog box that displays all the alarms that are correlated to the ticket, including the correlation for each GRE tunnel and its interface status.

Figure C-43 Alarm Correlation to GRE Tunnel Down Ticket

Event Correlation Hierarchy	Location
Link down due to admin down	ME-6524A#:GigabitEthernet1/...
— Interface status down	ME-6524A IP:GigabitEthernet1/25
— Interface status down	ME-6524B IP:GigabitEthernet1/25
— GRE tunnel down	ME-6524A GRE: Tunnel2<->ME-...
— Interface status down	ME-6524A IP: Tunnel2
— Interface status down	ME-6524B IP: Tunnel2
— GRE tunnel down	ME-6524A GRE: Tunnel3<->ME-...
— Interface status down	ME-6524A IP: Tunnel3
— Interface status down	ME-6524B IP: Tunnel3
— GRE tunnel down	ME-6524A GRE: Tunnel9<->ME-...
— Interface status down	ME-6524A IP: Tunnel9
— Interface status down	ME-6524B IP: Tunnel9
— GRE tunnel down	ME-6524A GRE: Tunnel6<->ME-...
— Interface status down	ME-6524A IP: Tunnel6
— Interface status down	ME-6524B IP: Tunnel6
— GRE tunnel down	ME-6524A GRE: Tunnel7<->ME-...
— Interface status down	ME-6524A IP: Tunnel7
— Interface status down	ME-6524B IP: Tunnel7

370854

As illustrated, the system provides the following report:

- Root cause—Link Down Due to Admin Down
- Correlated events:

  [GRE Tunnel Down, ME-6524AGRE:Tunnel2 < > ME-6524B GRE:Tunnel2]

  – [Interface Status Down, ME-6524A IP:Tunnel2]

  – [Interface Status Down, ME-6524B IP:Tunnel2]

  [GRE Tunnel Down, ME-6524AGRE:Tunnel3 < > ME-6524B GRE:Tunnel3]

  – [Interface Status Down, ME-6524A IP:Tunnel3]

  – [Interface Status Down, ME-6524B IP:Tunnel3]

  and so on.

Q-in-Q Subinterface Down Correlation Scenarios

Q-in-Q technology refers to the nesting of a VLAN header in an Ethernet frame in an already existing VLAN header. Both VLAN headers must be of the type 802.1Q. When one VLAN header is nested within another VLAN header, they are often referred to as *stacked VLANs*.

A subinterface is a logical division of traffic on an interface, such as multiple subnets across one physical interface. A subinterface name is represented as an extension to an interface name using dot notation, such as Interface Gigabit Ethernet 0/1/2/3.10. In this example, the main interface name is Gigabit Ethernet 0/1/2/3 and the subinterface is 10.

Q-in-Q Subinterface Down Correlation Example 1

Figure C-44 shows an example of devices connected via a stacked VLAN.

Figure C-44 Q-in-Q Subinterface Down Example 1

In this example:

- A physical link (Gi0/3 < > Gi4/3) is established between 7201-P1 and 6504E-PE3.
- On device 7201-P1 on Gi0/3, a subinterface (Gi0/3.100) is configured for IEEE 802.1Q encapsulation.
- A stacked VLAN is created across the link between 7201-P1 and 6504-PE3.

When the physical link between the interfaces is shut down, the following are generated:

- Link Down alarm on the interface.
- Subinterface Down alarm on Gi03/.100.
- Subinterface Down syslogs.
- Link Down syslogs (LINK-3-UPDOWN).
- Related faults.

The following correlation information is provided:

- The root cause is the Link Down alarm.
- The Subinterface Down alarm is correlated to the Link Down alarm.
- The subinterface syslogs are correlated to the Subinterface Down alarm.
- The syslogs and other related faults are correlated to the Link Down Alarm.

Q-in-Q Subinterface Down Correlation Example 2

In this example, using the devices in Figure C-44:

- On device 7201-P1 on Gi0/3, the following subinterfaces are configured:
  - Gi0/3.100
  - Gi0/3.101
- A local pseudowire tunnel is configured and links Gi0/3.100 with Gi0/3.101 for local switching.

When the Gi0/3.100 subinterface is shut down by the administrator, the following are generated:

- Subinterface Down alarm of the type Subinterface Admin Down.
- Subinterface Down syslogs.
- Local Switching Down.
- Related faults.

The Subinterface Admin Down event does not search for the root cause through the correlation mechanism.

Q-in-Q Subinterface Down Correlation Example 3

Figure C-45 shows an example of devices connected via a pseudowire tunnel configured on subinterfaces.

Figure C-45 Q-in-Q Subinterface Down Example 3

In this example:

- On device 7201-P1 on Gi0/3, a subinterface (Gi0/3.100) is configured for IEEE 802.1Q encapsulation.
- The subinterface (Gi0/3.100) is connected to a pseudowire tunnel.

When the Gi0/3.100 subinterface is shut down by the administrator, the following are generated:

- Subinterface Down alarm of the type Subinterface Admin Down.
- Subinterface Down syslogs.
- Pseudowire Tunnel Down.
- Related faults.

The Subinterface Admin Down event does not search for the root cause through the correlation mechanism.

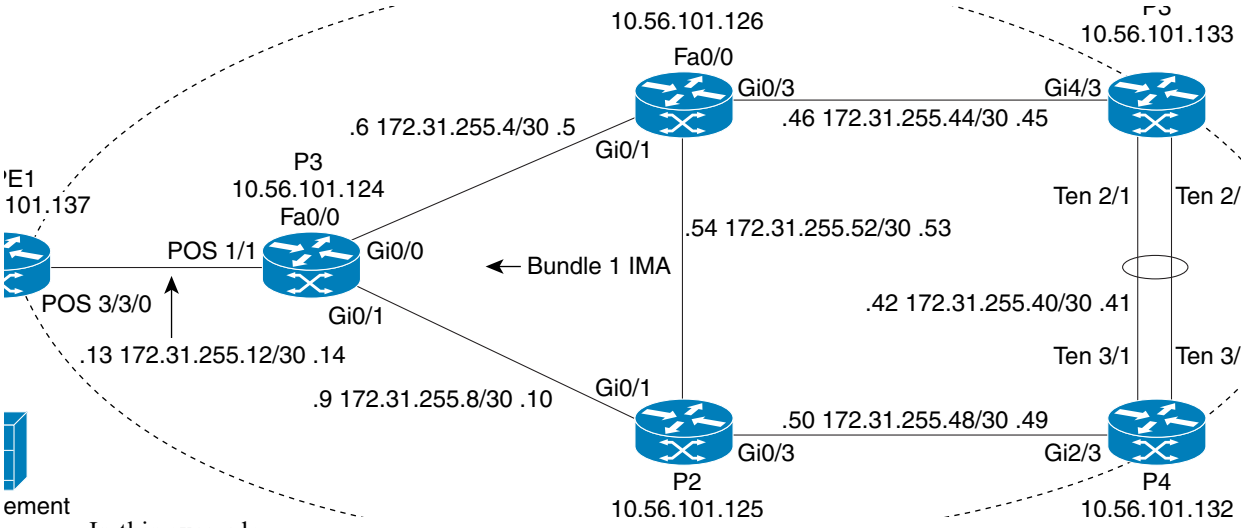
VSI Down Correlation Scenarios

Virtual Private LAN Service (VPLS) is a type of Layer 2 VPN that provides Ethernet-based multipoint-to-multipoint communication over MPLS networks. It allows geographically dispersed sites to share an Ethernet broadcast domain by connecting sites through pseudowires. Emulating the function of a LAN switch or bridge, VPLS connects the different customer LAN segments to create a single-bridged Ethernet LAN. Virtual switching instances (VSIs, also known as virtual forwarding instances, or VFIs), are the main component in the PE router that constructs the logical bridge. All VSIs that build a provider logical bridge are connected with MPLS pseudowires.

VSI Down Correlation Example 1

Figure C-46 shows an example of devices with VSI connected through pseudowires.

Figure C-46 VSI Down Example 1



In this example:

- A VSI is configured on PE1.
- The VSI uses pseudowire 1 (PW 1) and PW 2.

The VSI is shut down. The expected alarm hierarchy is:

- VSI Down >
  - Pseudowire tunnel 1 down > Pseudowire tunnel 1 syslogs
  - Pseudowire tunnel 2 down > Pseudowire tunnel 2 syslogs
  - Other related faults

Note For more information about the VSI Down alarm.

VSI Down Correlation Example 2

In this example, using the devices in Figure C-46, the VSI attachment circuit (the interface VLAN) is shut down. The expected alarm hierarchy is the same as in Example 1:

- VSI Down >
  - Pseudowire tunnel 1 down > Pseudowire tunnel 1 syslogs
  - Pseudowire tunnel 2 down > Pseudowire tunnel 2 syslogs
  - Other related faults

However, because Prime Network does not model the attachment circuit state, the VNE cannot issue an alarm when the interface VLAN state changes to Down. Therefore, the VSI Down alarm is the highest root cause.

VSI Down Correlation Example 3

In this example, using the devices in Figure C-46:

- A VSI is configured on PE4.
- The VSI uses the pseudowire tunnels 2 and 3.
- The VSI is connected to bridge 100; the binding to the VSI is done on interface VLAN 100.
- Two physical interfaces, Gi1/1 and Gi1/2, are associated to bridge 100.
- Interfaces Gi1/1 and Gi1/2 are shut down.

Note The attachment circuit connected to bridge 100 has two physical interfaces. As long as one interface is up, bridge 100 will be up. Bridge 100 will go down when the last interface switches from up to down.

The expected alarm hierarchy:

- Port Down/Link Down due to administrative down (Gi1/2) > Port Down/Link Down syslogs
- VSI Down >
  - Pseudowire tunnel 3 down > Pseudowire tunnel 1 syslogs
  - Pseudowire tunnel 2 down > Pseudowire tunnel 2 syslogs
- Other related faults

Root Cause Across Frame Relay, ATM, or Ethernet Clouds

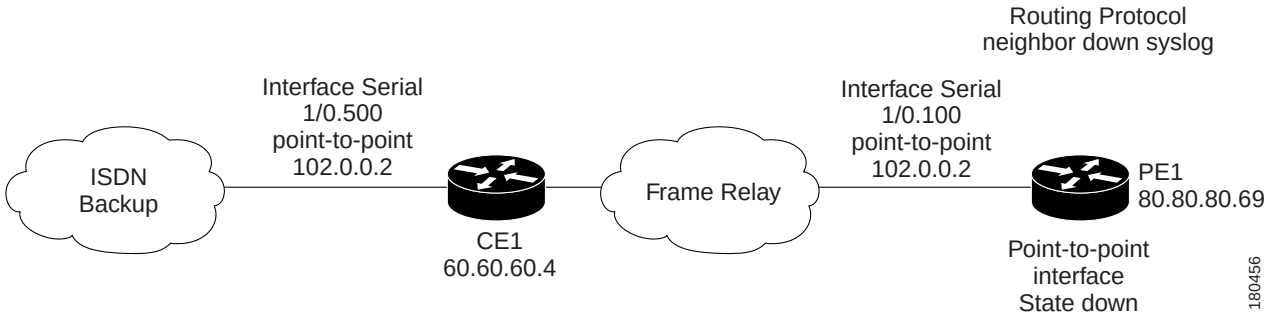
When a Layer 3 or Layer 2 event (for example, reachability problem, neighbor change, Frame Relay DLCI down, ATM PVC down) occurs, it triggers a flow along the physical and logical path modeled on the VNEs. This is done in order to correlate to the actual root cause of this fault. If the flow passes over a cloud along the path flow, it marks it as a potential root cause for the fault. If there is no other root cause found on the managed devices, then the cloud becomes the root cause. A ticket is then issued and the original event correlates to it.

Cloud Problem Alarm and Correlation Example

For some events, when there is no root cause found, a special Cloud Problem alarm is created. These events are then correlated to the alarm. If several events trigger the creation of a Cloud Problem alarm, one alarm instance is created and all events correlate to it.

In the example in Figure C-47, two devices that have OSPF configured are connected through a cloud. A malfunction occurs inside the unmanaged network that causes the OPSF Neighbor Down alarm to be generated. In this case, the OSPF Neighbor Down alarm is correlated to the Cloud Problem alarm.

Figure C-47 Cloud Correlation Example



On the PE1 device, the OSPF Neighbor Down alarm was received, and no root cause was detected in any of the managed devices. A disconnected link inside the unmanaged network caused the OSPF Neighbor Down alarm. The Cloud Problem service alarm is generated, and the OSPF Neighbor Down alarm on the PE1 is correlated to the Cloud Problem alarm.

MPLS Fault Scenarios

The following fault scenarios trigger automatic impact analysis calculation:

- Link Down Scenario, page C-48
- Link Overutilized/Data Loss Scenario, page C-48
- BGP Neighbor Loss Scenario, page C-49
- Broken LSP Discovered Scenario, page C-51
- MPLS TE Tunnel Down Scenario, page C-51
- Pseudowire MPLS Tunnel Down Scenario, page C-51

The following criteria are used in the tables that are described in the sections that follow:

- Impact Calculation—Describes the way in which the affected parties are calculated by system flows.
- Reported Affected Severity—Describes the kind of severity generated by the alarm.

Note Proactive impact analysis is performed only for links.

Link Down Scenario

Table C-4 lists the impact calculations and reported affected severities for a link down fault scenario.

Table C-4 Link Down Scenario

Impact and Affected Severity	Description
Impact calculation	Initiates an affected flow to determine the affected parties using the LSPs traversing the link.
Reported affected severity	• The Link Down alarm creates a series of affected severity updates over time. These updates are added to the previous updates in the Oracle database. In this case, the system provides the following reports: – The first link down report shows "X< >Y" as Potentially Affected. – Over time, the VNE identifies that this service is Real Affected or Recovered and generates an updated report (this applies only to cross-MPLS networks). – The Affected Parties tab of the Ticket Properties dialog box displays the latest severity, for example, Real Affected. – The Affected Parties Destination Properties dialog box displays both reported severities. This functionality is supported for Link Down only.

Link Overutilized/Data Loss Scenario

Table C-5 lists the impacted calculations and reported affected severities for a link overutilized/data loss fault scenario.

Table C-5 Link Overutilized/Data Loss Scenario

Impact and Affected Severity	Description
Impact calculation	Initiates an affected flow to determine the affected parties using the LSPs traversing the link.
Reported affected severity	Only reports on potentially affected.

BGP Neighbor Loss Scenario

Table 3-6 shows the impacted calculations and reported affected severities for a BGP neighbor loss fault scenario.

Table 3-6 BGP Neighbor Loss Scenario

Impact and Affected Severity	Description
Impact calculation	• Initiates a local affected flow to all VRFs that are present on the issuing device. Each local VRF that has route entries with a next hop IP address that was learned from the BGP neighbor that was lost collects VRFs from both sides and pairs them together as affected. • Supports a route reflector configuration, whereby during the affected search, affected parties are located on all BGP neighbors learned via the route reflector.
Reported affected severity	Only reports on real affected on the IBGP domain.

Note The affected only relate to Layer 3 VPN services.

BGP rules require all routers within an autonomous system to be fully meshed. For large networks, this requirement represents a severe scaling problem. Route reflectors enable a BGP entity to establish a single BGP connection with a peer, where through that single peer, routing information is learned from other peers. As a result, the number of BGP sessions and connections is greatly reduced.

Decreasing the number of BGP connections and using route reflectors further separates the data and control paths. For example, data packets going from A to B do not go through the route reflector, while the routing updates between A and B do.

Every BGP router is uniquely identified by a router ID. A route reflector is not a configuration of a specific router. A router may act as a route reflector if it has a BGP neighbor configured as a BGP client. A router may act as both a route reflector to some of its BGP neighbors (those that are configured as BGP clients) and a nonclient BGP neighbor to those BGP neighbors that are configured as nonclient BGP neighbors.

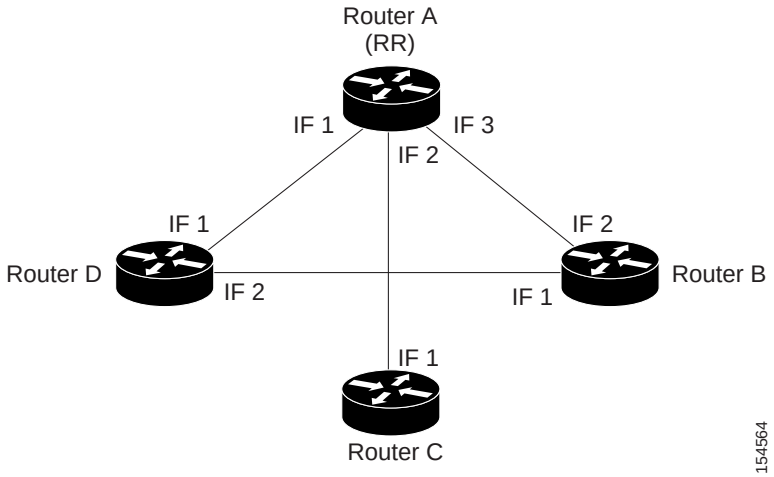
A route reflector uses the following logic when distributing routes to its BGP neighbors:

- A router advertises to its client peers all routes learned from other client and nonclient peers.
- A router advertises to its nonclient peers only routes received from client peers.

Router ID distribution follows the same logic described previously.

Prime Network modeling provides a list of one or more router IDs for each interface. This reflects the network behavior of receiving BGP updates from a BGP router (possessing that ID) through that interface. The VNE also maintains the nature of the relationships (client and nonclient) among the various VNEs representing the BGP routers. Figure C-48 shows an example.

Figure C-48 Route Reflector Example



In the example, the following configuration is applied:

- Router A (router ID A) has clients B, C, and D configured. Therefore it serves as the route reflector for these BGP routers.
- Routers B, C, and D all have Router A as a BGP nonclient neighbor.
- Router D and Router B also have each other configured as BGP nonclient neighbors.

In this case, in Prime Network, the following information is maintained by a VNE:

- Router B learns router ID D from interface 1.
- Router B learns router IDs A, C, and D from interface 2.
- Router C learns router IDs A, B, and D from interface 1.
- Router D learns router ID B from interface 2.
- Router D learns router IDs A, B, and C from interface 1.
- Router A learns router ID D from interface 1.
- Router A learns router ID C from interface 2.
- Router A learns router ID B from interface 3.

In the Figure C-48 example, if a BGP connection from Router A to Router B is lost, the following occurs:

- Router A notifies both Routers C and D of the loss of router ID B.
- Router C removes the ID of Router B from its tables and completely loses connectivity to it, resulting in a Real Affected impact analysis.
- Router D loses the ID of Router B learned from interface 1, but it still has the Router B ID that was learned through interface 2. Therefore, no impact analysis is performed.

If a BGP connection is lost from Router B to Router D, the following occurs:

- Router B does not notify Router A of its router ID loss, because Router A is configured in the Router B tables as a nonclient peer.
- Router D does not notify Router A of its router ID loss, because Router A is configured in Router D's tables as a nonclient peer.
- Router B notes that the ID of Router D is no longer learned through interface 1.

- Router D notes that the ID of Router B is no longer learned through interface 2.
- No impact analysis is performed.

Broken LSP Discovered Scenario

Table 3-7 lists the impacted calculations and reported affected severities for a broken LSP discovered fault scenario.

Table 3-7 Broken LSP Discovered Scenario

Impact and Affected Severity	Description
Impact calculation	Initiates an affected flow to determine all the affected parties using the LSP.
Reported affected severity	Only reports on Real Affected. When the Link Down alarm is cleared, all the correlated broken LSP alarms are auto-cleared.

MPLS TE Tunnel Down Scenario

Table 3-8 lists the impacted calculations and reported affected severities for an MPLS TE tunnel down fault scenario.

Table 3-8 MPLS TE Tunnel Down Scenario

Impact and Affected Severity	Description
Impact calculation	Initiates a flow to look for affected parties.
Reported affected severity	Only reports on real affected.

Pseudowire MPLS Tunnel Down Scenario

The following table lists the impacted calculations and reported affected severities for a pseudowire MPLS tunnel down fault scenario.

Table C-9 Pseudowire MPLS Tunnel Down

Impact and Affected Severity	Description
Impact calculation	Initiates a flow to look for the affected parties.
Reported affected severity	Only reports on real affected on the MPLS domain.

Managing Certificates

Managing Certificates chapter describes how to generate a Self-signed certificates and Certificate Signing Request (CSR) that can be used to obtain SSL certificates from a Certificate Authority such as Verisign, Digicert and so on. This chapter describes the following topics:

Generating Self-Signed Certificates and Certificate Signing Request

Generate a self-signed certificate and a Certificate Signing Request (CSR) by using the **Generate Self-Signed Certificate and Certificate Signing Request** option. When you generate a self-signed certificate, a new self-signed certificate in PEM format and a CSR file are created in the $ANAHOME/scripts/CSR/ directory. When you press enter in a command without specifying any value the script will select a default option automatically. For example, if you do not specify a domain name, the script by default picks the domain name as cisco.com.

Step 1 Execute $ANAHOME/local/scripts/selfsignedcert.pl.

Step 2 Choose **Generate Self-Signed Certificate and Certificate Signing Request(.csr)** and press **Enter**. The system prompts you to enter information as listed in the following table.

Table 33-1 Parameters and Description

Parameter	Description	Display Message
`Domain Name [cisco.com]:`	Enter the domain name. By default the script accepts cisco.com as domain name.	

`How many days is self-signed certificate valid for? [365]:`	Enter the number of days that you want the self-signed certificate to be valid for.	`writing new CSR (Certificate Signing Request) to /export/home/pn430/scripts/CSR/test.csr`
		`writing private key to /export/home/pn430/scripts/CSR/test.key`
		`Generating a 2048 bit RSA private key`
		`writing new private key to /export/home/pn430/local/scripts/cisco.com.key'`
		`You are about to be asked to enter information that will be incorporated into your certificate request.`
		`What you are about to enter is what is called a Distinguished Name or DN.`
		`There are quite a few fields but you can leave some blank.`
		`For some fields there will be a default value,`
		`If you enter '.', the field will be left blank.`

`Country Name (2 letter code) [GB]:`
`State or Province Name (full name) [Berkshire]:`
`Locality Name (eg, city) [Newbury]:`
	Enter the country name, state or province name and locality name,	

`Organization Name (eg, company) [My Company Ltd]:` `Organizational Unit Name (eg, section) []:`	Enter the organization name and Organizational unit name.	
`Common Name (eg, your name or your server's hostname) []:`	Enter the common name.	

Table 33-1 Parameters and Description

Parameter	Description	Display Message
`Email Address []:`	Enter the email address.	
`A challenge password []:` `An optional company name:`	(Optional) Enter a challenge password and an optional company name.	`CSR generated successfully (/export/home/pn430/scripts/CSR/cisco.com.csr)` `Use the CSR to obtain a certificate in PEM/CER format from a CA (Certificate Authority).` `New self-signed certificate in PEM format generated (/export/home/pn430/scripts/CSR/cisco.com.pem)`

Importing Certificate Authority or Self-Signed Certificate

Import a Certificate Authority (CA) signed certificate or self-signed certificate by using Import CA/Self-Signed Certificate option. You can either import the generated self-signed certificate or import a certificate generated by another system or third party by copying the .pem and .key (private key) files to the $ANAHOME/scripts/CSR directory. The .pem file provided is exported into PKCS12 format, and then converted to JKS format. The JKS file can be imported into Tomcat.

Step 1 Execute $ANAHOME/local/scripts/selfsignedcert.pl as PN user.

Step 2 Choose the **Import CA/Self-Signed Certificate** option and press **Enter**.

Step 3 Specify values for the following parameters and then press **Enter**:

Table 33-2 Parameters and Description

Parameters	Description
`Domain Name [cisco.com]:`	Enter the domain name.
`CA/self-signed certificate (.pem/.cer) file path:`	Enter the path to the CA signed certificate or self-signed certificate.
`private key file path:`	Enter the path to the private key.
`keystore password:`	Enter the Java KeyStore (JKS) password to set.
The following confirmation messages might appear, enter Yes or No to proceed further.	
`Existing certificate will be erased, wa.nt to proceed (Yes/No):`	Enter Yes to proceed or No to exit.
`Prime Network and Operation Report restart required applying certificate, do you want to restart (Yes/No):`	Enter Yes to proceed or No to exit. If you enter yes then a message similar to the following one appears: Restarting Prime Network and Operation Report.....Done Certificate $ANAHOME /scripts/CSR/cisco.com.pem imported to server successfully.

Generating System Events for a Close to Expire Digital Certificates

Prime Network generates system events when digital certificate of a Product's License expiry date is close to expiration.

The System Events are generated based on three scenarios and the following table lists the Severity for each scenarios.

Table 33-3 System Events Scenarios

Scenarios	No: of Systems Events Generated	Severity
License expires in a month	1	Minor
License expires in 14 days	1	Major
License expires in Thee days	1	Critical
License expiry is < = 0 days	1	Critical
License expiry > 30 days	1	Cleared

Also, Prime Network generates System Events for the Jars and Certificates that are about to expire.

Table 33-4 Certificates and the Impacted Applications

Certificate	Location	Impacted Application
JWS JARS	/export/home/pn51/Main/webstart/jars/jws	Prime Network GUI applications (Administrator, Events GUI, and Prime Network Vision)
XMP Platform	/export/home/pn51/XMP_Platform/conf/	Prime Network Web Server (Change and Configuration Management, VNE Customization Builder, and Network Discovery)
Pentaho	/export/home/pn51/pentaho/server/biserver-ee/tomcat/conf/	Operations Reports
Apache Server	/export/home/pn51/utils/linux/apache/conf/sheer.cert.cert	Prime Network Monitoring tool

Prime Network periodically checks (once a day) the expiration date, or on restart and forwards the system events for Digital certificates and JARS based on the following criteria.

- System Event with minor severity for Digital Certificates expiring in 30 days
- System Event with major severity for Digital Certificates expiring in 14 days
- System Event with critical severity for Digital Certificates expiring in 3 days
- System Event with critical severity for Digital Certificates expiring in 0 days
- System Event with cleared severity when the Digital Certificates is updated

Note Prime Network sends only one System Events for each severity. The cleared notification is initiated only when the Digital Certificate is reinstalled using a script.

Trouble Shooting

How can the Administrator obtain a new certificate or install them?

a. Administrator can generate the Digital certificate for Tomcat servers as a Self-Signed certificate or apply for/through third party Digital certificate using the scripts provided by Prime Network.

b. Digital certificate for GUI clients can be obtained only through Prime Network upgrade. You can obtain either during main release or Point Patch (PP).

– If you are upgrading Prime Network during Main release Digital certificate is automatically generated during installation of Prime Network.