Cisco Catalyst Center SD-Access LAN Automation Deployment Guide

Revised: May 8, 2024

LAN Automation: Step-by-Step Deployment

Cisco LAN automation simplifies network operations; frees IT staff from time-consuming, repetitive network configuration tasks; and creates a standard, error-free underlay network. LAN automation accelerates building the underlay network without the traditional network planning and implementation process.

This guide is based on Catalyst Center Release 2.3.3; however, an additional topic in the guide provides some information on the LAN automation process based on Catalyst Center Release 2.3.5 and later.

Note Cisco DNA Center has been rebranded as Catalyst Center. During the rebranding process, you will see both names used in different collaterals, but both names refer to the same product.

The steps and examples may vary based on your Catalyst Center version. For more information on configuring LAN automation and related features, see *Cisco Catalyst Center User Guide*.

Workflow

Cisco LAN automation provides the following key benefits:

- *Zero-touch provisioning*: Network devices are dynamically discovered, onboarded, and automated from their factory-default state to fully integrated in the network.
- *End-to-end topology*: Dynamic discovery of new network systems and their physical connectivity can be modeled and programmed. These new systems can be automated with Layer 3 IP addressing and routing protocols to dynamically build end-to-end routing topologies.
- *Resilience*: Cisco LAN automation integrates system and network configuration parameters that optimize forwarding topologies and redundancy. Cisco LAN automation enables system-level redundancy and automates best practices to enable best-in-class resiliency during planned or unplanned network outages.
- *Security*: Cisco-recommended network access and infrastructure protection parameters are automated, providing security from the initial deployment.
- *Compliance*: LAN automation helps eliminate human errors, misconfigurations, and inconsistent rules and settings that drain IT resources. During new system onboarding, LAN automation provides compliance across the network infrastructure by automating globally managed parameters from Catalyst Center.

In four main steps, the Cisco LAN automation workflow helps enterprise IT administrators prepare, plan, and automate greenfield networks:

Procedure

Step 1 **Plan**: Understand the different roles in the LAN automation domain. Plan the site and IP pool and understand the prerequisites for seed devices.

Step 2 **Design**: Design and build global sites. Configure global network services and site-level network services. Configure global device credentials. Design the global IP address pool and assign the LAN automation pool.

Step 3 **Discover**: Discover seed devices.

Step 4 **Provision**: Start and stop LAN automation:

a) Start LAN automation: Push the temporary configuration to seed devices, discover devices, upgrade the image, and push the initial configuration to discovered devices.

b) Stop LAN automation: Convert all point-to-point links to Layer 3.

Step 1: Plan

LAN automation planning is the first step in successfully building the underlay network. This section explains the aspects you must plan to ensure that the Cisco LAN automation support matrix aligns with the targeted underlay network environment.

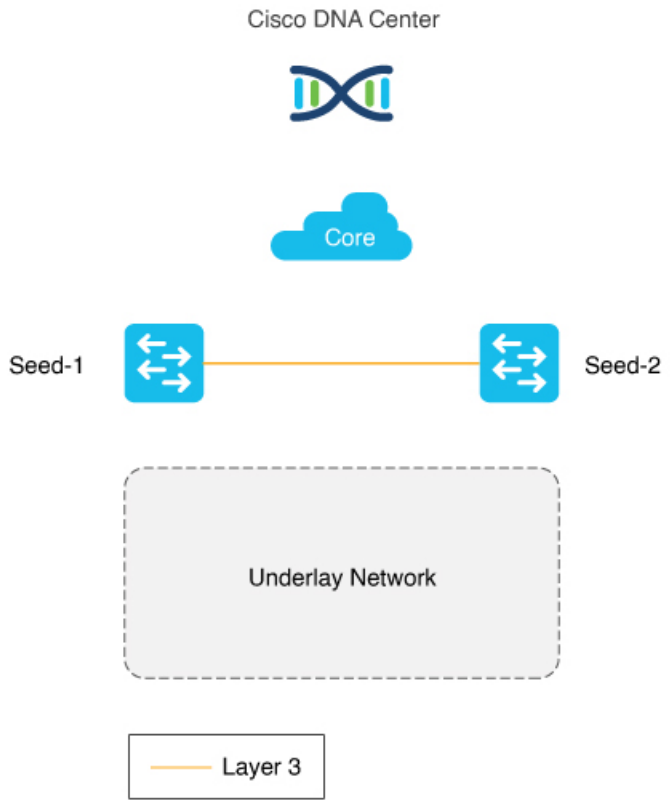
System Roles

Seed Device

The seed device is a predeployed system in the network and is the initial point through which Cisco LAN automation discovers and onboards new switches downstream. The seed device can be automated through technologies such as Cisco Plug n Play (PnP) and zero-touch provisioning, or configured manually. The following figure shows the seed device network boundaries between the Catalyst Center connection in the IP core and the to-be-discovered underlay network using LAN automation.

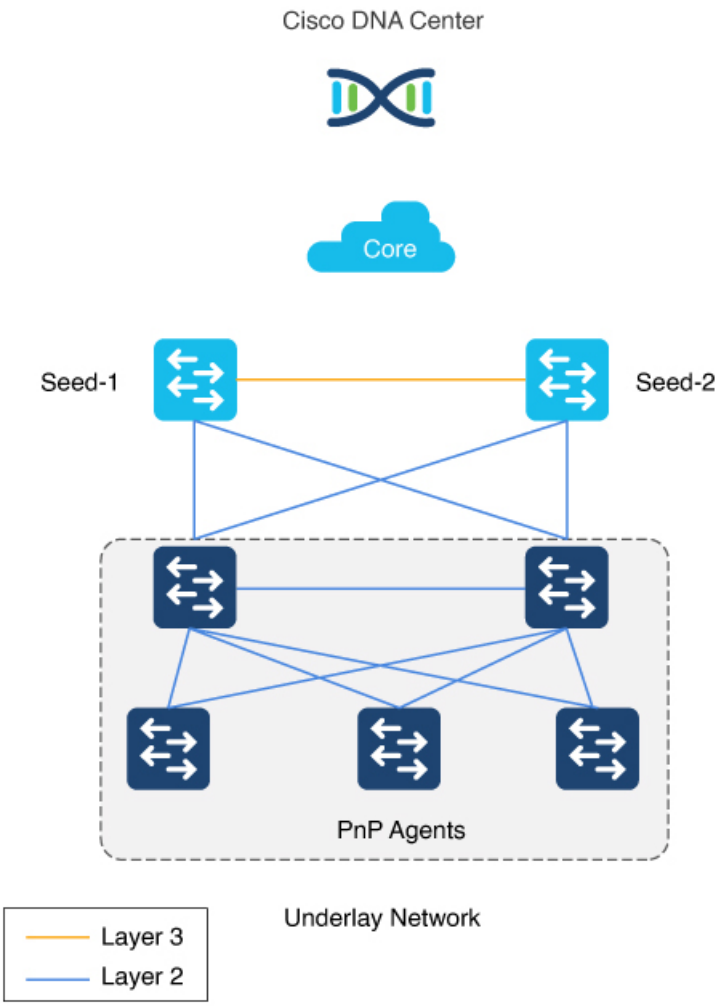
The peer seed (Seed-2 in the following figure) can also be automated via LAN automation. Only one seed device is required.

Device discovery happens only on the primary seed device interfaces.



PnP Agent

The PnP agent is a Cisco Catalyst switch with factory-default settings. The switch leverages the built-in day-0 mechanism to communicate with Catalyst Center and support the integrated PnP server function. Catalyst Center dynamically builds the PnP profile and configuration sets that enable complete day-0 automation. The following figure shows the PnP agent physical connection to the seed device.



Automation Boundary

In general, we recommend building structured and hierarchical network designs in enterprise networks to provide scalability and redundancy at every network tier. While the three-tier architecture is proven in large-scale enterprise campus networks, the network design varies based on the overall network size, physical connections, and so on. As part of the initial planning, the network admin must determine the physical topology to automate with Cisco LAN automation.

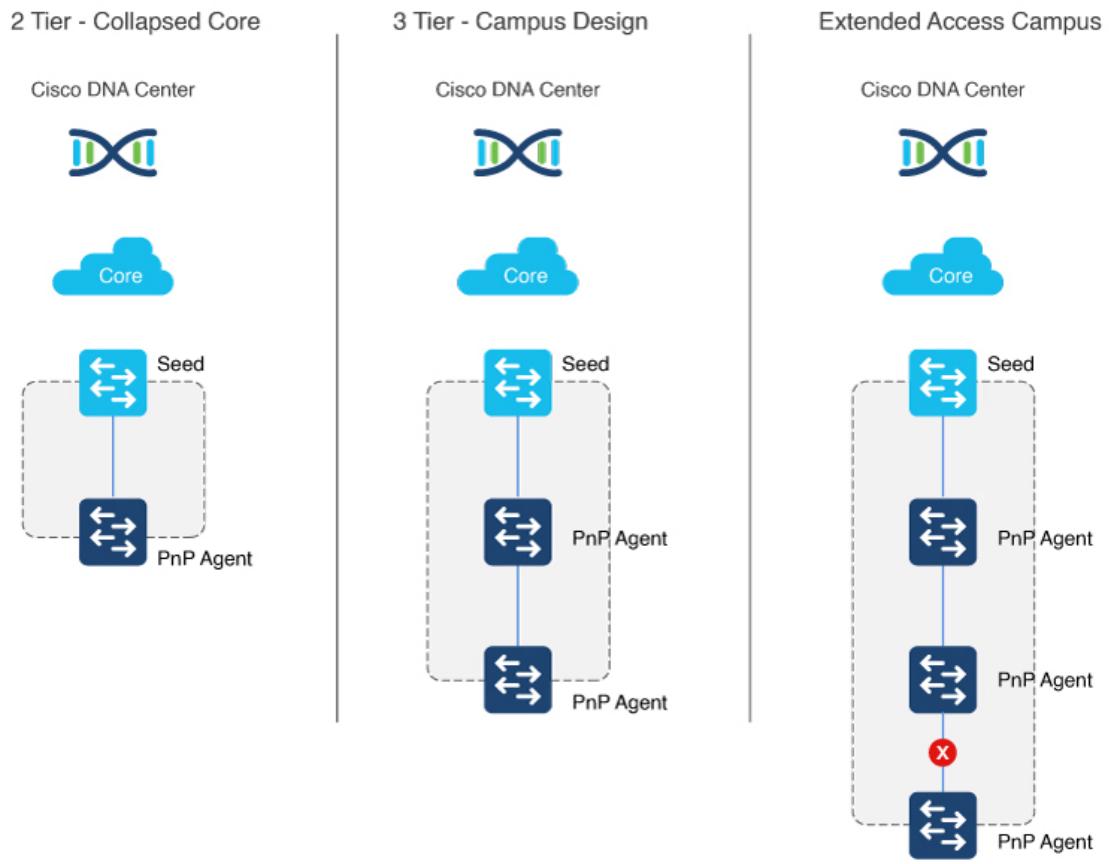
LAN automation in Catalyst Center supports a maximum of two hops from the initial automation boundary point device. In other words, to build the underlay network up to the access layer, the network admin must start the automation boundary from the core or distribution layer. Any additional network devices beyond two hops might be discovered but cannot be automated.

LAN automation initiates only on directly connected neighbors. Consider two scenarios:

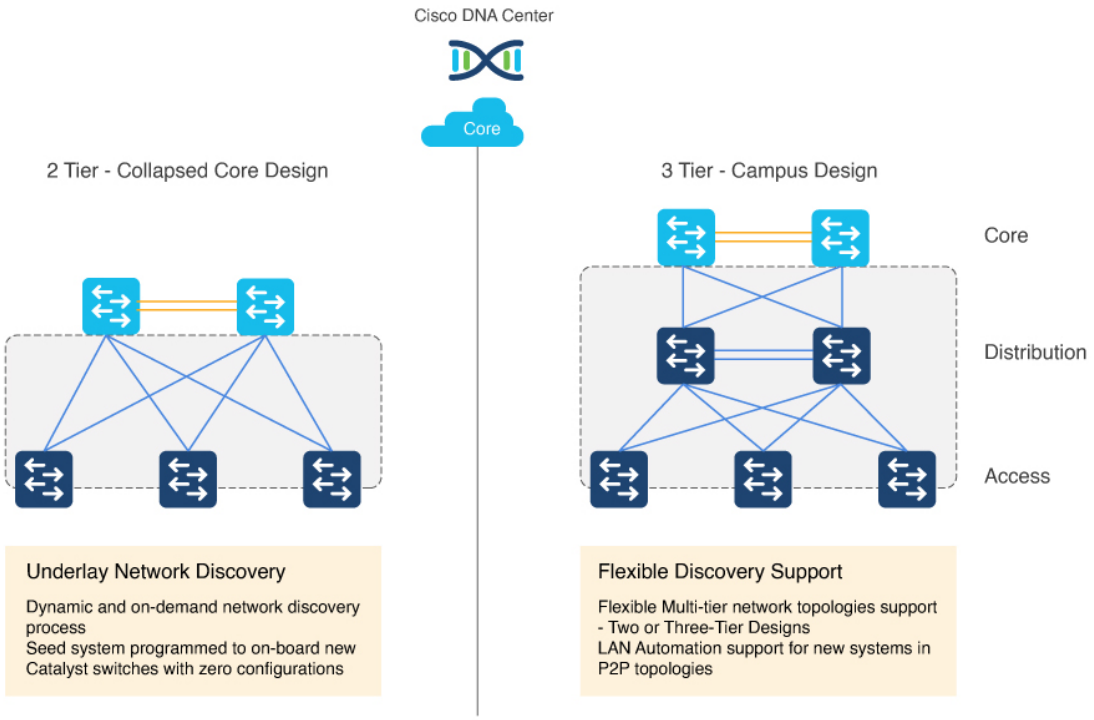
- Scenario 1: You have a three-tier network and you want to LAN automate distribution- and access-layer switches. Because distribution-layer switches (which are directly connected to the seed) participate in LAN automation, both distribution- and access-layer switches will be discovered and LAN automated.
- Scenario 2: You have a three-tier network and you want to LAN automate distribution- and access-layer switches. You already LAN automated the distribution layer. Later, you add access-layer switches to your network and you want to LAN automate

these switches. Because the distribution switches are already LAN automated and links converted to Layer 3, Tier 1 switches cannot be used as the seed. You must choose distribution as the seed in this scenario.

The following figure shows the automation boundary that Cisco LAN automation supports.



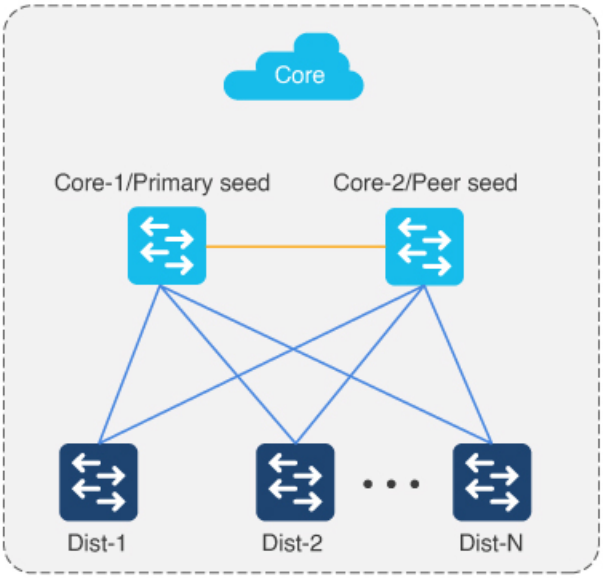
The following figure shows a two-tier and three-tier network design.



Multistep LAN Automation for Large Topologies: First Pass

Large topologies are brought up by performing LAN automation multiple times. During the first pass, distribution switches are brought up by choosing core devices as seed devices; the distribution switches come up as new devices.

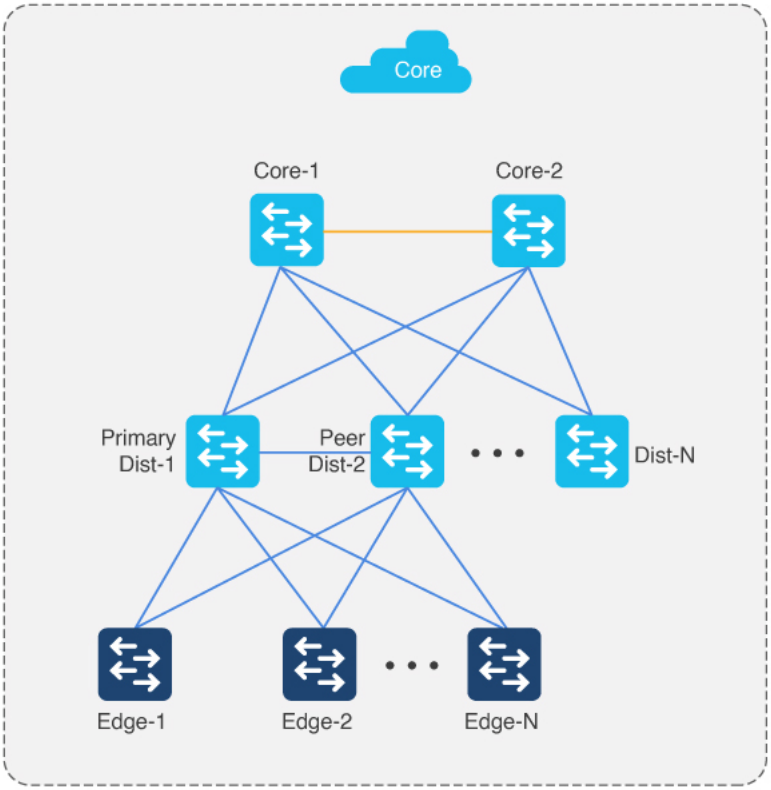
Note *N* is less than or equal to 50 devices at a time. All switches in the group can be booted in parallel or in a staggered fashion.



Multistep LAN Automation for Large Topologies: Second Pass with First Group

During the second pass, two of the distribution switches act as seed devices to bring up the edge devices as new devices. All new devices in this session must connect directly to the two distribution switches that act as seed devices. Repeat this process for the remaining set of distribution switches, two at a time.

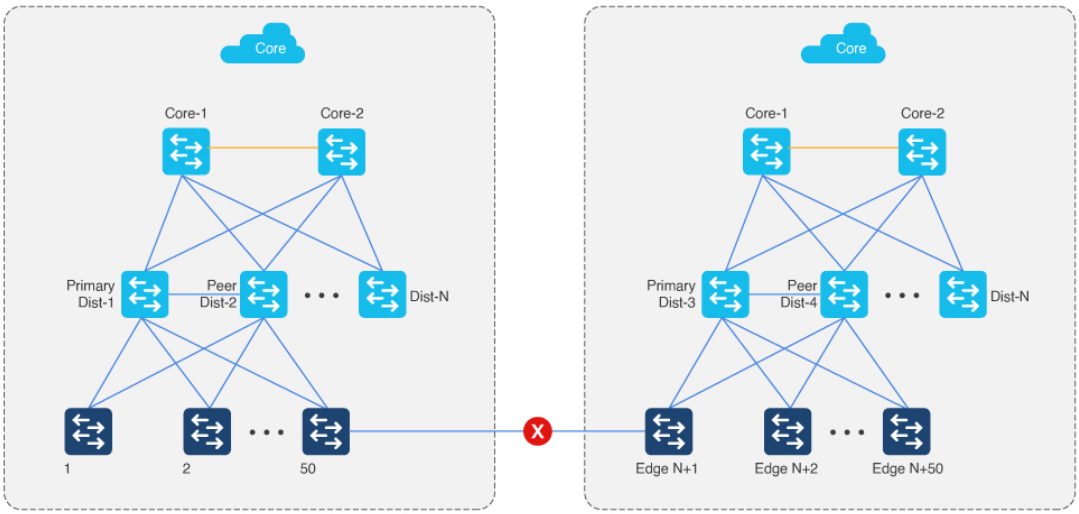
1. Repeat the second pass for each set of distribution to bring up the access/edge switches (where *N* is less than or equal to 50 devices at a time).
2. Connect uplinks from edges to the primary and peer distribution switches only.
3. Power down IOT/extended devices during the LAN automation session.
4. Distribution switches can be connected to other distribution switches.
5. There can be two tiers of devices below the seeds.
6. Always connect new devices to the primary seed device. Connection to the peer seed device is optional.



Multistep LAN Automation for Large Topologies: Second Pass with Second Group

Edge devices in one group cannot be connected to edge devices in another group. Newly discovered PnP devices in the LAN automation session cannot be connected to existing nonseed inventory devices.

Note In Catalyst Center 2.3.5 and later, you can establish links between the devices after LAN automation stops using the **Add Link** feature. For more information, see Create Link Between Interfaces, on page 60.



Link Configuration

- After all devices are added to the Catalyst Center inventory, you begin the process of Layer 3 link configuration by “stopping” the LAN automation session on the GUI.
- If you accidentally stop the LAN automation prematurely before all PnP devices are added to the Catalyst Center inventory, links are not configured on in-progress devices. You must delete the in-progress devices from the inventory, begin a new LAN automation session, bring the in-progress devices to the factory-default state, and reload the devices to rediscover them and get their links configured.
- This process starts the conversion of Layer 2 links to Layer 3 links, which is done by traversing the network graph built during new device onboarding. First, the lower device link is converted to a Layer 3 IP address. Next, the upper device link is converted to a Layer 3 IP address. Router IS-IS configuration is also performed during this step in the connecting links. During this phase, there might be a temporary loss of connectivity to the lower-tier device until the upper-tier link is configured. This phase can also result in an STP topology change when the Layer 2 links are converted to Layer 3.
- The process follows an algorithm that begins with the tier-three devices, followed by the tier-two devices, and completes with the tier-one devices.
- It is important to note that only the links between devices that participate in the current session are converted to Layer 3 links. Links between the newly discovered PnP device and the existing nonseed inventory device are not converted to Layer 3.
- Consider the following scenarios when a LAN-automated device is deleted from the inventory:
  - Scenario 1: If the edge device is single-homed (connected to only one intermediate node) and the intermediate node is deleted from the inventory, then the /31 point-to-point link IP address is deleted from Catalyst Center (IPAM) but may not be unconfigured from the edge device, which is still in the inventory. This is because the edge device can become unreachable from Catalyst Center due to the point-to-point interface between the intermediate node and the fabric border being unconfigured before the one on the edge device. In this case, log in to the edge device CLI and set the interface connected to the deleted device to default configuration. This avoids duplicate IP address assignment during LAN automation workflows later due to the released IP addresses still being present on the device. You can later use the LAN automation workflow to add a new link from the edge device to the new intermediate node or border node (as required) instead of manually configuring the IP addresses.

- Scenario 2: If the edge device is dual-homed (connected to two intermediate nodes) and one of the intermediate nodes is deleted from the inventory, then the /31 point-to-point link IP address is deleted from Catalyst Center (IPAM) and is unconfigured from the edge device as well. There is no manual configuration required on the edge devices.

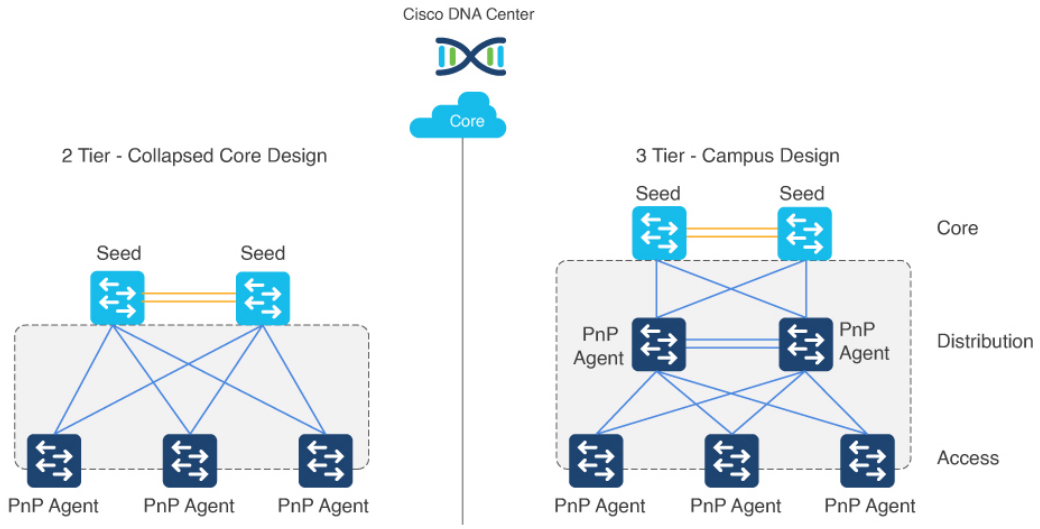
Catalyst Center 2.3.5 and later provide the support for day-*n* link configurations (add and delete link). For more information, see Create Link Between Interfaces, on page 60.

Constraints

- LAN automation does not automate the onboarding of a StackWise Virtual (SVL) switch via PnP. SVL switch can only be used as a seed device.
- LAN automation does not support stack renumbering.
- For platform support, see Supported Switches for Each Role at Different Layers, on page 11.

Supported Switches for Each Role at Different Layers

The following figure shows supported device families for the seed and PnP agent at different layers.



Layer	Role	Supported Switch Series
Distribution	Seed	Catalyst 3850, 9200, 9400, 9500, 9600
Access	PnP Agent	Catalyst 3850, 9200, 9300, 9400, 9500, 9600

Layer	Role	Supported Switch Series
Core	Seed	Catalyst 3850, 9200, 9300, 9400, 9500, 9600
Distribution	Pnp Agent	Catalyst 3850, 9200, 9300, 9500, 9600
Access	PnP Agent	Catalyst 3850, 9200, 9300, 9400, 9500, 9600

Cisco LAN Automation Product Support Matrix

Role[1]	Product Model[2]	Network Module[3]
Seed PnP agent	C9606R C9600-SUP-1 C9600-SUP-1/2 C9600X-SUP-2	Seed: any uplinks and module ports are supported PnP agent: 100G interfaces are not supported
Seed PnP agent	C9500-32C C9500-32QC C9500-24Y4C C9500-48Y4C C9500X-28C8D	—
Seed PnP agent	C9500-12Q C9500-24Q C9500-40X C9500-16X	Any front-panel ports[4]
Seed PnP agent	C9404R C9407R C9410R	Sup-1[5] Sup-1XL[3] Sup-1XL-Y[3] Any line card
Seed PnP agent	C9400-SUP-1 C9400-SUP-1XL C9400-SUP-1XL-Y C9400X-SUP-2XL C9400X-SUP-2	—

Role[1]	Product Model[2]	Network Module[3]
Seed PnP agent	C9300-24S C9300-24T C9300-24P C9300-24U C9300-24H C9300-48S C9300-48T C9300-48P C9300-48U C9300-48H C9300-24UX C9300-24UXB C9300-24UB C9300-48UXM C9300-48UN C9300-48UB C9300L-48UXG C9300L-24UXG C9300L-24P C9300L-48P C9300L-48T C9300L-24T C9300LM-48UX-4Y C9300LM-48U-4Y C9300LM-24U-4Y C9300LM-48T-4Y C9300X-12Y C9300X-24Y C9300X-24HX C9300X-48HXN C9300X-48HX C9300X-48TX	Any uplinks and module ports

Role[1]	Product Model[2]	Network Module[3]
Seed PnP agent	C9200-24T C9200-24P C9200-24PB C9200-48T C9200-48P C9200-48PB C9200-48PL C9200-24PXG C9200-48PXG C9200L-24T C9200L-24P C9200L-48T C9200L-48P C9200L-48PL C9200L-24PXG C9200L-48PXG C9200CX-12T-2X2G C9200CX-12P-2X2G C9200CX-8P-2X2G	Any uplinks and module ports
Seed PnP agent	WS-C3850-24T WS-C3850-48T WS-C3850-24P WS-C3850-48P WS-C3850-48F WS-C3850-24U WS-C3850-48U WS-C3850-24XU WS-C3850-12X48U WS-C3850-12S WS-C3850-24S WS-C3850-12XS WS-C3850-24XS WS-C3850-48XS	Any uplinks and module ports

[1] Catalyst Center 2.1.2 and later supports configuring C9400, C9500, or C9600 StackWise Virtual (SVL) switches as a seed for LAN automation. LAN automation does not automate the onboarding of a StackWise Virtual switch via PnP. StackWise Virtual switch can only be used as a seed device.

[2] LAN automation is supported only on the products or platforms listed here. For the supported Cisco IOS XE and Catalyst Center versions, see *Cisco Catalyst Center Compatibility Matrix*.

[3] LAN automation does not support a dedicated management port. For C9500H and C9600 switches, the convertible ports can only be used in seed device. The convertible ports do not come up when the switches are used as PnP device.

[4] Breakout cable support is available only on the seed devices. For discovered devices, LAN automation does not support a breakout cable, because it requires some extra configurations that will stop the PnP agent on the factory-default devices.

[5] The 40-G uplink is supported on 16.11.1 and later.

Site Planning

Use the Catalyst Center Design application to create the required sites, buildings, and floors. Consider how the primary seed and peer seed will be connected to the new devices—for example, will they all belong to the same site or follow a hierarchy? Consider also how to share IP pools across different sites, buildings, and floors. One option is to have a pool specific to a site. Another option is to share a common LAN pool for all sites in the hierarchy. If the devices are onboarded across multiple LAN automation sessions, ensure that the required IP pools are available across the various sites in the hierarchy.

Note After devices are provisioned, the site cannot be changed. For this reason, we recommend that you complete LAN automation before you provision devices.

IP Pool Planning

IP pools for LAN automation are created by first creating a global pool in Catalyst Center, followed by a site-specific LAN IP pool, which LAN automation allocates internally, as follows:

1. One part of the IP pool is reserved for a temporary DHCP server. The size of this pool depends on the size of the parent LAN pool. For example, if the parent pool is 192.168.10.0/24, a subpool of size /26 is allocated for the DHCP server. If the pool size is larger than /24, the algorithm keeps increasing the size of the DHCP pool, up to a maximum of a /23 subpool (512 IP addresses). Therefore, a /24 pool reserves 64; a /23 pool reserves 128; a /22 pool reserves 256; and anything larger reserves 512 IP addresses for the DHCP server. The minimum pool size to start LAN automation is /25; that reserves /27 or 32 IP addresses for the DHCP pool. This IP pool is reserved temporarily for the duration of the LAN automation discovery session. After the LAN automation discovery session completes, the DHCP pool is released, and the IPs are returned to the LAN pool. Because the DHCP pool is usually the largest contiguous segment of IPs required, the pool should have at least one such segment available. If the pool is too fragmented, it cannot allocate the DHCP pool and the LAN automation session ends with an IP pool allocation error.

2. Another part of the IP pool is reserved internally with a subpool size of /27. This subpool is for allocating single IPs for Loopback0 and Loopback60000 always. Also, two consecutive IPs for point-to-point L3 links are allocated from this subpool if no separate overlapping IP pool is provided. This internally reserved subpool is used throughout the LAN automation sessions for providing IPs as long as it has IPs available. In case the IPs are exhausted, a new /27 subpool is created and IPs are allocated from that subpool. These subpools are released only when all the allocated IPs are released as part of the devices being deleted from Catalyst Center. Otherwise, the subpools remain throughout the process and are not allowed to be removed. Due to this internal subpool allocation logic, the IP pool usage in IPAM counts the subpools instead of the actual IPs allocated to the devices.

3. If a shared or link overlapping IP pool is provided for the point-to-point L3 links, then the subpool of size /27 is reserved internally from the shared pool instead of the main IP pool. The subpools are automatically deleted when all the allocated IPs from the pool are released.

When a dedicated (single) IP pool is used to build the underlay networks, each of the devices discovered via LAN automation gets a unique /31 per interface for point-to-point connection, and a unique /32 for Loopback0 and the underlay multicast.

Link Overlapping IP Pool or shared IP pool is used to optimize the IPv4 addressing in the underlay network by allowing overlapping /31 IP addresses for a multisite deployment. Hosts in different sites can get duplicate IP addresses on the /31 links. The /31s in the underlay are not advertised outside of the fabric site and hence there is no need for them to be unique. However, the /32 loopback needs to be unique to every device, and should be advertised to the global routing table to identify the device in the entire network.

There are two valid roles that a LAN IP pool can have:

- **Link Overlapping IP Pool**: A pool with this role is optional for a LAN automation session. If provided, the allocation of IP addresses is only on the point-to-point L3 links.
- **Main IP Pool** (**Principal IP Address Pool** in Catalyst Center 2.3.5 and later) : A pool with this role is mandatory for every LAN automation session. This is the pool that is used for all management-related IP addressing such as loopbacks, multicast, and DHCP. If the **Link Overlapping IP Pool** is not provided, then the **Main IP Pool** is the default fallback pool for the L3 links IP addressing.

Note When the seed device for LAN automation session is in a different site than the discovered device site, then the same shared IP pool cannot be used with the same seed and different discovered device site. This is to avoid the allocation of duplicate IP to the same seed device.

IP Pool Usage Example

Imagine you want to LAN automate 10 devices using the same pool, where each device has one link to the primary seed and another link to the secondary.

Consider a 192.168.199.0/24 pool. When LAN automation starts, a /26 pool is reserved for the DHCP addresses. In this example, 192.168.199.1 to 192.168.199.63 are reserved and assigned to VLAN 1 for the 10 devices.

Next, a /27 pool is reserved for loopback addresses. If there is no shared IP pool, then this pool is used for point-to-point links as well. Because there are 10 devices with two links each, a total of 2*10*2 = 40 IP addresses are reserved for point-to-point links and 10 loopback addresses are reserved.

In total, 60 IP addresses are reserved for the 10 devices: 10 for each VLAN 1, 10 for each loopback, and 40 for the point-to-point links between devices and seeds.

After LAN automation stops, the VLAN 1 IP addresses are released back to the pool, and 90 addresses are allocated for the LAN automation session.

Note the following:

- The same IP pool can be used for multiple discovery sessions. For example, you can run one discovery session and discover the first set of devices. After discovery completes, you can provide the same IP pool for a subsequent LAN automation session. Similarly, you can choose one LAN pool for one discovery session and another LAN pool for a second discovery session.
- Every time you start LAN automation, it checks for 64 available IP addresses in the IP pool. If you decide to run LAN automation multiple times with the same pool, use at least a /24 pool. If you plan to LAN automate only once for the IP pool, a /25 pool suffices.
- Don't use an address pool that is in use elsewhere in the network, such as an address pool that belongs to the loopback or to other addresses configured on the device.

Site-Specific CLI and SNMP Configuration

To start LAN automation, a site-specific CLI and SNMPv2 read or SNMPv3 configuration is required. Use the Catalyst Center Design application to configure the site-specific CLI and SNMP. Save the configuration for the site that is used for LAN automation. If you configure the credentials at the global level, they are visible at the site level. You must click the radio button for the specific site and then save the configuration to make it available for LAN automation.

Note SNMPv2 write credentials are not required and if configured, it won't be pushed to the device during LAN automation.

Configuration on Seed Devices

When configuring the seed devices, follow these guidelines:

- The system maximum transmission unit (MTU) value must be at least 9100.
- Turn on IP routing on the seed devices.
- Set up routing between the seed service and Catalyst Center so that Catalyst Center has IP reachability to the LAN IP pool subnet.
- We recommend that you use the default interfaces connected to PnP agents. If the peer seed device has IP interfaces configured on the interfaces connected to PnP agents, those links don't get configured. If you want to configure the peer device interfaces connected to PnP agents, use the default interfaces and perform an inventory synchronization on the peer seed device. LAN automation works only when the ports are Layer 2. The ports on Cisco Catalyst 6000 are Layer 3 by default. Convert the ports to Layer 2 before starting LAN automation.
- Configure device credentials and SNMP credentials on the seed devices.
- If the seed devices have Layer 3 interfaces configured, ensure that there are no conflicts with any of the IP pools provided in Catalyst Center. Check the IP addresses which are configured manually.
- Ensure that the seed devices don't have any other interfaces connected to another DHCP server running in VLAN 1.
- If loopback is not configured on the seed devices, LAN automation configures loopback on the seed.
- If any configuration changes are made on the seed devices before running LAN automation, synchronize the seed devices with the Catalyst Center inventory.

- Assign the seed devices to a site. (You don't have to provision the seed devices for LAN automation.)

Additional recommended configurations on seed devices:

- **Run multiple discovery sessions for devices across sites connected to the same seed**: If you plan to run multiple discovery sessions to onboard devices across different buildings and floors connected to the same seed devices, we recommend that you block the ports for PnP agents that do not participate in the upcoming discovery session.

  For example, imagine that seed devices are in Building-23 and are connected to PnP agents on Floor-1 and Floor-2. Floor-1 devices are connected on interfaces Gig 1/0/10 through Gig 1/0/15. Floor-2 devices are connected on interfaces Gig 1/0/16 through Gig 1/0/20. For the discovery session on Floor-1, we recommend that you shut down ports connected to Gig 1/0/16 to Gig 1/0/20. Otherwise, the PnP agents connected to Floor-2 might also get DHCP IPs from the server running on the primary seed device. Because these interfaces aren't selected for the discovery session, they remain as stale entries in the PnP database. When you run the discovery session for Floor-2, the discovery doesn't function correctly until these devices are deleted from the PnP application and write erase/reloaded. Therefore, we recommend that you shut down other discovery interfaces.

- **Endpoint/client integration**: For Catalyst Center 1.2.8 and earlier, if there are clients connected to a switch that is being discovered, those clients contend for DHCP IP and might exhaust the pool, causing LAN automation to fail. Therefore, we recommend that you connect the client after LAN automation is complete.

  This endpoint/client integration restriction does not apply to Catalyst Center 1.2.10 and later. Clients can remain connected while the switch is undergoing LAN automation.

PnP Agent Initial State

Ensure that the device that you want to LAN automate is running the Advantage license level. Otherwise, some commands are not pushed.

Note Catalyst Center 2.3.5 and later support automatic license upgrade for C9000 and C3850 series switches.

New PnP agents have factory defaults and are ready to start LAN automation.

If you are reusing existing network devices, ensure the following:

- PnP agents must have the required license that allow you to push the LISP, IS-IS routing, and CTS-related CLI commands. Use the **show license** command to see the current license level. If required, upgrade the license.
- PnP agents should not have stale certificate or keys from the previous runs.
- Restore the switch configurations to factory default using the following commands:
  - For Cisco IOS XE 16.11 and earlier, use:

```
[CLI config mode]

    no pnp profile pnp-zero-touch
    no crypto pki certificate pool
    Also remove any other crypto certs shown by "show run | inc crypto"
    crypto key zeroize
    config-register 0x2102 or 0x0102 (if not already)
    do write
    end

[CLI exec mode]

    delete /force nvram:*.cer
    delete /force stby-nvram:*.cer (if a stack)
```

```
delete /force flash:pnp-reset-config.cfg
write erase
reload (enter no if asked to save)
```

- For Cisco IOS XE 16.12.x or later, use:

```
[CLI exec mode]

pnp service reset no-prompt
```

Step 2: Design

The design phase is the second step in LAN automation. During the design phase, you:

1. Design and build global sites.
2. Configure global and local network services.
3. Configure global device credentials.
4. Design the global IP address pool and assign the LAN automation pool for the required site from the global pool.

Design and Build a Site

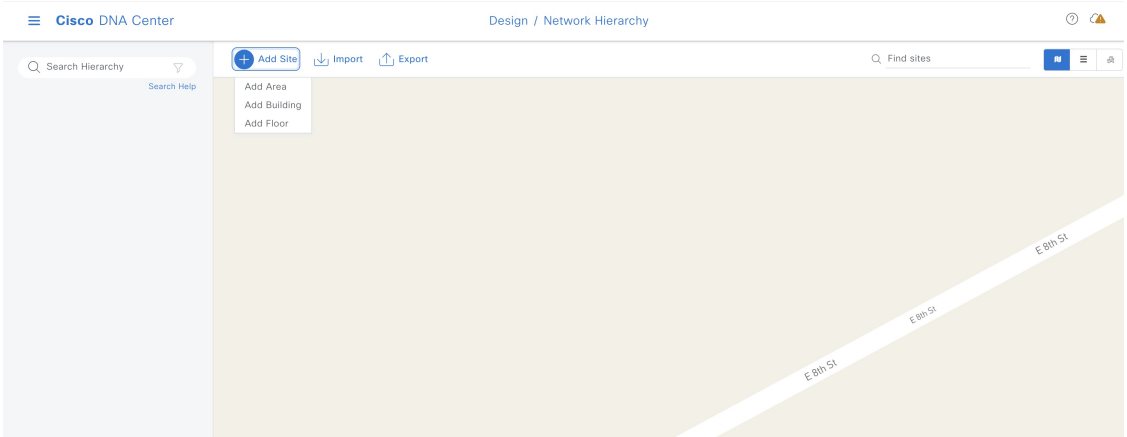
This section explains how to design and build a site.

Procedure

Step 1 From the Catalyst Center home page, click the menu icon and choose **Design** > **Network Hierarchy**.

Step 2 Create a site and add buildings and floors.

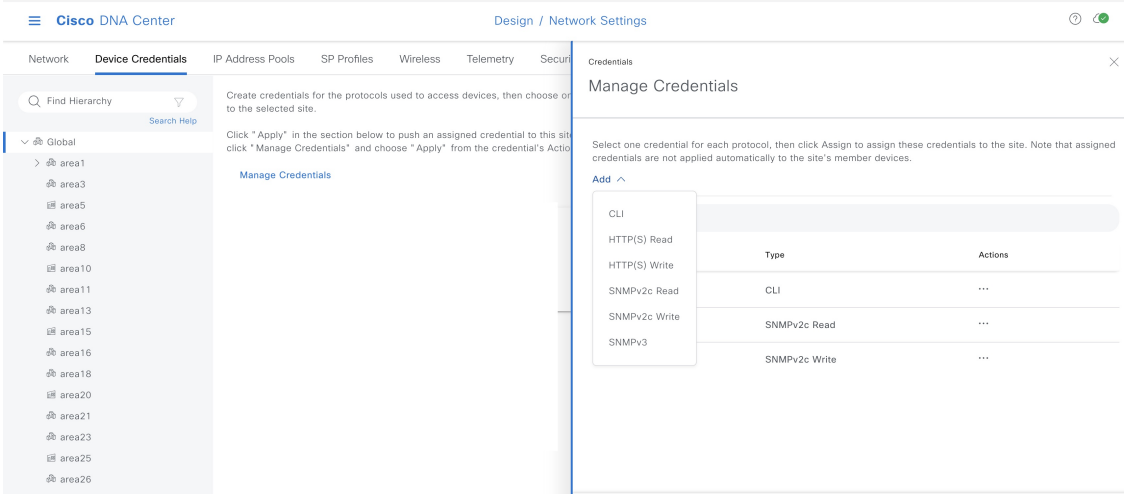
- To create a site, choose **+ Add Site** > **Add Area**.
- To add a building, choose **+ Add Site** > **Add Building**.
- To add a floor, choose **+ Add Site** > **Add Floor**.



Step 3 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Device Credentials**.

Step 4 Click **Manage Credentials** and add the following credentials:

- **CLI**
- **SNMPV2C Read**



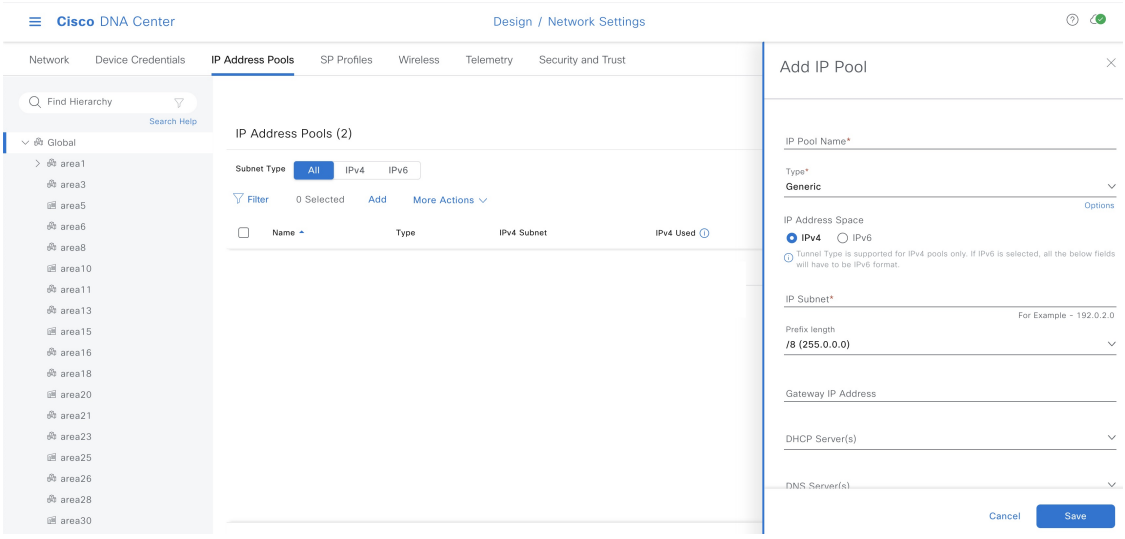
Note If you want to use the same device credentials for all sites, click **Global** in the left navigation tree and set the credentials.

Do not use `cisco` as the username.

Step 5 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **IP Address Pools**.

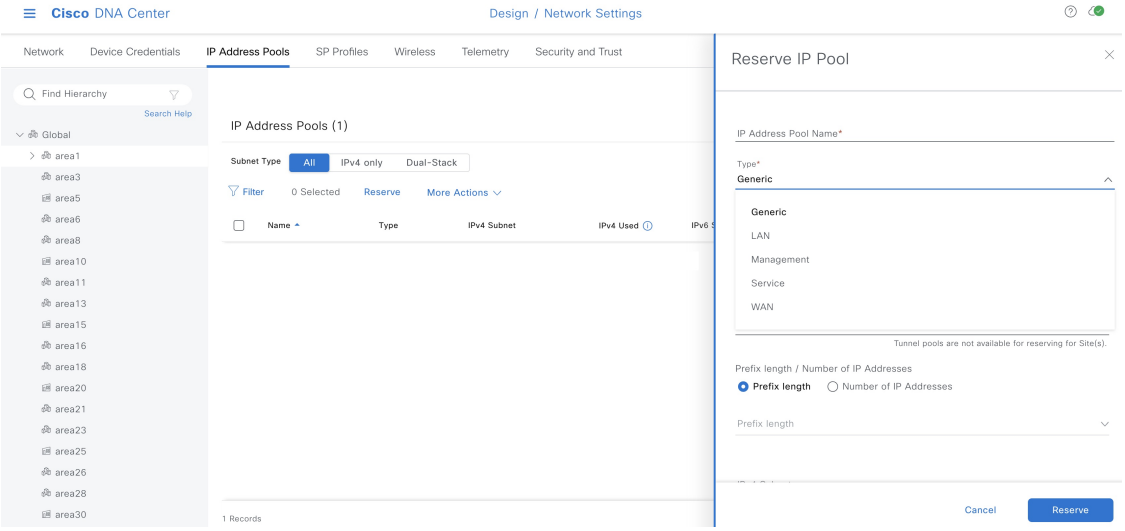
Step 6 From the left hierarchy tree, choose **Global** and click **Add**.

Create a dedicated IP address pool to use for the underlay infrastructure. Do not use an address pool that is already in use in the network. For example, do not use an address pool that belongs to a loopback or other addresses configured on the device.



Step 7 From the left hierarchy tree, choose a site and click **Reserve**.

Step 8 In the **Reserve IP Pool** window, from the **Type** drop-down list, choose **LAN**.



Step 3: Discover

Device discovery is the third step in successfully building the underlay network.

Before creating and running a discovery profile, review the underlay configuration of the seed device.

Create Discovery Profile

This section explains how to create a discovery profile.

Procedure

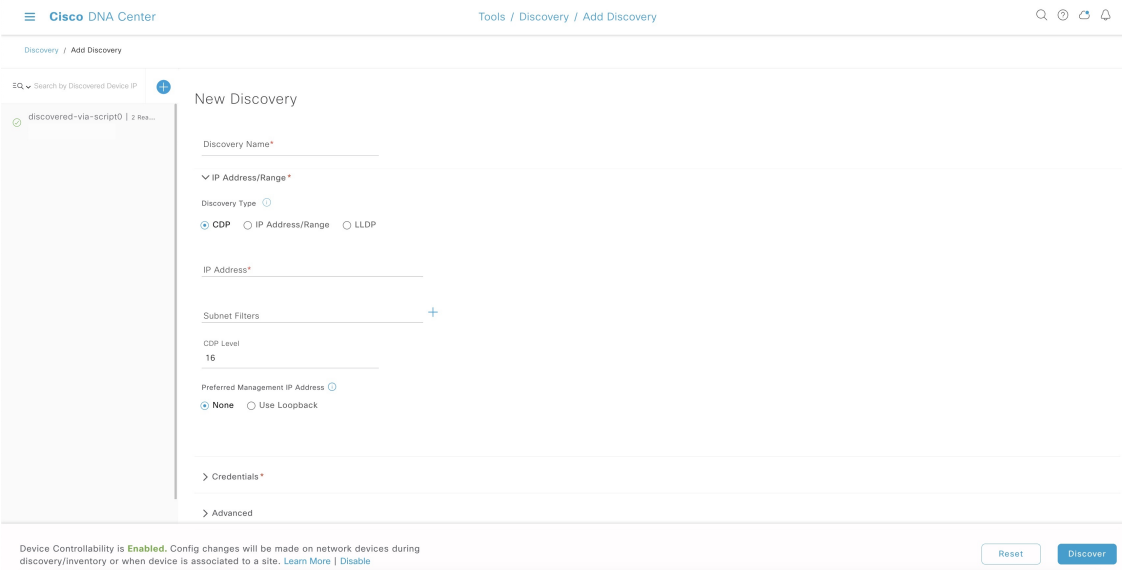
Step 1 From the Catalyst Center home page, click the menu icon and choose **Tools** > **Discovery**.

Step 2 In the **Discovery** window, click **Add Discovery**.

Step 3 In the **New Discovery**window, enter the following details:

- **Discovery Name**: Name of the discovery profile.
- **IP Address/Range**: The IP address can be any Layer 3 interface or loopback on any switch that Catalyst Center can access. If you are discovering the primary and peer seeds together, enter an IP range. Click the appropriate radio button and enter the details accordingly.
- **Credentials**: Enable at least one CLI and one SNMP credential. Click **Add Credentials** to add the credentials.
- **Advanced**: Specify one or more protocols for the discovery scan to use. Choose **SSH** and/or **Telnet**.

  Note If you choose SSH, ensure that the seed is configured for SSH.

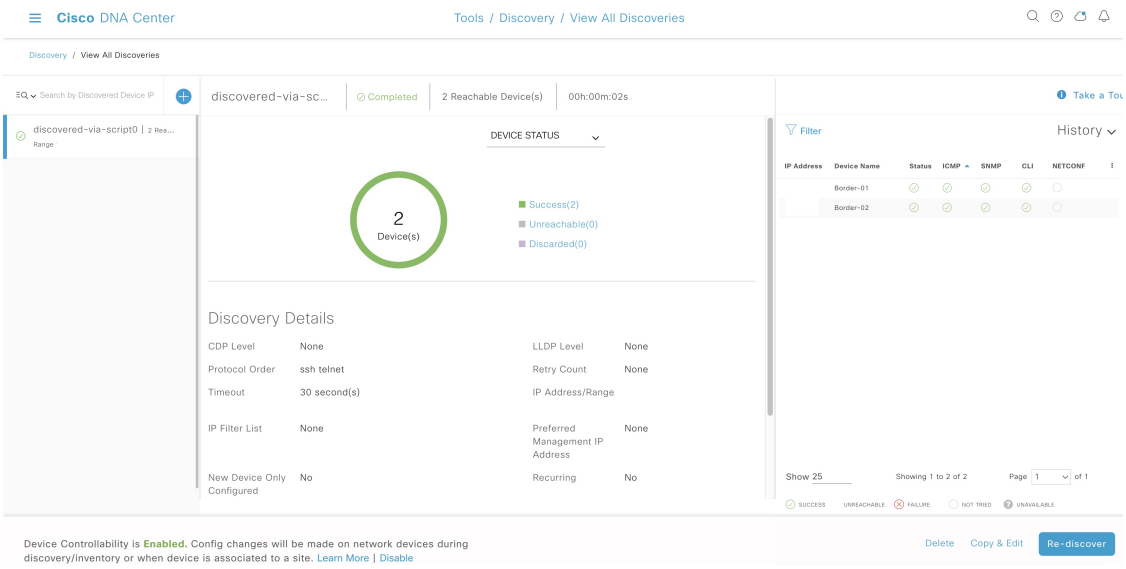


Step 4 Click **Discover**.

Step 5 Choose a discovery schedule and click **Start**.

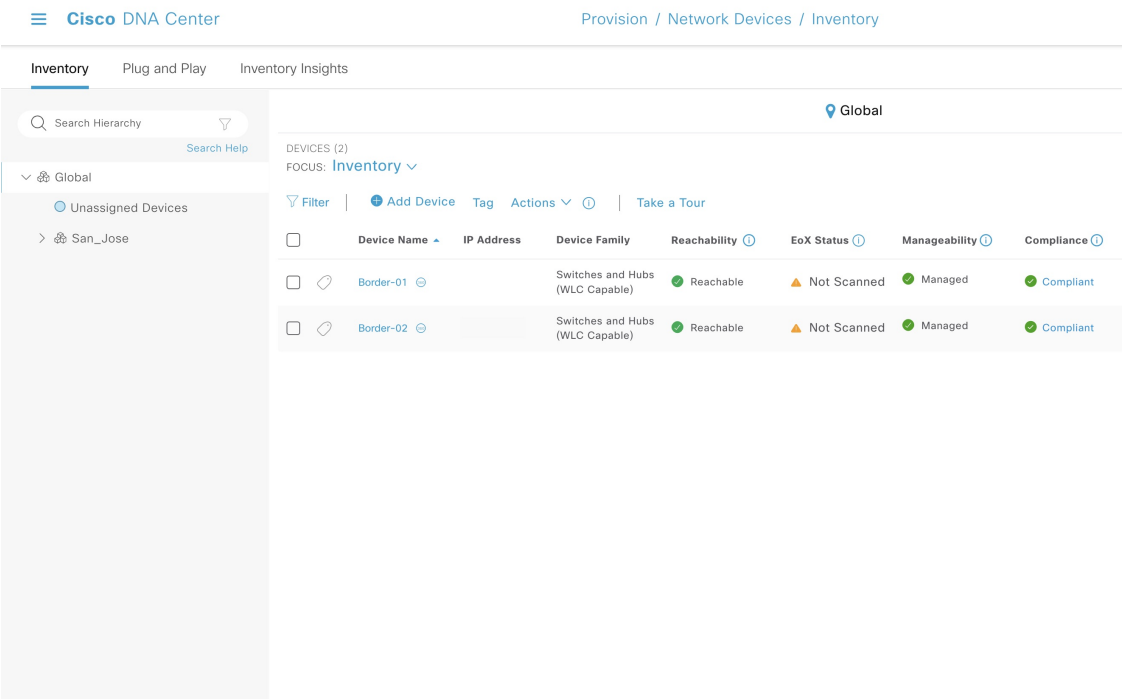
You can view the status and results of the scan in the **Discoveries** window.

Note The discovery process takes some time. Ensure that there are no failures after the process completes.

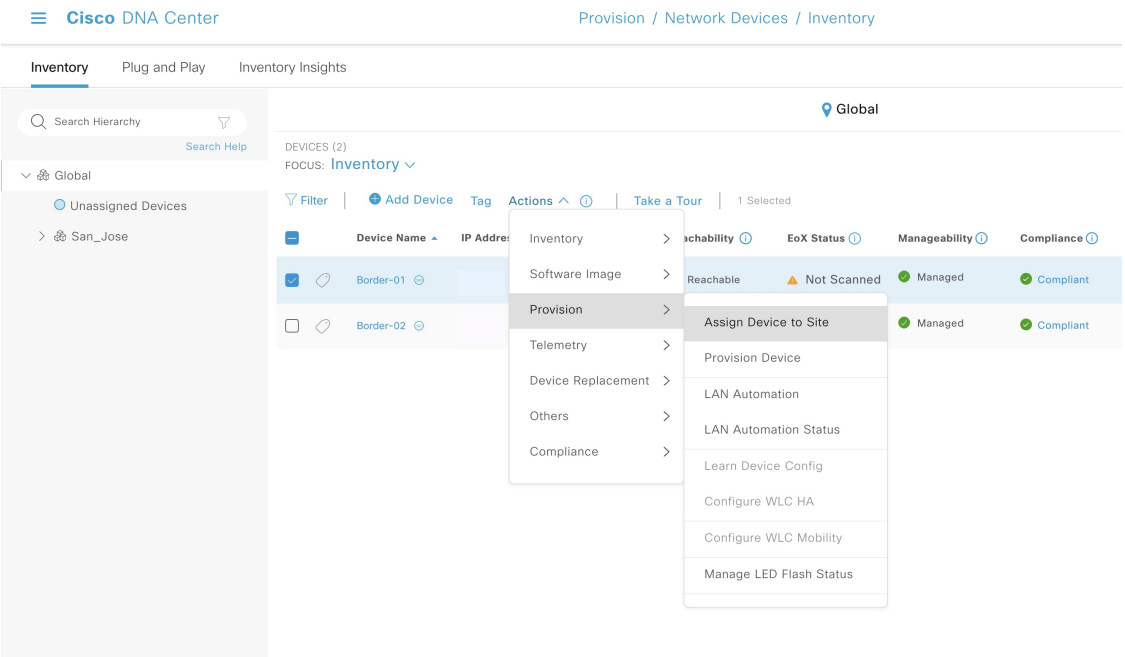


Step 6 To verify that the discovered device is added to the inventory, click the menu icon and choose **Provision** > **Inventory**.

Note Make sure that the discovered device's **Reachability** status is *Reachable* and **Manageability** status is *Managed*.



Step 7 To assign the device to site from inventory, select the device and from the **Actions** menu, choose **Provision** > **Assign Device to Site**.

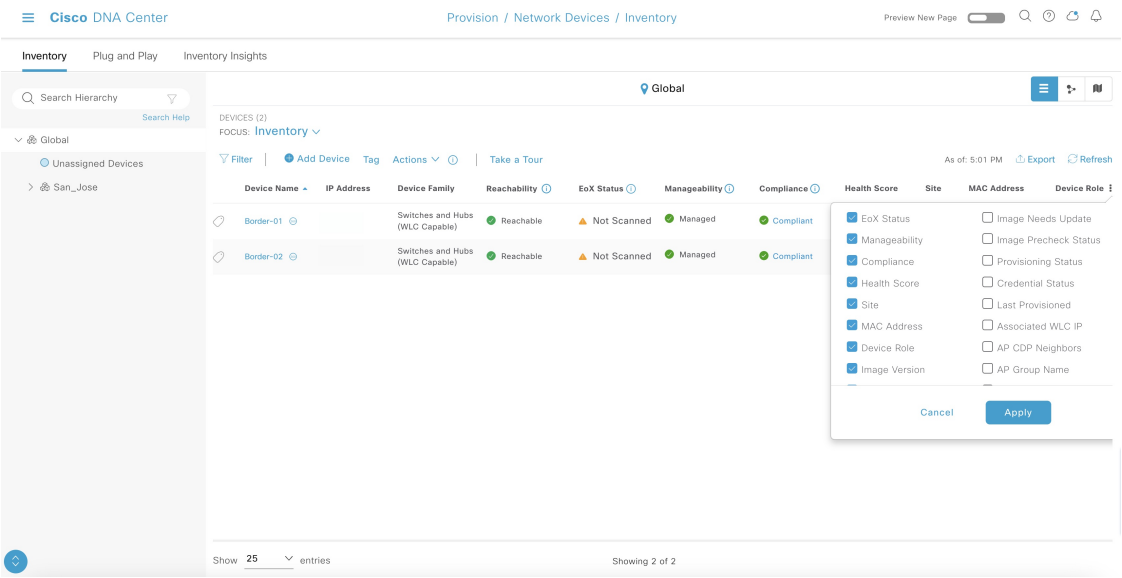


Step 8 In the **Assign Device to Site** window, choose a site and click **Apply**.

For Catalyst Center 1.2.6 and earlier, ensure that both the primary and peer seeds are in the same site and same floor (although they can be physically on different floors).

The discovered device is added to the selected site.

Note If you don't see the **Site** column in the **Inventory** window, click ⋮, check the **Site** check box, and click **Apply**.



Steps to Consider Before Starting LAN Automation

Take the following considerations into account before starting the LAN automation process.

IP Pool Subnet Reachability from Catalyst Center

LAN automation discovery uses the LAN pool to reach PnP agents. Catalyst Center should be able to reach the IPs allocated from the LAN pool. For example, if the LAN pool is 192.168.10.0, Catalyst Center should have the correct route to reach this subnet. To test the reachability, create an SVI (VLAN 1 interface) on the primary seed device and do a ping test between Catalyst Center and the seed. Refer to the following sample code.

```
[On seed device]

Switch(config)#interface vlan1
Switch(config-if)#ip address 192.168.99.1 255.255.255.0
Switch(config-if)#end

[On Catalyst Center CLI console]

[Sat Jun 23 05:55:18 UTC] maglev@10.195.192.157
$ ping 192.168.99.1
PING 192.168.99.1 (192.168.99.1) 56(84) bytes of data.
64 bytes from 192.168.99.1: icmp_seq=1 ttl=252 time=0.579 ms
64 bytes from 192.168.99.1: icmp_seq=2 ttl=252 time=0.684 ms
64 bytes from 192.168.99.1: icmp_seq=3 ttl=252 time=0.541 ms

[On seed device]

Switch(config)#default int vlan 1
Interface Vlan1 set to default configuration
```

If the ping test fails, the route is not set up correctly on Catalyst Center.

Static Route Addition for LAN Pool

Catalyst Center hardware has multiple physical interfaces with each serving different categories of communication. See the *Cisco Digital Network Architecture Center Appliance Installation Guide* for recommended interface connections, IP routing, and static assignment. In a single-home design, Catalyst Center performs the host function with the default gateway providing IP routing. In a multi-home design, Catalyst Center must have a static route to the LAN automation networks via the enterprise-facing interface.

Figure 1: IP Addressing for Single-Home and Multi-Home Designs

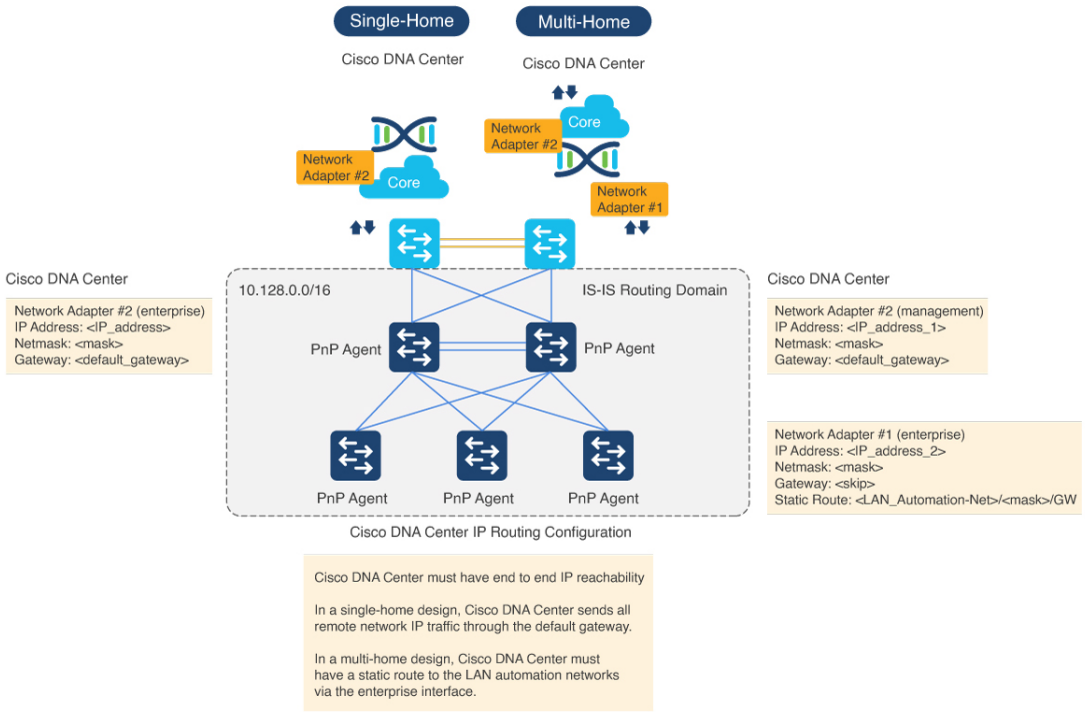
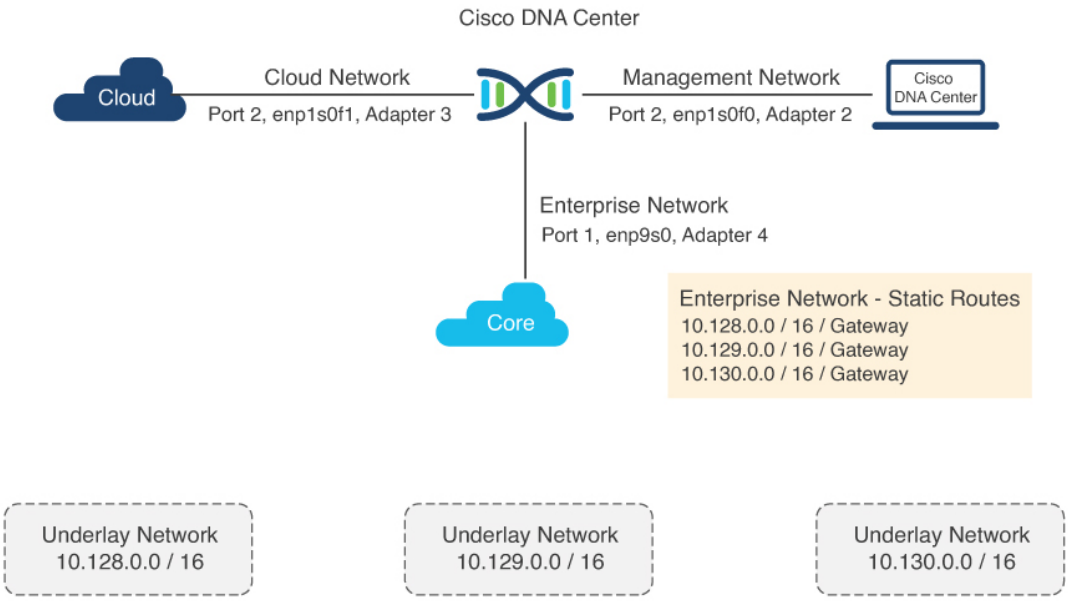


Figure 2: Static IP Routing Design



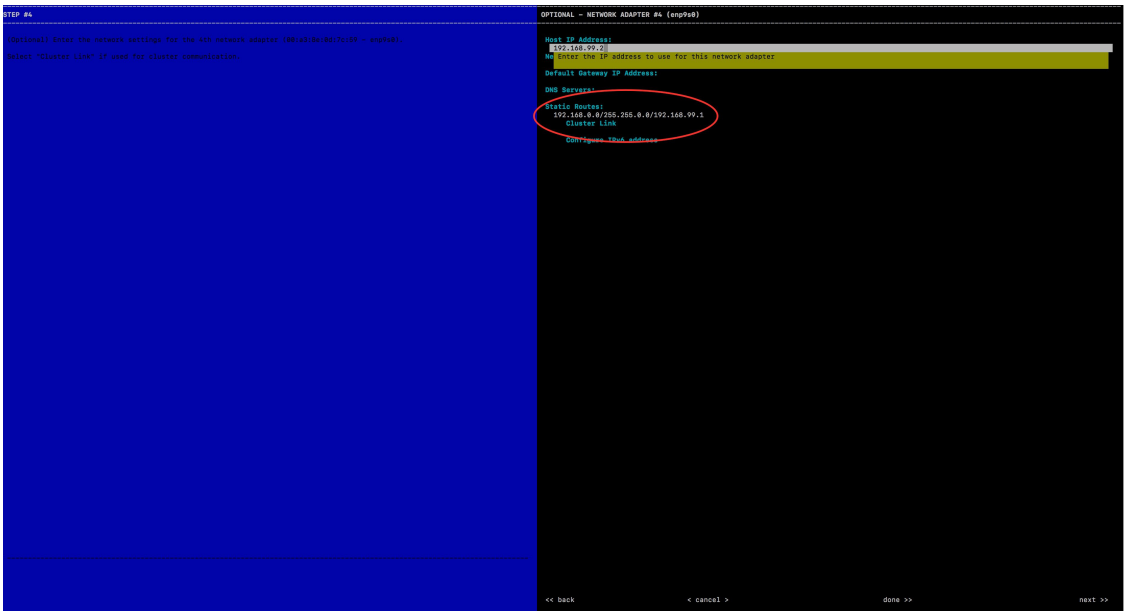
If the network design is a multi-home design, one way to fix the IP reachability issue is to add a static route on Catalyst Center. A network administrator can add a static route during the initial Catalyst Center configuration or later via a maglev command. (Don't use the Linux `route` command, because maglev APIs don't pick the correct information if the route is modified using the `route` command.)

For a single-home design, check the routing between the seed and Catalyst Center.

To add a static route on Catalyst Center:

Procedure

Step 1 On the Catalyst Center console, enter the command `sudo maglev-config update`. The config wizard opens.



Step 2 Enter the static route and click **Next**. The config wizard validates and configures host networking.

Step 3 Ensure that the correct interface is selected to add the static route. Otherwise, click **Next** until the correct interface is displayed on which to configure the route.

Step 4 Leave the **Network Proxy** field blank. When the proxy validation fails, skip the proxy settings.

Step 5 Click **Proceed** to apply the changes to the controller.
It takes from 5 to 6 minutes to add a static route. You can ignore any warning messages.

PnP Agent Initial State Before Starting LAN Automation

Procedure

Step 1 Before starting LAN automation, make sure that the PnP agent is in **System Configuration Dialog** state.

```
FIPS: Flash Key Check : Key Not Found, FIPS Mode Not Enabled
cisco C9300-24T (X86) processor with 1418286K/6147K bytes of memory.
Processor board ID FCW2137G032
2048K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:.
11264000K bytes of Flash at flash:.
0K bytes of WebUI ODM Files at webui:.

Base Ethernet MAC Address          : f8:7b:20:48:d8:80
Motherboard Assembly Number        : 73-17952-06
Motherboard Serial Number          : FOC21354B06
Model Revision Number              : A0
Motherboard Revision Number        : A0
Model Number                       : C9300-24T
System Serial Number               : FCW2137G032


%INIT: waited 0 seconds for NVRAM to be available
```

```
        --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
```

Step 2 Do not press **Yes** or **No**. Leave the device in the same state.

Note If the device does not stop at this initial prompt and moves ahead, check the device config-register value using the CLI command `show ver | inc register`. In some cases, the value might be *0x142*. Change the config-register value to *0x102* or *0x2102* and save the configuration. Check the CLI again; it shows *Configuration register is 0x142 (will be 0x102 at next reload)*.

If the device comes up with the older config-register value even after changing the value to 0x102 or 0x2102 and reloading the device, configure `no system ignore startupconfig switch all` on the device, save the configuration, and reload.

For Cisco Catalyst 9000 series switches, use `pnp service reset no-prompt`.

Stack Considerations

- Follow the same procedure for the stack. Allow extra time to make sure that all members in the stack are up. Do not start LAN automation until all switches are up.
- LAN automation is always initiated on the active switch. When all switches in a stack are booted together, the switch with the lowest MAC address (assuming no switch priority is configured) becomes active. The second lowest switch becomes the standby, and so on. Some customers require that the first switch is always active. In this case, if all switches are booted together and the first switch does not have the lowest MAC address, it does not become the active. To ensure that the first switch is the active, boot the switches in a staggered manner. That is, boot switch 1. After 120 seconds, boot switch 2, and so on. This ensures that the switch becomes active in the correct order: switch 1 is active, switch 2 is standby, and so on. However, when you reload, the order is not maintained and the switches obtain their role depending on their MAC address.
- To make sure that the switches maintain their order after reload, it is a good practice to assign switch priorities to ensure that the switches always come up in the same order. The highest priority is 15. When priorities are assigned, they take preference over the switch MAC address. Assigning switch priorities does not change the NVRAM configuration. The values are written to ROMMON and persist after reload or write erase. As an example, see the following sample code.

  ```
  3850_edge_2#switch 1 priority ?
    <1-15>  Switch Priority
  3850_edge_2#switch 1 priority 14
  WARNING: Changing the switch priority may result in a configuration change for that switch. Do
  you want to continue?[y/n]? [yes]: y
  ```

  You might have to clean up the switch after assigning priorities, because some certificates will have been configured on the switch during boot up. To clean up the switch, see PnP Agent Initial State.

Note Do not start LAN automation until all switches in the stack are up.

If you are consoled in to the standby/member switches, do not press Enter, even though the screen says *console is now available, Press RETURN to get started*. Monitor the active switch, which should be at the **System Configuration Dialog** state.

If LAN automation is already running and you don't want to stop it, shut the seed link connecting to the PnP agent. That way, discovery doesn't occur until you are ready to bring up the link.

Unplug the Management Port

Connect PnP agents directly to seed devices. Do not connect PnP agents to any other network (for example, the management network) or any network that can provide DHCP through another server on VLAN 1.

Ensure That Seed Ports Are Layer 2

Ensure that the seed ports connected to the PnP agents are Layer 2 and defaulted. For example, Cisco Catalyst 6500 and 9500H ports are Layer 3 by default.

Ensure That Primary Seed Port Does Not Block STP

Ensure that the port on the primary seed connecting to the PnP agents does not block STP.

Ensure That the Device Is Not Present in Inventory

This section applies to devices that were discovered or LAN automated at any point.

If the devices to discover in an upcoming LAN automation session are already present in the inventory, complete the following steps to remove them from the inventory.

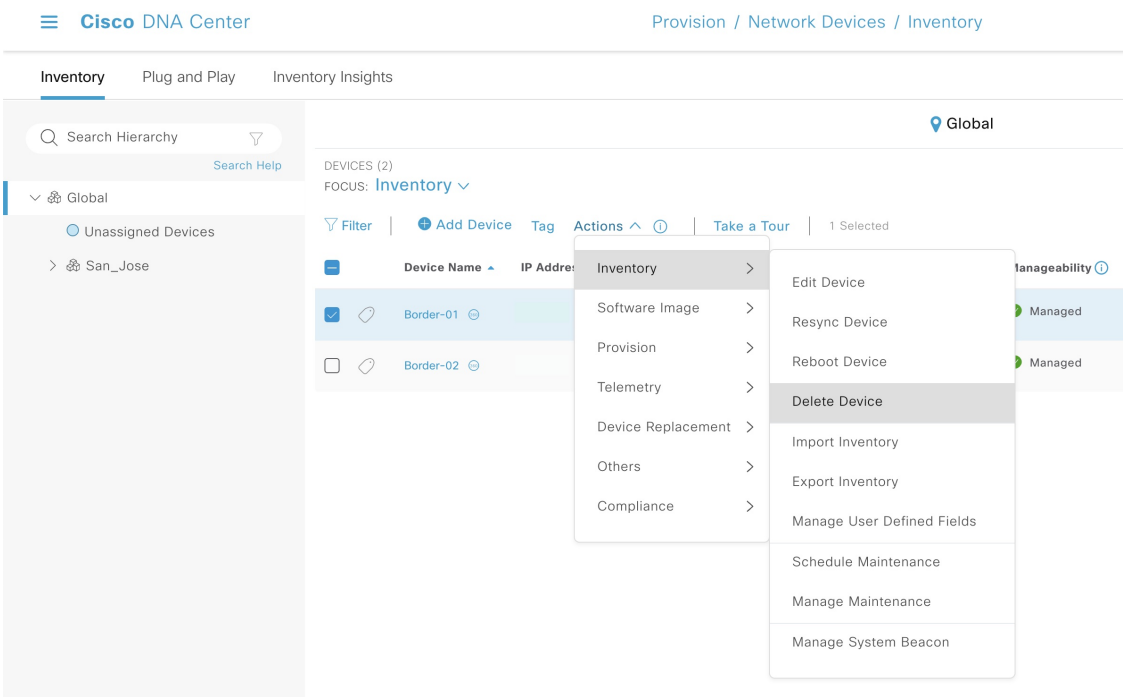
Before you begin

If a device was provisioned and added to the fabric, remove it from the fabric and unprovision it before you remove it from the inventory.

Procedure

Step 1 From the Catalyst Center home page, click the menu icon and choose **Provision** > **Inventory**.

Step 2 Filter the devices by **Serial Number** and then from the **Actions** drop-down list, choose **Inventory** > **Delete Device**.



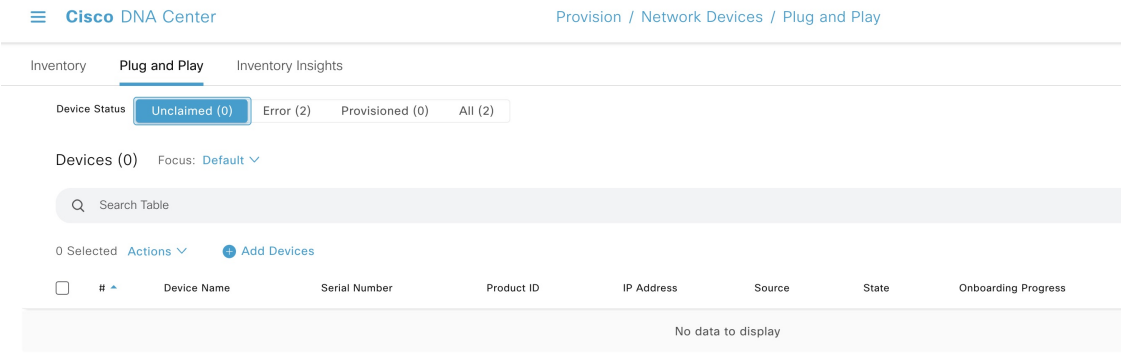
Ensure That the Device Is Not Present in PnP

If the devices to discover in an upcoming LAN automation session are already available in PnP, complete the following steps to remove them from PnP before you run the discovery. Otherwise, the discovery won't work correctly.

Procedure

Step 1 From the Catalyst Center home page, click the menu icon and choose **Provision** > **Plug and Play**.

Step 2 From the **Device Status** filter, choose **Unclaimed**. Make sure that the device (**Serial Number**) being discovered is not available under **Unclaimed**.



Step 3 If the device is available, console into the device and remove the PnP profile:

```
[on PNP agent]

3850_edge_2#show run | sec pnp-zero-touch
pnp profile pnp-zero-touch
 transport https ipv4 192.168.99.2 port 443

3850_edge_2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
3850_edge_2(config)#no pnp profile pnp-zero-touch
3850_edge_2
```

For Cisco IOS XE 16.12.x or later, use:

```
pnp service reset no-prompt
```

Step 4 Check the check box of the device in the **Unclaimed** section and choose **Actions** > **Delete**.

Use the Advantage License

Ensure that the PNP agent is running the Advantage license level.

Ensure That the PNP Agent is in INSTALL Mode

For the image upgrade to occur during LAN automation, the PnP agent must be in INSTALL mode.

Image upgrade through LAN automation occurs in the background.

Procedure

Step 1 After PnP discovers the device, Catalyst Center checks whether any golden image is marked for the switch family (Cisco Catalyst 9300 or 3850) of the discovered device. To check whether a golden image is selected, choose **Design** > **Image Repository**.

If the golden image is marked and the discovered device is not running the golden image, LAN automation upgrades the discovered device to the golden image. If not, Catalyst Center skips the image upgrade and proceeds to pushing the initial device configuration.

Step 2 If you want LAN automation to upgrade the image on the discovered device, ensure that the device is running in INSTALL mode. Image upgrade through LAN automation does not occur if the device is in BUNDLE mode.

Step 3 If the device is in BUNDLE mode and you want to proceed with LAN automation, remove the golden image for that particular switch family **Design** > **Image Repository**.

Step 4: Provision

Provisioning is the final step in the LAN automation process. It is divided into two stages:

1. Device discovery and onboarding (starting LAN automation).

   When LAN automation starts, it:

   - Pushes the loopback and IS-IS configuration to the primary and peer seed devices and the temporary configuration to the primary seed device, enabling discovery and onboarding of the PnP agent.

Note Catalyst Center 2.3.3 and later support `is-type level-2-only` as part of IS-IS configurations.

- Discovers new devices.
- Upgrades the image and pushes the configuration to discovered devices.

Note The image is updated only if a golden image is marked for that switch type under the Catalyst Center home page > **Design** > **Image repository**.

When LAN automation starts, the temporary configuration is pushed to the primary seed device, which discovers and onboards the PNP agent. Next, the PNP agent image is upgraded and basic configurations such as loopback address, system MTU, and IP routing are pushed to the PNP agent.

2. Interface configuration (stopping LAN automation).

   When LAN automation stops:

   - The discovery phase ends and all point-to-point links between the seed and discovered devices and between the discovered devices (a maximum of two hops) are converted to Layer 3.
   - All temporary DHCP and VLAN 1 configurations on the seed and discovered devices are removed. The DHCP subpool is returned to the LAN automation pool.

Start LAN Automation

For LAN automation, you must select the primary seed device, peer seed device, site for seed device, LAN IP pool, and interface. Optionally, you can select the device prefix, hostname CSV file, configurable IS-IS password, and so on.

Interface Selection

Interfaces on the primary seed device participate in the new device discovery and L3 configuration. The interfaces on seed devices provide a filter to directly connect PnP agents that can be onboarded through the LAN automation session. For example, consider four directly connected PnP agents: device-1 through Gig1/0/10, device-2 through Gig 1/0/11, device-3 through Gig 1/0/12, and device-4 through Gig 1/0/13. If you choose Gig 1/0/11 and Gig 1/0/12 as part of the discovery interfaces, LAN automation discovers only device-1 and device-2. If device-3 and device-4 also try to initiate the PnP flow, they are filtered, because they are connected through interfaces that are not selected during the LAN automation session. This mechanism lets you restrict the discovery process.

Interface selection also lets you choose interfaces between the primary seed and the peer seed to configure with Layer 3 links. If there are multiple interfaces between the primary and peer seeds, you can choose to configure any set of these interfaces with Layer 3 links. If no interfaces are chosen, they aren't configured with Layer 3 links.

The option to choose a peer seed interface is not available. Interfaces between peer seed and PnP agents are automatically inferred based on the topology information gathered from the device. The topology information is built on the CDP information available on the device.

Site Selection

Sites can be selected for seed devices and PnP agents. Currently, there is one site for seed device(s) and one site for PnP agents.

LAN Pool Selection

The LAN pool is selected based on PnP agent site information. To start LAN automation, select a LAN pool from the list of LAN pools available for a particular site. You can select the same LAN pool for multiple LAN automation sessions. For example, you can run one discovery session and discover the first set of devices. After the discovery session completes, you can provide the same IP pool for subsequent LAN automation sessions. Similarly, you can select a different LAN pool for different discovery sessions. Make sure that you select a LAN pool with enough remaining capacity.

IS-IS Password

- If you enter a value, enter the same password that is configured on the seed. If you enter a value that is different from the password configured on the primary and peer seeds, an error is returned.
- If the password on the primary and peer seeds does not match, an error is returned.

If you enter a value in the IS-IS Password field:

- If the primary seed has an IS-IS password configured, LAN automation configures the primary seed's IS-IS password on the PnP devices (and on the peer seed, if it doesn't already have the password).
- If the primary seed doesn't have an IS-IS password but the peer does, LAN automation configures the peer seed's IS-IS password on the PnP devices and on the primary seed.
- If the primary and peer seeds don't have an IS-IS password configured and you enter a value in the password field, LAN automation configures the user-entered password on the PnP devices and on the primary and peer seeds.

If you leave the IS-IS Password field blank:

- If the primary seed has an IS-IS password configured, LAN automation configures the primary seed's IS-IS password on the PnP devices (and on the peer seed, if it doesn't already have the password).
- If the primary seed doesn't have an IS-IS password but the peer does, LAN automation configures the peer seed's IS-IS password on the PnP devices and on the primary seed.
- If the primary and peer seeds don't have an IS-IS password configured, LAN automation uses the default value "cisco" for the PnP devices and for both seeds.

Hostname Mapping

- **Default**: If no value is entered, LAN automation sets the hostname as **Switch**, followed by the loopback address. Example: **Switch-192-168-199-100**.
- **Device Name Prefix**: The device prefix is used to generate hostnames for discovered devices. LAN automation keeps the site counter and generates the name using the prefix and the current site counter. For example, if the device prefix is *Building-23-First-Floor*, LAN automation generates device names such as *Building-23-First-Floor-1*, *Building-23-First-Floor-2*, and so on.
- **Hostname Map File Format**: Catalyst Center expects a CSV file with the hostname and serial number (hostname,serial number) as shown in the following example. For stack LAN automation, the CSV file lets you enter one hostname and multiple serial numbers per row. Use commas to separate serial numbers.

Note If both device name prefix and hostname map file are used, then the hostname map file takes precedence and the device name prefix will not be used.

A	B
Edge1	FCW2048Cxxx
Edge2	FCW2131Lxxx, FCW2131Gxxx, FCW2131Gxxx, FCW2131Gxxx
Edge3	FOC2052Xxxx, FCW2052Cxxx, FCW2052Fxxx
Edge4	FXS2131Qxxx

Before you begin

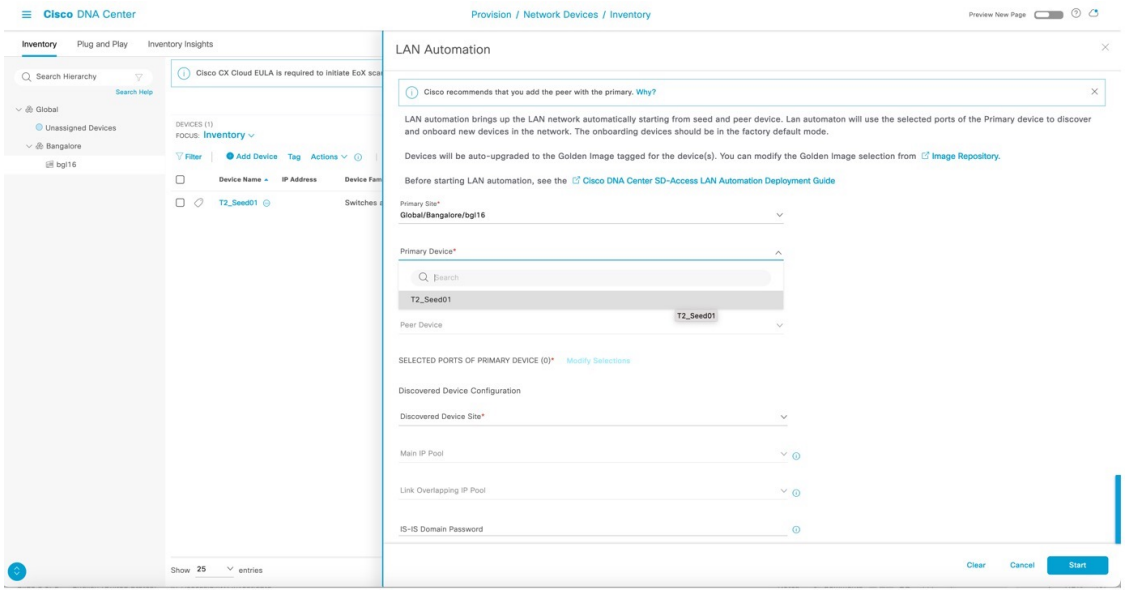
For Catalyst Center 2.3.5 and later, see Provision LAN Automation, on page 50.

Procedure

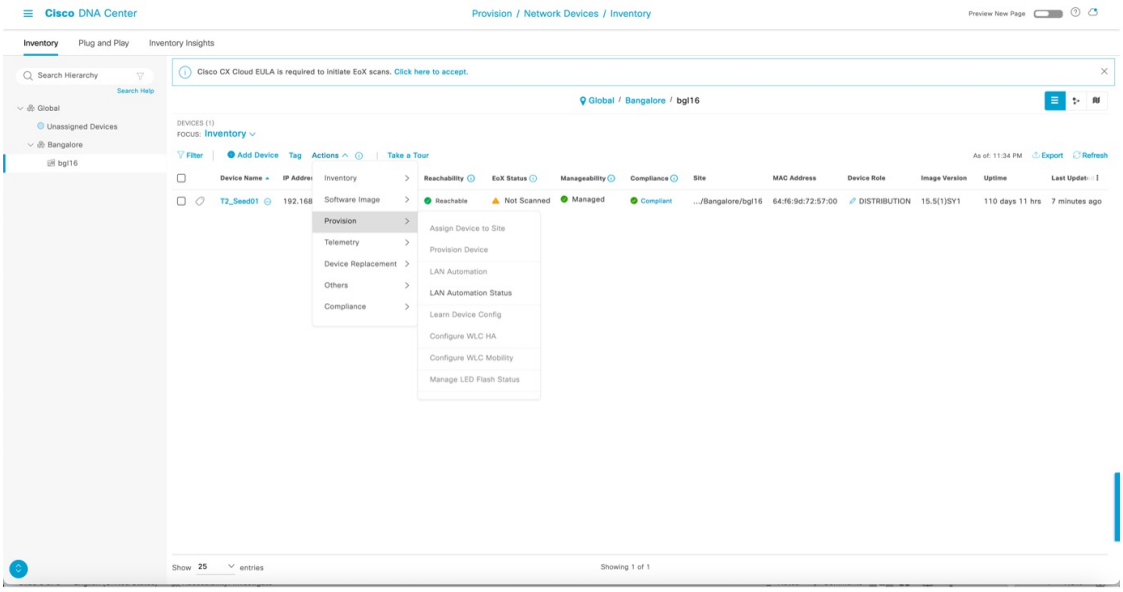
Step 1 From the Catalyst Center GUI, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

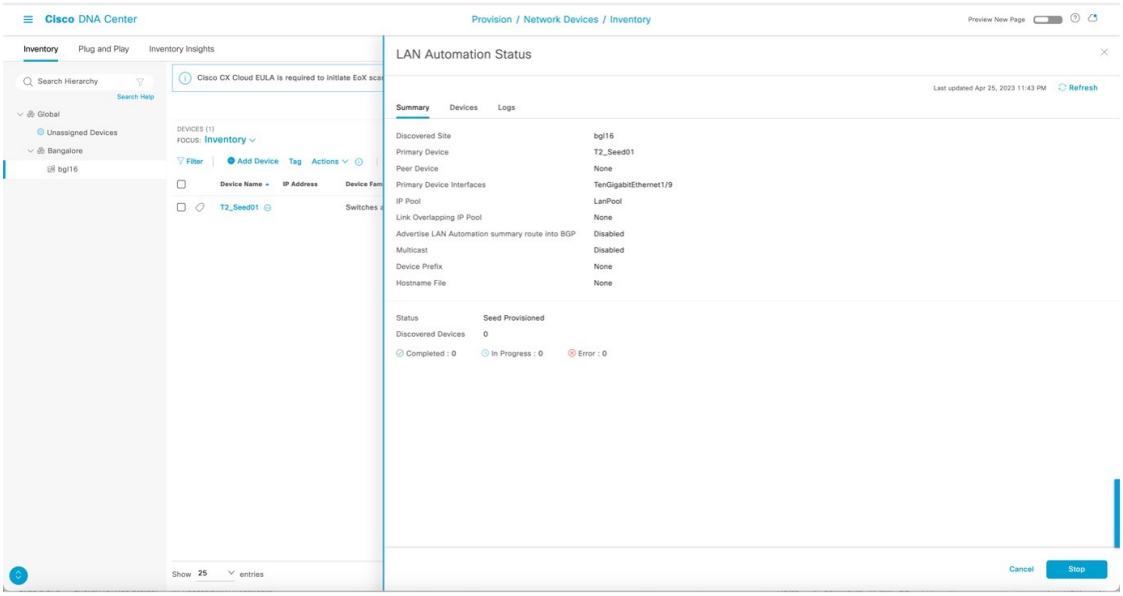
Step 2 In the **Inventory** window, choose **Actions** > **Provision** > **LAN Automation**.

Step 3 Enter the required details and click **Start**.



Step 4 After LAN automation starts, click **LAN Automation Status** to monitor the progress.





After LAN automation starts, the following sample configuration is pushed to the seed device(s).

Primary Seed Configuration

Primary Seed Configuration

```
!exec: enable
!
system mtu 9100
!
ip multicast-routing
ip pim ssm default
!
```

Loopback IP and IS-IS configuration. (If the secondary seed is configured, it also gets configured with the loopback IP and IS-IS configuration.)

```
interface Loopback0
   ip address 10.4.210.123 255.255.255.255
   description Fabric Node Router ID
!
router isis
   net 49.0000.0100.0421.0123.00
   domain-password *
   is-type level-2-only
  metric-style wide
  nsf ietf
   log-adjacency-changes
   bfd all-interfaces
   passive-interface Loopback0
   default-information originate
!
interface Loopback0
ip router isis

clns mtu 1400

ip pim sparse-mode
exit
!
```

DHCP pool information:

```
ip dhcp pool nw_orchestration_pool
  network 10.4.218.0 255.255.255.192
  option 43 ascii 5A1D;B2;K4;I10.4.249.241;J80;
  default-router 10.4.218.1
  class ciscopnp
    address range 10.4.218.2 10.4.218.62
!
ip dhcp class ciscopnp
  option 60 hex 636973636f706e70
!
ip dhcp excluded-address 10.4.218.1
!
```

VLAN 1 configuration:

```
vlan 1
!
interface Vlan1
  ip address 10.4.218.1 255.255.255.192
  no shutdown
  ip router isis
  clns mtu 1400
   bfd interval 500 min_rx 500 multiplier 3
   no bfd echo
exit
!
```

Primary Seed Configuration

Switch port configuration on interfaces used for discovery. (Each discovery interface on the primary seed device gets this configuration.)

```
interface TenGigabitEthernet1/1/8
  switchport
  switchport mode access
  switchport access vlan 1
!
interface TenGigabitEthernet1/1/7
   switchport
   switchport mode access
  switchport access vlan 1
exit
```

Multicast configuration (optional; only configured if the multicast check box is checked).

If the Rendezvous Point (RP) for the underlay multicast needs to be the border, ensure to start LAN automation with multicast enabled using a switch that is planned to be the border as the seed device.

If the peer seed is configured, these multicast CLIs are pushed on the peer seed as well. The same rp-address is used to configure Loopback60000 on both the primary and peer seeds.

```
interface Loopback60000
  ip address 10.4.218.67 255.255.255.255
  ip pim sparse-mode
  ip router isis

ip pim register-source Loopback0
ip pim rp-address 10.4.218.67
```

Secondary Seed Configuration

```
!exec: enable
!
system mtu 9100
!
ip multicast-routing
ip pim ssm default
!
interface Loopback0
  ip address 10.4.210.124 255.255.255.255
  description Fabric Node Router ID
!
router isis
   net 49.0000.0100.0421.0124.00
   domain-password *
   is-type level-2-only
   metric-style wide
   nsf ietf
   log-adjacency-changes
   bfd all-interfaces
   passive-interface Loopback0
   default-information originate
!
interface Loopback0
ip router isis
clns mtu 1400
ip pim sparse-mode
exit
!
```

Note Catalyst Center 2.3.3 and later support `is-type level-2-only` as part of the IS-IS configuration.

Step 5 After device discovery starts, view logs on the PnP agent.

Note Do not press the Enter key on the PnP agent yet.

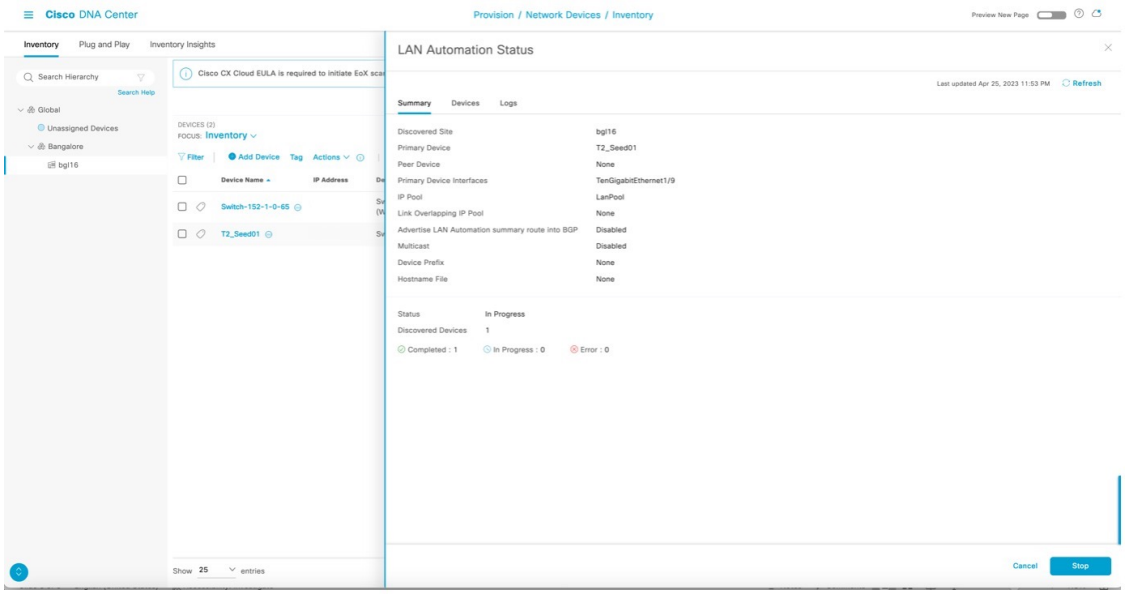
```
%INIT: waited 0 seconds for NVRAM to be available

         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:

Press RETURN to get started!

*Aug  2 23:13:50.440: %SMART_LIC-5-COMM_RESTORED: Communications with the Cisco Smart Software Manager
 or satellite restored
*Aug  2 23:13:51.314: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-1875844429 has been
 generated or imported
*Aug  2 23:13:51.315: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Aug  2 23:13:51.355: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.  Issue "write memory" to
 save new IOS PKI configuration
*Aug  2 23:13:51.418: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-1875844429.server
has been generated or imported
*Aug  2 23:13:52.071: %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively
 down
*Aug  2 23:13:53.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to down
*Aug  2 23:14:00.112: %HMANRP-6-EMP_ELECTION_INFO: EMP active switch 1 elected: EMP_RELAY: Mgmt port
 status DOWN, reelecting EMP active switch

*Aug  2 23:14:00.112: %HMANRP-6-EMP_NO_ELECTION_INFO: Could not elect active EMP switch, setting emp
 active switch to 0: EMP_RELAY: Could not elect switch with mgmt port UP
*Aug  2 23:14:02.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 23:14:04 UTC Thu Aug 2
 2018 to 23:14:02 UTC Thu Aug 2 2018, configured from console by vty0.
Aug  2 23:14:02.000: %PKI-6-AUTHORITATIVE_CLOCK: The system clock has been set.
Aug  2 23:14:02.462: %PNP-6-PNP_DISCOVERY_DONE: PnP Discovery done successfully
Aug  2 23:14:07.847: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.  Issue "write memory" to
save new IOS PKI configuration
Aug  2 23:14:16.348: %AN-6-AN_ABORTED_BY_CONSOLE_INPUT: Autonomic disabled due to User intervention
 on console. configure 'autonomic' to enable it.
%Error opening tftp://255.255.255.255/network-confg (Timed out)
Aug  2 23:14:25.263: AUTOINSTALL: Tftp script execution not successful for Vl1.
```

Step 6 After the device is discovered, Catalyst Center checks if a golden image is marked for the switch family of the discovered device. If a golden image is marked and the discovered device is not running the golden image, LAN automation first upgrades the discovered device to the golden image. If not, Catalyst Center skips the image upgrade and pushes the initial device configuration. The following logs show when the image is upgraded.

```
Oct  5 19:20:11.437: MCP_INSTALLER_NOTICE:
Installer: Source file flash:cat9k_iosxe.16.06.04s.SPA.bin is in flash, Install directly
Oct  5 19:20:12.450: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct  5 19:20:12 provision.sh:
%INSTALL-5-OPERATION_START_INFO: Started install package flash:cat9k_iosxe.16.06.04s.SPA.bin
Oct  5 19:20:22.778: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct  5 19:20:22 packtool.sh:
%INSTALL-5-OPERATION_START_INFO: Started expand package flash:cat9k_iosxe.16.06.04s.SPA.bin
Oct  5 19:21:26.034: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct  5 19:21:26 packtool.sh:
%INSTALL-5-OPERATION_COMPLETED_INFO: Completed expand package flash:cat9k_iosxe.16.06.04s.SPA.bin
Oct  5 19:22:09.861: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct  5 19:22:09 provision.sh:
%INSTALL-5-OPERATION_COMPLETED_INFO: Completed install package flash:{<package_name>}


***
*** --- SHUTDOWN NOW ---
***
```

```
Oct  5 19:22:20.950: %SYS-5-RELOAD: Reload requested by controller. Reload Reason: Image Install.
                          Chassis 1 reloading, reason - Reload command
                                                  Oct  5 19:22:30.501 FP0/0: %PMAN-5-EXITACTION: Process
 manager is exiting: reload fp action requested
Oct  5 19:22:

Initializing Hardware...
```

Catalyst Center pushes part of the configuration, allowing the devices to be onboarded and managed by Catalyst Center. **LAN Automation Status** displays *In Progress*, **Discovered Devices Status** displays the aggregate status of all devices being discovered, and the **Devices** tab displays the status of individual devices being discovered.

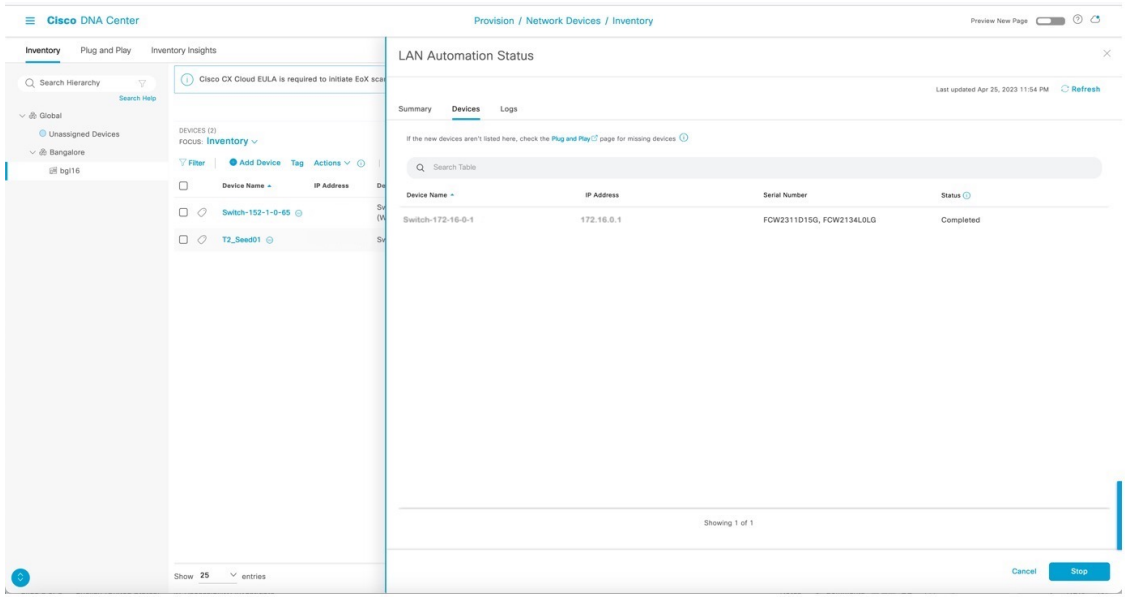


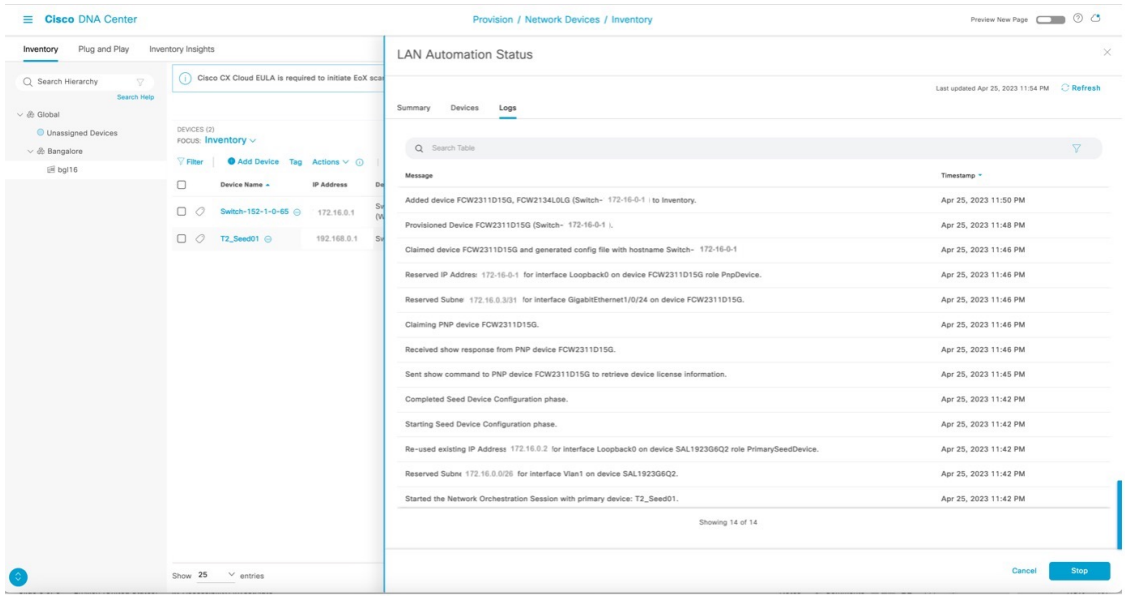
Step 7 View the logs on the PnP agent, as shown in the following example. It is safe to press return on the console if you want to. When you press return, the hostname changes to the value entered in the **Hostname Mapping** field when you started LAN automation.

```
Aug  2 23:14:50.682: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed state to up
Aug  2 23:14:51.487: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to up
Aug  2 23:14:51.681: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed
state to up
Aug  2 23:14:51.854: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/23, changed state to up
Aug  2 23:14:52.487: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, changed
 state to up
Aug  2 23:14:52.855: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/23, changed
 state to up
000123: Aug  2 23:16:17.345: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named dnac-sda has been generated
 or imported
000124: Aug  2 23:16:17.423: Configuring snmpv3 USM user, persisting snmpEngineBoots. Please Wait...

000125: Aug  2 23:16:17.474: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state
 to up
000126: Aug  2 23:16:17.479: %CLNS-6-DFT_OPT: Protocol timers for fast convergence are Enabled.
000128: Aug  2 23:16:17.489: %BFD-6-BFD_IF_CONFIGURE: BFD-SYSLOG: bfd config apply, idb:Vlan1
000129: Aug  2 23:16:18.423: %CLNS-3-BADPACKET: ISIS: LAN L1 hello, packet (9097) or wire (8841)
length invalid from f87b.2077.b147 (Vlan1)
000130: Aug  2 23:16:18.502: %BFD-6-BFD_SESS_CREATED: BFD-SYSLOG: bfd_session_created, neigh 204.1.183.1
 proc:ISIS, idb:Vlan1 handle:1 act
000131: Aug  2 23:16:19.269: %BFDFSM-6-BFD_SESS_UP: BFD-SYSLOG: BFD session ld:1 handle:1 is going
```

```
UP
000132: Aug  2 23:16:19.494: %CLNS-5-ADJCHANGE: ISIS: Adjacency to 0100.1001.0001 (Vlan1) Up, new
adjacency
000133: Aug  2 23:16:20.289: %PNPA-DHCP Op-43 Msg: Op43 has 5A. It is for PnP
000134: Aug  2 23:16:20.289: %PNPA-DHCP Op-43 Msg: After stripping extra characters in front of 5A,
 if any

000135: Aug  2 23:16:20.289: %PNPA-DHCP Op-43 Msg: _pdoon.2.ina=[Vlan1]
000136: Aug  2 23:16:20.289: %PNPA-DHCP Op-43 Msg: _papdo.2.eRr.ena
000137: Aug  2 23:16:20.289: %PNPA-DHCP Op-43 Msg: _pdoon.2.eRr.pdo=-1
000138: Aug  2 23:16:30.010: %CLNS-5-ADJCHANGE: ISIS: Adjacency to 9324-SN-BCP-1 (Vlan1) Up, new
adjacency
```

After all devices are discovered, the **Discovered Devices** status changes to *Completed* and the discovered devices are added to the inventory.





Step 8 From the Catalyst Center home page, click the menu icon and choose **Provision** > **Inventory** and filter by serial number. The newly discovered switches appear as *Managed*.

The following example shows a sample configuration pushed to discovered devices.

```
!
archive
log config
logging enable
logging size 500
hidekeys
!
!
!
service timestamps debug datetime msec
!
service timestamps log datetime msec
!
service password-encryption
!
service sequence-numbers
!
! Setup NTP Server
! Setup Timezone & Daylight Savings
!
ntp server 10.4.250.104
!
! ntp update-calendar
!
! clock timezone <timezoneName> <timezoneOffsetHours> <timezoneOffsetMinutes>
! clock summer-time <timezoneName> recurring
!
! Disable external HTTP(S) access
! Disable external Telnet access
! Enable external SSHv2 access
!
no ip http server
!
no ip http secure-server
!
ip ssh version 2
!
ip scp server enable
!
line vty 0 15
! maybe redundant
login local
transport input ssh
! maybe redundant
transport preferred none
! Set VTP mode to transparent (no auto VLAN propagation)
! Set STP mode to Rapid PVST+ (prefer for non-Fabric compatibility)
! Enable extended STP system ID
! Set Fabric Node to be STP Root for all local VLANs
! Enable STP Root Guard to prevent non-Fabric nodes from becoming Root
! Confirm whether vtp mode transparent below is needed
vtp mode transparent
!
spanning-tree mode rapid-pvst
!
spanning-tree extend system-id
! spanning-tree bridge priority 0
! spanning-tree rootguard
! spanning-tree portfast bpduguard default
```

```
no udld enable
!
errdisable recovery cause all
!
errdisable recovery interval 300
!
ip routing
!Config below applies only on underlay orchestration
!
! Setup a Loopback & IP for Underlay reachability (ID)
! Add Loopback to Underlay Routing (ISIS)
!
interface loopback 0
description Fabric Node Router ID
ip address 10.4.218.97 255.255.255.255
ip router isis
!
!
! Setup an ACL to only allow SNMP from Fabric Controller
! Enable SNMP and RW access based on ACL
!
snmp-server view DNAC-ACCESS iso in
!
snmp-server group DNACGROUPAuthPriv v3 priv read DNAC-ACCESS write DNAC-ACCESS
!
snmp-server user admin DNACGROUPAuthPriv v3 auth MD5 C1sco123 priv AES 128 C1sco123
!
!
! Set MTU to be Jumbo (9100, some do not support 9216)
!
system mtu 9100
! FABRIC UNDERLAY ROUTING CONFIG:
!
! Enable ISIS for Underlay Routing
! Specify the ISIS Network ID (e.g. encoded Loop IP)
! Specific the ISIS domain password
! Enable ISPF & FRR Load-Sharing
! Enable BFD on all (Underlay) links
!
router isis
net 49.0000.0100.0421.8097.00
domain-password <password>
is-type level-2-only
metric-style wide
nsf ietf
! fast-reroute load-sharing level-1
log-adjacency-changes
bfd all-interfaces
! passive-interface loopback 0
!
!
!
interface vlan1
bfd interval 500 min_rx 500 multiplier 3
no bfd echo
!
!
!This config goes to subtended node

username lan-admin privilege 15 password 0 C1sco123
!
enable password C1sco123
!
!
```

```
hostname CL-9300_7
!
interface vlan1
ip router isis
!
!
end
```

Note Catalyst Center 2.3.3 and later support `is-type level-2-only` as part of the IS-IS configuration.

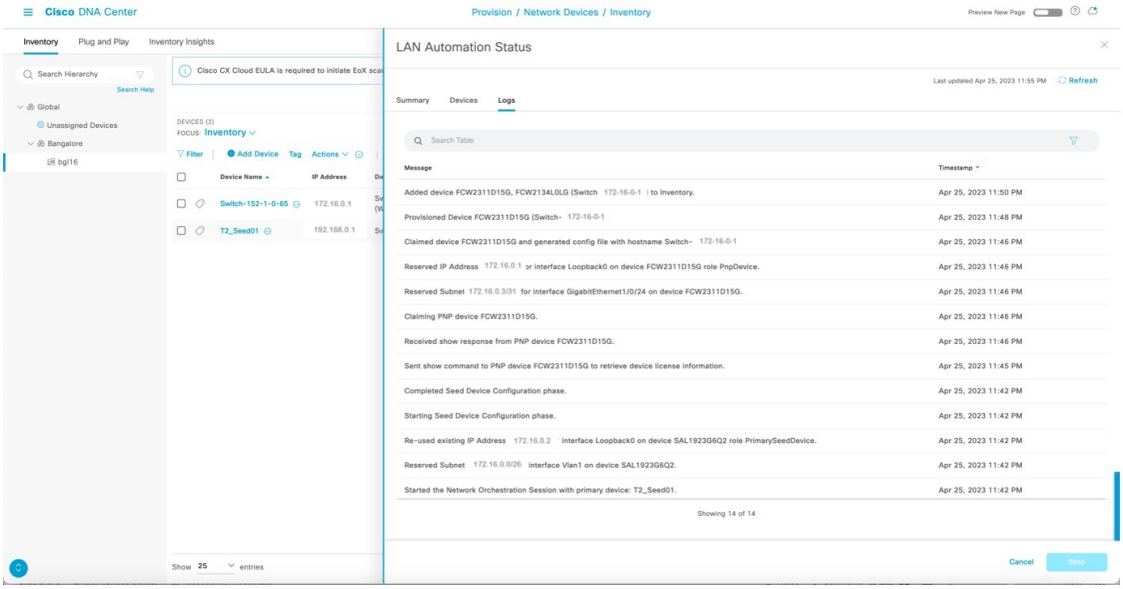
Step 9 After the **Discovered Devices** status changes to *Completed* and all discovered devices are displayed in the inventory as *Managed*, you can stop LAN automation. However, before stopping LAN automation, check the **Topology** page to make sure that the links between the discovered device and primary and peer seed are displayed. Choose **Tools** > **Topology** and click the physical links between the seed and discovered device. Make sure that the interfaces are correct.

If the physical links are not visible, resynchronize the seed device where the physical links connect. After resync, check the **Topology** page again to make sure that the links are visible before stopping LAN automation.

Stop LAN Automation

You can stop LAN automation to finish discovering all required devices and to prevent inadvertent discovery of additional devices.

In the **LAN Automation Status** window,click **Stop**.



After you click **Stop**:

- The remainder of the configuration is pushed to network devices, which includes converting the point-to-point links from Layer 2 to Layer 3.
- The VLAN 1 configuration is removed and the VLAN 1 IP addresses are returned to the LAN automation pool.
- The device is onboarded in Catalyst Center and assigned to the site.

After the LAN automation stop process is initiated, the **LAN Automation Status** changes to *STOP in Progress*.

After LAN automation stops, the following sample configuration is pushed to the discovered device.

The network orchestration service issues a RESYNC for seed and PnP devices to retrieve the state of all links. After the initial RESYNC completes, it pushes the Layer 3 configuration on all Layer 2 links. Finally, it reissues RESYNC to resynchronize the cluster's link state.

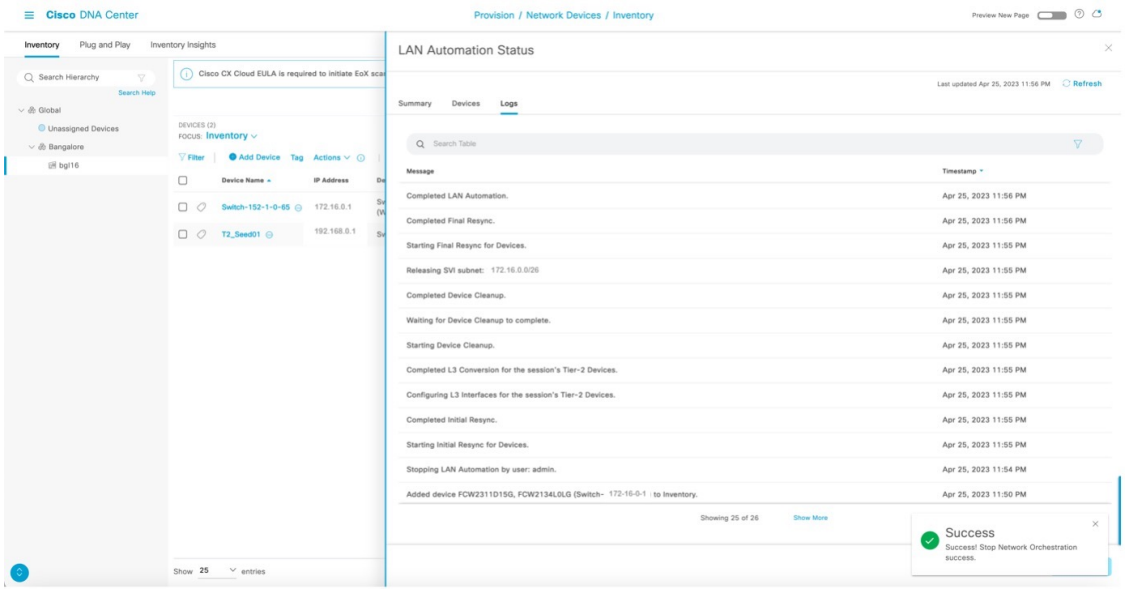
The Layer 3 link configuration is pushed when network orchestration stops. (Each interface pair gets its configuration.)

```
interface GigabitEthernet1/0/13
 description Fabric Physical Link
 no switchport
 dampening
 ip address 192.168.2.97 255.255.255.252
 ip router isis
 logging event link-status
 load-interval 30
 bfd interval 500 min_rx 50 multiplier 3
 no bfd echo
 isis network point-to-point
```

After all the point-to-point links between the seeds and discovered devices—including links between peer seed and discovered devices—are configured, the devices are added to the site and synced to Catalyst Center.

The LAN automation process completes and the **LAN Automation Status** changes to *Completed*.

Check the LAN automation logs.



Add Switches and Links to an Existing LAN-Automated Stack

This section describes how to add a new switch, add an existing switch, or configure a link in a LAN-automated stack.

Add a New Switch

This section explains how to add a brand new switch that was never present in Catalyst Center.

You can add switches to a stack that is already LAN automated and in provisioned state without having to LAN automate or discover the new switch.

Procedure

Step 1 Make sure that the switch was not part of Catalyst Center earlier. (The switch should not be discovered and present in the inventory.)

Step 2 Make sure that the switch being added has the same image and license version as the provisioned standalone/stack. Use the commands `show ver` and `show license right-to-use` to verify the image and license version.

Step 3 Make sure that the switch is in the same boot mode as the stack. It should be in either INSTALL (preferred) or BUNDLE mode.

```
9300_Edge_1#show ver | inc INSTALL
*    1 62    C9300-48U          16.6.3            CAT9K_IOSXE           INSTALL
     2 62    C9300-48U          16.6.3            CAT9K_IOSXE           INSTALL
     3 62    C9300-48U          16.6.3            CAT9K_IOSXE           INSTALL
     4 62    C9300-48U          16.6.3            CAT9K_IOSXE           INSTALL
```

Step 4 Use the stack cable to connect the new switch to the stack. Then, power it on. After 2 to 3 minutes, the new switch is added to the stack as a standby (if one switch is already present in the stack) or as a member (if two or more switches are already present in the stack).

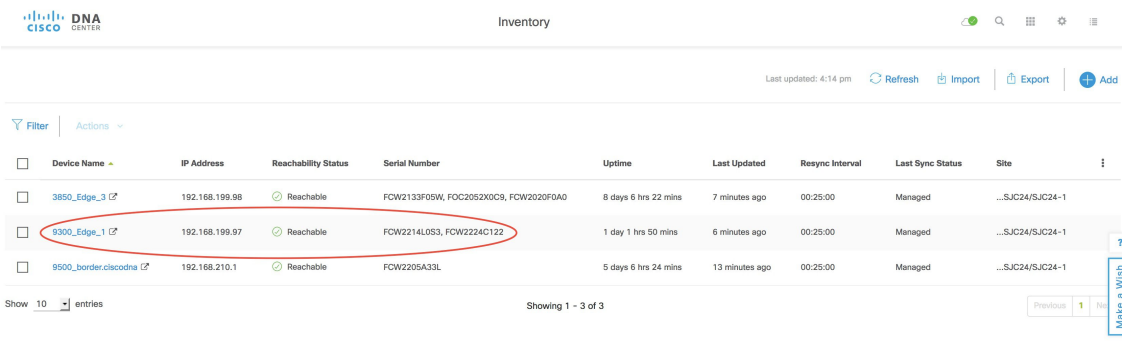
Step 5 Check the output of the commands `show ver` and `show switch` to make sure that the new switch is added. The output of the `show ver` command consists of serial numbers for all switches.

Step 6 After the switch is added to the stack, go to **Inventory**, select the original provisioned switch/stack, and perform a resync.

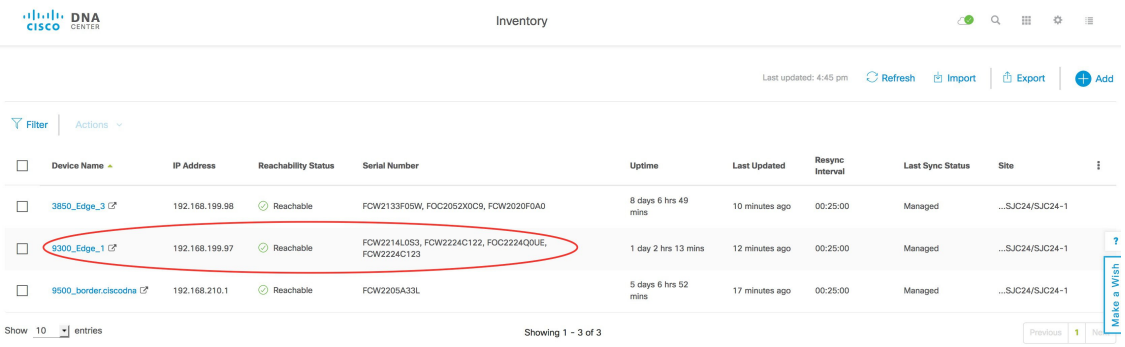
Step 7 After the sync completes, the new serial number is displayed, completing the addition process.

Note You can add more than one switch at a time. Repeat this procedure, making sure to use the correct cabling.

The following image shows the serial number before the new switch is added.



The following image shows the serial number after the new switch is added.



Add an Existing Switch

This section explains how to add an existing switch that was already present in Catalyst Center.

If the switch being added was previously LAN automated (part of another stack/standalone) or was discovered by PnP, to add it, you must first remove the switch physically and then remove its entry from the inventory and PnP application/database.

Remove the Switch from Inventory

If the switch is a standalone, from the Catalyst Center home page, click **Inventory** and select the switch to remove. Choose **Actions** > **Delete Device**. If the switch is part of a stack, remove the switch physically, and then resync the original stack. After the sync completes, the removed switch serial number does not appear in the inventory.

Remove the Switch from PnP

- If the switch is a standalone, first unconfigure `pnp profile pnp-zero-touch` from the switch and then delete the entry from the PnP database under **Device**.
- If the switch is part of a stack, remove the switch physically. Make sure that the removed switch does not have `pnp profile pnp-zero-touch`; then, delete the entry from the PnP database under **Device**.

Configure Additional Links After LAN Automation Stops

Use this method when you want to configure:

- Additional links between the primary and peer seed devices or between distribution devices after LAN automation stops
- Uplinks from the newly added stack switch to the primary and peer seeds

If you chose the Enable Multicast option the first time LAN automation ran on the device, do not choose Enable Multicast when you configure additional links. Complete the following steps and when LAN automation stops, go to the newly configured Layer 3 ports and manually configure **ip pim sparse-mode** under the interface.

Before you begin

For Catalyst Center 2.3.5 and later, see Create Link Between Interfaces, on page 60.

Procedure

Step 1 Check the output of the command **show cdp neighbors** to make sure that the neighbor connected to the new link is displayed. The following sample configuration shows a new link connected to port *Ten 4/1/5* on switch *9300_Edge-7*. On the other end, the link is connected to switch *9500_border-6* via port *For 1/0/1*.

```
9300_Edge-7#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
9500_border.cisco.com
                 Ten 1/1/5         173             R S I  C9500-12Q For 1/0/1
9500_border-6.cisco.com
                 Ten 4/1/5         136             R S I  C9500-12Q For 1/0/1
```

Step 2 Make sure that the ports to which the link is connected (*Ten 4/1/5* and *For 1/0/1*) do not have any Layer 3 configurations on them. If they have Layer 3 configurations, use the default interfaces connected to the new uplink being added and resynchronize both devices.

Step 3 From the Catalyst Center home page, choose **Provision** > **LAN Automation**.

Step 4 In the **Primary Device** field, enter the switch (for example, **`9500_border-6`**) to which the new link is connected.

Step 5 In the **Peer Device** field, enter the switch (for example, **`9300_Edge-7`**) where you want to configure the new link.

Step 6 Select the port on the primary device where the uplink connects; that is, the port where the PnP device is connected (for example, **`For 1/0/1`**).

Step 7 Use the same LAN automation pool that was used to provision the original stack.

Step 8 Start LAN automation. Wait for 2 minutes and then stop LAN automation. Because there is no new device discovery to perform, you don't have to go through the entire LAN automation process. After you stop LAN automation, both ports connected to the uplink are configured with an IP address from the same LAN automation pool.

Step 9 As shown in the following example, after LAN automation stops and completes, both ports are configured for Layer 3 from the LAN pool.

```
9300_Edge-7#show run int t4/1/5
Building configuration...

Current configuration : 325 bytes
!
interface TenGigabitEthernet4/1/5
 description Fabric Physical Link
 no switchport
 dampening
 ip address 192.168.199.85 255.255.255.252
 ip router isis
 logging event link-status
 load-interval 30
 bfd interval 100 min_rx 100 multiplier 3
 no bfd echo
 isis network point-to-point

9500_border-6#show run int Fo1/0/1
Building configuration...
```

```
Current configuration : 327 bytes
!
interface FortyGigabitEthernet1/0/1
 description Fabric Physical Link
 no switchport
 dampening
 ip address 192.168.199.86 255.255.255.252
 ip router isis
 logging event link-status
 load-interval 30
 bfd interval 100 min_rx 100 multiplier 3
 no bfd echo
 isis network point-to-point
end
```

Note If you are familiar with APIs, the preceding IP address addition can also be achieved manually through APIs. However, we recommend adding IP addresses through LAN automation, because it updates all table entries. Another advantage of LAN automation is that when the device is removed from the inventory, all associated IP addresses are released. If IP addresses are configured manually through APIs, they are not released.

Move an Uplink to the Newly Added Switch

You cannot move an uplink from a stack that is already provisioned to a newly added switch in a LAN-automated stack.

Use a 40-G Interface on the Cisco Catalyst 9400

For 16.11.1 and later, Cisco IOS enables the 40-G port on bootup if the following conditions are met:

- The switch must have its day-0, factory-default configuration. (For information about how to bring a device back to its day-0 configuration, see PnP Agent Initial State, on page 18.)
- For a single supervisor, a 10-G/1-G SFP cannot be inserted in any of the SUP ports (ports 1 to 8). A 40-G QSFP must be inserted in ports 9 or 10.
- For a dual supervisor, a 10-G/1-G SFP cannot be inserted in any of the SUP ports (ports 1 to 8). A 40-G QSFP must be inserted in port 9 only.

Troubleshoot LAN Automation

If you encounter any problems, collect the root cause analysis (RCA) file, which is helpful for troubleshooting. At the CLI, enter:

```
$ sudo rca
```

For a three-node cluster, collect the RCA file for each cluster.

Additional Information: LAN Automation in Catalyst Center Release 2.3.5 and later

The following topic provides information on the LAN automation provisioning based on Catalyst Center Release 2.3.5. The steps and examples may vary for later versions.

For more information on the LAN automation configuration and related features in your Catalyst Center version , see *Cisco Catalyst Center User Guide*.

Provision LAN Automation

Start and stop LAN automation.

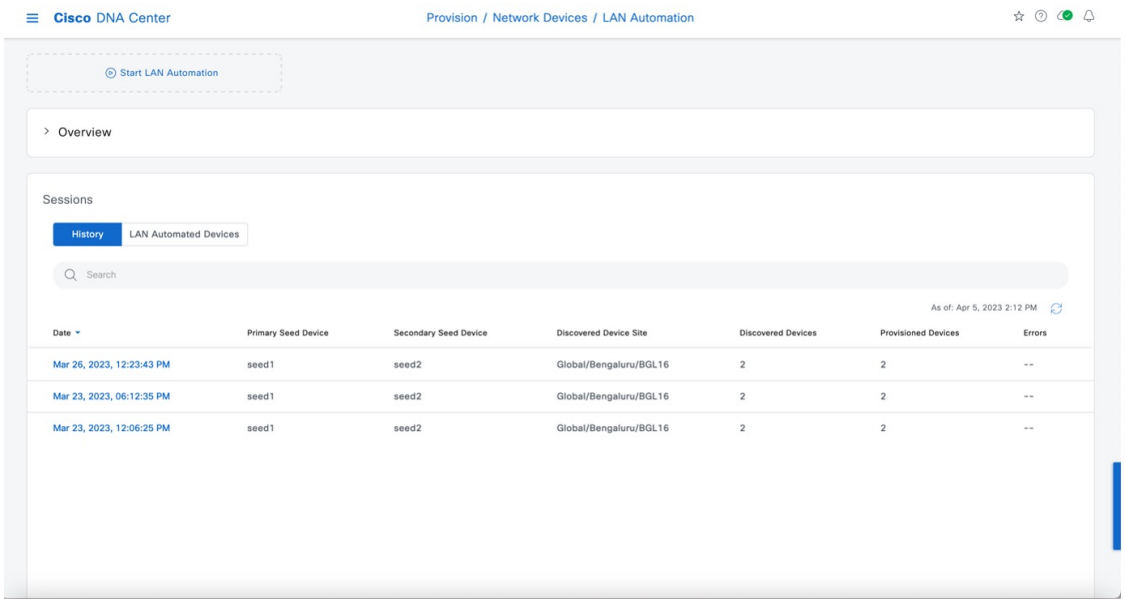
Before you begin

The following topic describes the LAN automation procedure based on Catalyst Center 2.3.5. The steps may vary based on your Catalyst Center version.

Procedure

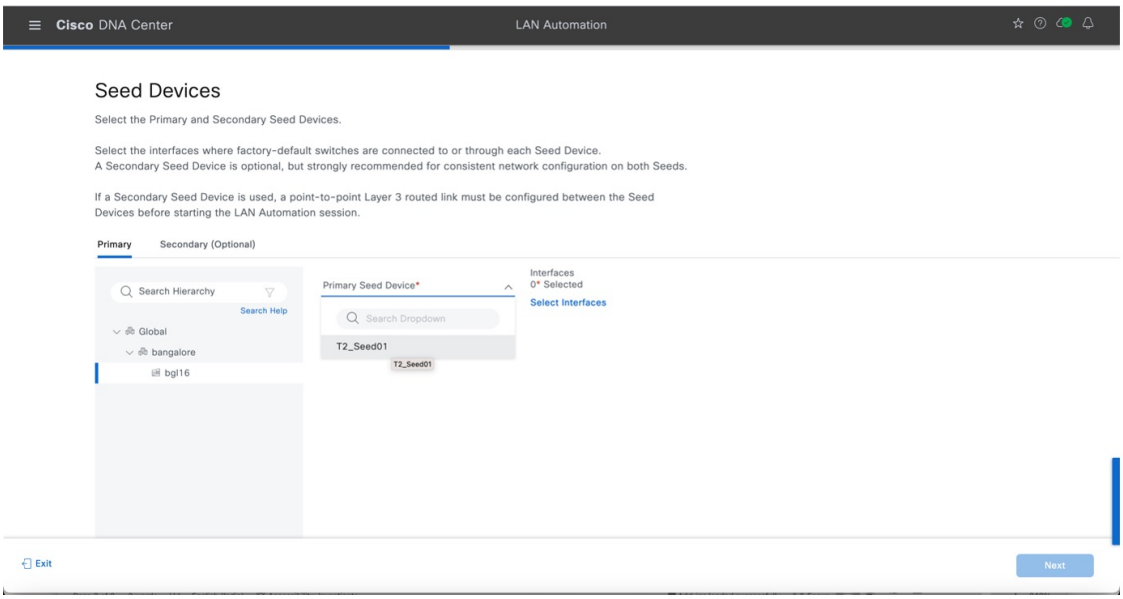
Step 1 From the top-left corner, click the menu icon and choose **Provision** > **LAN Automation**.

Step 2 In the **LAN Automation** window, click **Start LAN Automation**.

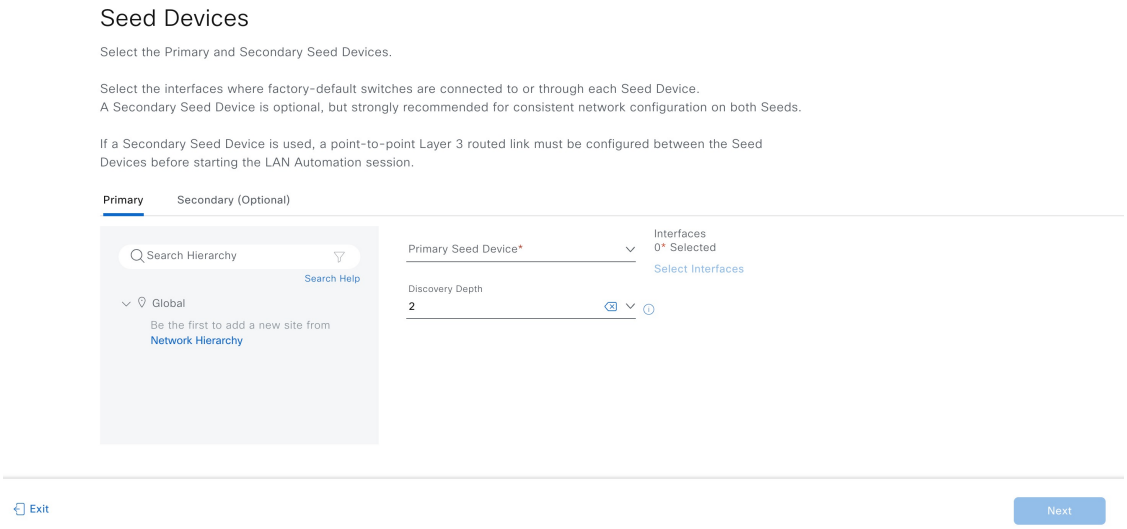


Step 3 In the **Seed Devices** window, do the following:

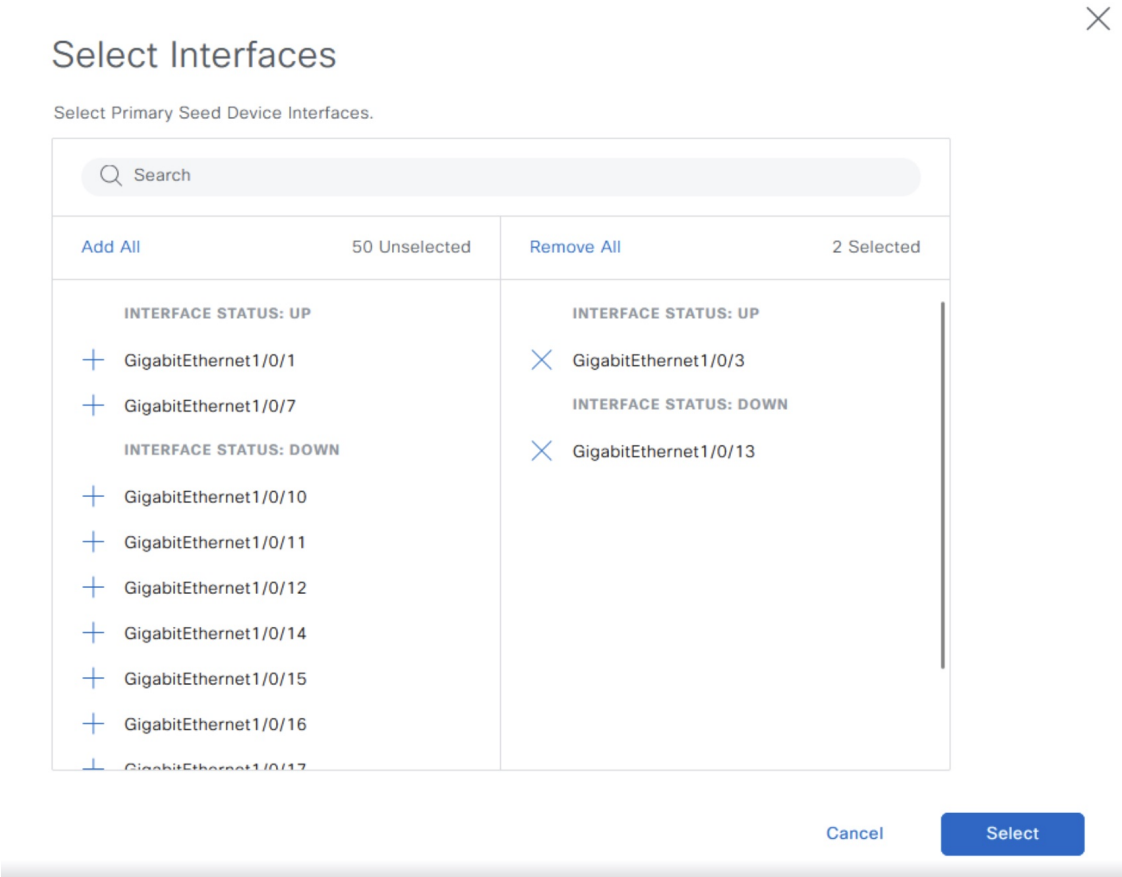
- Select the **Primary Seed Device** and its Plug and Play (PnP) interfaces.
- (Optional) Select the **Secondary Seed Device** and its PnP interfaces.



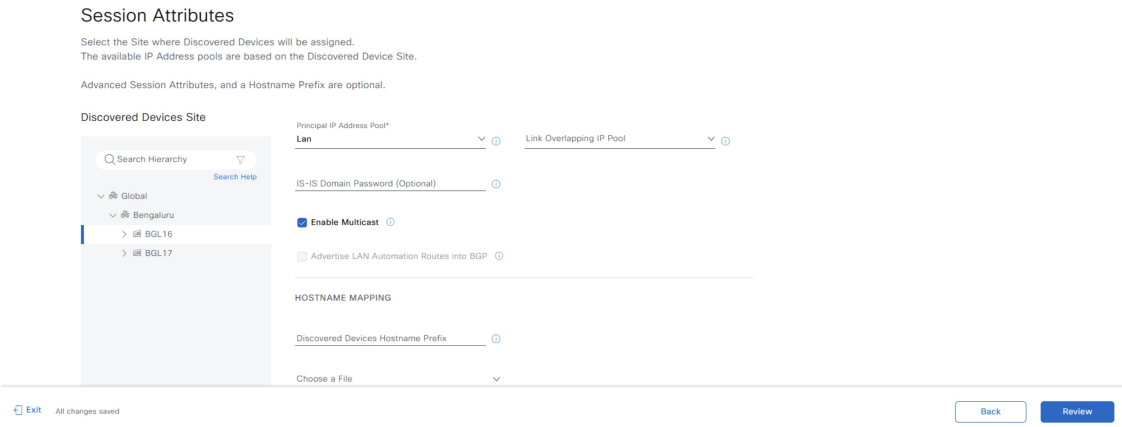
In Catalyst Center Release 2.3.7.5 and later, you can add a discovery depth level for LAN automation. Devices are LAN automated up to the specified level below the primary seed device. The default value is 2. You can review the discovery depth in the summary window and see the specified value in the session details window after the LAN automation starts.



To select the interfaces, in the **Select Interfaces** window, choose the interfaces and click **Add Selected**.



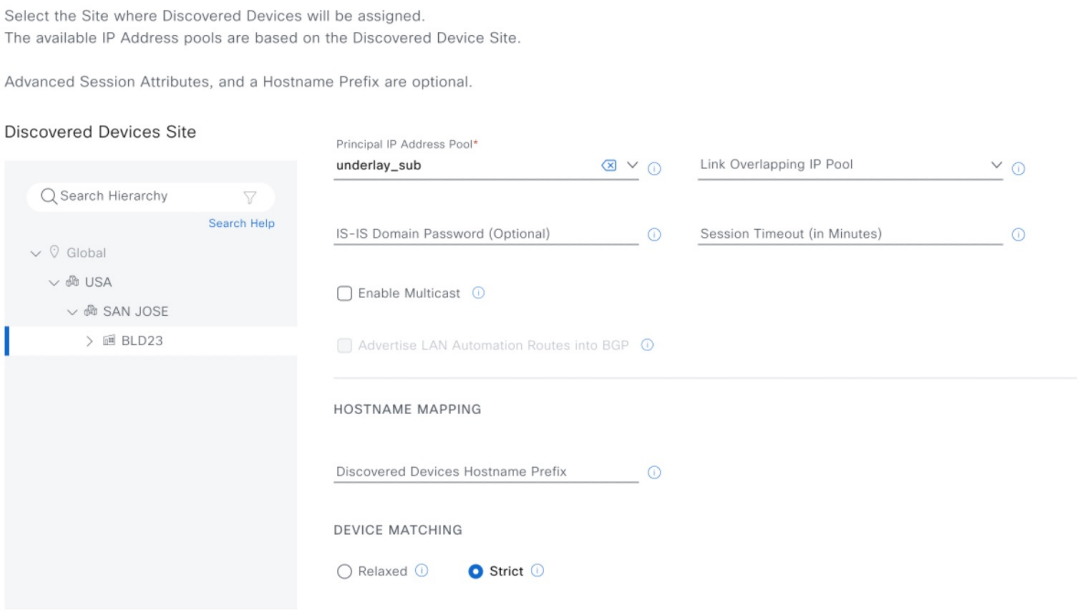
Step 4 In the **Sessions Attributes** window, select the **Principal IP Address Pool** and add the other details as required.



In Catalyst Center Release 2.3.7.5 and later, you can specify the following session attributes.

- **Session Timeout**: Specifies a timeout value for the LAN automation session. LAN automation stops automatically when the specified time limit is reached. The value is specified in minutes and the valid range is 20 through10080.
- **Device Matching**: Specifies the method for device discovery.

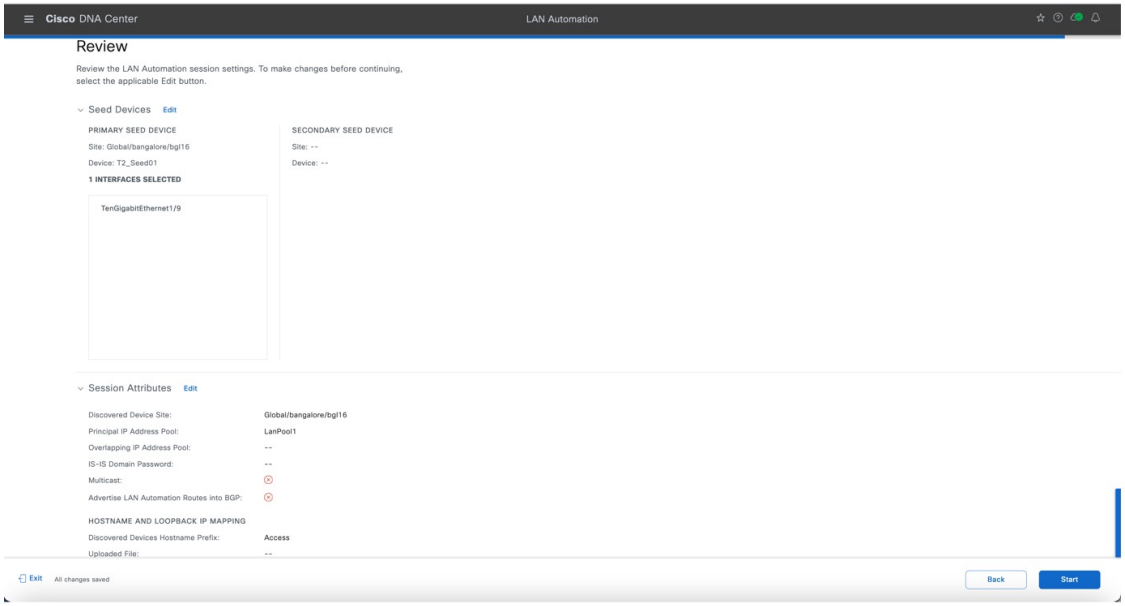
- **Relaxed**: Hostname and loopback IP is assigned to the discovered device if the device's serial number matches the uploaded device list.
- **Strict**: Device discovery is restricted to the list of devices provided. You can discover a maximum of 50 devices. To add or edit devices, see Manage Devices in Strict Discovery Mode, on page 66.



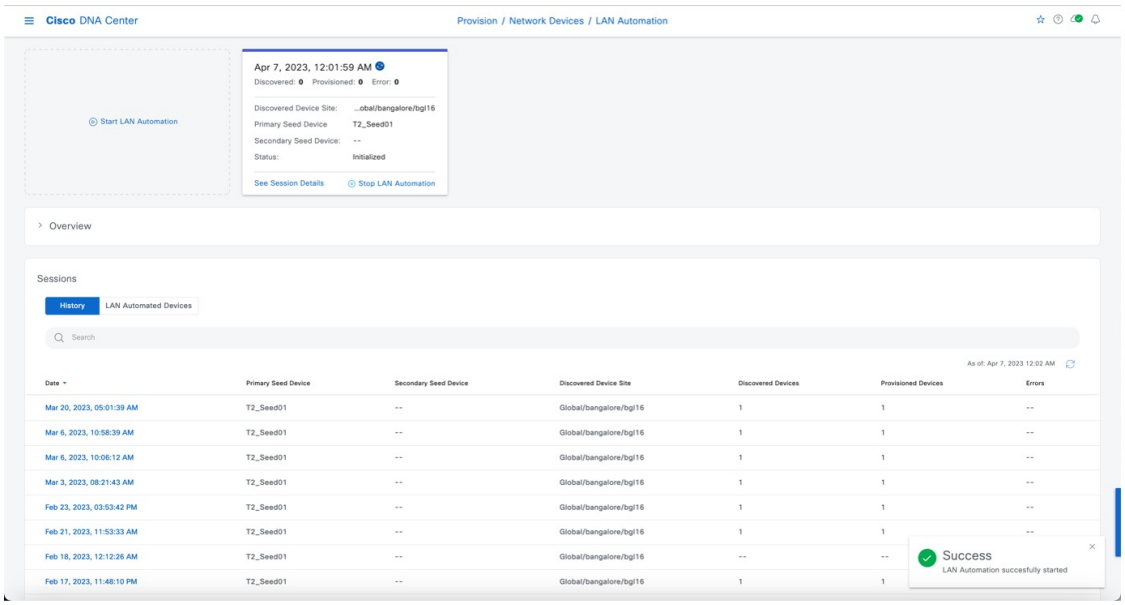
You can review the session attributes in the summary window and view them in the device details window after the LAN automation is complete.

Step 5 Click **Review**.

Step 6 After reviewing the configurations, click **Start** to start the LAN automation.

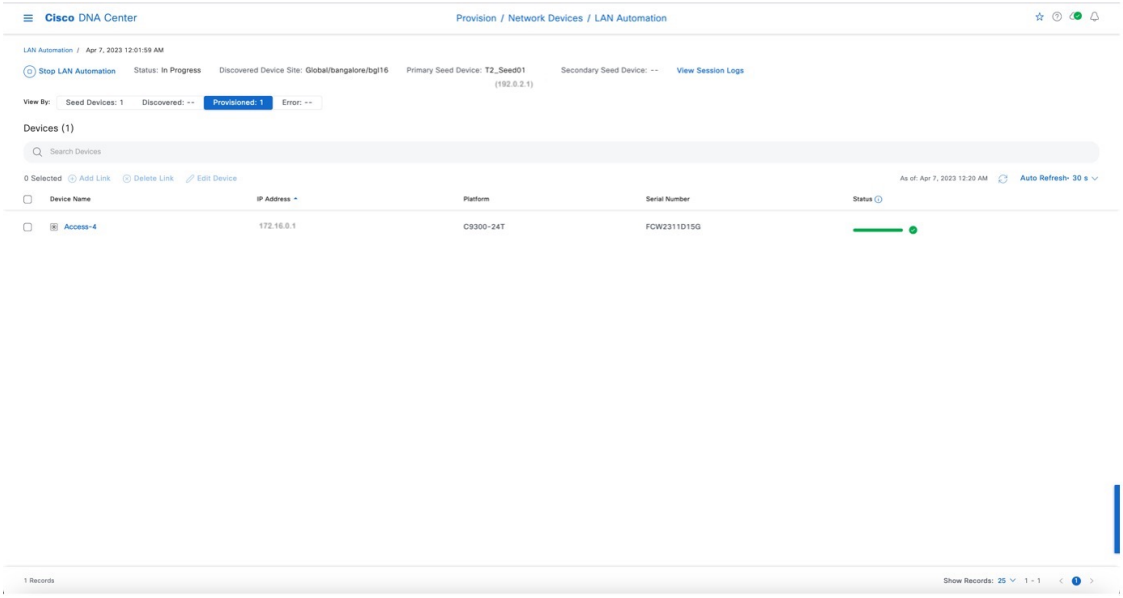


The LAN automation session is created and a tile for the session is displayed in the **LAN Automation** window.

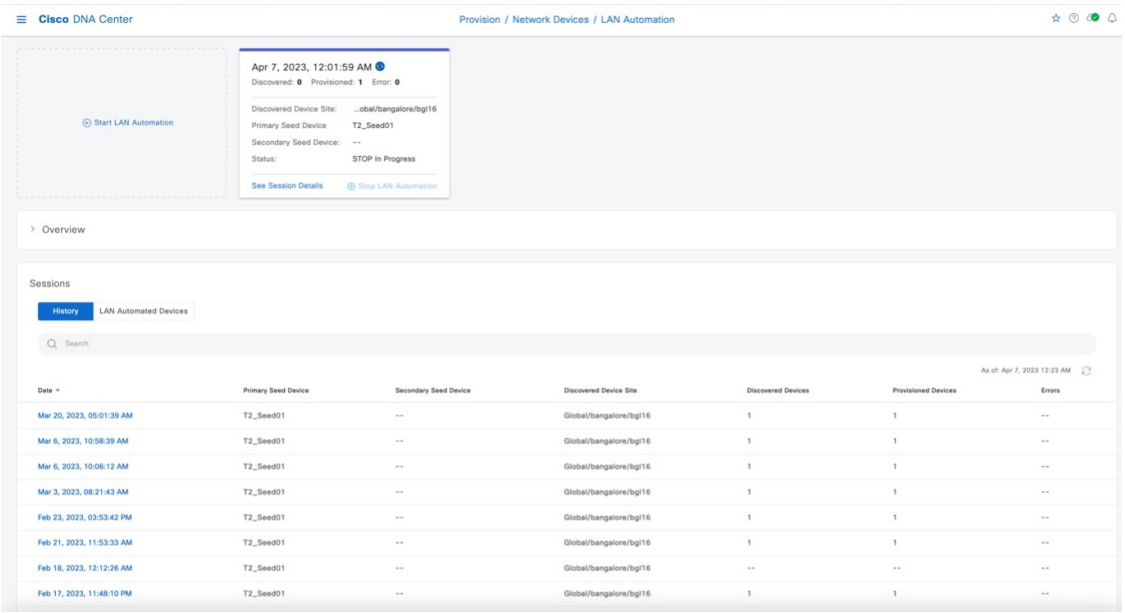


To view the details of the session, click **See Session Details** in the tile. To view the logs for a session, click **View Session Logs** in the session details window.

The session details window displays the status of the LAN automation session and the devices that are being LAN automated. You can filter the data and see details of the seed devices, discovered devices, provisioned devices, or the error messages. You can stop the LAN automation process when all the devices are provisioned and the progress bar in the **Status** column shows as complete.



To stop LAN automation for the session, click **Stop LAN Automation** in the session details window or in the session tile. The LAN automation status changes to *STOP in Progress*.

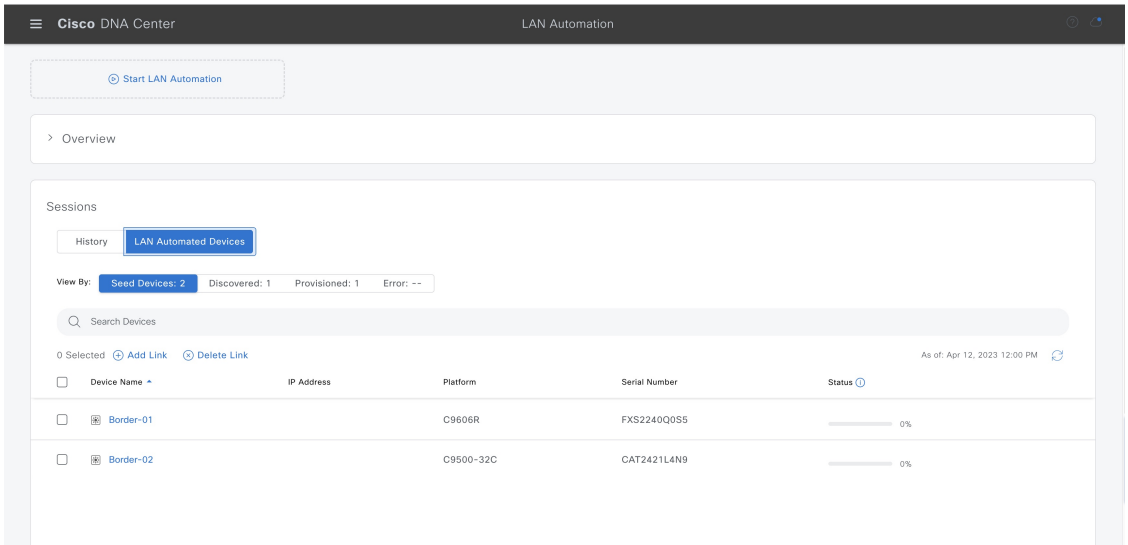


The **History** tab displays the history of LAN automation sessions in your network. You can use the search field to search for specific text in history. Click the hyperlinked date to view the session details.

The **LAN Automated Devices** tab displays the details of the LAN automated devices. You can use the search field to filter the data based on specific text. Click one of the following toggle buttons to filter the data:

- Seed Devices: Displays the data for seed devices
- Discovered: Displays the data for discovered devices.
- Provisioned: Displays the data for provisioned devices.

- Error: Displays the data for devices with errors.

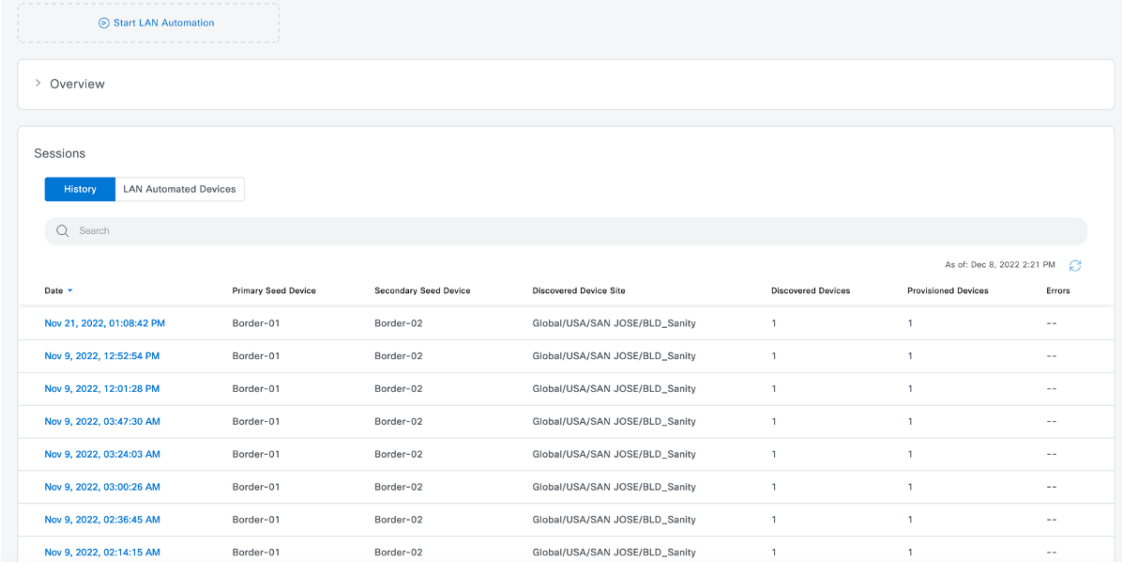


Check Device Logs and Configurations

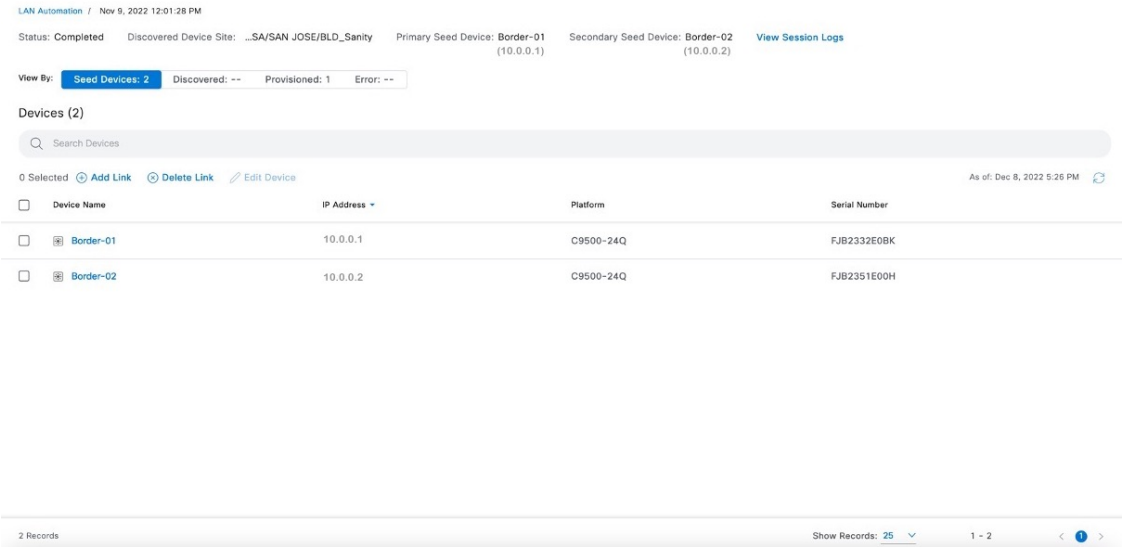
View the LAN automation session logs, device-specific logs, and configurations that are pushed on the device.

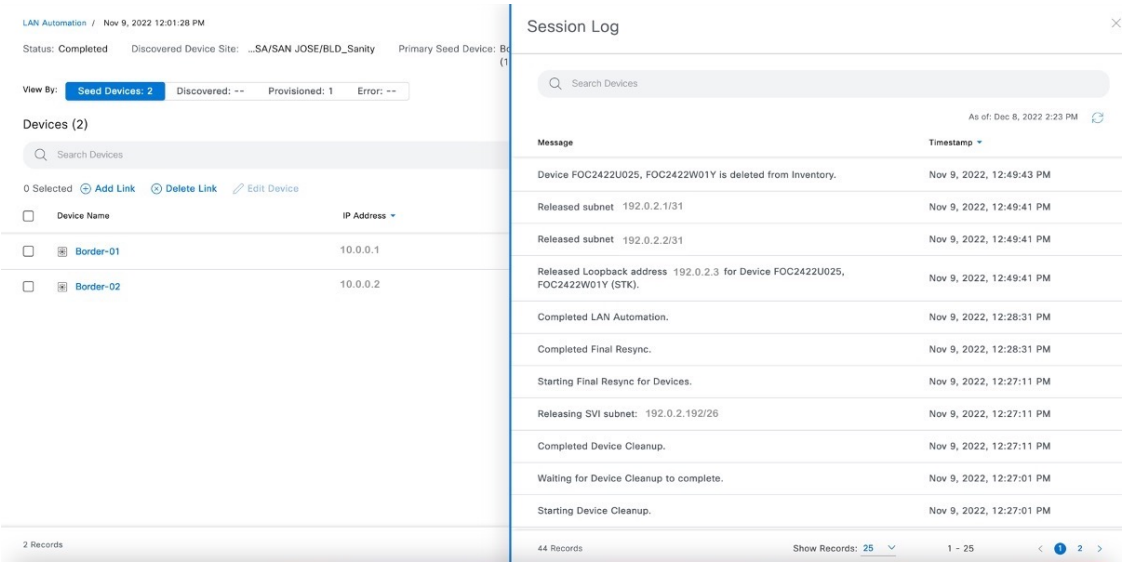
Procedure

Step 1 In the **LAN Automation** window, click the **History** tab in the **Sessions** area and click the hyperlinked date to view the session details.



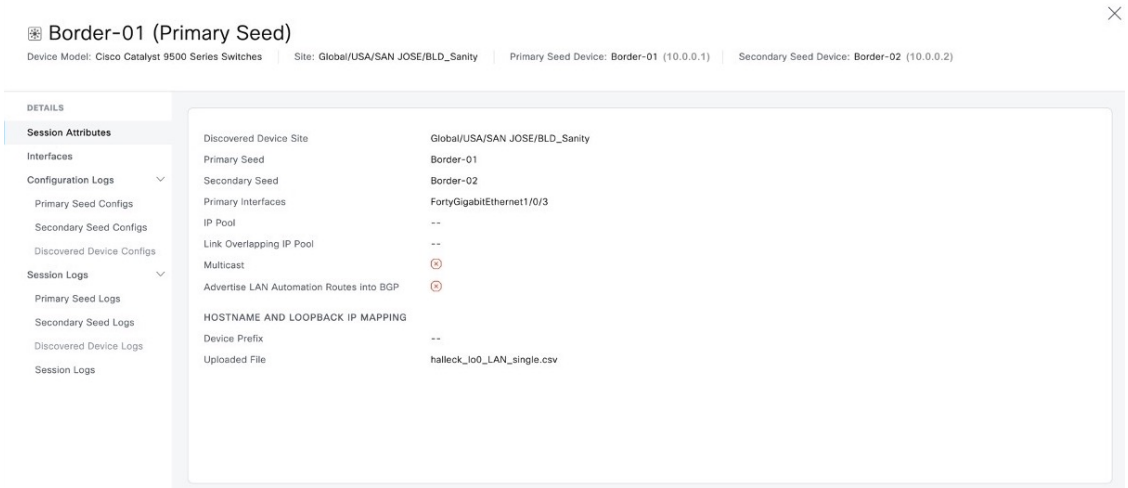
Step 2 To view the logs for a session, click **View Session Logs** in the session details window.



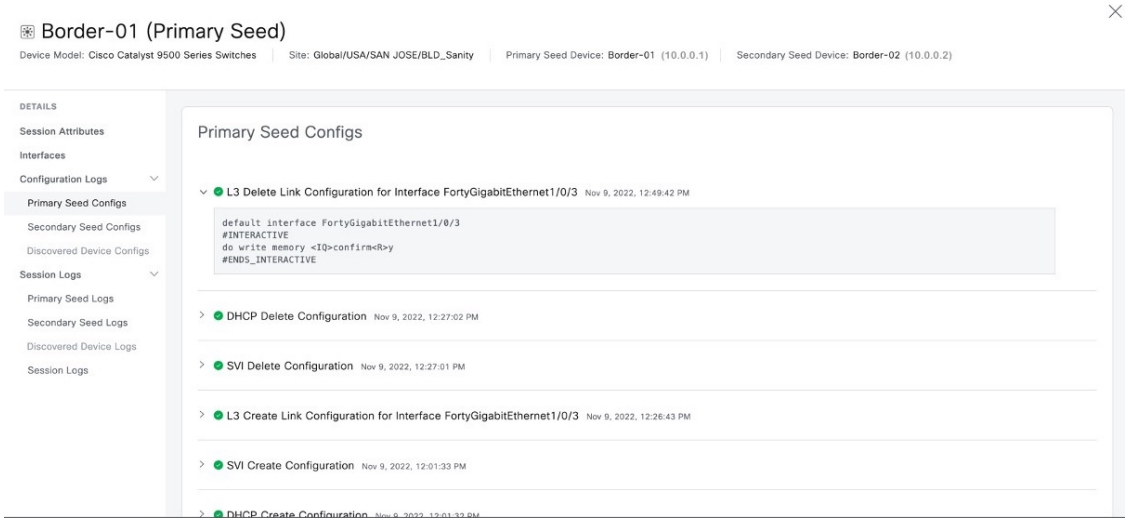


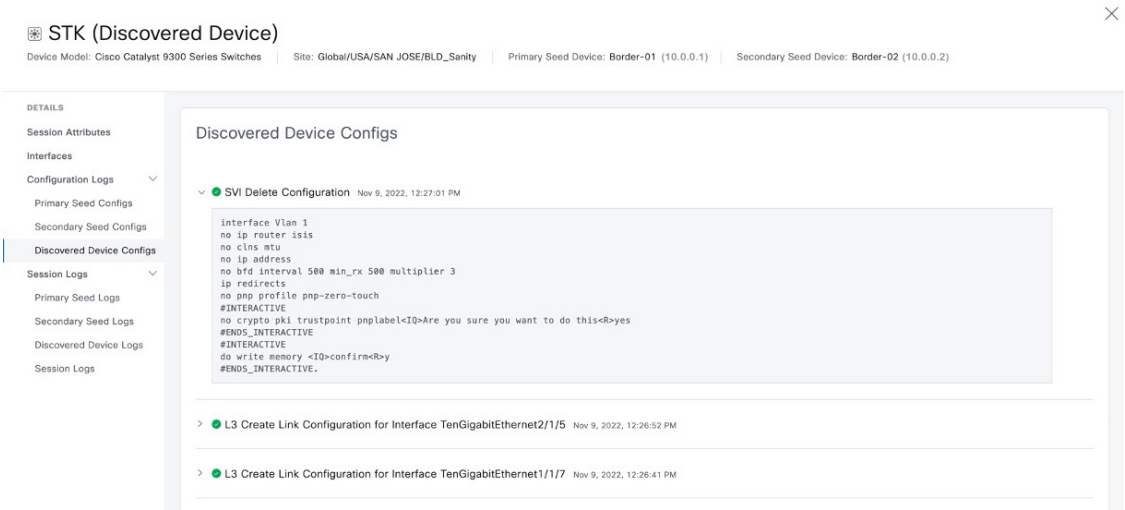
Step 3 To view the device-specific logs and configurations, click on the device name in the session details window. Use the toggle button to filter the devices.

The device details are displayed.

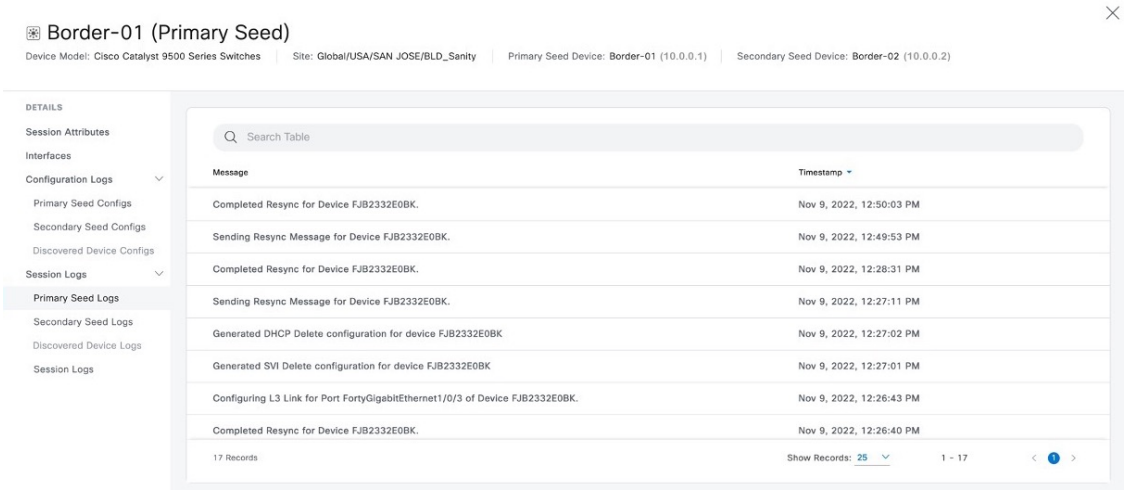


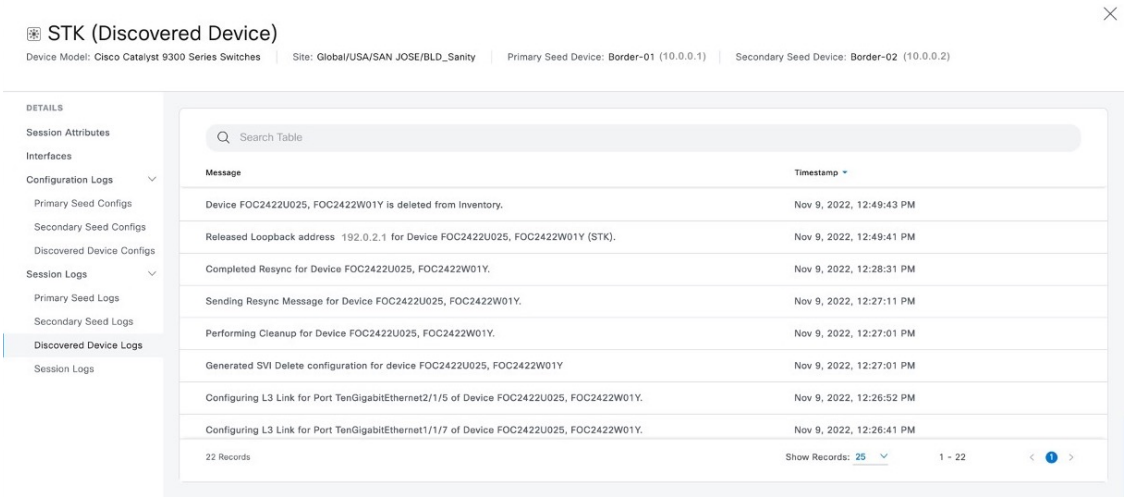
Step 4 To view the configurations that are pushed to the device, expand **Configuration Logs** in the left pane and select the device configuration.





Step 5 To view the device-specific logs, expand **Session Logs** in the left pane and the select the device log.





Create Link Between Interfaces

Configure additional links between interfaces after LAN automation stops.

Before you begin

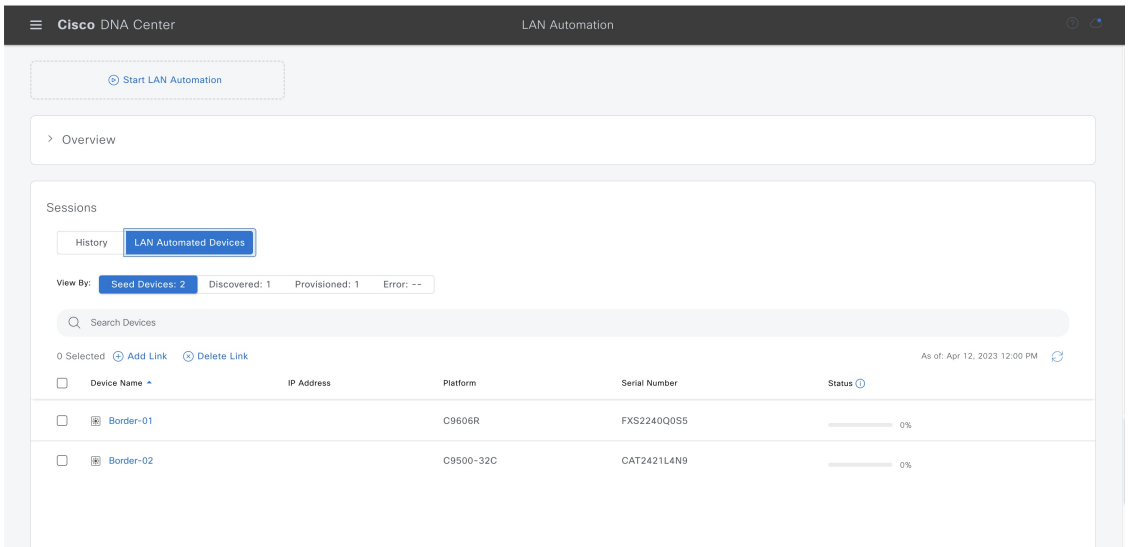
The following topic describes the steps to configure additional links between interfaces based on Catalyst Center 2.3.5. The steps may vary based on your Catalyst Center version.

Procedure

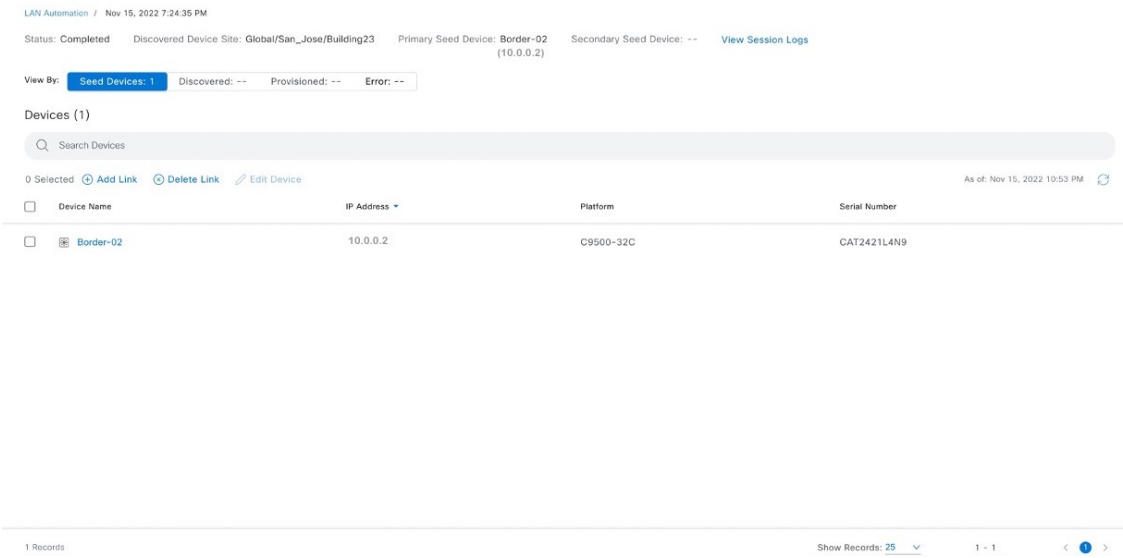
Step 1 From the top-left corner, click the menu icon and choose **Provision** > **LAN Automation**.

Step 2 Use one of the following options:

- Option 1: In the **LAN Automation Devices** tab of the LAN Automation window, click **Add Link**.

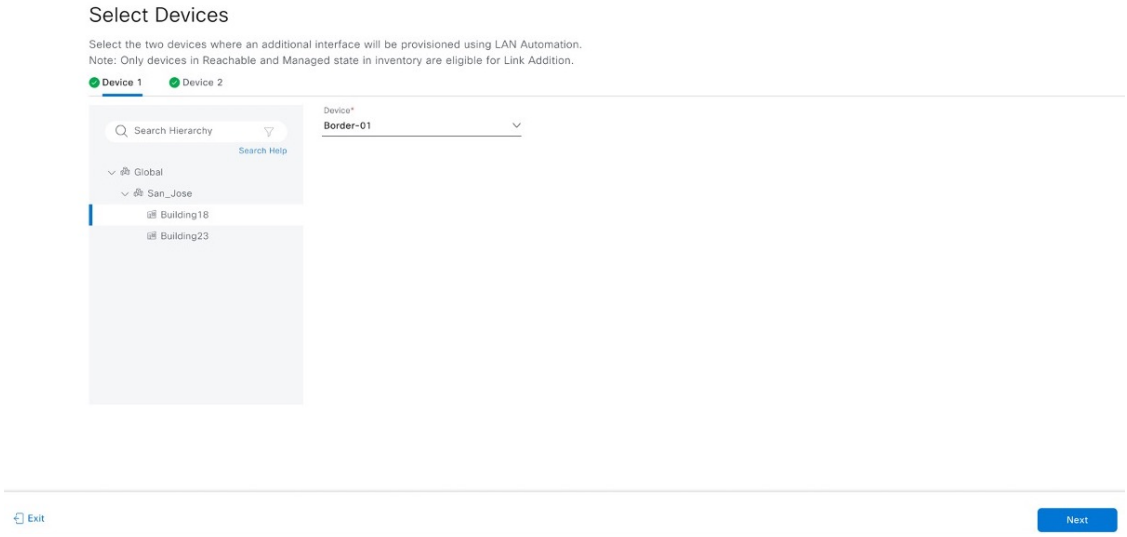


- Option 2: In the **History** tab, click on a session date to view the session details and click **Add Link**.

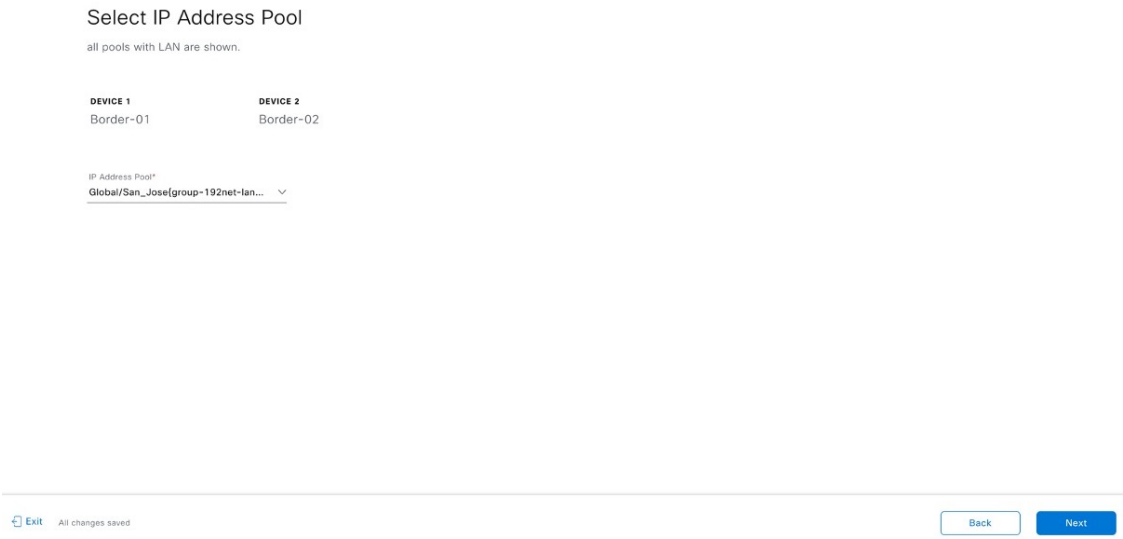


Step 3 Follow these steps in the **Add Link** workflow:

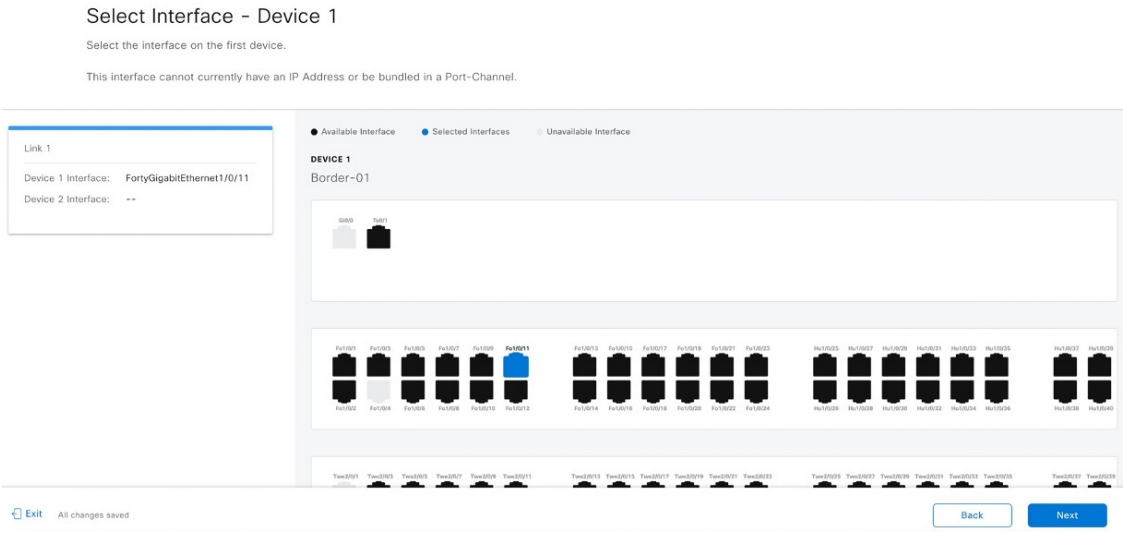
a) Select the two devices to establish the link.

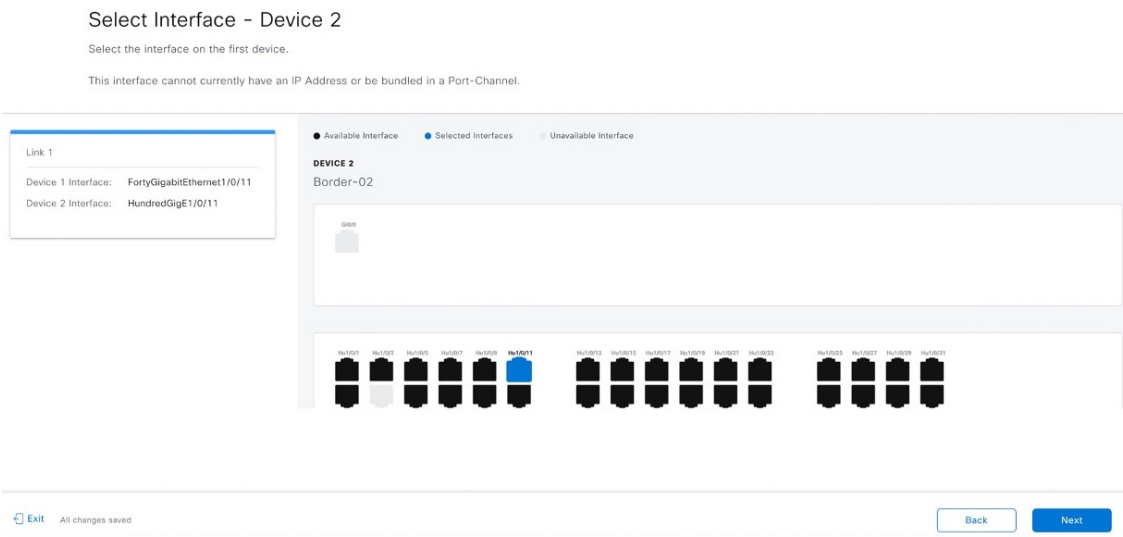


b) Select an IP address pool within the LAN. Ensure that the IP address pool is reachable from Catalyst Center.

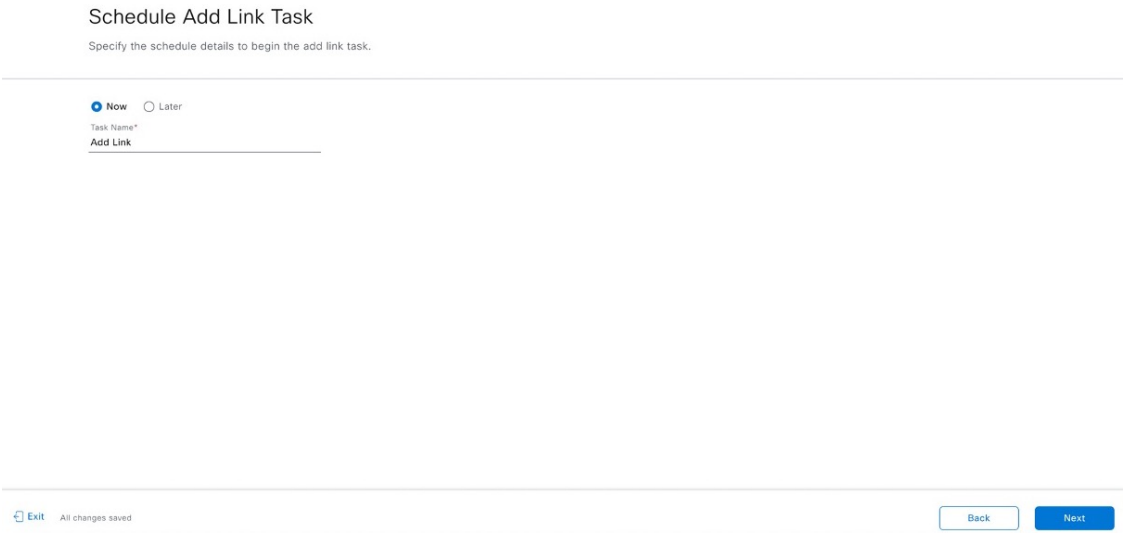


c) Select the interfaces on both the devices between which you want to establish a connection.

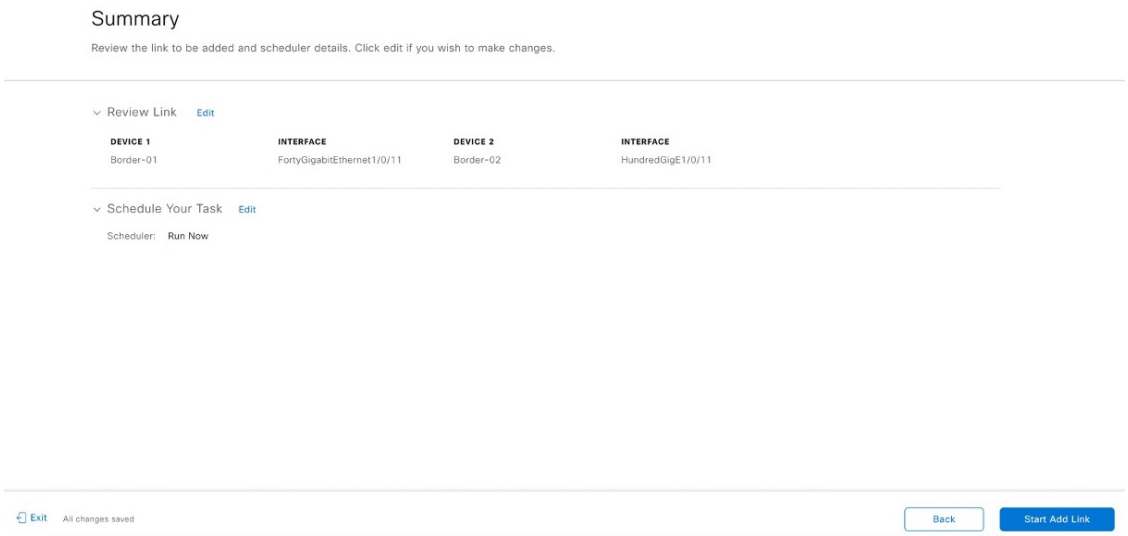




d) Click **Now** or **Later** to indicate when you want to provision the link. Enter a name for the task in the field provided.



e) In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.



f) Click **Start Add Link**.

The **Link Configuration Started Successfully** window appears.

Step 4 To see the status of the configuration, click **View Status in Activities**.

What to do next

To delete a link:

- Click **Delete link**.
- Select the devices and the interfaces.
- Click **Start Delete Link**.

Edit LAN Automated Devices

In Catalyst Center Release 2.3.7.5 and later, you can edit the hostname and Loopback0 interface IP address of a LAN automated device.

Before you begin

Ensure that you've reserved LAN IP pools and discovered the devices through LAN automation.

Note

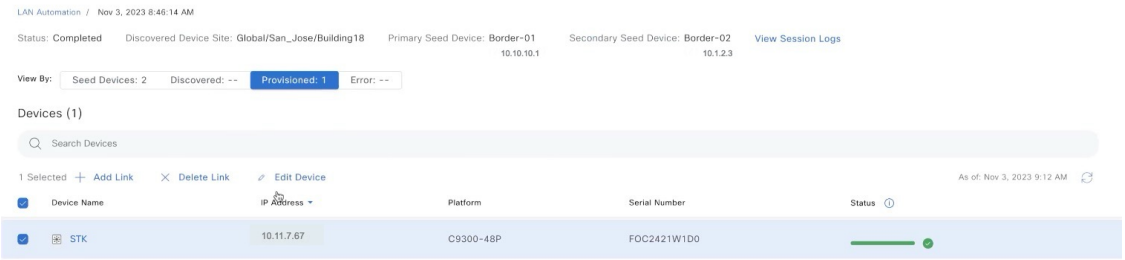
- In a Day-*1* scenario, the devices that you want to edit must be in a **Managed** state in the Catalyst Center inventory.
- You can edit the Loopback0 interface IP address for a maximum of 25 devices in a single Day-*1* workflow.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **LAN Automation**.

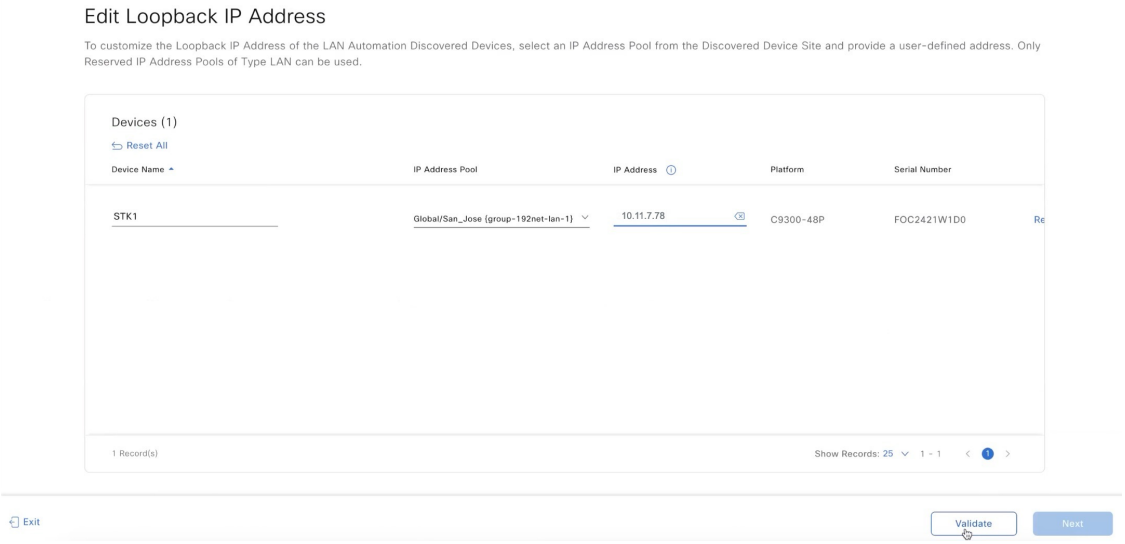
Step 2 In the **LAN Automation** window, click the **LAN Automated Devices** tab.

Step 3 Check the check box next to the device that you want to edit and click **Edit Device**.



Step 4 In the **Edit Devices** window, edit the **Device Name**, **IP Address Pool**, and **IP Address** fields, as required.

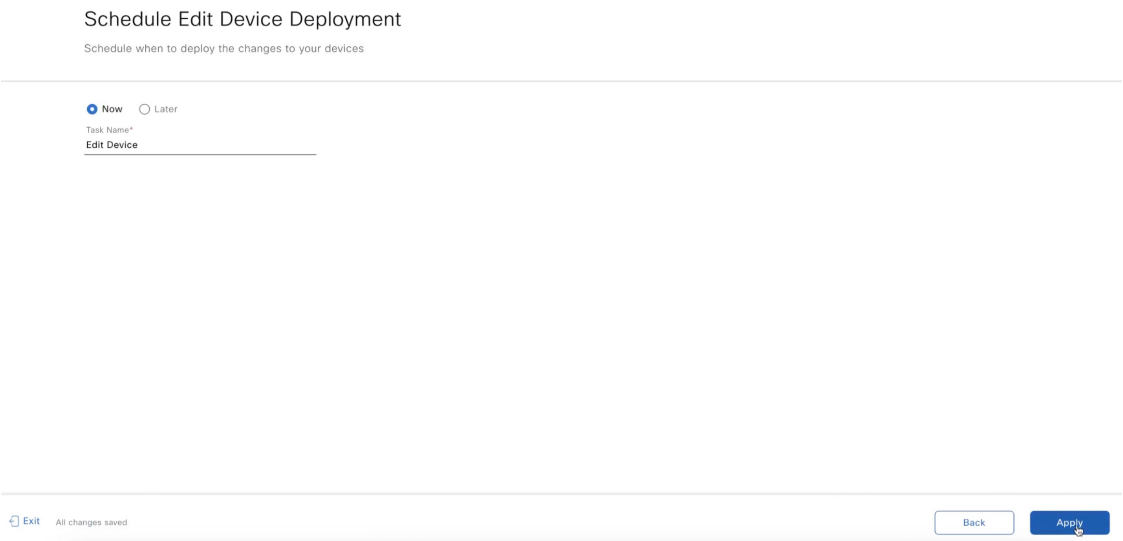
Enter the IP address without a subnet mask and ensure that the IP address is within the range of the selected IP address pool.



Step 5 Click **Validate** to validate the IP address allocation.

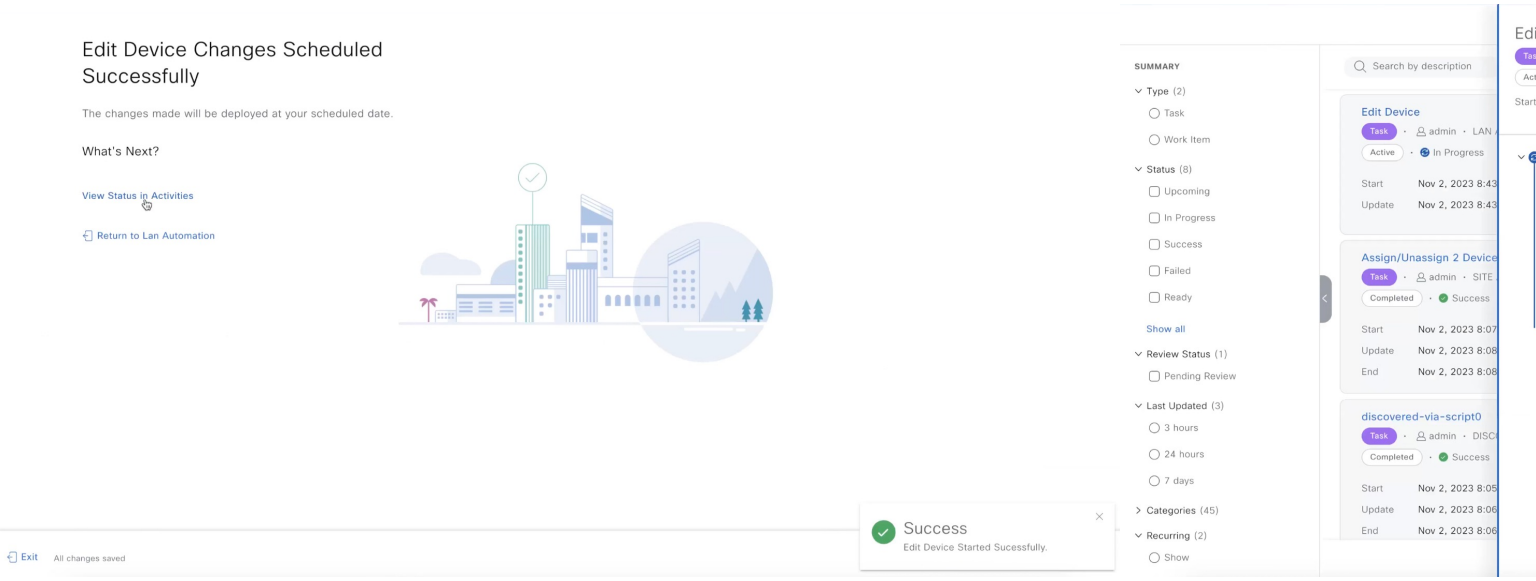
Step 6 After validation, click **Next**.

Step 7 Choose **Now** or **Later** to schedule the edit device deployment and click **Apply**.



What to do next

You can view the status of the edit task under the **Activities** > **Task** window.



Manage Devices in Strict Discovery Mode

In Catalyst Center Release 2.3.7.5 and later, you can choose between the **Relaxed** or **Strict** mode for device matching during discovery. In **Strict** mode, device discovery is restricted to the list of devices provided. Use the following procedure to add, edit, or delete devices from the list.

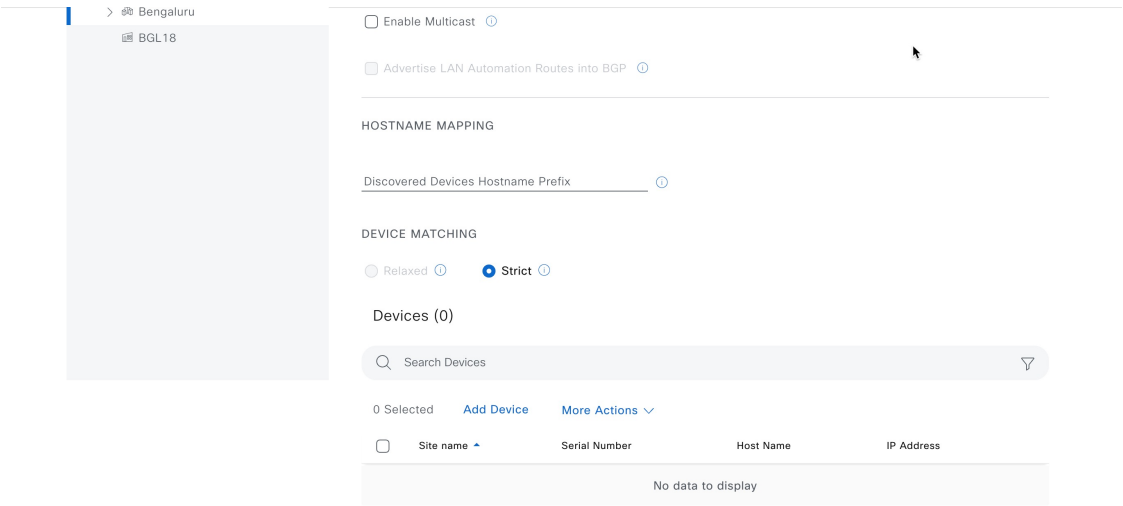
Procedure

Step 1 In the **LAN Automation** window, click **Start LAN Automation**.

Step 2 Add the seed devices, and click **Next**.

Step 3 In the **Session Attributes** window, in the left pane, select a building or a floor.

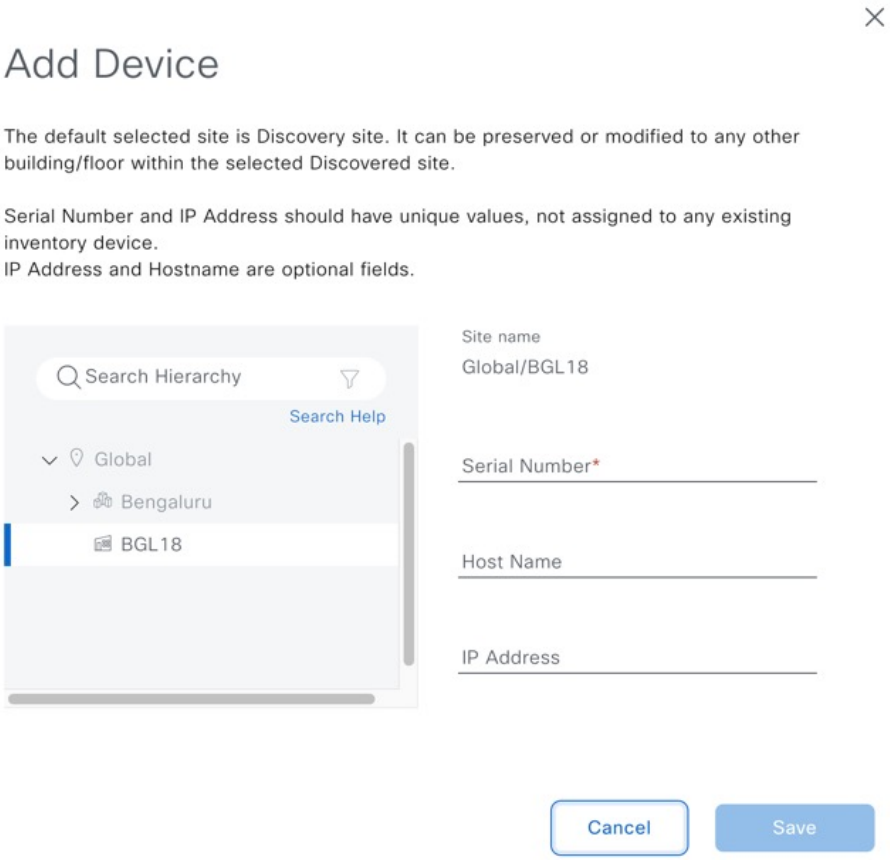
Step 4 Under **Device Matching**, select the **Strict** option.



Note It is mandatory to add a device list if you have selected an area as the site. When you select an area, the **Strict** mode is chosen automatically, and the **Relaxed** mode is disabled.

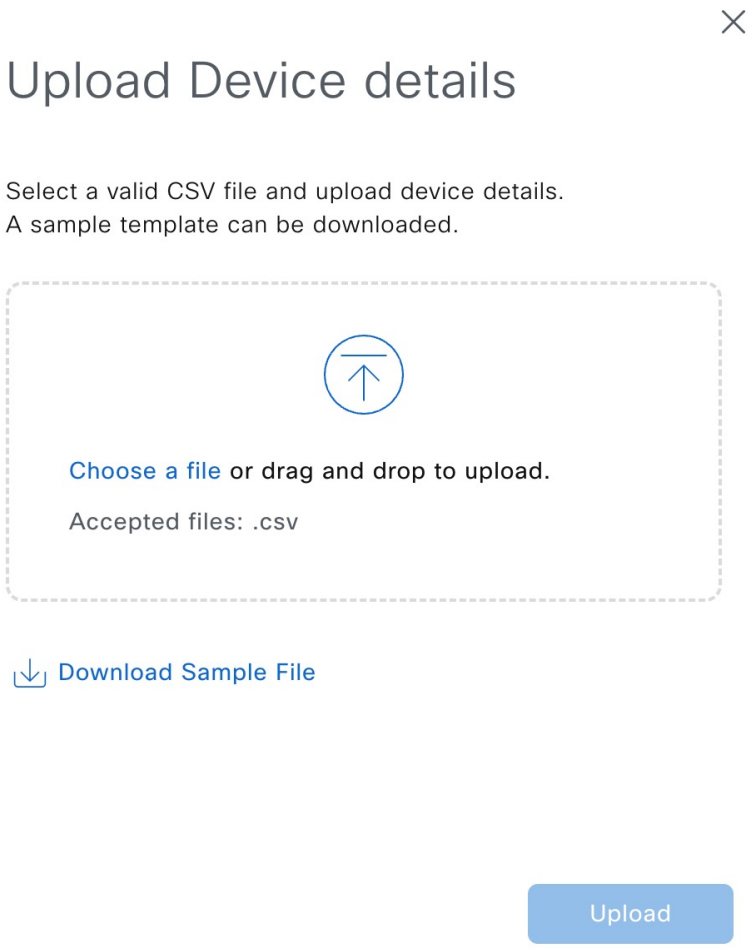
Step 5 Add devices using one of the following options:

- **Add Device**: Use this option to add a single device.
  - In the **Devices** table, click **Add Device**.
  - In the **Add Device** window, do the following:
    - **a.** If you've chosen an area, select a building or a floor as the site.
    - **b.** Enter a **Serial Number** for the device.
    - **c.** (Optional) Enter **Host Name** and **IP Address**.
    - **d.** Click **Save**.



- **Upload Device**: Use this option to add devices from a CSV file.
  - **a.** In the **Devices** table, click **More Actions** and choose **Upload Device**.
  - **b.** In the **Upload Device Details** window, drag and drop the CSV file into the boxed area or click **Choose a file** and browse to the CSV file.

    You can also download a sample template file.
  - **c.** Click **Upload**.



Step 6 To edit a device from the list of devices to be discovered, do the following:

a) Check the check box next to the device that you want to edit and choose **More Actions** > **Edit Device**.

b) Edit the device details, as required.

You can edit only one device at a time.

c) Click **Save**.

Step 7 To delete a device from the list of devices to be discovered, do the following:

a) Check the check box next to the device that you want to delete and choose **More Actions** > **Delete Device**.

You can select multiple devices to delete.

b) Click the **Delete** icon and confirm the delete action.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018–2022 Cisco Systems, Inc. All rights reserved.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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.