Cisco DNA Center SD Access LAN Automation Deployment Guide

LAN Automation: Step-by-Step Deployment  2
Workflow  2
Step 1: Plan  3
Step 2: Design  11
Step 3: Discover  14
Step 4: Provision  23
Add Switches and Links to an Existing LAN-Automated Stack  37
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 SD Access overlay network without the traditional network planning and implementation process.

This guide is based on Cisco DNA Center Release 1.2.6.

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 uncompromised 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 Cisco DNA Center.

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

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Plan</th>
<th>Design</th>
<th>Discover</th>
<th>Provision</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Understand the different roles in the LAN automation domain. Plan the site and IP pool and understand the prerequisites for seed devices.</td>
<td>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.</td>
<td>Discover seed devices.</td>
<td>Start and stop LAN automation:</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td>a) Start LAN automation: Push the temporary configuration to seed devices, discover devices, upgrade the image, and push the initial configuration to discovered devices.</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td>b) Stop LAN automation: Convert all point-to-point links to Layer 3.</td>
</tr>
</tbody>
</table>
**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 Cisco DNA 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.

**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 Cisco DNA Center and support the integrated PnP server function. Cisco DNA 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.

![Cisco DNA Center™](image)

**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 Cisco DNA 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.
Supported Switches for Each Role at Different Layers

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

![Diagram showing supported switches for different roles at different layers]

Cisco LAN Automation Product Support Matrix

<table>
<thead>
<tr>
<th>Role</th>
<th>Product Model</th>
<th>Network Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seed PnP agent</td>
<td>C9500-12Q</td>
<td>Any front-panel ports</td>
</tr>
<tr>
<td></td>
<td>C9500-24Q</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C9500-40X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C9500-16X</td>
<td></td>
</tr>
<tr>
<td>Seed PnP agent</td>
<td>C9404R</td>
<td>Sup-1</td>
</tr>
<tr>
<td></td>
<td>C9407R</td>
<td>Sup-1XL</td>
</tr>
<tr>
<td></td>
<td>C9410R</td>
<td>Sup-1XL-Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Any line card</td>
</tr>
<tr>
<td>Seed PnP agent</td>
<td>C9300-24T</td>
<td>Any uplinks and module ports</td>
</tr>
<tr>
<td></td>
<td>C9300-24P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C9300-24U</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C9300-48T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C9300-48P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C9300-48U</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C9300-24UX</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C9300-48UXM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C9300-48UN</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>Product Model</td>
<td>Network Module</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Seed</td>
<td>C6807-XL</td>
<td>Sup6T</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Any uplinks and module ports</td>
</tr>
<tr>
<td>Seed</td>
<td>C6880-X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C6880-X-LE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Any uplinks and module ports</td>
</tr>
<tr>
<td>Seed</td>
<td>C6816-X-LE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C6832-X-LE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C6824-X-LE-40G</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C6840-X-LE-40G</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Any front-panel ports</td>
</tr>
<tr>
<td>Seed</td>
<td>WS-C4503-E</td>
<td>Sup9-E</td>
</tr>
<tr>
<td>PnP agent</td>
<td>WS-C4506-E</td>
<td>Sup8-E</td>
</tr>
<tr>
<td></td>
<td>WS-C4507R+E</td>
<td>Any uplinks and module ports</td>
</tr>
<tr>
<td></td>
<td>WS-4510R+E</td>
<td></td>
</tr>
<tr>
<td>Seed</td>
<td>WS-C3850-24T</td>
<td>Any uplinks and module ports</td>
</tr>
<tr>
<td>PnP agent</td>
<td>WS-C3850-48T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3850-24P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3850-48P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3850-48F</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3850-24U</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3850-48U</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3850-24XU</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3850-12X48U</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3850-12S</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3850-24S</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3850-12XS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3850-24XS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3850-48XS</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>Product Model1</td>
<td>Network Module</td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Seed</td>
<td>WS-C3650-24TS</td>
<td>Any uplinks and module ports</td>
</tr>
<tr>
<td></td>
<td>WS-C3650-48TS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3650-24PS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3650-48PS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3650-48FS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3650-24TD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3650-48TD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3650-24PD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3650-24PDM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3650-48PD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3650-48FD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3650-8X24PD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3650-12X48FD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3650-48TQ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3650-48PQ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3650-48FQ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3650-48FQM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3650-8X24UQ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3650-12X48UQ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3650-12X48UR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C3650-12X48UZ</td>
<td></td>
</tr>
</tbody>
</table>

1 LAN automation does not support a dedicated management port.
2 LAN automation does not support a breakout cable.
3 LAN automation does not support a 40-G uplink.

**Site Planning**

Use the Cisco DNA 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 the following constraints:

- In Release 1.1.x, LAN automation lets you choose only one site for the seed, peer seed, and PnP devices, meaning all devices must belong to a single site.

- 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 Cisco DNA 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. The second part of the IP pool is used for link configuration between connected devices that participate in the discovery session. Participating devices are primary seed, peer seed, and discovered devices in the discovery session. All links between these devices are configured with Layer 3 as required for IS-IS routing. The only exceptions are the links connected to the primary seed device that are not selected while starting discovery. These links could be links between seed devices or links between seed and discovered devices. For each configured link, a /30 subpool (4 IP addresses) is allocated. For example, in a topology that contains four links, LAN automation allocates 16 IP addresses for the Layer 3 link configuration.

3. The third part of the IP pool is used to allocate a single loopback IP per discovered device. If the seed device or peer seed devices do not have loopback IPs configured, they are also configured with the loopback IPs. Internally, the IPAM library allocates a /27 pool for single IPs. For example, when the LAN pool requests the first loopback IP for a device, the IPAM library allocates a /27 pool (32 IP addresses) and returns one IP from this pool. On subsequent requests, the library continues to give IPs from the previously allocated /27 pool until it runs out of IPs. So for a /27 IP, the same internal pool is used for the 30 IP allocation. Currently, only 30 of the 32 IPs in the internal pool can be used for loopbacks. If the internal pool cannot be used for IP allocation, another /27 pool is allocated for additional single IP allocation. In this case, loopback allocation for discovered device number 31 results in a new /27 subpool allocation.

**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 /30 pool is reserved for the point-to-point links, and a /27 pool is reserved for loopback addresses. Because there are 10 devices with two links each, a total of 2*10*4 = 80 IP addresses are reserved for point-to-point links and 10 loopback addresses are reserved.

In total, 100 IP addresses are reserved for the 10 devices: 10 for each VLAN 1, 10 for each loopback, and 80 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 128 available IP addresses in the IP pool. If you decide to run LAN automation multiple times with the same pool, you should 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 primary and peer seed device.

Site-Specific CLI and SNMP Configuration

To start LAN automation, a site-specific CLI and SNMPv2 read/write or SNMPv3 configuration is required. Use the Cisco DNA Center Design application to configure the site-specific CLI and SNMPP. 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.

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 Cisco DNA Center so that Cisco DNA Center has IP reachability to the LAN IP pool subnet.

• We recommend that you use the default interfaces connected to discovery devices. If the peer seed device has IP interfaces configured on the interfaces connected to discovery devices, those links don't get configured. If you want to configure the peer device interfaces connected to discovery devices, 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 and Cisco Catalyst 9500H devices 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 Cisco DNA Center.

• Ensure that the seed devices don't have any other interfaces connected to another DHCP server running in VLAN 1.

• If any configuration changes are made on the seed devices before running LAN automation, synchronize the seed devices with the Cisco DNA 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 discovery devices that do not participate in the upcoming discovery session.

  For example, imagine that seed devices are in Building-23 and are connected to discovery devices 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 discovery devices 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 block the ports for the discovery interfaces that are not required.

- **Endpoint/client integration:** Similarly, 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.

**Discovery Device Initial State**

The initial state of discovery devices depends on the usage.

New discovery devices have factory defaults and are ready to start LAN automation.

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

- Discovery devices must have the required license that can push the LISP, IS-IS routing, and CTS-related CLIs. Use the `show license` command to see the current license level and upgrade the license, if required.
- Discovery devices should be in a clean state. They should not have stale certificate, keys, and so on from the previous runs.
- Bring the device back to the factory defaults by clearing the following from the switch console:

  ```
  [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)
  write
  [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)
  ```

**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 network services 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 Cisco DNA Center home page, click **Design**.

**Step 2**  
Go to **Network Hierarchy > Add Site**.

**Step 3**  
Similarly, add buildings and floors.

**Step 4**  
Go to **Design > Network Settings > Device Credentials**.

**Step 5**  
Click **Add** and enter the CLI credentials.

**Step 6**  
Click **SNMPV2C Read** and enter the SNMP read credentials.

**Step 7**  
Click **SNMPV2C Write** and enter the SNMP write credentials.
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.

The **Enable Password** field is mandatory.

---

**Step 8**

Go to **Design > Network Settings > IP Address Pools**.

**Step 9**

Click **Global** in the left navigation tree and click **Add IP Pool**.

**Step 10**

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 IP pool that consists of a loopback address or other addresses configured on primary and peer seed devices.

---

**Step 11**

Go to **Design > Network Settings > Site**.
**Step 12**  At the site level, click **Reserve IP Pool**. 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 Cisco DNA Center home page, choose **> Discovery**. You can also access the **Discovery** page from the **Tools** section of the Cisco DNA Center home page.

**Step 2**  On the **New Discovery** page, 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 Cisco DNA 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** to add the credentials.
- **Advanced**: Specify one or more protocols for the discovery scan to use. Click the **SSH** and/or **Telnet** radio button.

**Note**: If you choose SSH, ensure that the seed is configured for SSH.
Step 3  
Click **Start**. The Discovery settings and details are displayed.

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

Step 4  
To verify that the discovered device is added to the Inventory page, go to **Inventory**.
Make sure that the discovered device has a Reachability Status of Reachable and a Last Inventory Collection Status of Managed.

**Step 5**  
To add the discovered seed to the same site, choose Provision > Devices > Inventory.

**Step 6**  
Select the device and go to Actions > Assign Device to Site. For Cisco DNA 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).

**Step 7**  
On the Assign Device to Site page, choose a site from the Choose a site drop-down list.

**Step 8**  
Click Apply. The discovered device is added to the selected site.
If you don’t see the Site column on the Device Inventory page, click ![Site](Site.png), 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 Cisco DNA Center

LAN automation discovery uses the LAN pool to reach discovery devices. Cisco DNA Center should be able to reach the IPs allocated from the LAN pool. For example, if the LAN pool is 192.168.10.0, Cisco DNA Center should have the correct route to reach this subnet. To test the reachability, create an SVI on the primary seed device and ping a test between Cisco DNA Center and the seed. Refer to the following sample code.
If the ping test fails, the route is not set up correctly on Cisco DNA Center.

**Static Route Addition for LAN Pool**

Cisco DNA 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, Cisco DNA Center performs the host function with the default gateway providing IP routing. In a multi-home design, Cisco DNA 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*
If the network design is a multi-homed design, one way to fix the IP reachability issue is to add a static route on Cisco DNA Center. A network administrator can add a static route during the initial Cisco DNA 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 Cisco DNA Center.

To add a static route on Cisco DNA Center:

**Procedure**

**Step 1** On the Cisco DNA 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.

Discovery Device Initial State Before Starting LAN Automation

Procedure

Step 1 Before starting LAN automation, make sure that the discovered device 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 config. 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.

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 Discovery Device 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, close the seed link connecting to the discovery device. That way, discovery doesn't occur until you are ready to open the port.
**Unplug the Management Port**

Connect discovery devices directly to seed devices. Do not connect discovery devices 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 discovery devices are Layer 2 and defaulted. For example, Catalyst 6500 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 discovery devices is not STP blocking.

**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 Cisco DNA Center home page, choose **Tools > Inventory**.

**Step 2**
Filter the devices by **Serial Number** and then choose **Actions > Delete**.

**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 Cisco DNA Center home page, choose **Tools > Network Plug and Play.**

Step 2  Go to **Devices > 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:

```bash
(on discovery device)
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
```

Step 4  Check the check box of the device in the **Unclaimed** section and click **Delete.**

---

**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 discovery device.
   - Discovers 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 Cisco DNA Center home page > **Design > Image repository.**

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 discovery devices that can be onboarded through the LAN automation session. For example, consider four directly connected discovery devices: 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 discovery devices 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 discovery devices. Currently, there is one site for seed device(s) and one site for discovery devices.

**LAN Pool Selection**

The LAN pool is selected based on discovery device 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**: Cisco DNA 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.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge1</td>
<td>FCW2048Cxxx</td>
</tr>
<tr>
<td>Edge2</td>
<td>FCW2131Lxxx, FCW2131Gxxx, FCW2131Gxxx, FCW2131Gxxx</td>
</tr>
<tr>
<td>Edge3</td>
<td>FOC2052Xxxx, FCW2052Cxxx, FCW2052Fxxx</td>
</tr>
<tr>
<td>Edge4</td>
<td>FXS2131Qxxx</td>
</tr>
</tbody>
</table>

**Procedure**

**Step 1** From the Cisco DNA Center home page, choose **Provision > Devices > LAN Automation**.
Step 2  Enter the required details and click **Start**.

Step 3  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

!exec: enable
!
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 *
ispf level-1-2
metric-style wide
nsf ietf
log-adjacency-changes
bfd all-interfaces
passive-interface Loopback0
default-information originate
!
interface Loopback0
ip router isis
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
!
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
bfd interval 500 min_rx 500 multiplier 3
no bfd echo
exit
!
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
Secondary Seed Configuration

```
!exec: enable
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 *
ispf level-1-2
metric-style wide
nsf ietf
log-adjacency-changes
bfd all-interfaces
passive-interface Loopback0
default-information originate
!
interface Loopback0
ip router isis
exit
!
```

Step 4  
After device discovery starts, view logs on the discovery device.

**Note**  
Do not press the Enter key on the discovery device 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-config (Timed out)
```
Step 5
After the device is discovered, Cisco DNA 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, Cisco DNA 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 19:21:26.034: %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
%INSTALL-5-OPERATION_COMPLETED_INFO: Completed install package flash:{<package_name>}

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

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...

Cisco DNA Center pushes part of the configuration, allowing the devices to be onboarded and managed by Cisco DNA 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 6
View the logs on the discovery device, as shown in the following example. It is safe to press the Enter key on the console if you want to. When you press the Enter key, the hostname changes to the value entered in the Hostname Mapping field when you started the 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
After all devices are discovered, the **Discovered Devices** status changes to **Completed** and the discovered devices are added to the inventory.
Step 7  
From the Cisco DNA Center home page, choose **Tools > Inventory** and filter by serial number. The newly discovered switches appear as **Managed**.

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

```plaintext
! 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 udl 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 cisco
ispf level-1-2
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

**Step 8** 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 stop LAN automation to finish discovering all required devices and to prevent inadvertent discovery of additional devices. 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 Cisco DNA 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.)

```plaintext
interface GigabitEthernet1/0/13
  description Fabric Physical Link
  no switchport
dampening
  ip address 192.168.2.97 255.255.255.252
  ip router isis
  ip lisp source-locator Loopback0
  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 Cisco DNA 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, 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 Cisco DNA 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 Cisco DNA 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.

![Image showing serial number before addition](image.png)

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

![Image showing serial number after addition](image2.png)
Add an Existing Switch

This section explains how to add an existing switch that was already present in Cisco DNA 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 Cisco DNA 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

**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 Cisco DNA 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 the new link is to be configured.

**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 used.

```
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 lisp source-locator Loopback0
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 lisp source-locator Loopback0
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.
### Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

### Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

### Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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](http://www.cisco.com/go/offices).