Cisco Wide Area Application Services Monitoring Guide

Software Version 4.3.1
November 30, 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-23801-02

Cisco Wide Area Application Services Monitoring Guide

CONTENTS

Preface

This preface describes the audience, organization, and conventions of the *Cisco Wide Area Application Services Monitoring Guide*. It also provides information about how to obtain related information.

Audience

This publication is for experienced system and network administrators who have specific knowledge in the following areas:

- Networking and data communications
- Network security
- Router and switch configuration

Organization

This publication is organized as follows:

Chapter	Description
Chapter 1, "Monitoring WAAS Using WAAS Central Manager"	Describes how to use WAAS Central Manager to monitor your WAAS devices.
Chapter 2, "Monitoring Traffic Interception"	Describes different methods to monitor traffic interception.
Chapter 3, "Monitoring WAAS Using SNMP"	Describes how to use SNMP to monitor your WAAS devices.
Chapter 4, "Monitoring WAAS Using XML API"	Describes how to use WAAS XML API to monitor your WAAS devices.
Chapter 5, "Monitoring WAAS Using Cisco Network Analysis Module"	Describes how to use Cisco Network Analysis to monitor your WAAS devices.

Related Documentation

For additional information on the Cisco WAAS software, see the following documentation:

- *Release Note for Cisco Wide Area Application Services*
- *Cisco Wide Area Application Services Quick Configuration Guide*
- *Cisco Wide Area Application Services Configuration Guide*
- *Cisco Wide Area Application Services Command Reference*
- *Cisco Wide Area Application Services API Reference*
- *Cisco Wide Area Application Services Upgrade Guide*
- *Cisco WAAS Installation and Configuration Guide for Windows on a Virtual Blade*
- *Cisco WAAS Troubleshooting Guide for Release 4.1.3 and Later*
- *Cisco WAAS on Service Modules for Cisco Access Routers*
- *Cisco SRE Service Module Configuration and Installation Guide*
- *Configuring Cisco WAAS Network Modules for Cisco Access Routers*
- *WAAS Enhanced Network Modules*
- *Cisco Wide Area Application Services Online Help*
- *Using the Print Utilities to Troubleshoot and Fix Samba Driver Installation Problems*
- *Regulatory Compliance and Safety Information for the Cisco Wide Area Virtualization Engines*
- *Cisco Wide Area Virtualization Engine 274 and 474 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 574 Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*
- *Cisco Wide Area Application Engine 512 and 612 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7326 Hardware Installation Guide*

- *Cisco Wide Area Application Engine 7341, 7371, and 674 Hardware Installation Guide*
- *Installing the Cisco WAE Inline Network Adapter*
- *Using Cisco NAM 4.1 Reporting with Cisco WAAS*
- *Cisco Wide Area Application Services vWAAS Installation and Configuration Guide*

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** font
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font
Selecting a menu item in paragraphs	**Option > Network Preferences**
Selecting a menu item in tables	Option > Network Preferences

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Obtaining Documentation and Submitting a Service Request

For information about obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Monitoring WAAS Using WAAS Central Manager

This chapter describes how to use WAAS Central Manager to monitor network health, device health, and traffic interception of the WAAS environment.

This chapter contains the following sections:

For more information about using WAAS Central Manager, see the "Monitoring and Troubleshooting Your WAAS Network" chapter in the Cisco Wide Area Application Services Configuration Guide.

Monitoring WAAS Network Health

This section describes how to use WAAS Central Manager to monitor the health of the WAAS environment. From a secure web browser, log in to WAAS Central Manager using either its hostname or IP address on port 8443 as follows:

https://*CM-Host-Name_or_IP Address*:8443

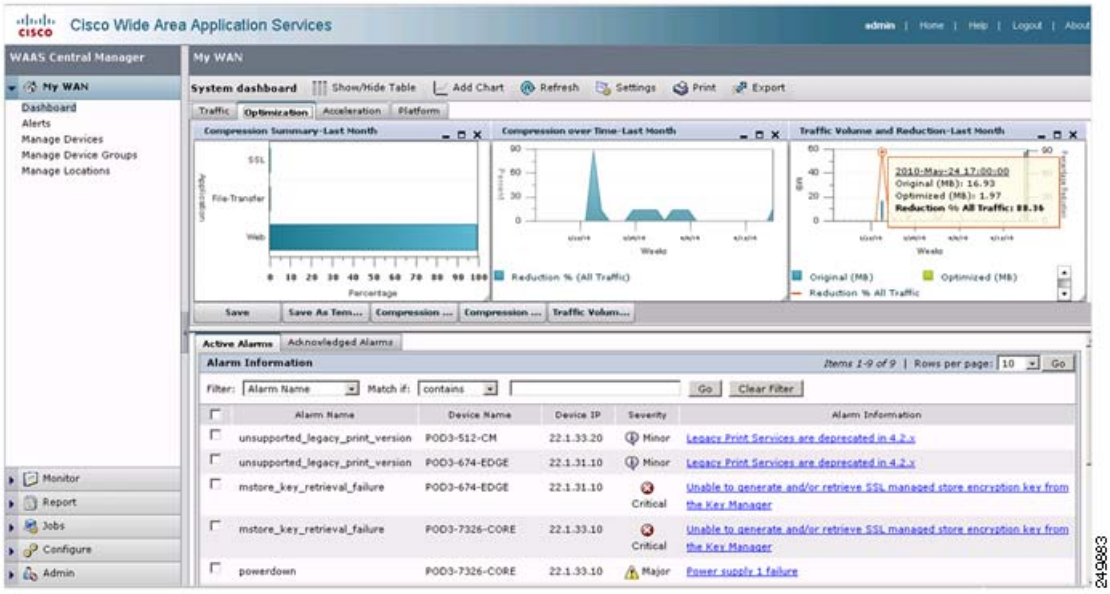
You must have proper username and password credentials to log in to WAAS Central Manager.

This section contains the following topics:

Using the WAAS Dashboard

You can view general and detailed information about your WAAS network by choosing My WAN > Dashboard. The System Dashboard window appears, which by default displays the Optimization tab (see Figure 1-1).

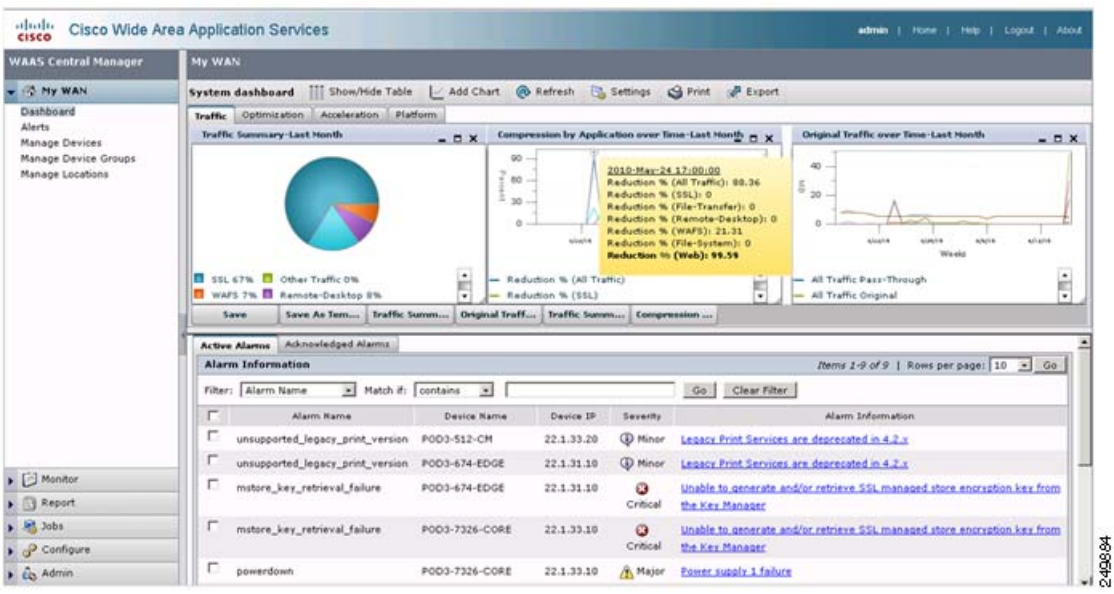
Figure 1-1 WAAS Central Manager: Dashboard Optimization Tab



The charts provide a snapshot of overall WAAS network health. Various reporting options are available from each tab. You can select charts and customize them for a specific time frame. Navigating over a chart or a cross point on a chart displays additional useful information.

Figure 1-2 shows a sample of the traffic dashboard which you can view by clicking the Traffic tab.

Figure 1-2 WAAS Central Manager: Dashboard Traffic Tab



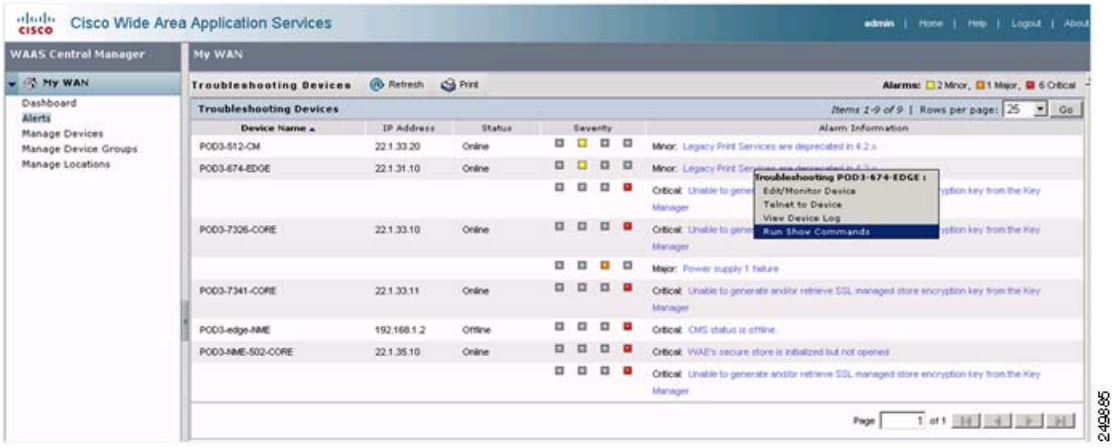
The dashboard also displays any network-wide alarms that may be present. Additional information is provided when you navigate to the alarm hyperlink or simply click it. From the Active Alarms tab, you can acknowledge alarms, which are then moved to the Acknowledged Alarms tab.

The alarms are classified as Critical, Major, or Minor depending on the impact the issue might have upon the WAAS environment. You can use the filter option to display alarms by severity, device IP address or name, and so forth. Filter match criteria is case sensitive.

Viewing Alarms

You can view alarms by choosing My WAN > Alerts. The Troubleshooting Devices window appears (see Figure 1-3).

Figure 1-3 WAAS Central Manager: Troubleshooting Devices



The screen provides a good overall view of outstanding alarms where you can take an action or acknowledge the alarms per device.

Common Alarms include:

Alarm 17001 (join_timeout) WCCP service join timeout.

Severity: Major

Category: Communications

Description: The device cannot join the WCCP service group within 10 minutes. Traffic redirection to the WAE cannot occur until the WAE can join.

Action: Restart the WCCP configuration by disabling WCCP on all the WAEs in the farm that present this alarm, waiting 5 minutes, and then reenabling WCCP on these WAEs.

Alarm 17002 (rtr_unreachable) WCCP Router Unreachable Alarm.

Severity: Major

Category: Communications

Description: The device cannot receive ISUs from the router for more than 30 seconds. Network connectivity between the router and WAE is down or the WCCP configuration on the WAE is not consistent with that of the router. This situation results in a failure to join the router in the WCCP farm.

Action: Check the configuration on the router and the WAE that raised the alarm. Check connectivity between the WAE and the router for which the alarm is raised.

Alarm 17003 (rtr_unusable) WCCP Router Unusable Alarm.

Severity: Minor

Category: Communications

Description: The device cannot join the WCCP farm due to mismatching capabilities. The assignment method, redirect method, or return method are not matching with the capability offered by the router.

Action: Check and modify the capability configuration on the WAE or the router to match the capability supported in the farm.

Alarm 17004 (missing_assignment) WCCP Missing Assignment alarm.

Severity: Major

Category: Communications

Description: The device has joined the WCCP farm but does not have any assignments. Traffic redirection to the device does not occur. The possible reasons for this to happen could be: 1) if using mask assignment, the mask value of the device is not consistent with the rest of the farm; 2) the device lost all assignments to other devices with higher weights in the farm; or 3) the device cannot communicate to all routers in the farm and thus is not given any assignments. The alarm is raised if the WAE does not acquire assignments within three minutes after a change in the farm.

Action: Check configuration and connectivity to all routers and take corrective action as needed.

Alarm 17005 (mask_mismatch) Configured mask mismatch for WCCP.

Severity: Major

Category: Communications

Description: The device cannot join the WCCP farm because its configured mask does not match the operational mask of the farm. Traffic redirection to the WAE cannot occur until the WAE can join.

Action: Check the WCCP mask configuration on all WAEs to ensure that they are configured with the same mask.

Alarm 330001 (svcdisabled) -service name- service has been disabled.

Severity: Critical

Category: Processing

Description: The node manager tried restarting the specified service but the service kept restarting. The number of restarts has exceeded an internal limit and the service has been disabled.

Action: The device may have to be reloaded for the service to be reenabled.

Alarm 330002 (servicedead) -service name- service failed.

Severity: Critical

Category: Processing

Description: A critical service has failed. Attempts will be made to restart this service but the device may run in a degraded state.

Action: The device could reboot itself to avoid instability. Examine the syslog for messages relating to cause of service failure.

Alarm 335000 (alarm_overload) Alarm Overload State has been entered.

Severity: Critical

Category: Quality of service

Description: The Node Health Manager issues this to indicate that the device is raising alarms at a rate that exceeds the overload threshold.

Action: Access the device and determine what services are raising the alarms. Take corrective action to resolve the issues with the individual services.

Alarm 335001 (keepalive) Keepalive failure for -application name-. Timeout = n seconds.

Severity: Critical

Category: Quality of service

Description: The Node Health Manager issues this message to indicate that an application has not issued a keepalive to the Node Health Manager for the last *n* seconds. The application's health is in question.

Action: Access the device and determine what state the specific application is in. Take corrective action to resolve the issues that are keeping the application from running properly.

Alarm 445000 (disk_failure) A disk has failed.

Severity: Critical

Category: Equipment

Description: The System Monitor issues this message to indicate that one of the disks attached to a device has a severe error.

Action: Access the device and execute the **show disk details** CLI command. If the problem persists, replace the disk.

Alarm 445001 (core_dump) A user core file has been generated.

Severity: Major

Category: Processing

Description: The System Monitor issues this to indicate that one or more of the software modules has generated a core file.

Action: Access the device, check the directory /local1/core_dir, retrieve the core file through FTP, and contact Cisco TAC.

Alarm 445013 (powerdown) Power supply is down.

Severity: Major

Category: Processing

Description: The System Monitor indicates that one of the power supplies is down.

Action: Check the power supplies.

Alarm 445019 (license_failure) WAAS product license is missing.

Severity: Critical

Category: Processing

Description: The System Monitor indicates that either the WAAS product license has not been purchased or the License Management system has not been configured.

Action: Execute the **show license** CLI command to verify that the License Management system has been configured. Purchase the WAAS product license and configure the License Management system with the **license add** command.

Alarm 445022 (eth_detection_failed) Detection of one of the network interfaces has failed.

Severity: Critical

Category: Equipment

Description: The System Monitor indicates that the system networking hardware has a severe error. Interfaces and related features will not work properly.

Action: Reboot the device. If the alarm does not clear, reset the BIOS settings to the defaults before rebooting again. If the alarm does not clear, contact Cisco TAC.

Alarm 700002 (cms_clock_alarm) Device clock is not synchronized with the primary CM.

Severity: Major

Category: Environment

Description: If this device is a WAE, its clock needs to be synchronized with the primary WAAS Central Manager to make time-sensitive features like statistics, status monitoring, and event scheduling work correctly. If this device is a standby WAAS Central Manager, its clock needs to be synchronized with the primary WAAS Central Manager to make the WAAS Central Manager failover work.

Alarm 700006 (cms_wae_secure_store) Secure Store is initialized but not opened.

Severity: Critical

Category: Environment

Description: The WAE's secure store is initialized but not opened by the user. The WAE will reject updates from WAAS Central Manager if they contain updates to preposition, dynamic share, and WAFS core password and user configuration until the secure store is opened.

Action: Open secure store using the **cms secure-store open** CLI command or by entering the password in the WAAS Central Manager GUI.

Alarm 700008 (mstore_key_retrieval_failure) CMS/Management agent failed to generate and/or retrieve SSL managed store encryption key from Key Manager.

Severity: Critical

Category: Processing

Description: This alarm indicates one of following issues:

- The WAAS Central Manager device is not reachable
- Secure store on WAAS Central Manager is initialized but not open
- The Key Manager process on the WAAS Central Manager device is not running or failing to respond
- Key Manager cannot process key generation or retrieval request. If this issue is present, the WAAS device cannot process a configuration update received from WAAS Central Manager if it contains SSL certificate and key pair information.

Action: Check to see if the WAAS Central Manager device is reachable (TCP connections from the WAE to the WAAS Central Manager on port 443). Check the following log files for additional information about the error:

- On WAE: /local1/errorlog/kc.log on WAE
- On WAAS Central Manager: /local1/errorlog/km/km.log

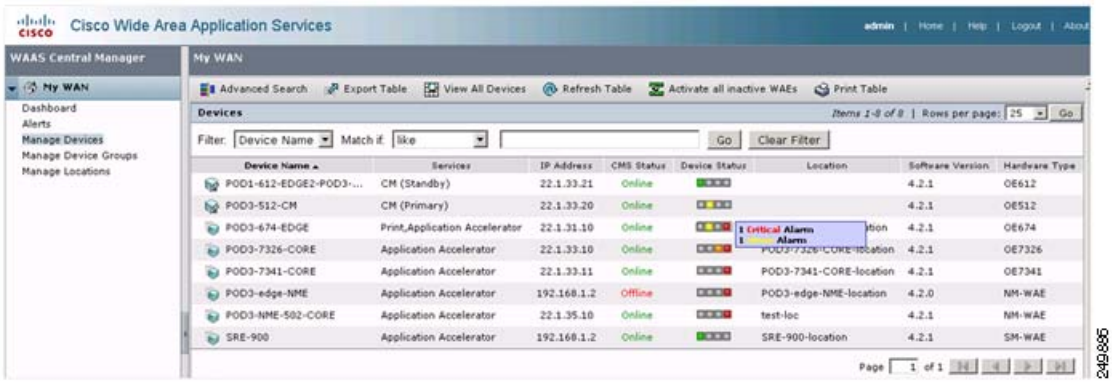
Action: Fix the clock on the device or the primary WAAS Central Manager.

For a complete list of alarm conditions, see the *Alarm Book* located in the WAAS 4.2.1 Software Download area on Cisco.com.

Viewing WAE Device Status

The Cisco WAAS Central Manager devices page provides a quick status overview of each Cisco WAE deployed throughout the network that is registered against that particular WAAS Central Manager. You can manage devices by choosing My WAN > Manage Devices. The Devices window appears (see Figure 1-4).

Figure 1-4 WAAS Central Manager: Manage Devices



Each device reports a CMS Status of either online or offline, which alerts the administrator to the state of the Cisco WAE at that time. If the Central Management System (CMS) service is disabled or network connectivity is unavailable to that particular Cisco WAE, it is reported as offline. WAAS Central Manager cannot synchronize configuration data with an offline Cisco WAE and cannot fetch new reporting data.

If a device shows up as offline, confirm the status by using telnet or SSH to access the device and entering the **show cms info** command. In addition, you should use commands such as **show stat connection** to verify that the device is participating in traffic optimization.

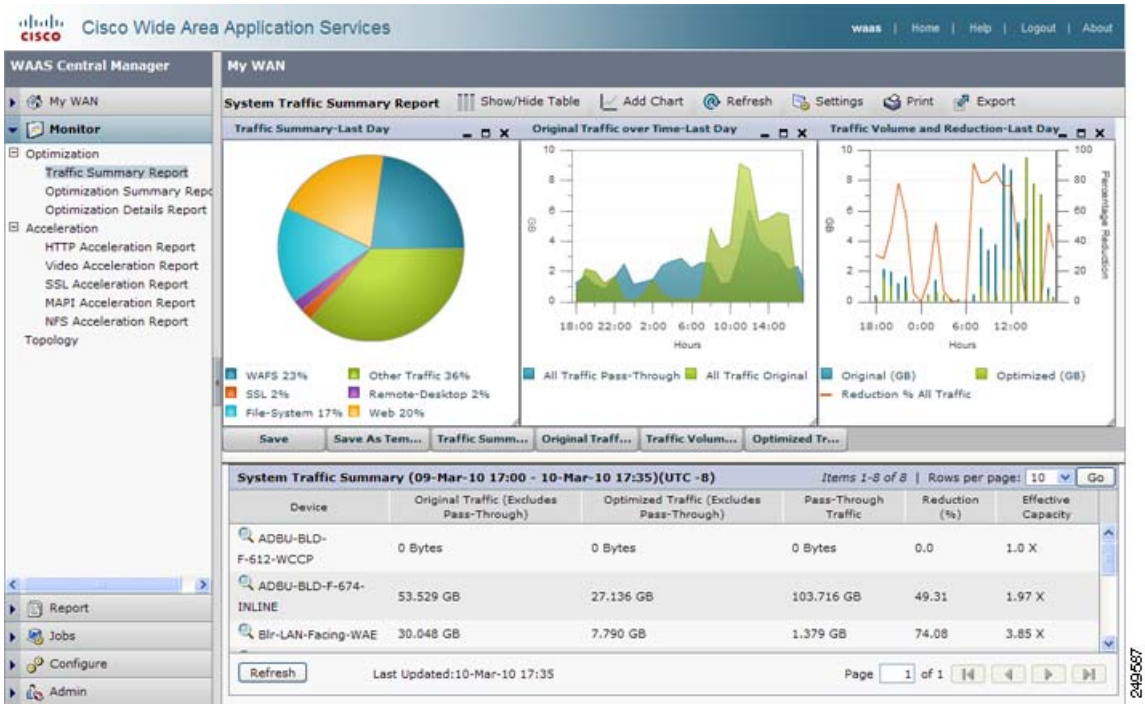
The Devices window also presents some key information such as device name, service mode, IP address, software version, and so forth. Ideally, all the WAEs in the WAAS network should be running the same OS version. At a minimum, the primary WAAS Central Manager and secondary WAAS Central Manager (if there is one) should be on the same version.

Device health is indicated by the device status highlighting any outstanding alarms. You can navigate to the device by clicking on the device icon. For large deployments, use the Filter option to display devices by device name, service mode, and status.

Monitoring Optimization

You can access system-wide traffic statistics by choosing My WAN > Monitor > Optimization > Traffic Summary Report. The System Traffic Summary Report window appears (see Figure 1-5).

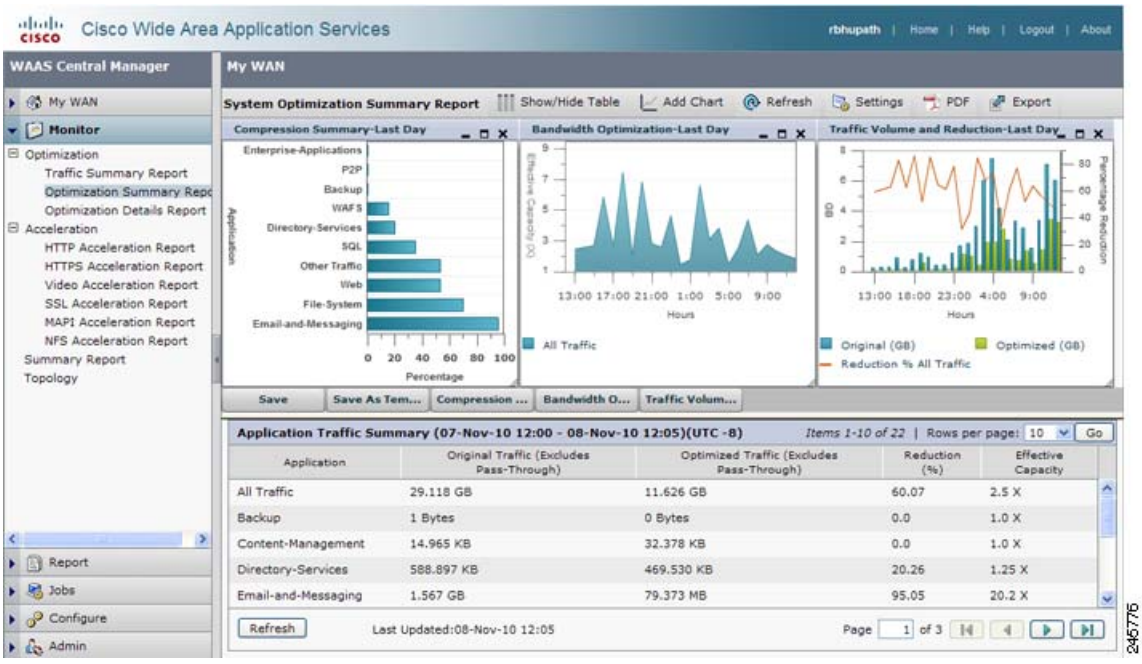
Figure 1-5 WAAS Central Manager: System Traffic Summary Report



Several reporting options are available for both optimization and protocol specific application accelerator acceleration reporting. The System Traffic Summary table provides device-level optimization statistics that are useful to determine if the WAAS devices are configured properly for optimal traffic acceleration.

You can access system-wide optimization statistics by choosing My WAN > Monitor > Optimization > Optimization Summary Report. The System Optimization Summary Report window appears (see Figure 1-6).

Figure 1-6 Optimization Summary Report



The System Optimization report provides application level optimization reports, highlighting reduction and effective capacity. You can use this data to modify policies and adjust optimization options.

The Acceleration reports provide device-level application accelerator specific statistics.

Monitoring System Operation

You can monitor the system operation by choosing My WAN > Monitor > Summary Report. The Summary Report displays.

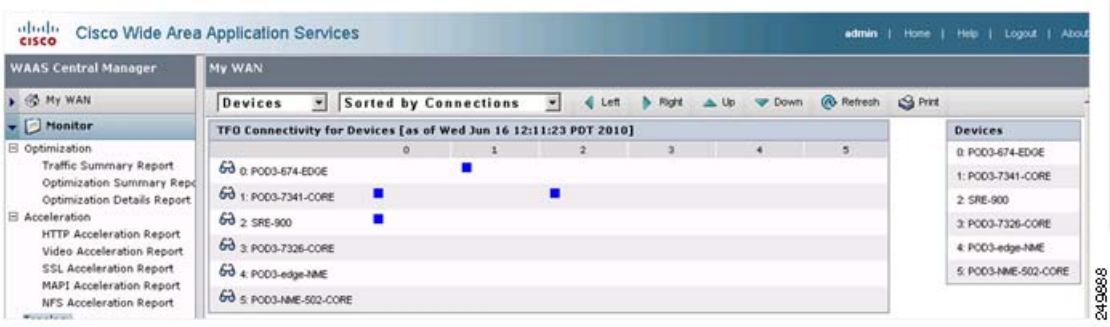
Figure 1-7 Summary Report

The Summary report is a predefined report that can be used to monitor the system operation. The Summary Report can be customized to display the charts that you require. Use the Add Chart option to select the charts that you want to be displayed on this report. Only 12 charts can be displayed in the report. You can customize any of the chart settings by using the Settings option.

Monitoring Topology

You view peering relationships by choosing My WAN > Monitor > Topology. The TFO Connectivity for Devices window appears (see Figure 1-8). A bidirectional relationship is required for any optimization between the peers.

Figure 1-8 WAAS Central Manager: TFO Connectivity for Devices

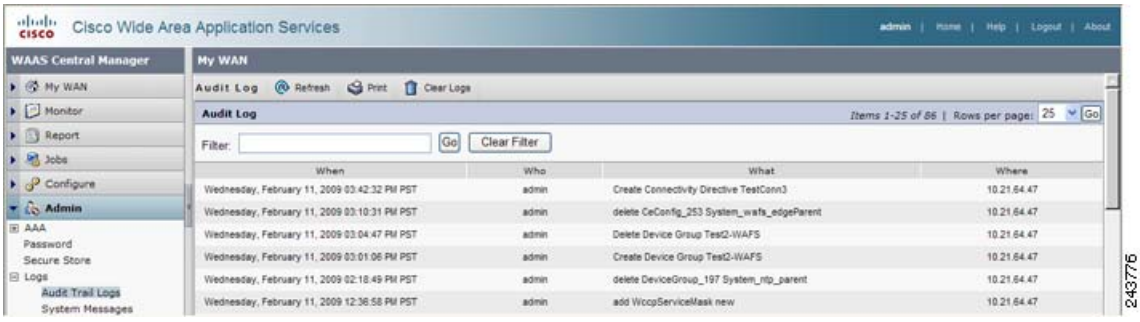


The topology information is important for troubleshooting and for deployment sizing exercises, especially for large deployments where any site-to-site communication is required.

Monitoring Audit Trail Logs, System Messages, and WAAS Central Manager Logs

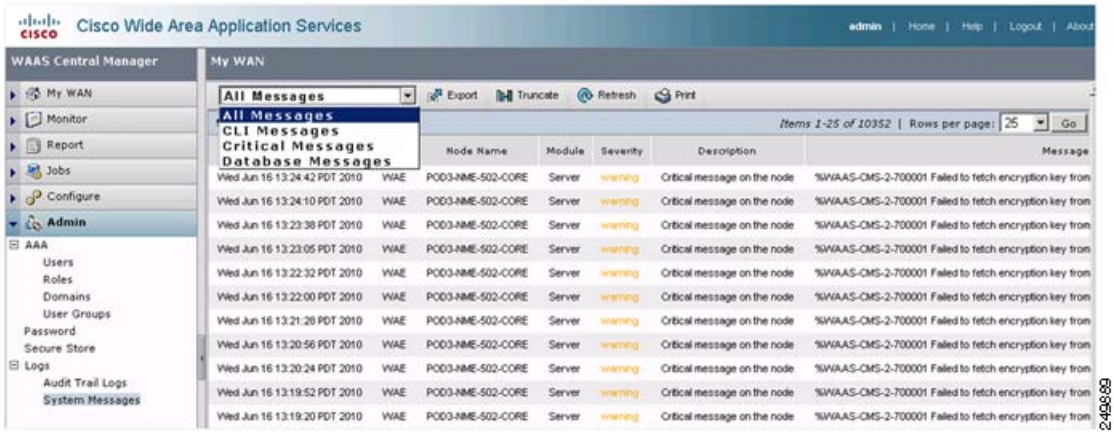
You can view the Audit Trail Logs to track the last actions performed by a particular user that you created using the WAAS Central Manager GUI, which can be used to centrally create and manage two different types of administrator user accounts (device-based CLI accounts and roles-based accounts) for your WAAS devices. To view the Audit Trail Logs, choose My WAN > Admin > Logs > Audit Trail Logs. The Audit Trail Logs window appears (see Figure 1-9).

Figure 1-9 WAAS Central Manager: Audit Trail Logs



You can view system wide-system logs by choosing My WAN > Admin > Logs > System Messages. The System Messages window appears (see Figure 1-10). You can choose the system messages to view CLI, critical, or database messages.

Figure 1-10 WAAS Central Manager: System Messages



For a complete list of available errors, see the *Error Message Book* in the WAAS 4.2.1 Software Download area on Cisco.com.

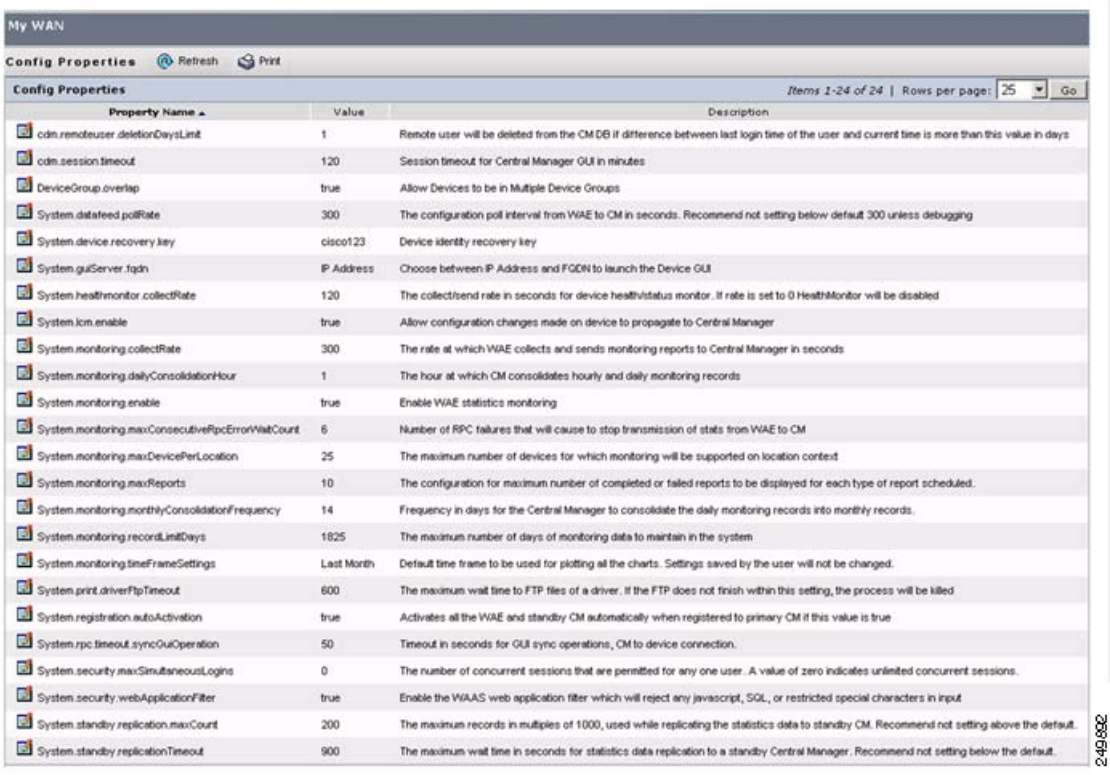
You can view the WAAS Central Manager logs by choosing My WAN > Devices > WAAS-CM > Admin > Logs. The System Messages Log window appears (see Figure 1-11).

Figure 1-11 Figure 8: WAAS Central Manager: System Messages Log

Viewing System Properties

You can view and modify the current system properties by choosing My WAN > Configure > System Properties. The Config Properties window appears (see Figure 1-12). From this window, you can modify the preconfigured system properties to alter the default behavior of the system. For more information, see the *Cisco Wide Area Application Services Configuration Guide* chapter on "Configuring Other System Settings."

Figure 1-12 WAAS Central Manager: System Properties



Monitoring WAAS Device Health

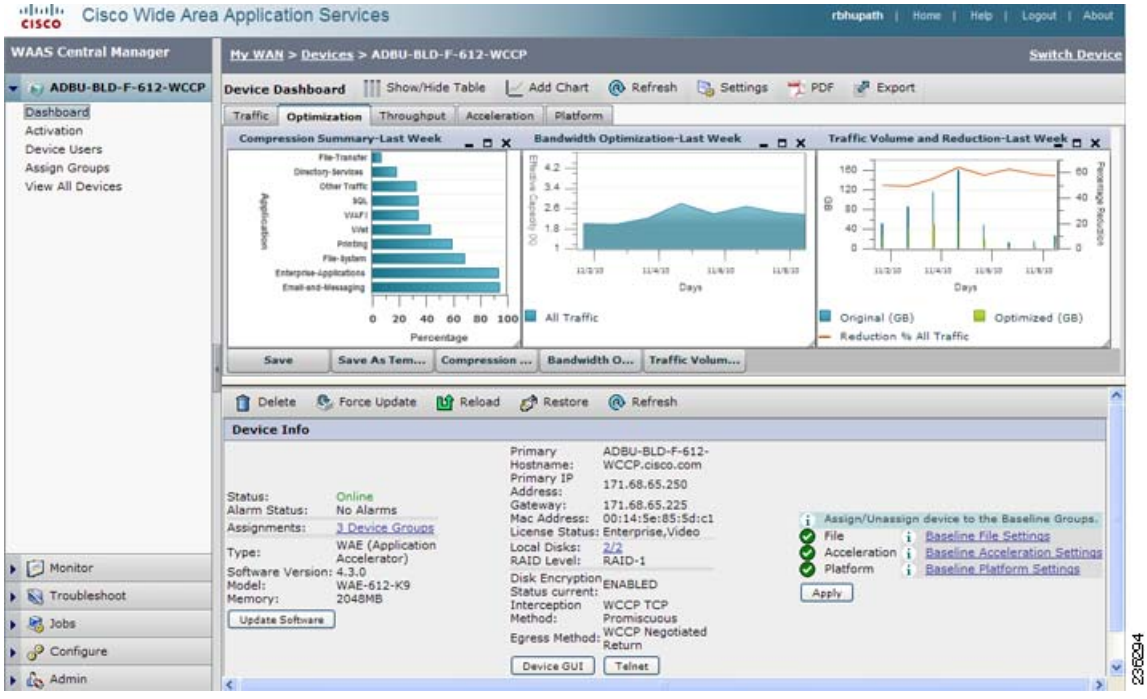
You can use WAAS Central Manager to monitor and configure all devices in the WAAS network. WAAS Central Manager provides detailed information about a WAAS device configuration, device hardware statistics, and traffic optimization reports.

This section contains the following topics:

Viewing the Device Dashboard

You can manage devices individually by choosing My WAN > Devices > *Device_Name*. The Device Dashboard window appears (see Figure 1-13).

Figure 1-13 WAAS Central Manager: Device Dashboard

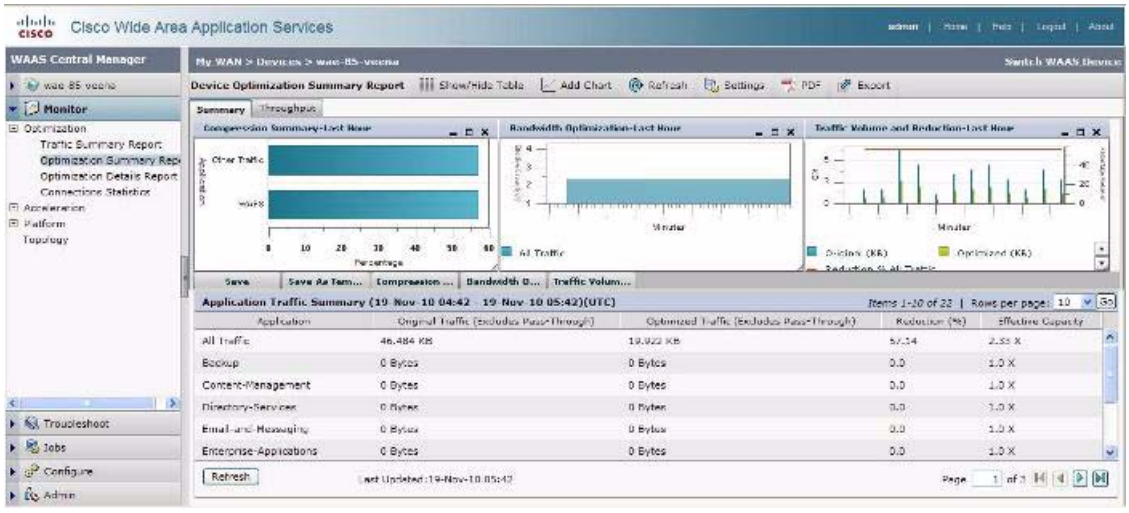


The Device Dashboard provides an overview of the device, such as the WAAS hardware and software, and the configured interception mechanism. You can customize the charts and save the custom settings. You can also access the device GUI or telnet to the device.

Viewing Optimization Reports

You can view optimization reports by choosing My WAN > Devices > *Device_Name* > Monitor > Optimization > Optimization Summary Report. The Device Optimization Summary Report window appears (see Figure 1-14).

Figure 1-14 WAAS Central Manager: Device Optimization Summary Report



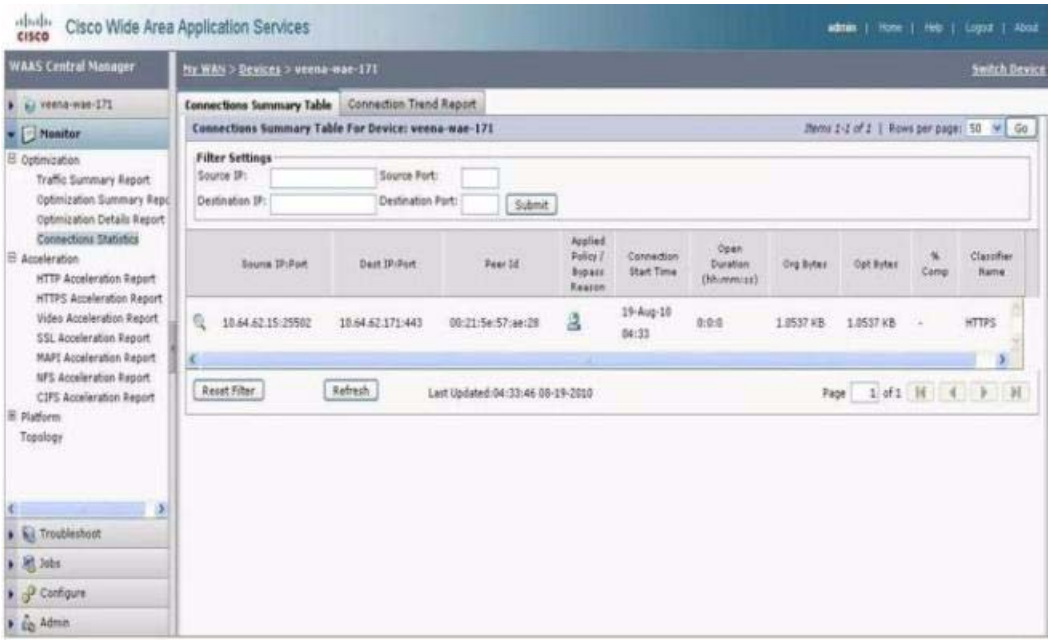
This report includes Summary and Throughput reports. These are optimization reports that provide traffic optimization statistics for predefined applications and insight into which applications are getting the most optimization and which ones may need additional fine tuning.

For more information about optimization reports, see the "Monitoring and Troubleshooting Your WAAS Network" chapter in the Cisco Wide Area Application Services Configuration Guide.

Viewing Connection Statistics

You can view per-connection statistics by choosing My WAN > Devices > *Device_Name* > Monitor > Optimization > Connection Statistics. The Connection Statistics report displays the device's Connections Summary Table (see Figure 1-15) and a Connection Trend Report (see Figure 1-15).

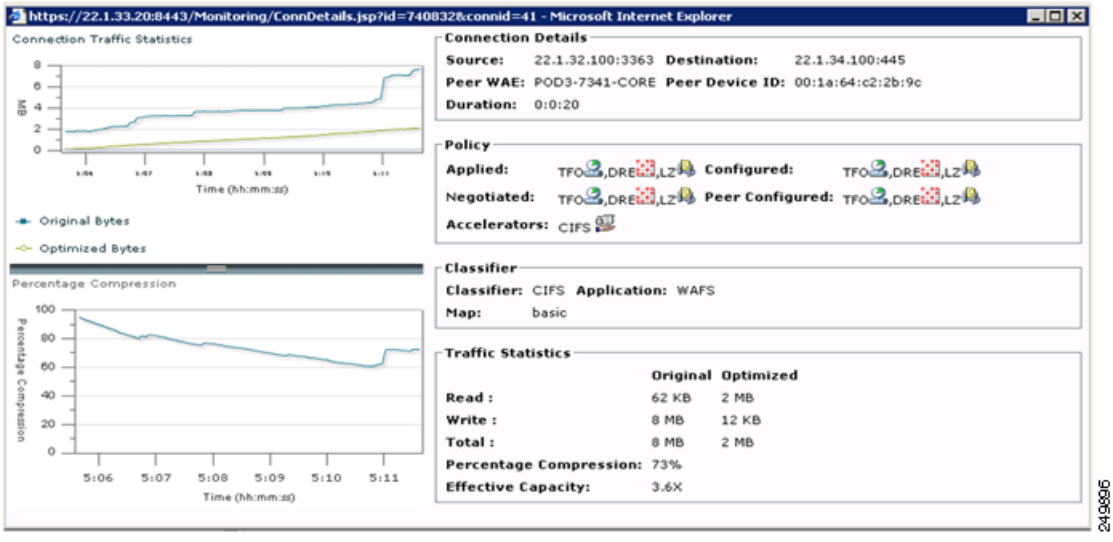
Figure 1-15 WAAS Central Manager: Connections Summary Table



The Connections Summary Table lists all the active flows served by the selected WAE. The output provides key details about the flow by highlighting type of traffic, peer ID, percent compression, applied policies, and so forth.

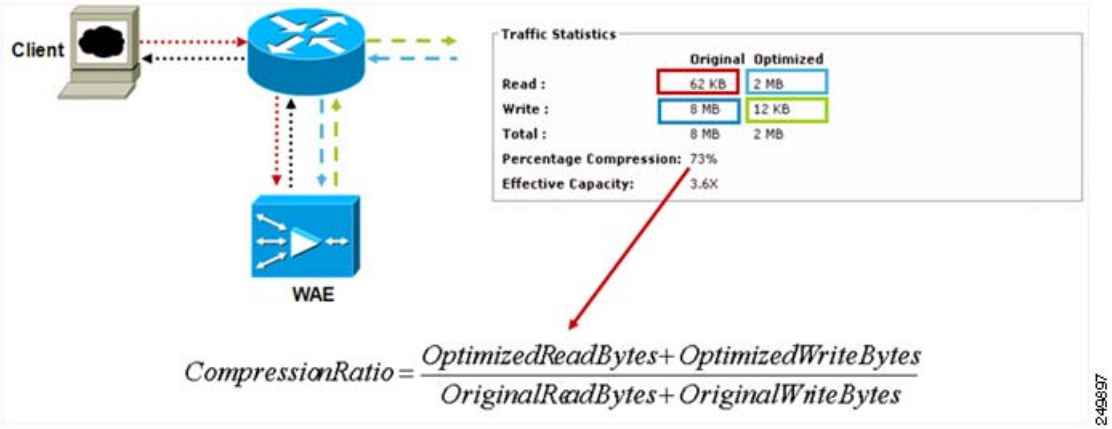
To view additional details per flow, click the magnifying glass icon. The flow details pop-up window opens, which provides connection statistics over time that can be used for troubleshooting or reporting (see Figure 1-16). This pop-up window updates automatically.

Figure 1-16 WAAS Central Manager: Flow Details Pop-Up Window



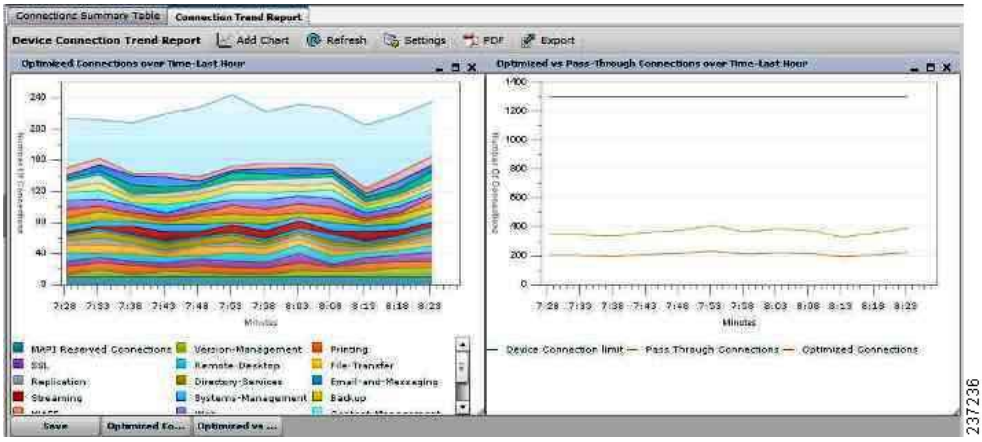
The traffic statistics provides compression ratios, effective capacity, and byte values for the original and optimized sockets. Figure 1-17 illustrates how to interpret the displayed data.

Figure 1-17 Interpreting Traffic Statistics



The Connection Trend Report provides data on the optimized and pass through connections of all the traffic processed on the device. You can use this data to monitor the connection trends of all the applications on the device.

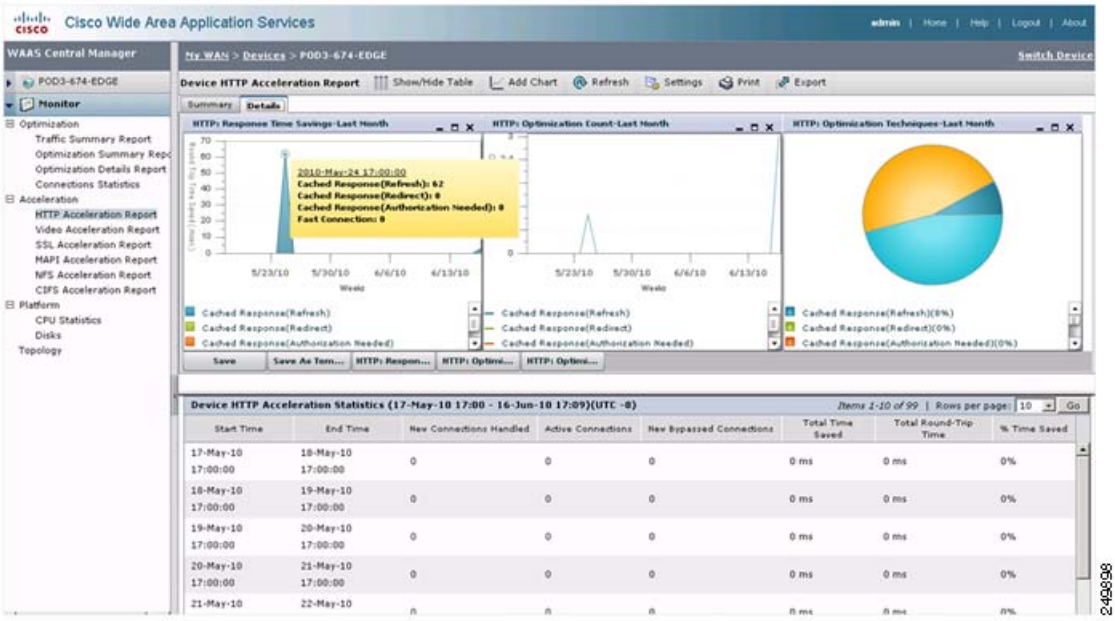
Figure 1-18 Connection Trend Report



Viewing Accelerations Reports

You can view acceleration reports for any application optimizer by choosing My WAN > Devices > *Device_Name* > Monitor > Acceleration > HTTP Acceleration Report. The Device HTTP Acceleration Report window appears (see Figure 1-19).

Figure 1-19 WAAS Central Manager: Device HTTP Acceleration Report



Viewing CPU Statistics

You can view WAAS device CPU utilization by choosing My WAN > Devices > *Device_Name* > Monitor > Platform > CPU Statistics. The CPU Usage window appears (see Figure 1-20).

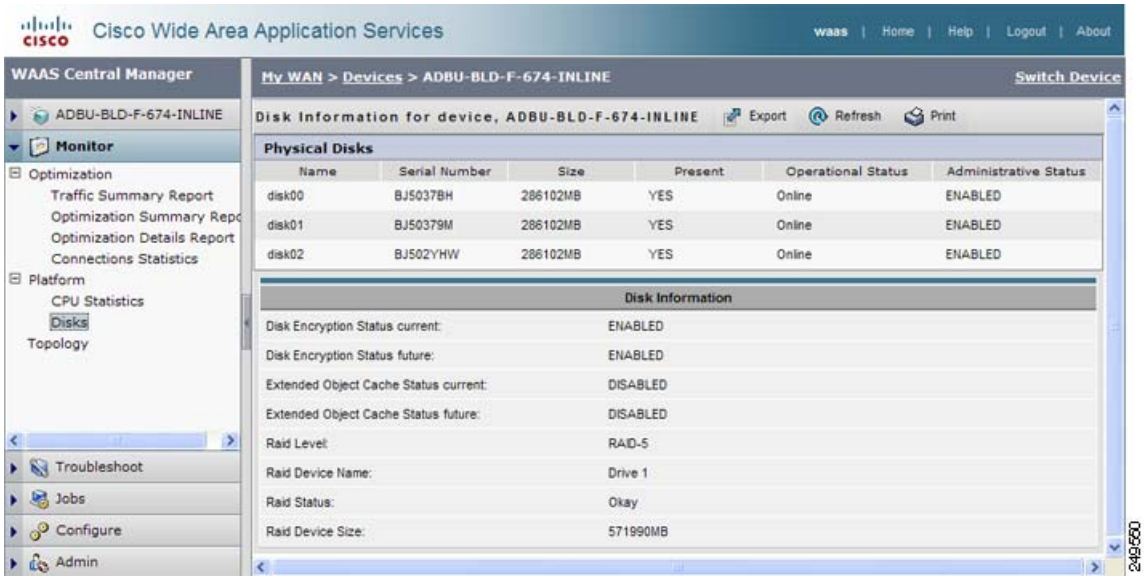
Figure 1-20 WAAS Central Manager: CPU Usage

For a more complete view, change the CPU graph time length to a week or month. High CPU usage does not necessarily mean that there is an issue; it should be looked at in combination with other statistics to rule out any degradation in optimization. Other factors to consider include degradation in optimization or low compression, and so forth.

Viewing Disk Health and Status

You can check the disk status for an individual WAE by choosing My WAN > Devices > *Device_Name* > Monitor > Platform > Disk. The device Disk Information window appears (see Figure 1-21).

Figure 1-21 WAAS Central Manager: Disk Information



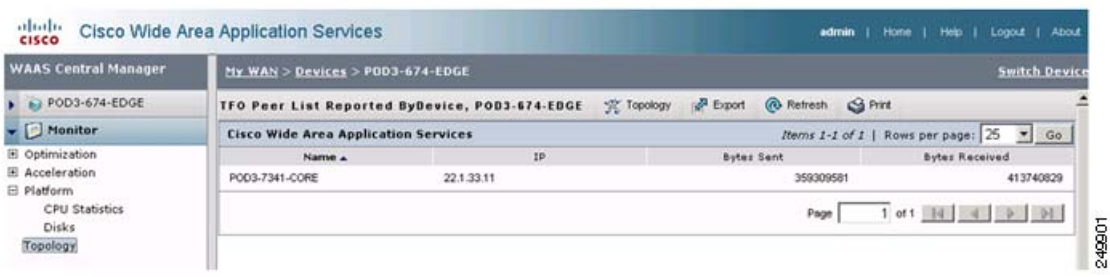
The operational status can be Online, Defunct, Missing, <null>, or Rebuilding. Under normal working conditions, the operation status should be Online. The Rebuilding status indicates that the RAID pairing is in progress and should clear after a while (depending on disk size and hardware platform of the WAE).

The view also displays disk size, RAID, disk encryption, and extended CIFS cache feature status.

Viewing Device Peering Status

You can view the device peering status at any given time to validate the traffic flows and optimal acceleration for these traffic flows by choosing My WAN > Devices > *Device_Name* > Monitor > Topology. The device TFO Peer List window appears (see Figure 1-22).

Figure 1-22 WAAS Central Manager: TFO Peer List



The peer list provides details about data sent and received for each peer. Branch site WAEs should have higher received numbers because all the traffic should be flowing from the data center towards the branch sites.

To view the overall topology, click the Topology icon.

Viewing Device Logs

You can view the device logs by choosing My WAN > Devices > *Device_Name* > Admin > Logs. The System Message Log window appears (see Figure 1-23).

Figure 1-23 WAAS Central Manager: System Message Log

Running CLI Commands from the WAAS Central Manager GUI

You can run various CLI **show** commands to display additional useful information by choosing My WAN > Devices > *Device_Name* > Troubleshoot > CLI Commands > Show Commands. The Show Commands for WAAS window appears (see Figure 1-24).

Figure 1-24 WAAS Show Commands

To display a command output, from the command drop-down list, select the **show** command and specify any optional command arguments. The output displays in a pop-up window. The sections that follow describe the output of some of the **show** commands. For details about the command options and output, see the *Cisco Wide Area Application Services Command Reference*.

This section contains the following topics:

show cms info Command Output

The **show cms info** command output provides the WAE registration information along with the last configuration synchronization time with WAAS Central Manager, which is useful when you suspect an application policy configuration issue (see Figure 1-25).

Figure 1-25 Command Output: show cms info

Output of command - *show cms info*

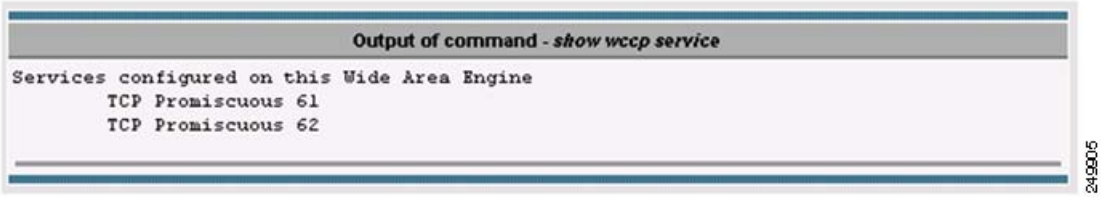
```
Device registration information :
Device Id                           = 740832
Device registered as                = WAAS Application Engine
Current WAAS Central Manager        = 22.1.33.20
Registered with WAAS Central Manager = 22.1.33.20
Status                              = Online
Time of last config-sync            = Wed Jun 16 21:27:45 2010

CMS services information :
Service cms_ce is running
```

249004

show wccp service Command Output

The **show wccp service** command output indicates if the WAE is configured for service groups 61 and 62 (see Figure 1-26).

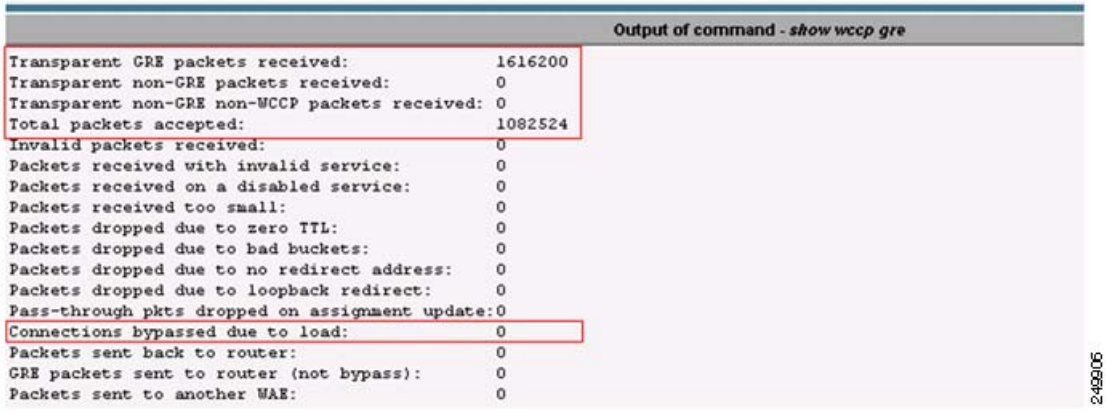
Figure 1-26 Command Output: show wccp service



show wccp gre Command Output

The **show wccp gre** command output includes three packets received counters, one of which should be incrementing to indicate that the WAE is receiving redirected packets (see Figure 1-27).

Figure 1-27 Command Output: show wccp gre



If the device is under heavy load and no new flows can be optimized, the Bypass Due to Load counter increments. A non-zero value for this counter indicates that the device is under overload or has gone in overload and should be further investigated.

show statistics connection Command Output

The **show statistics connection** command output displays the current optimized, auto-discovery, pass-through, and reserved flows (see Figure 1-28). The reduction ratio also displays for each active connection.

Figure 1-28 Command Output: show statistics connection

```
Output of command - show statistics conn
Current Active Optimized Flows:                        3
   Current Active Optimized TCP Plus Flows:            1
   Current Active Optimized TCP Only Flows:            1
   Current Active Optimized TCP Preposition Flows:     0
Current Active Auto-Discovery Flows:                   0
Current Reserved Flows:                                15
Current Active Pass-Through Flows:                     0
Historical Flows:                                      28


D:DRE,L:LZ,T:TCP Optimization RR:Total Reduction Ratio
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO

ConnID         Source IP:Port          Dest IP:Port            PeerID Accel RR
     1      22.1.34.100:42300      22.1.32.100:3389 00:1a:64:c2:2b:9c T     00.0%
     2      22.1.34.100:42308      22.1.31.10:50139 00:1a:64:c2:2b:9c TDL   48.4%
    11       22.1.32.100:4009       22.1.34.100:445 00:1a:64:c2:2b:9c TCDL  12.4%
```

249907

To view additional details for each flow, include the optional **conn-id** argument as follows:

show statistics connection conn-id *conn-id-number*

show statistics connection optimized cifs Command Output

The **show statistics connection optimized cifs** command output displays the connection optimized by the CIFS application accelerator (see Figure 1-29).

Figure 1-29 Command Output: show statistics connection optimized cifs

```
Output of command - show statistics connection opt cifs
Current Active Optimized Flows:                        3
   Current Active Optimized TCP Plus Flows:            1
   Current Active Optimized TCP Only Flows:            1
   Current Active Optimized TCP Preposition Flows:     0
Current Active Auto-Discovery Flows:                   0
Current Reserved Flows:                                15
Current Active Pass-Through Flows:                     0
Historical Flows:                                      28


D:DRE,L:LZ,T:TCP Optimization RR:Total Reduction Ratio
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO

ConnID         Source IP:Port          Dest IP:Port            PeerID Accel RR
    11       22.1.32.100:4009       22.1.34.100:445 00:1a:64:c2:2b:9c TCDL  12.3%
```

249908

show statistics accelerator cifs detail Command Output

The **show statistics accelerator cifs detail** command output displays statistics for the CIFS application accelerator, which is useful when troubleshooting connections handled by the CIFS application accelerator (see Figure 1-30).

Figure 1-30 Command Output: show statistics accelerator cifs detail

Output of command - *show statistics accelerator cifs det*

```
CIFS:
   Global Statistics
   -----------------
   Time Accelerator was started:                                    Sat Jun  5 05:48:47 2010
   Time Statistics were Last Reset/Cleared:                         Sat Jun  5 05:48:47 2010
   Total Handled Connections:                                       7
   Total Optimized Connections:                                     3
   Total Connections Handed-off with Compression Policies Unchanged: 0
   Total Dropped Connections:                                       0
   Current Active Connections:                                      1
   Current Pending Connections:                                     0
   Maximum Active Connections:                                      3
   Number of local reply generating requests:                       9716
   Number of remote reply generating requests:                      7930
   The Average time to generate a local reply (msec):               3
   Average time to receive remote reply (ms):                       10503
```

249909

The output highlights current active flows and historic flows handled by the application accelerator. Depending on the application accelerator, additional information is available that indicates application-specific optimization details.

show statistics dre Command Output

The **show statistics dre** command output displays the compression ratios for both encode and decode and includes details about DRE age, cache size available, and used percentage (see Figure 1-31).

Figure 1-31 Command Output: show statistics dre

```
Output of command - show statistics dre
Cache:
    Status: Usable, Oldest Data (age): 50d
    Total usable disk size: 116735 MB,  Used: 0.63%
      Hash table RAM  size:    436 MB,  Used: 0.00%

Connections:   Total (cumulative): 31   Active: 3

Encode:
   Overall: msg:       6201, in:    798 KB, out:    157 KB, ratio:  80.25%
       DRE: msg:        154, in:   6673 B, out:   9973 B, ratio:   0.00%
DRE Bypass: msg:       6064, in:    791 KB
        LZ: msg:       6124, in:    858 KB, out:    156 KB, ratio:  81.75%
 LZ Bypass: msg:         77, in:      0 B
    Avg latency:      0.128 ms     Delayed msg:          0
  Encode th-put:   1004 KB/s
  Message size distribution:
    0-1K=100%  1K-5K=0%  5K-15K=0%  15K-25K=0%  25K-40K=0%  >40K=0%
Decode:
   Overall: msg:      25377, in:    358 MB, out:    645 MB, ratio:  44.52%
       DRE: msg:      25251, in:    357 MB, out:    643 MB, ratio:  44.51%
DRE Bypass: msg:      26539, in:   1527 KB
        LZ: msg:      20110, in:    296 MB, out:    296 MB, ratio:   0.29%
 LZ Bypass: msg:       5267, in:  63570 KB
    Avg latency:      0.450 ms
  Decode th-put:  57907 KB/s
  Message size distribution:
    0-1K=3%  1K-5K=14%  5K-15K=23%  15K-25K=13%  25K-40K=14%  >40K=30%
```

249910

The output also includes LZ compression ratios for both encode and decode.

show statistics tfo Command Output

The **show statistics tfo** command output displays total, active, pending and bypass connection counts handled by the WAE (see Figure 1-32).

Figure 1-32 Command Output: show statistics tfo

```
Output of command - show statistics tfo
  Total number of connections                          : 31
  No. of active connections                            : 3
  No. of pending (to be accepted) connections          : 0
  No. of bypass connections                            : 1
  No. of normal closed conns                           : 25
  No. of reset connections                             : 3
     Socket write failure                              : 0
     Socket read failure                               : 0
     WAN socket close while waiting to write           : 0
     AO socket close while waiting to write            : 0
     WAN socket error close while waiting to read      : 0
     AO socket error close while waiting to read       : 0
     DRE decode failure                                : 0
     DRE encode failure                                : 0
     Connection init failure                           : 0
     WAN socket unexpected close while waiting to read : 0
     Exceeded maximum number of supported connections  : 0
     Buffer allocation or manipulation failed          : 0
     Peer received reset from end host                 : 3
     DRE connection state out of sync                  : 0
     Memory allocation failed for buffer heads         : 0
     Unoptimized packet received on optimized side     : 0
```

249911

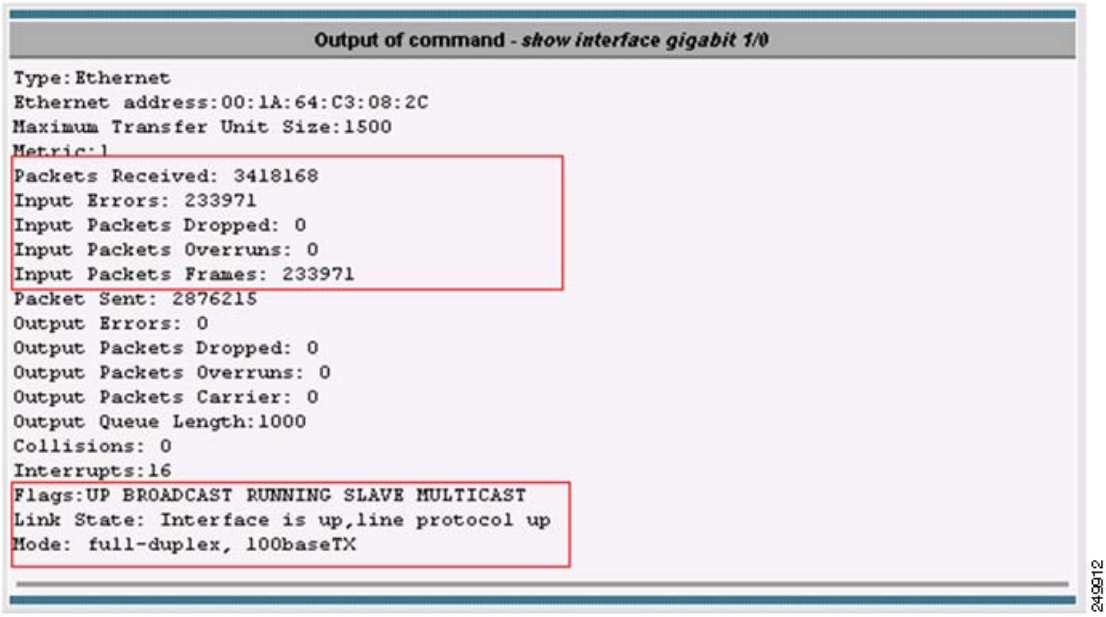
The output also provides connection reset counts that indicate the cause of a connection reset.

Note Pay special attention to the connection reset counter because it may indicate a problem outside the WAAS appliance.

show interface gig 1/0 Command Output

The **show interface gig 1/0** command output indicates the interface status, speed/duplex, packets sent and received, and any errors encountered (see Figure 1-33).

Figure 1-33 Command Output: show interface gig I10

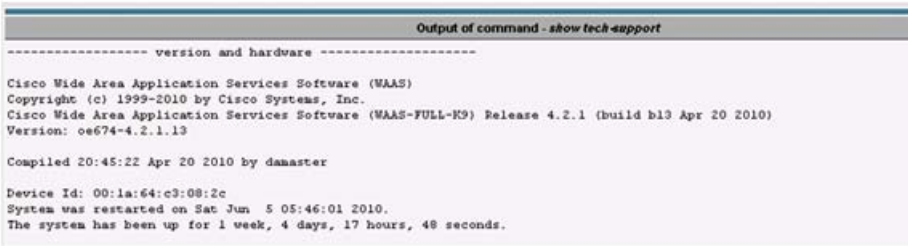


A speed and duplex mismatch is one of the most common reasons for poor performance.

show tech-support Command Output

The **show tech-support** command output displays key outputs for various CLI commands and can be used for monitoring and troubleshooting tasks (see Figure 1-34).

Figure 1-34 Command Output: show tech-support



CHAPTER 2

Monitoring Traffic Interception

This chapter describes how to use traffic interception to monitor your WAAS devices and contains the following sections:

Verifying WCCPv2 Interception

This section describes several IOS and WAAS WCCP commands that are available to verify if WCCP interception is working correctly.

This section contains the following topics:

show ip wccp IOS Command Output

The **show ip wccp** IOS command output provides WCCP inventory including number of routers, WAEs or service group, packets redirected, and forwarding and return method. This is the most commonly used CLI command to verify if WCCP interception is working correctly.

The command syntax is as follows:

show ip wccp [*service_group#*] **[detail]**

The following examples show how to use the command both with and without the optional argument and keyword.

Figure 2-1 highlights the area of the **show ip wccp** IOS command output that show that there is one intercepting router and one WAE registered to Service Group 61.

Figure 2-1 Command Output Sample 1: show ip wccp

```
Router# show ip wccp
Global WCCP information:
    Router information:
        Router Identifier:                    10.88.81.242
        Protocol Version:                     2.0

    Service Identifier: 61
        Number of Service Group Clients:      1
        Number of Service Group Routers:      1
        Total Packets s/w Redirected:         68755
          Process:                            2
          CEF:                                68753
        Service mode:                         Open
        Service access-list:                  -none-
        Total Packets Dropped Closed:         0
        Redirect access-list:                 -none-
        Total Packets Denied Redirect:        0
        Total Packets Unassigned:             0
        Group access-list:                    -none-
        Total Messages Denied to Group:       0
        Total Authentication failures:        0
        Total Bypassed Packets Received:      0
--More--
```

Client = WAE

249915

Figure 2-2 highlights the area of the **show ip wccp** IOS command output that shows that the Total Packets s/w Redirect counter is incrementing on software-based platforms (for example, Cisco ISR).

Figure 2-2 Command Output Sample 2: show ip wccp

```
Router# show ip wccp
Global WCCP information:
    Router information:
        Router Identifier:                  10.88.81.242
        Protocol Version:                   2.0

    Service Identifier: 61
        Number of Service Group Clients:    1
        Number of Service Group Routers:    1
        Total Packets s/w Redirected:       68755
          Process:                          2
          CEF:                              68753
        Service mode:                       Open
        Service access-list:                -none-
        Total Packets Dropped Closed:       0
        Redirect access-list:
        Total Packets Denied Redirec
        Total Packets Unassigned:
        Group access-list:
        Total Messages Denied to Gro
        Total Authentication failures:      0
        Total Bypassed Packets Received:    0
--More--
```

Verify That Counters Are Incrementing on Software-Based Platforms (e.g. ISR)

249916

Figure 2-3 highlights the area of the **show ip wccp** IOS command output that shows that the Total Packets s/w Redirect counter is not incrementing on hardware-based platforms (for example, Cisco Catalyst 6500).

Figure 2-3 Command Output Sample 3: show ip wccp

```
Router# show ip wccp
Global WCCP information:
    Router information:
        Router Identifier:                  10.88.81.242
        Protocol Version:                   2.0

    Service Identifier: 61
        Number of Service Group Clients:    1
        Number of Service Group Routers:    1
        Total Packets s/w Redirected:       102
          Process:                          1
          CEF:                              101
        Service mode:                       Open
        Service access-list:                -none-
        Total Packets Dropped Closed:       0
        Redirect access-list:
        Total Packets Denied Redirec
        Total Packets Unassigned:
        Group access-list:
        Total Messages Denied to Gro
        Total Authentication failures:      0
        Total Bypassed Packets Received:    0
--More--
```

Verify That Counters Are Not Incrementing on Hardware-Based Platforms (e.g. Cat6k)

249917

The **show ip wccp** *service_group#* **detail** IOS command output provides information about state, redirection and return methods used, connect time, and so forth. Figure 2-4 shows an example output from a software-based platform where the default redirection and assignment methods are used.

Figure 2-4 Command Output Sample 1: show ip wccp service_group# detail

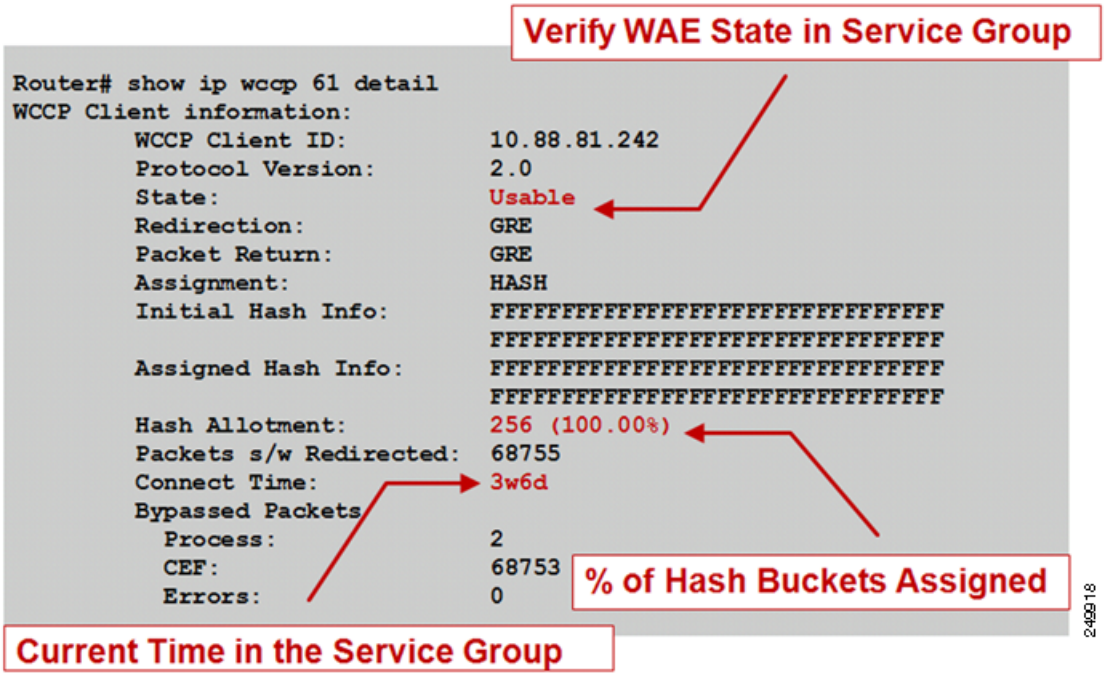
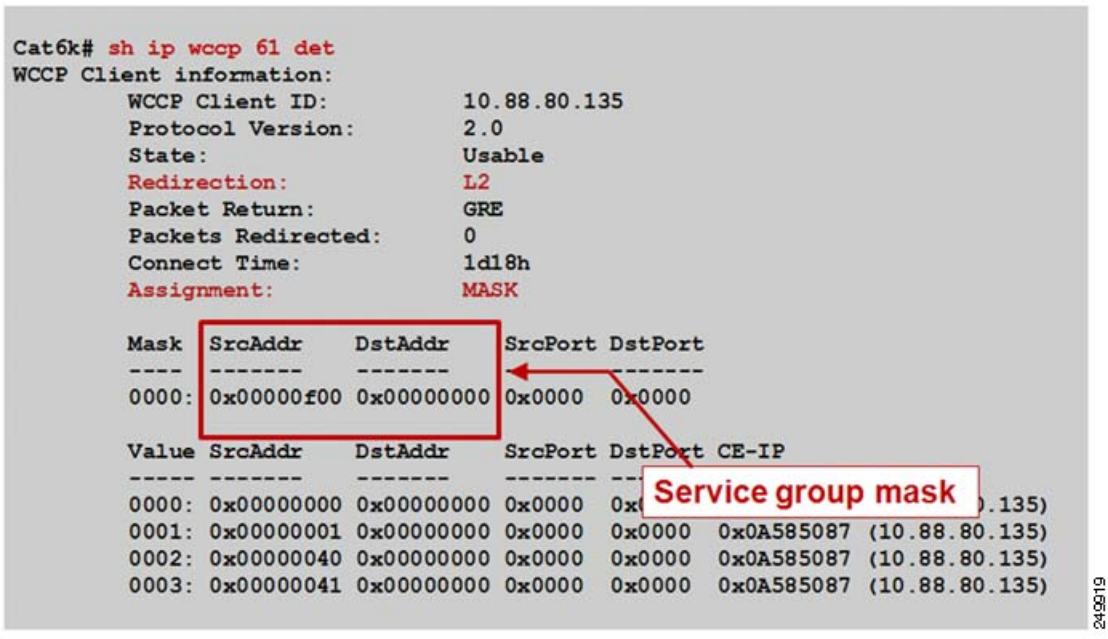


Figure 2-5 shows an example output from a hardware-based platform that is configured for L2 redirect and mask assignment. The CLI output is slightly different, reflecting these configured parameters.

Figure 2-5 Command Output Sample 2: show ip wccp service_group# detail



show wccp WAAS Command Outputs

You can use the **show wccp** WAAS commands that are available from the WAE CLI to verify that WCCP is configured and operating properly.

The command syntax is as follows:

show wccp {services | status | routers | gre}

Figure 2-6 shows output examples of the **show wccp services**, **show wccp status**, and **show wccp routers** WAAS commands.

Figure 2-6 Command Output: show wccp services, show wccp status, and show wccp routers

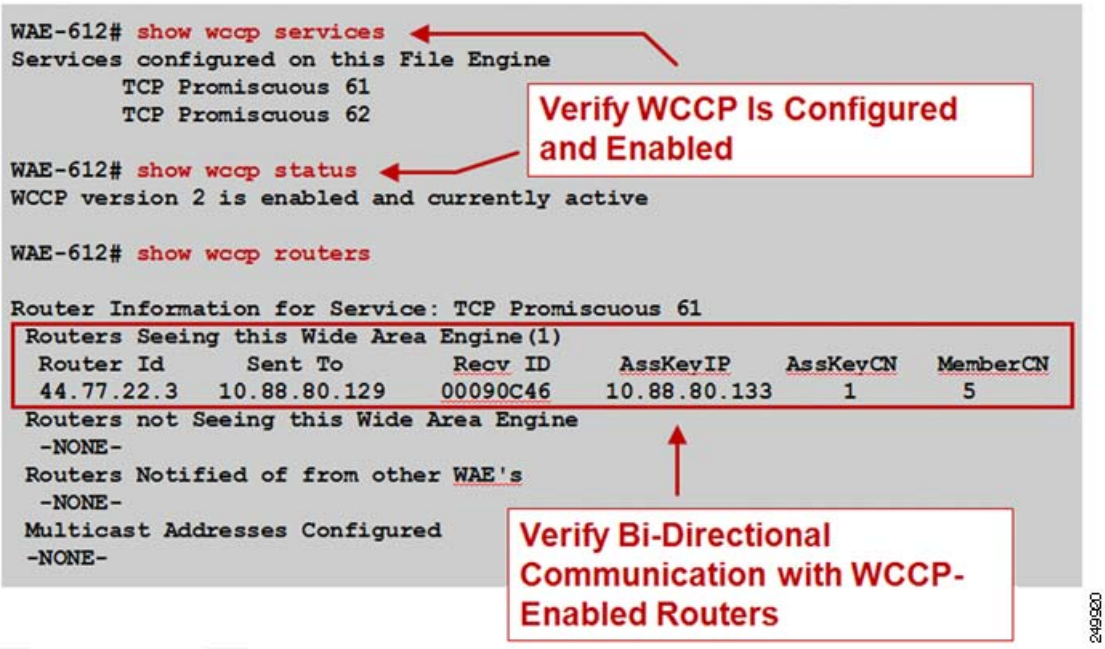


Figure 2-7 shows an output example of the **show wccp gre** WAAS command.

Figure 2-7 Command Output: show wccp gre

```
WAE-612# show wccp gre
Transparent GRE packets received:                    5531561
Transparent non-GRE packets received:                0
Transparent non-GRE non-WCCP packets received:       0
Total packets accepted:                              5051
Invalid packets received:                            0
Packets received with invalid service:               0
Packets received on a disabled service:              0
Packets received too small:                          0
Packets dropped due to zero TTL:                     0
Packets dropped due to bad buckets:                  0
Packets dropped due to no redirect address:          0
Packets dropped due to loopback redirect:            0
Pass-through pkts dropped on assignment update:      0
Connections bypassed due to load:                    0
Packets sent back to router:                         0
GRE packets sent to router (not bypass)              0
Packets sent to another WAE:                         0
GRE fragments redirected:                            0
GRE encapsulated fragments received:                 0
Packets failed encapsulated reassembly:              0
Packets failed GRE encapsulation:                    0
--More--
```

Either of These Counters Should Be Incrementing If WCCP Redirection Is Working

249921

Verifying Inline Interception

Figure 2-8 and Figure 2-9 show how to use the **show interface** command to verify inline interception configuration and proper operation.

Figure 2-8 Command Output Sample 1: show interface

```
WAE-612# show interface inlineGroup 1/0

Interface is in intercept operating mode.
Standard NIC mode is off.
Disable bypass mode is off.
VLAN IDs configured for inline interception: All
Watchdog timer is enabled.
Timer frequency: 1600 ms.
Autoreset frequency 500 ms.
The watchdog timer will expire in 1452 ms.
WAE-612#
```

Intercept Operating Mode or Bypass Operating Mode

Check vlan(s)

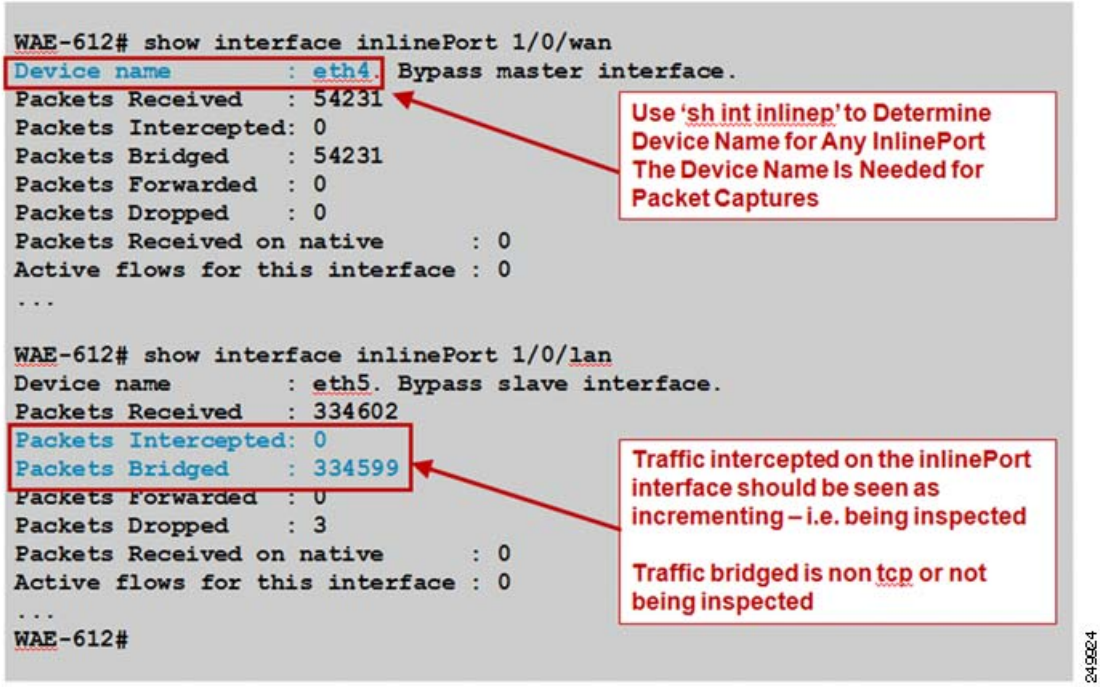
249923

The differences between the two operating modes are as follows:

- Intercept operating mode—Packets are passed to WAAS for potential optimization.

- Bypass operating mode—Mechanical bypass between ports in InLineGroup during failure or administrative shutdown.

Figure 2-9 Command Output Sample 2: show interface



For more information about troubleshooting WCCP, see the *WAAS Troubleshooting Guide* available on Cisco DocWiki.

CHAPTER 3

Monitoring WAAS Using SNMP

This chapter describes how to use Simple Network Management Protocol (SNMP) to monitor your WAAS devices. SNMP is an interoperable standards-based protocol that allows for external monitoring of WAAS devices through an SNMP agent.

For more information about using and configuring SNMP, see the "Configuring SNMP Monitoring" chapter in the *Cisco Wide Area Application Services Configuration Guide*.

This chapter contains the following sections:

Information About Supported MIBs

This section describes the Cisco-specific MIBs that are supported by WAAS as follows:

MIB	Description
ACTONA-ACTASTOR-MIB	Provides statistics for the CIFS transparent accelerator and statistics and log traps for the legacy mode WAFS component in WAAS.
CISCO-CDP-MIB	Displays the ifIndex value of the local interface. For 802.3 repeaters on which the repeater ports do not have ifIndex values assigned, this value is a unique value for the port and is greater than any ifIndex value supported by the repeater. In this example, the specific port is indicated by the corresponding values of cdpInterfaceGroup and cdpInterfacePort, where these values correspond to the group number and the port number values of RFC 1516.

MIB	Description
CISCO-CONFIG-MAN-MIB	Represents a model of configuration data that exists in various locations: • running—In use by the running system • terminal—Attached hardware • local—Saved locally in NVRAM or in flash memory • remote—Saved to a server on the network This MIB includes only operations that are specifically related to configuration, although some of the system functions can be used for general file storage and transfer.
CISCO-CONTENT-ENGINE-MIB	MIB module for the Cisco WAAS device from Cisco Systems. The following objects from this MIB are supported: • cceAlarmCriticalCount • cceAlarmMajorCount • cceAlarmMinorCount • cceAlarmHistTableSize
EVENT-MIB	Defines event triggers and actions for network management purposes. The MIB is published as RFC 2981.
HOST-RESOURCES-MIB	Manages host systems. The term *host* implies any computer that communicates with other similar computers connected to the Internet. The HOST-RESOURCES-MIB does not necessarily apply to devices whose primary function is communications services (terminal servers, routers, bridges, monitoring equipment). This MIB provides attributes that are common to all Internet hosts, for example, personal computers and systems that run variants of UNIX.
IF-MIB	Supports querying for interface-related statistics including 64-bit interface counters. These counters include received and sent octets, unicast, multicast, and broadcast packets on the device interfaces. All the objects from ifXEntry are supported except for ifCounterDiscontinuityTime. This MIB is documented in RFC 2233.
MIB-II	Internet Standard MIB that is documented in RFC 1213 and is for use with network management protocols in TCP/IP-based Internets. This MIB is found in the RFC1213-MIB file in the v1 directory on the download site (other MIBs are in the v2 directory).
SNMP-COMMUNITY-MIB	Documented in RFC 2576.
SNMP-FRAMEWORK-MIB	Documented in RFC 2571.
SNMP-NOTIFICATION-MIB	Documented in RFC 3413.
SNMP-TARGET-MIB	Documented in RFC 3413.
SNMP-USM-MIB	Documented in RFC 2574.

MIB	Description
SNMPv2-MIB	Documented in RFC 1907. This MIB supports the following notifications: • coldStart • linkUp • linkDown • authenticationFailure
SNMP-VACM-MIB	Documented in RFC 2575.

Downloading Supported MIBs

All supported MIB files can be downloaded from the following Cisco FTP locations:

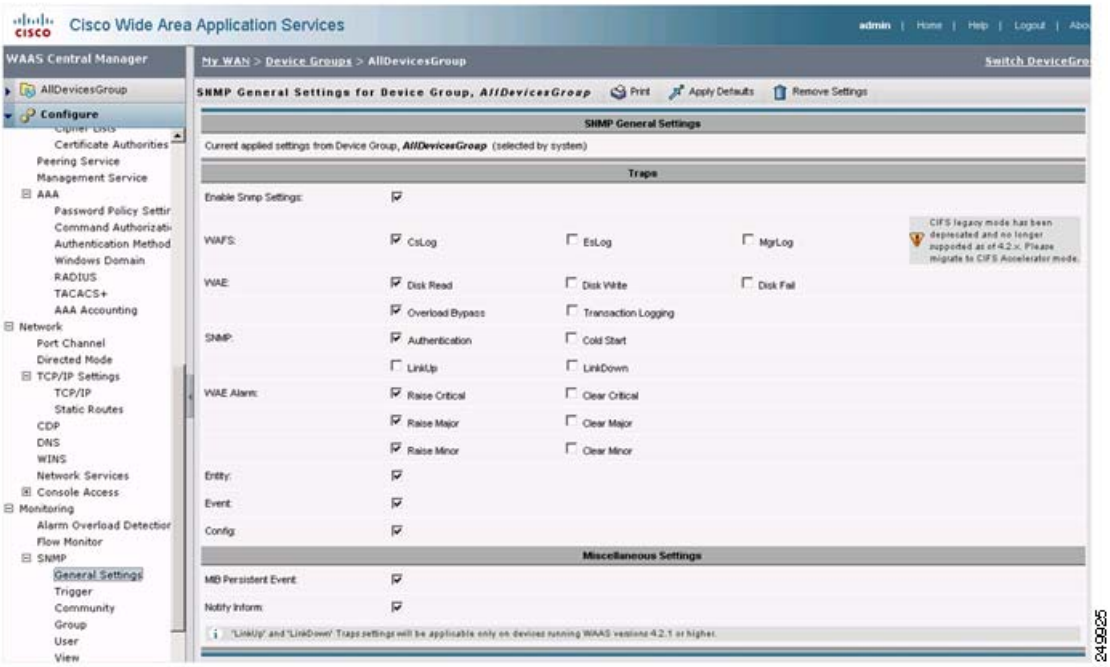
- ftp://ftp.cisco.com/pub/mibs/v2
- ftp://ftp.cisco.com/pub/mibs/v1

The MIB objects that are defined in each MIB are described in the MIB files and are self-explanatory.

Viewing and Enabling SNMP Traps

You can view the SNMP traps options available on the WAAS system by choosing My WAN > Device Group > AllDevicesGroup > Configure > Monitoring > SNMP > General Settings. The SNMP General Settings window appears (see Figure 3-1).

Figure 3-1 SNMP General Settings Window



For information about enabling SNMP traps from the SNMP General Settings window, see the "Configuring SNMP Monitoring" chapter in the *Cisco Wide Area Application Services Configuration Guide*.

Information About Common SNMP MIB OIDS

This section describes the common SNMP trap OIDs.

Object	**cceAlarmCriticalRaised**
OID	**1.3.6.1.4.1.9.9.178.2.0.7**
Status	**current**
MIB	**CISCO-CONTENT-ENGINE-MIB**; View Supporting Images
Trap Components	**cceAlarmHistId** **cceAlarmHistModuleId** **cceAlarmHistCategory** **cceAlarmHistInfo** **cceAlarmHistTimeStamp**
Description	A module has raised a Critical alarm.

Object	**coldStart**
OID	**1.3.6.1.6.3.1.1.5.1**
Status	**current**
MIB	**SNMPv2-MIB**; View Supporting Images
Description	The SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.

Object	**cceAlarmCriticalCleared**
OID	**1.3.6.1.4.1.9.9.178.2.0.8**
Status	**current**
MIB	**CISCO-CONTENT-ENGINE-MIB**; View Supporting Images
Trap Components	**cceAlarmHistId** **cceAlarmHistModuleId** **cceAlarmHistCategory** **cceAlarmHistInfo** **cceAlarmHistTimeStamp**
Description	A module has cleared a Critical alarm.

Object	**cceFailedDiskName**
OID	**1.3.6.1.4.1.9.9.178.1.5.1**
Type	**OCTET STRING**
Permission	**accessible-for-notify**
Status	**current**
MIB	**CISCO-CONTENT-ENGINE-MIB**; View Supporting Images
Description	The name of the disk on which disk-failure event occurred.
Object	**ciscoContentEngineDiskFailed**
OID	**1.3.6.1.4.1.9.9.178.2.0.6**
Status	**current**
MIB	**CISCO-CONTENT-ENGINE-MIB**; View Supporting Images
Trap Components	**cceFailedDiskName**
Description	A Content Engine data drive failed. This object supersedes ciscoContentEngineDataDiskFailed. Additional information about the error is logged to syslog.

Viewing and Configuring SNMP Triggers

You can view and configure SNMP triggers on the WAAS system. You can configure custom triggers to generate additional SNMP traps for other MIB objects of interest to your particular configuration.

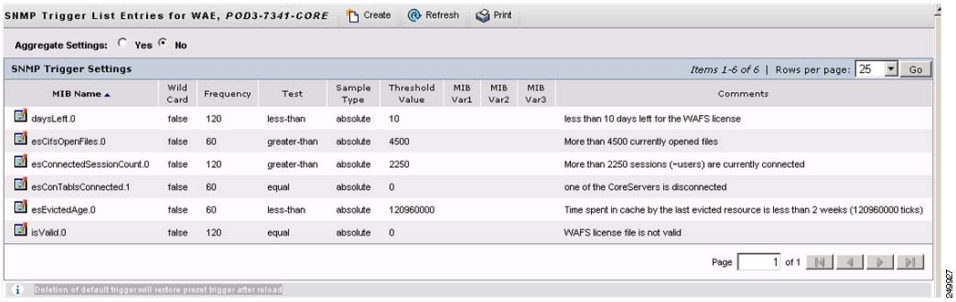
There are six default triggers on the WAE. When default triggers are deleted and the configuration is saved, reloading the device brings them back. Figure 3-2 shows the default triggers.

Procedure

Step 1 Choose **My WAN > Device Group > AllDevicesGroup > Configure > Monitoring > SNMP > Trigger**.

The Trigger List Entries window appears, displaying the list of default and configured triggers (Figure 3-2).

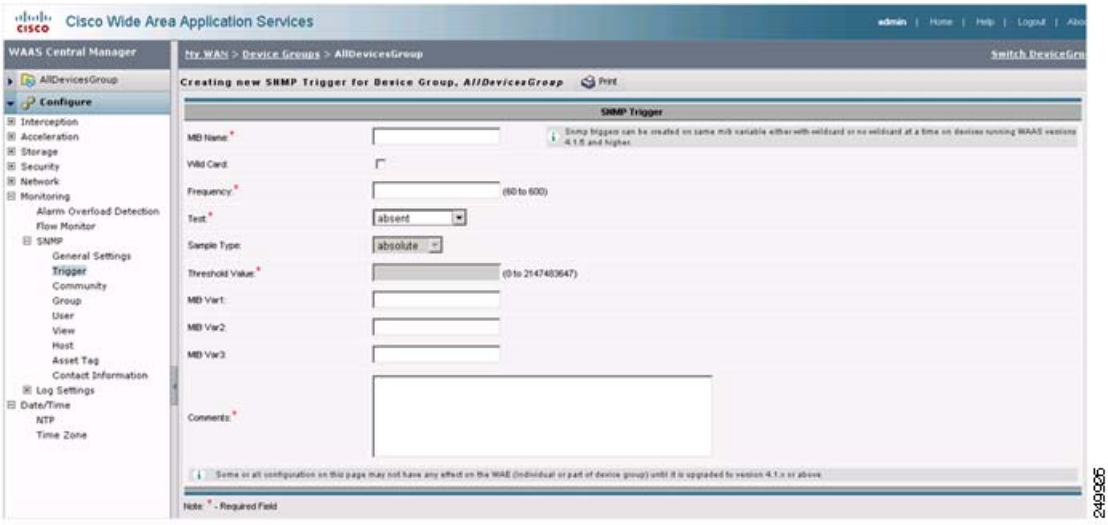
Figure 3-2 SNMP Trigger List



Step 2 To create a trigger, from the Trigger List Entries window, click the create icon.

The Create new SNMP Trigger window appears (Figure 3-3).

Figure 3-3 Create SNMP Trigger



Step 3 Configure the new SNMP trigger.

For information about configuring an SNMP trigger, see the see the "Configuring SNMP Monitoring" chapter in the *Cisco Wide Area Application Services Configuration Guide*.

CHAPTER 4

Monitoring WAAS Using XML API

This chapter describes how to use the WAAS API to monitor your WAAS devices and how to use soapUI with the WAAS API interface.

This chapter contains the following sections:

Information About the XML-Based API

The WAAS Central Manager Web Service provides an XML-based API that supports monitoring device status and information, alarms, and statistics. It does not support device configuration.

For more information about the XML API, see the *Cisco Wide Area Application Services API Reference*.

The following services are offered:

- Device Configuration Service (DeviceConf)
- Traffic Acceleration Service (TrafficStats)
- CIFS Statistics Service (CIFSStats)
- Video Streaming Statistics Service (VideoStats)
- HTTP and HTTPS Statistics Service (HttpStats and HttpsStats)
- MAPI Statistics Service (MapiStats)
- NFS Statistics Service (NfsStats)
- SSL Statistics Service (SslStats)
- Events Service (AlarmStatus)
- Status Service (DeviceStatus)

To obtain the WSDL file defined for a particular service in the WAAS Central Manager monitoring API implementation, you submit a URL to the service with a ?wsdl suffix as follows:

https://<host/ip>:8443/ws/*service_name*?wsdl

To query a service for information, you send an XML-formatted SOAP request to the service at the following URL:

https://<host/ip>:8443/ws/*service_name*

Using the Traffic Acceleration Service

You can retrieve traffic and application statistics for individual WAEs, device groups, and for the WAAS network using the Traffic Acceleration service (TrafficStats Web Service), which performs one or more of the following actions:

- retrieveTrafficStats—Retrieves the overall statistics collected on either a WAAS device, WAEs within a device group, or all system-wide WAEs.
- getMonitoredApplications—Retrieves a list of all types of applications known in the scope of the system.
- retrieveAppTrafficStats—Retrieves overall traffic statistics collected on either a WAAS device, WAEs within a device group, or all system-wide WAEs. The traffic is further filtered based on the specified application names.
- retrieveCPUUtilization—Retrieves the CPU utilization information for a specified WAE.
- retrieveConnection—Retrieves overall connection details for the current time.
- retrieveConnectionTrendStats—Retrieves overall connection trend details of applications collected on a device.
- retrievePeakThroughPutStats—Retrieves the peak throughput values collected on a device.
- retrieveAverageThroughPutStats—Retrieves the average throughput values collected on a device.

Using the Events and Status Service

You can retrieve alarm information, device status, and disk status using the Events and Status service (AlarmStatus Web Service), which performs one or more of the following actions:

- retrieveAllAlarms—Retrieves all alarms.
- retrieveAlarmByName—Retrieves a list of all alarms filtered by the name of the WAE or WAE group, the object type, or the alarm name.
- retrieveAlarmBySeverity—Retrieves a list of all active alarms for the specified WAE or WAE group, further filtered on alarm severity.
- getDeviceStatus—Retrieves the device status.
- getDiskStatus—Retrieves the physical disk status.
- getDiskInformation—Retrieves information about the disk.
- getDiskEncryptStatus—Retrieves the disk encryption status.
- getMonitoredAOs—Retrieves the operational status of application accelerators for either a WAAS device, WAEs within a device group, or all system-wide WAEs.
- getMonitoredAOsByWaeIDs—Retrieves the operational status of application accelerators for a list of device IDs.

Using soapUI to Access the WAAS API Interface

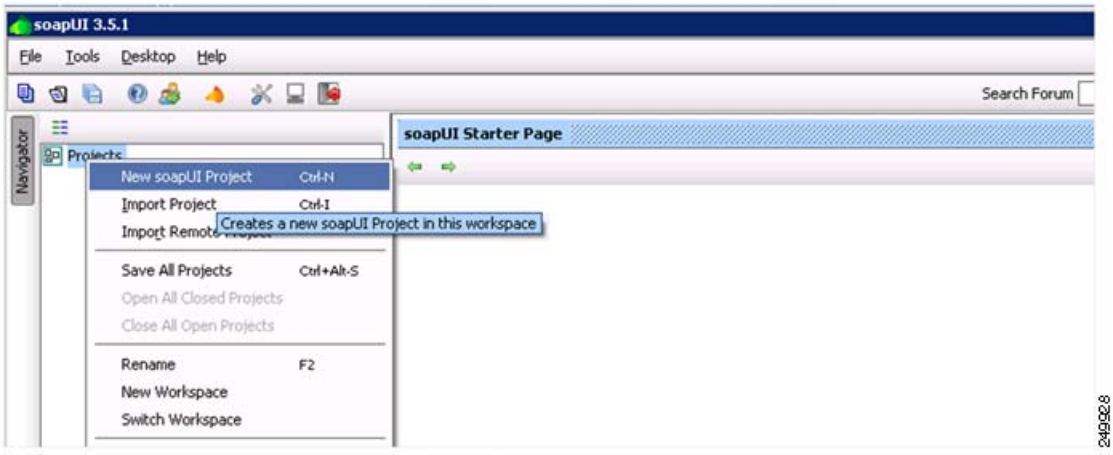
You can access the WAAS API interface using third-party tools such as soapUI, WebInject, ApacheCXF, and so forth. The soapUI website (http://www.soapui.org/) offers a free software version that you can download and install on a client PC. The procedure in this section describes how to create a project using soapUI after you install and start the software.

Procedure

Step 1 Right-click the project to create a project (Figure 4-1).

For example, WAAS-Project.

Figure 4-1 soapUI: Create New Project



The New soapUI Project pop-up window appears.

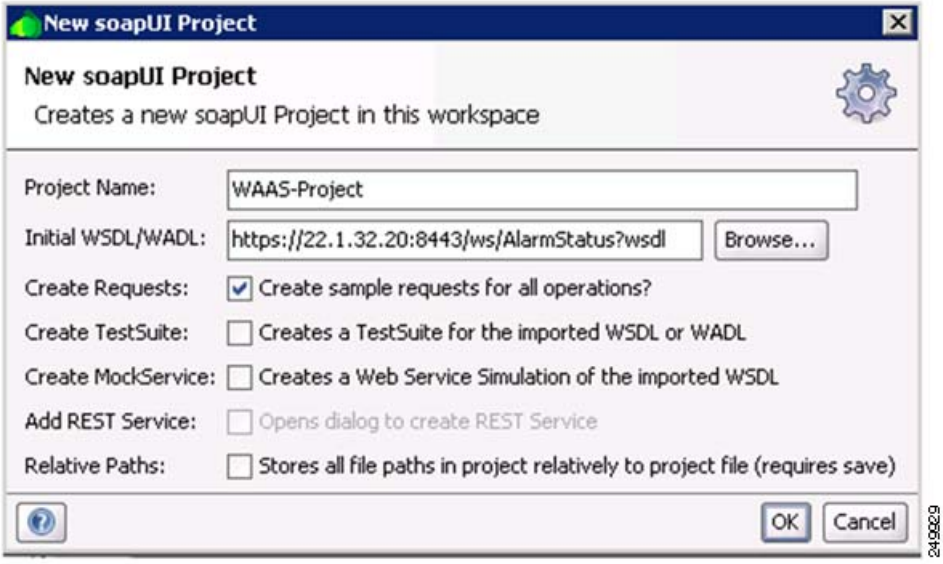
Step 2 From the New soapUI Project pop-up window (Figure 4-2), do the following:

a. Enter the WSDL URL.

b. Check the **Create Requests** check box.

c. Click **Ok**. A progress window appears while the data is gathered, which may take several seconds to load.

Figure 4-2 soapUI: New Project PoP-Up Window

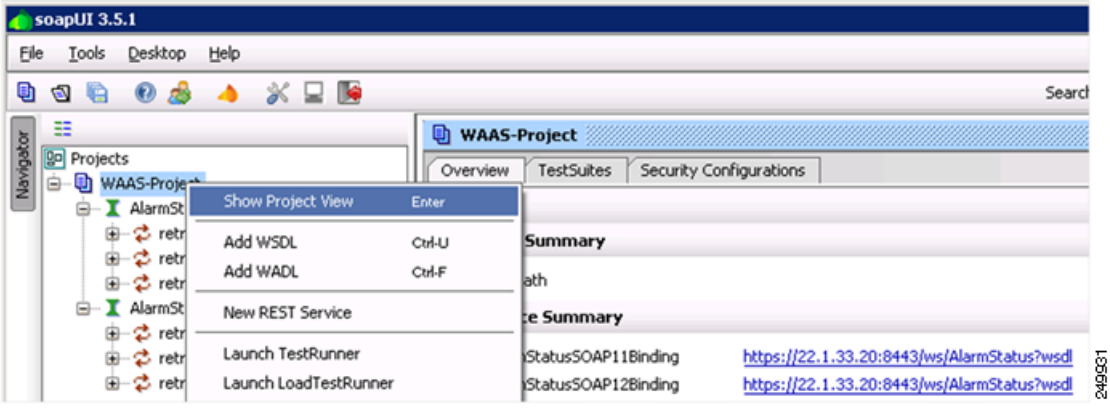


After the WSDL loads, the available navigation options appear.

Step 3 Specify security credentials by doing the following:

a. Right-click the new project (such as WAAS-Project) to display the pop-up menu and click **Show Project View** from the menu (Figure 4-3).

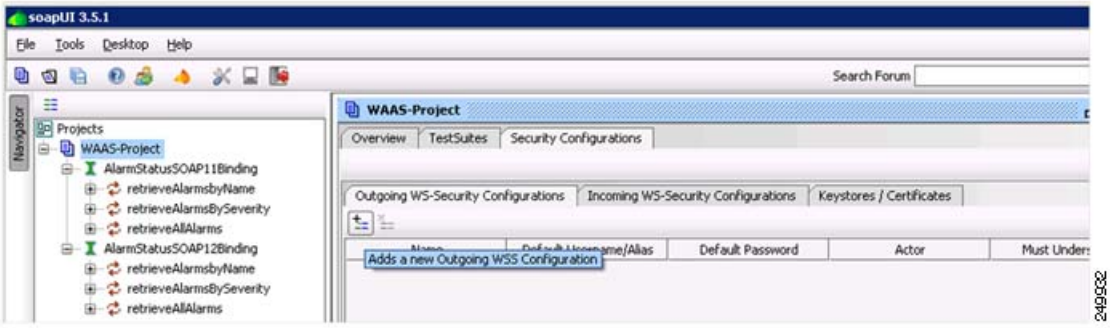
Figure 4-3 soapUI: Show Project View



The project window appears.

b. From the project window, add a new WSS by clicking the **Security Configurations** tab and click the plus sign (+) below the Outgoing WS-Security Configurations tab (Figure 4-4).

Figure 4-4 soapUI: Add New WSS



The New Outgoing WSS Configuration pop-up window appears.

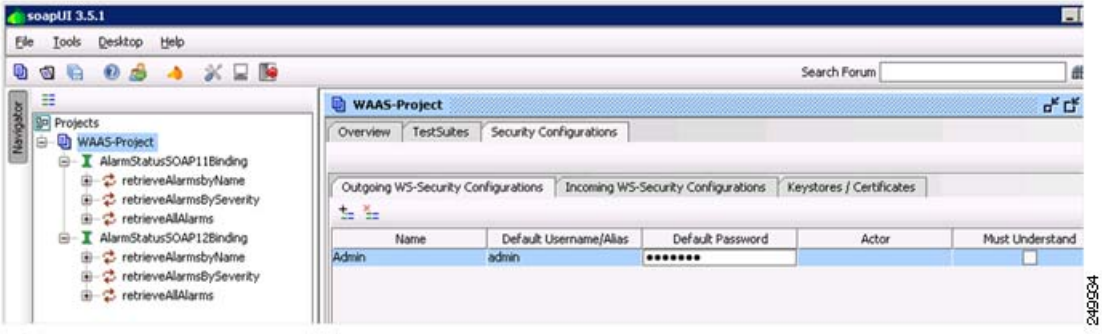
c. From the New Outgoing WSS Configuration pop-up window, enter a name for the new WSS (such as Admin) and click **OK** (Figure 4-5).

Figure 4-5 soapUI: New Outgoing WSS Configuration Pop-Up Window

The pop-up window closes and the Outgoing WS-Security Configuration tab displays the new WSS.

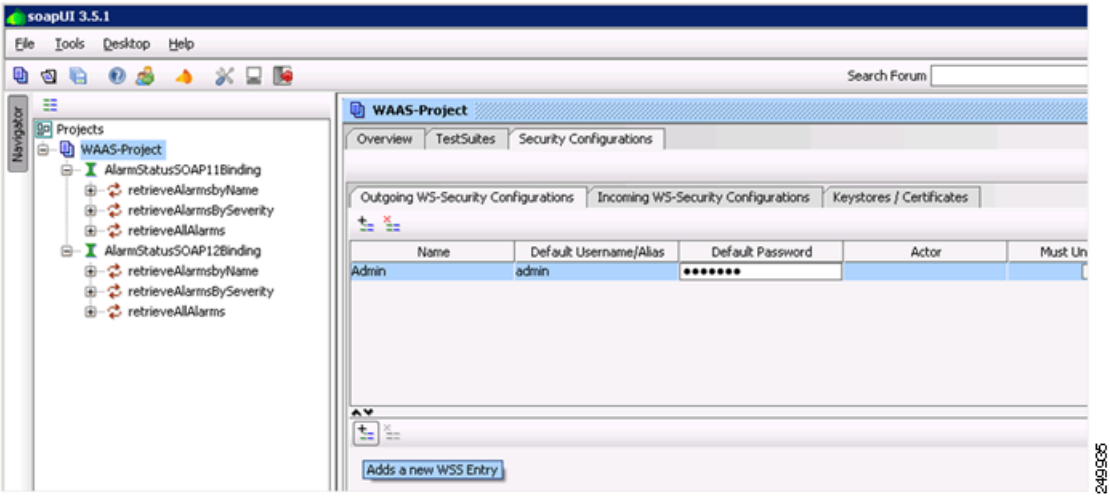
d. From the Outgoing WS-Security Configuration tab, enter the device username and password (Figure 4-6).

Figure 4-6 soapUI: WSS Username and Password



e. Click the plus sign (+) in the lower pane to add a new WSS Entry (Figure 4-7).

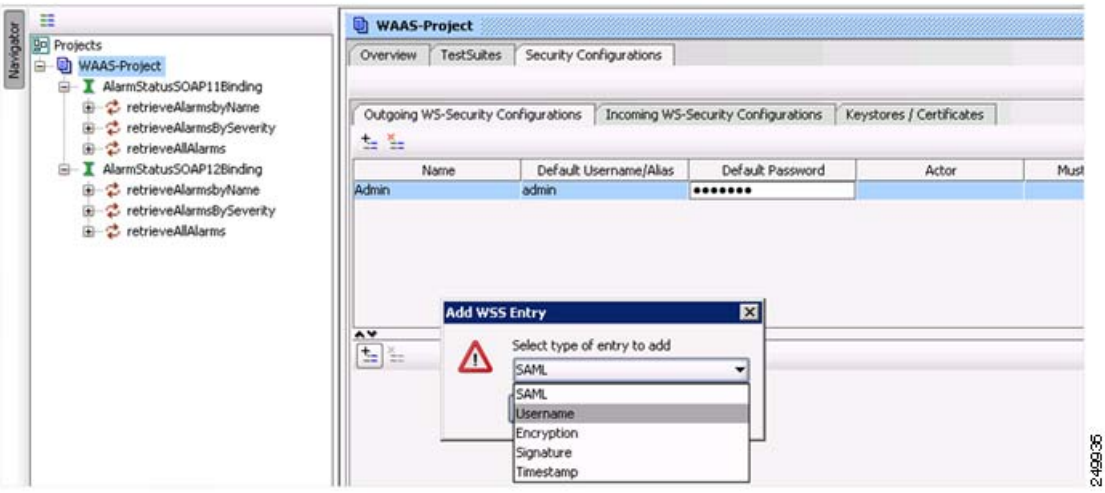
Figure 4-7 soapUI: Add WSS Entry



The Add WSS Entry pop-up window appears.

f. From the Add WSS Entry pop-up window's Select Type of Entry to Add drop-down list, choose **Username** (Figure 4-8).

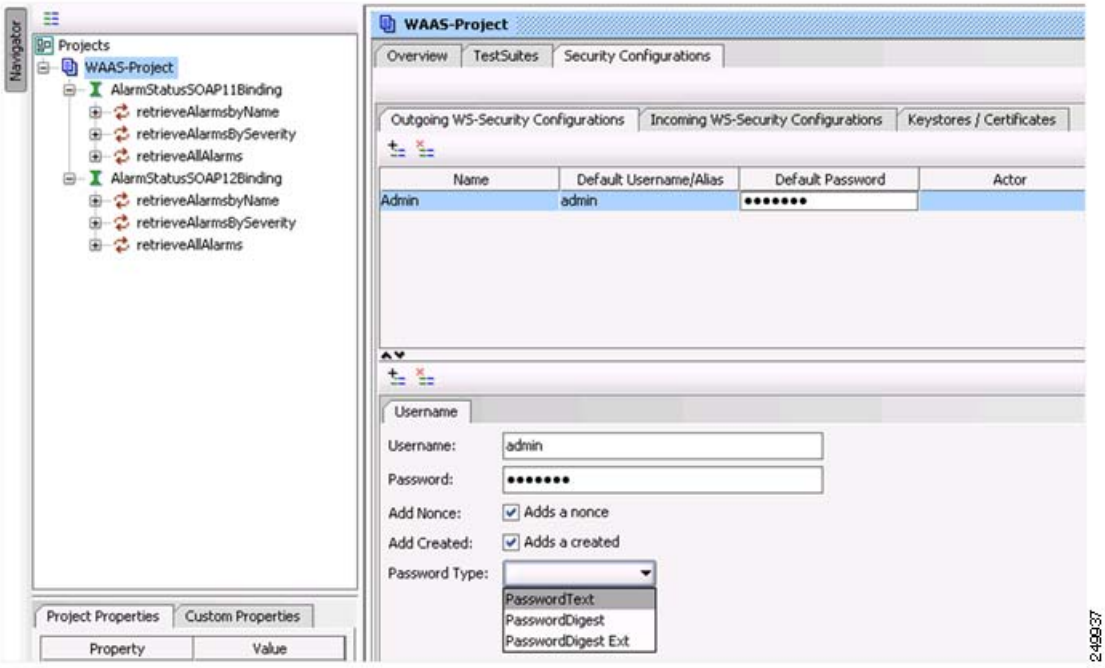
Figure 4-8 soapUI: Add WSS Entry



The pop-up window closes and the lower pane of the Outgoing WS-Security Configuration tab displays the Username tab with your username and password already populated.

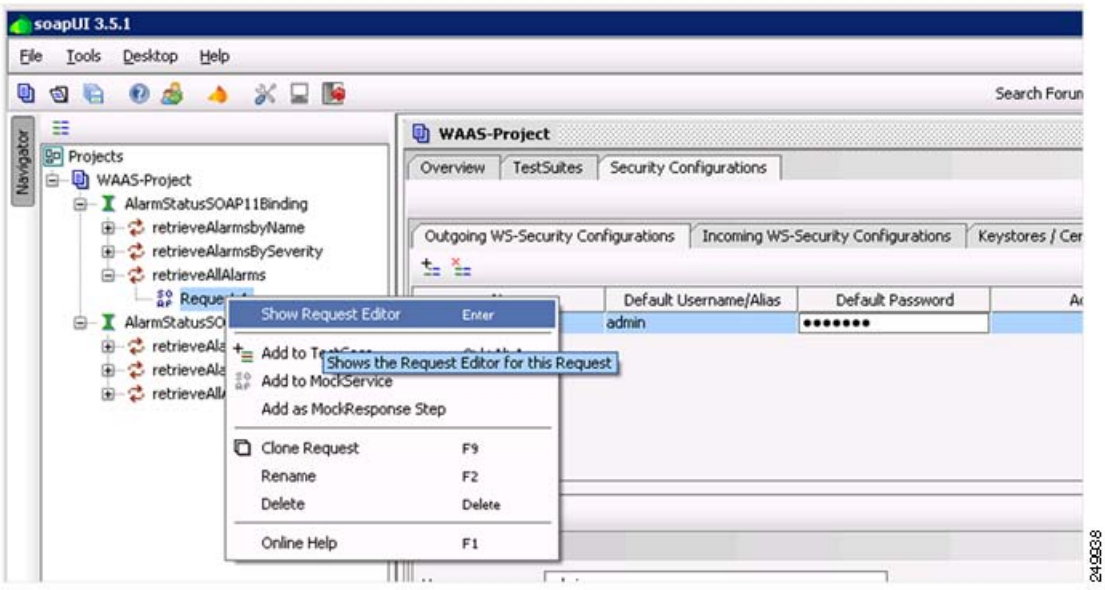
g. From the Username tab's Password Type drop-down list, choose **PasswordText** (Figure 4-9).

Figure 4-9 soapUI: Password Type



Step 4 From the Projects tree on the left, click **+** to expand one of the listed items, double-click **Request x** to display the pop-up menu, and choose **Show Request Editor** from the menu (Figure 4-10).

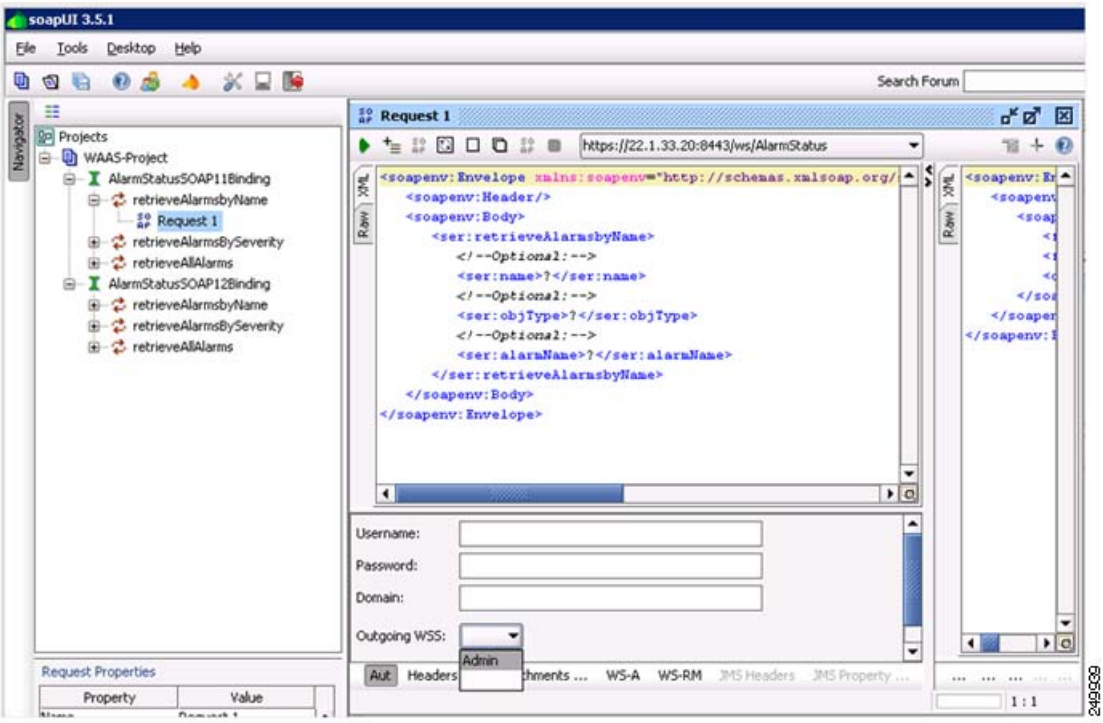
Figure 4-10 soapUI: Show Request Editor



The Request Editor window appears.

Step 5 From the Request Editor window, click **Aut** at the bottom and choose **Admin** from the Outgoing WSS drop-down list (Figure 4-11).

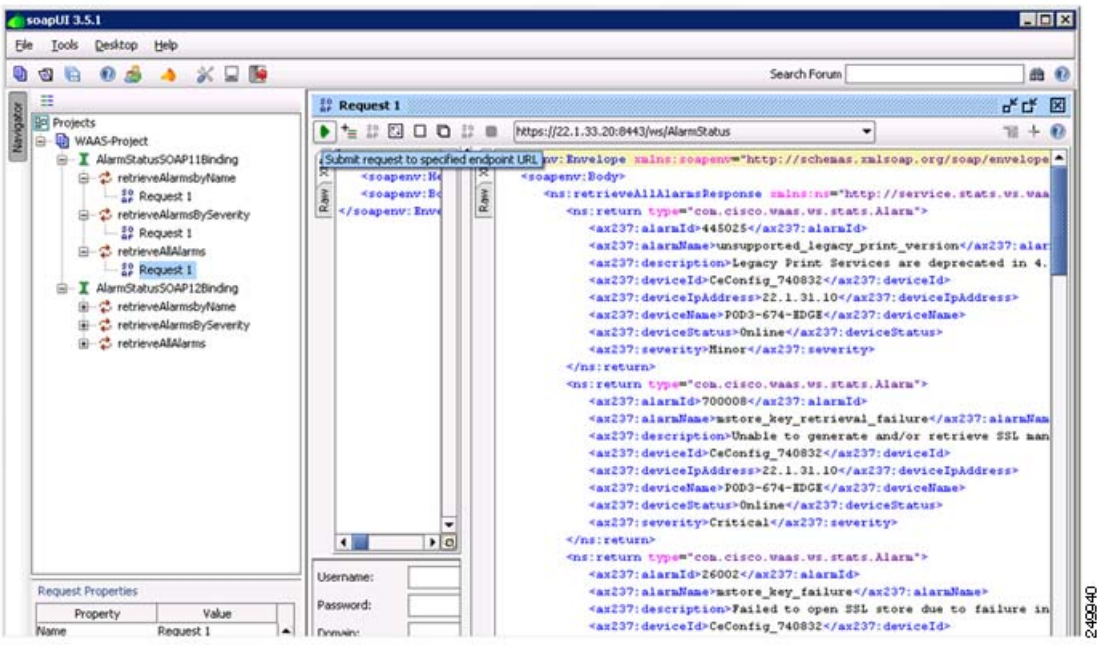
Figure 4-11 soapUI: Request Editor



Step 6 Verify the WSDL URL and click **Submit** to query the device.

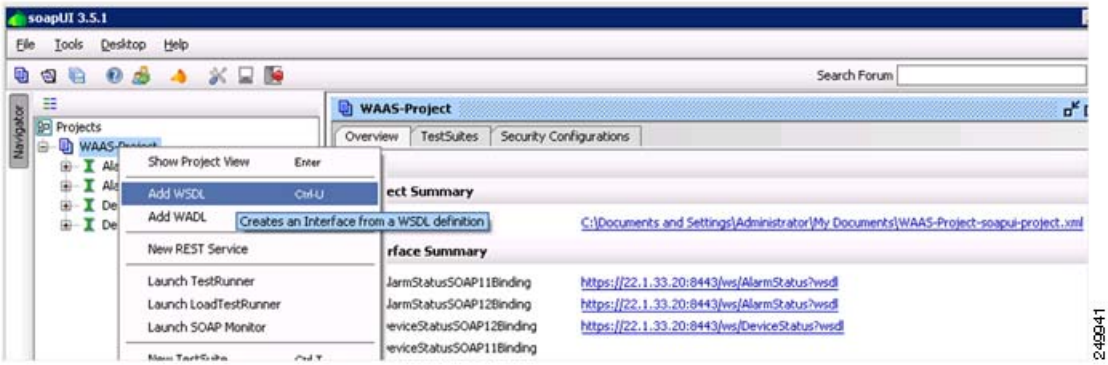
After the request is complete, the data in XML format appears (Figure 4-12).

Figure 4-12 soapUI: Data in XML Format



Step 7 (Optional) To add more WSDL, right-click the project to display the pop-up menu and choose **Add WSDL** from the menu (Figure 4-13).

Figure 4-13 soapUI: Add WSDL



CHAPTER 5

Monitoring WAAS Using Cisco Network Analysis Module

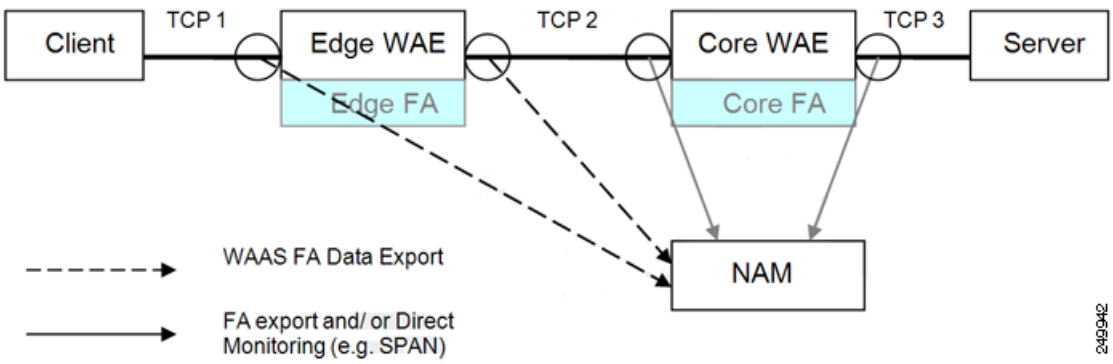
This chapter describes Cisco Network Analysis Module (NAM), which you can use to monitor your WAAS devices.

This chapter contains the following sections:

Information About NAM

NAM monitors network and application response time (ART) by analyzing the exchanges of TCP packets between clients and application servers. NAM version 4 has been enhanced to process and analyze data received from the WAAS FlowAgent and accurately calculate the ART of WAAS optimized flows. A FlowAgent runs on WAAS devices to collect TCP packet data and send the flow data to NAM for analyzing and reporting (Figure 5-1).

Figure 5-1 NAM Monitoring of WAAS Devices



NAM provides the following monitoring functions:

- Monitoring Client-Edge Connections—By monitoring the TCP connections between the clients and the WAAS edge device (Connection TCP-1 in the above picture), the following ART metrics can be measured:
  - Total Delay (TD) as experienced by the client
  - Total Transaction Time as experienced by the client
  - Bandwidth usage (bytes/packets) before compression
  - Number of transactions and connections
  - Network RTT broken down into two segment: client-edge and edge-server
- Monitoring Edge-Core Optimized Connections—By monitoring the spoofed TCP connections between the edge and core WAAS devices (Connection TCP-2 in the above picture), the following additional ART metric can be measured: Bandwidth usage (bytes/packets) after compression.
- Monitoring Edge-Core Connections—By monitoring the TCP connections between the core WAAS devices and the servers (Connection TCP-3 in the above picture), additional ART metrics can be measured:
  - Application (Server) Delay (without proxy acceleration/caching server)
  - Network RTT between the core WAAS device and the servers

The sections that follow show how to configure WAAS to enable monitoring by NAM and how to configure NAM to monitor specific WAAS functions.

For more information about NAM, see the following documentation URLs:

- Complete NAM documentation set:

  http://www.cisco.com/en/US/products/sw/cscowork/ps5401/tsd_products_support_series_home.html

- *Cisco WAAS NAM Virtual Service Blade Installation and Configuration Guide*:

  http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_virtual_blade/4.2/install/guide/waas/waas42install.htm

Configuring a WAAS Device to Export Data to NAM

This procedure describes how to configure a WAAS device to export WAAS flow record data to NAM.

Procedure

Step 1 From the WAAS Central Manager, choose **My WAN > Device Group > AllDevicesGroup > Configure > Monitoring > Flow Monitor**.

The Flow Monitoring Settings window appears (Figure 5-2).

Figure 5-2 WAAS Central Manager: Flow Monitoring Settings

Step 2 From the Flow Monitoring Settings window, do the following:

a. Check the Enable check box to enable data export.

b. In the Destination box, enter the NAM IP address.

c. Click **Submit**.

The WAAS is now ready to export flow record data. To specify the WAAS data that NAM is to monitor, see the "Configuring NAM to Monitor WAAS Devices" section on page 5-3.

Configuring NAM to Monitor WAAS Devices

This section provides an overview of the WAAS data source functions that NAM can monitor and describes how to specify the WAAS data that NAM monitors.

Note You do not need to add any export-enabled WAAS devices in to NAM because NAM can detect them.

This section contains the following topics:

Information About Using NAM to Monitor WAAS Devices

NAM uses WAAS data sources to monitor traffic collected from different WAAS segments: Client, Client WAN, Server WAN, and Server. Each WAAS segment is represented by a data source. You can set up NAM to monitor and report other traffic statistics of the WAAS data sources (such as application, host, and conversation information) in addition to the monitored ART metrics.

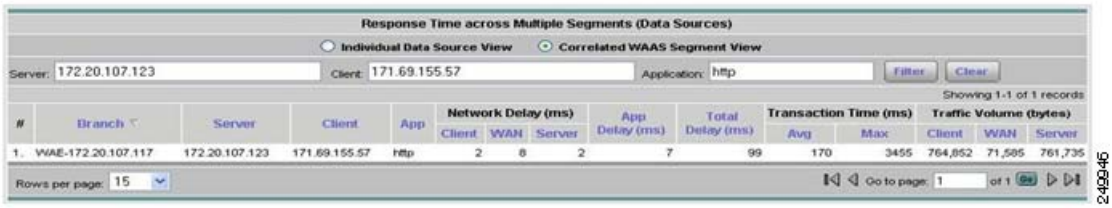
The use of data source depends upon on the WAAS deployment scenario. Table 5-1 describes several common WAAS deployment scenarios and their applicable data sources.

Table 5-1 WAAS Deployment Scenarios

Deployment Scenario	Edge WAE Data Source	Core WAE Data Source
• Clients in the branch • Servers in the core (data center) • NAM in the core	Client	Server Server WAN
• Clients in the branch • Servers in the core (data center) • NAM in the core	Client Client WAN	Server
• Servers in the branch • Clients in the core (data center) • NAM in the core	Server	Client Client WAN
• Servers in the branch • Clients in the core (data center) • NAM in the branch	Server Server WAN	Client
• Servers and clients in the branch and the core (data center) • NAM in the core	Client Server	Client Server Client WAN Server WAN
• Servers and clients in the branch and the core (data center) • NAM in the branch	Client Server Client WAN Server WAN	Client Server

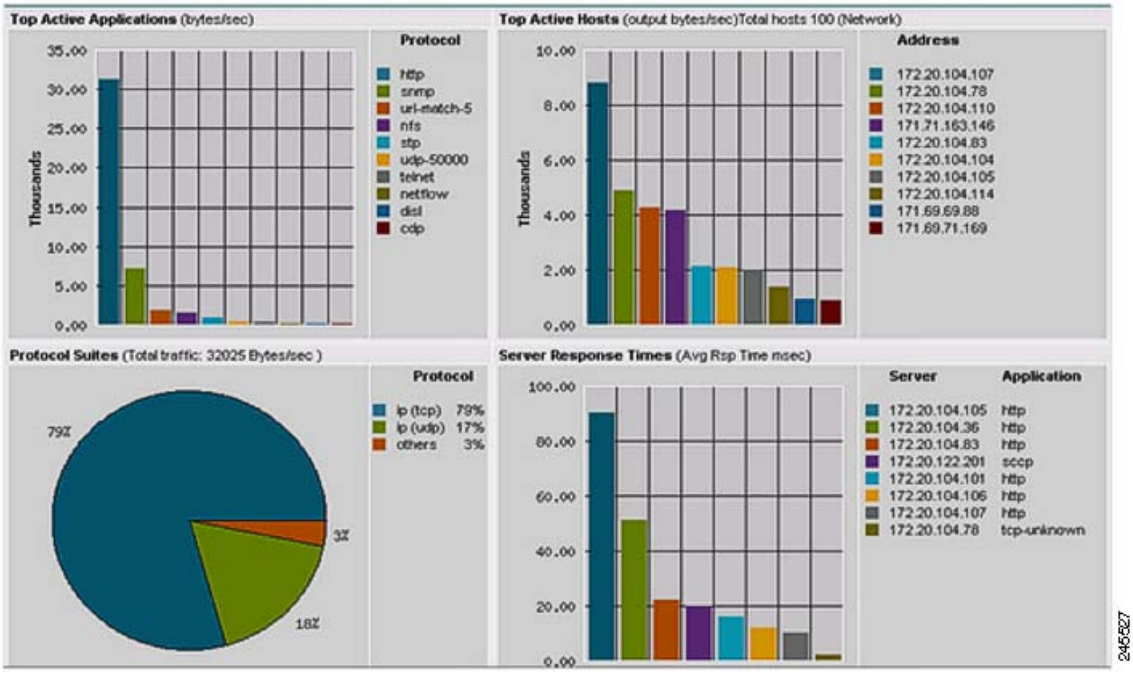
In NAM version 4.1 and later, correlated data and combined segments are displayed as one row per client-server as shown in Figure 5-3.

Figure 5-3 NAM Sample Data Source Display



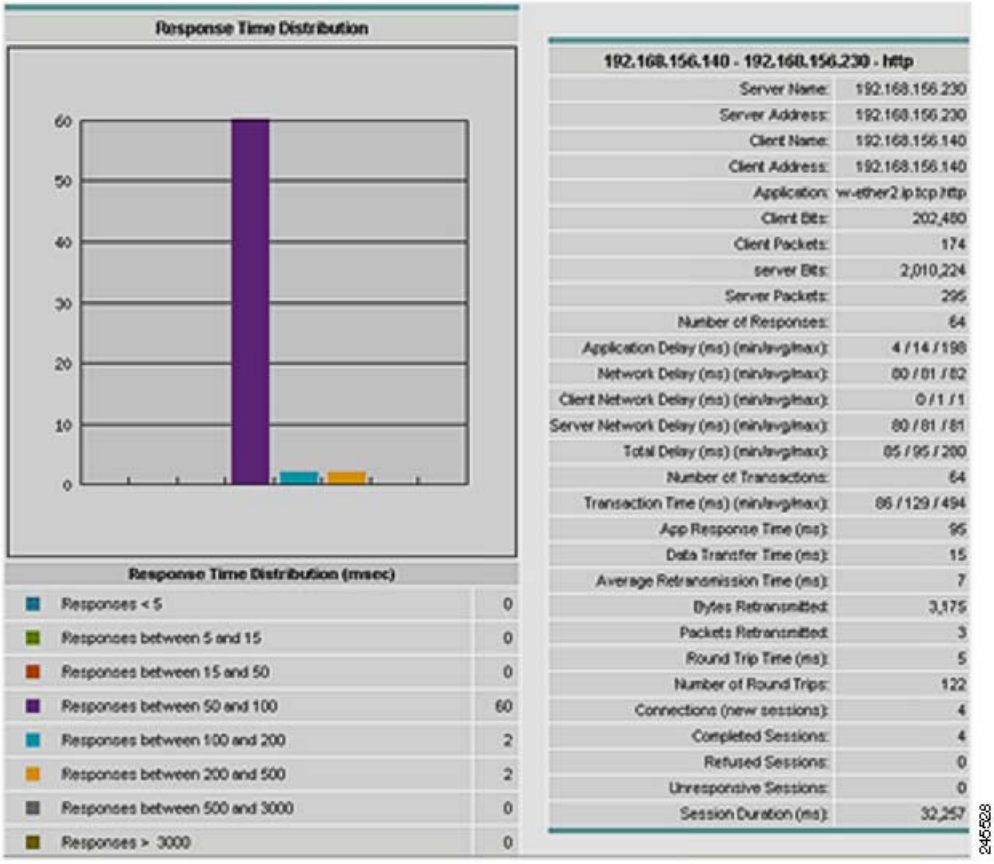
NAM can display data about the network applications, protocols in use, and the most active or highly utilized clients and servers (see Figure 5-4).

Figure 5-4 NAM Network Application, Protocol, Host, and Server Report



You can generate various reports to view client, server, or application response times and top active applications, active hosts, and so forth (see Figure 5-5).

Figure 5-5 NAM Response Time Report



Specifying WAAS Device Data Sources to Monitor

You can configure NAM to monitor the following WAAS data sources:

- Client—Export the original (LAN side) TCP flows originated from its clients to NAM for monitoring.
- Client WAN—Export the optimized (WAN side) TCP flows originated from its clients to NAM for monitoring.
- Server WAN—Export the optimized (WAN side) TCP flows from its servers to NAM for monitoring.
- Server—Export the original (LAN side) TCP flows from its servers to NAM for monitoring.
- Pass-Through—(NAM 4.1 and later only) Export the flows that traverses WAAS without being optimized.

For information about how to configure NAM to monitor a WAAS device, see the *Using Cisco NAM 4.1 Reporting with Cisco WAAS* whitepaper on Cisco.com:

For additional information about configuring and using NAM, see the *User Guide for Cisco Network Analysis Module Traffic Analyzer.*