

Configuring Inband Management and Out-of-Band PnP, Release 4.1.1

Table of Contents

New and changed information . . . 1
Inband management in External fabrics and Classic LAN fabrics . . . 2
  Inband management . . . 2
  Prerequisites . . . 3
Inband POAP management in External fabrics and Classic LAN fabrics . . . 5
  Inband POAP . . . 5
  Prerequisites . . . 5
  Guidelines and limitations . . . 6
  Enable inband management and POAP on External fabrics and Classic LAN fabrics . . . 6
  Add switches . . . 7
    Pre-provision switches to a fabric . . . 7
    Import switches using the bootstrap mechanism . . . 7
  Add an interface . . . 8
  Add a policy to a fabric . . . 8
  Recalculate and deploy configurations on a switch . . . 9
Inband management and inband POAP in Data Center VXLAN EVPN fabrics . . . 10
  Prerequisites for inband and out-of-band management . . . 11
  Guidelines and limitations . . . 12
  Enable inband POAP on Data Center VXLAN EVPN fabrics . . . 13
  Import switches in a Brownfield deployment . . . 14
  Pre-provision switches through inband POAP . . . 14
  Add a policy for Data Center VXLAN EVPN fabrics . . . 15
  Change the fabric management mode . . . 15
Secure POAP . . . 17
  Prerequisites for secure POAP . . . 17
Out-of-Band PnP in Campus VXLAN EVPN fabrics . . . 18
  About Out-of-Band PnP in Campus VXLAN EVPN fabrics . . . 18
  Enable Out-of-Band PnP . . . 18
  Import switches using the bootstrap method . . . 19
  Enable DHCP for PnP . . . 19
Copyright . . . 21

New and changed information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Release Version	Feature	Description
Nexus Dashboard 4.1.1	Improved navigation and workflow when configuring inband management and out-of-band PnP	Beginning with Nexus Dashboard 4.1.1, the navigation and workflow when configuring inband management and out-of-band PnP in Nexus Dashboard have been enhanced.

Inband management in External fabrics and Classic LAN fabrics

Starting with the Nexus Dashboard 4.1 release, **Classic LAN** is considered an upper-level category, under which you can find these fabric types:

- Enhanced Classic LAN (both for creating new deployments and onboarding existing networks)
- Legacy Classic LAN (for onboarding existing networks)

See Editing Classic LAN Fabric Settings for more information.

Inband management

Cisco Nexus devices have dedicated out-of-band (OOB) management ports (mgmt0) to manage devices via telnet or SSH connections.

You can manage Cisco Nexus devices through inband using front panel ports either by assigning management IP addresses on one of the ports or using loopback or SVI. By default, (mgmt0) interface is part of management VRF.

In Nexus Dashboard by default, VRF is used for inband management, you can use other defined VRFs for inband management for nexus devices. Inband Management is the ability to administer a network through LAN connection.

You can import or discover switches with inband connectivity for External and Classic LAN fabrics in Brownfield deployments only. Enable inband management per fabric, while configuring or editing the Fabric settings. You cannot import or discover switches with inband connectivity using POAP.

After configuration, the Fabric tries to discover switches based on the VRF of the inband management. The fabric template determines the VRF of the inband switch using seed IP. If there are multiple VRFs for the same seed IP, then no intent will be learned for seed interfaces. You must create intent or configuration manually.

After configuring or editing the Fabric settings, you must Deploy Config. You cannot change the inband management settings after you import inband managed switches to the Fabric. If you uncheck the check box, the following error message is generated.

```
Inband IP <<IP Address>> cannot be used to import the switch,
please enable Inband Mgmt in fabric settings and retry.
```

After the switches are imported to the Fabric, you must manage the interfaces to create intent. Create the intent for the interfaces that you are importing the switch. Edit\update the Interface configuration. When you try to change the Interface IP, for this inband managed switch, an error message is generated:

```
Interface <<interface_name>> is used as seed or next-hop egress interface
```

for switch import in inband mode.
IP/Netmask Length/VRF changes are not allowed for this interface.

While managing the interfaces, for switches imported using inband management, you cannot change the seed IP for the switch. The following error will be generated:

<<switch-name>>: Mgmt0 IP Address (<ip-address>) cannot be changed,
when is it used as seed IP to discover the switch.

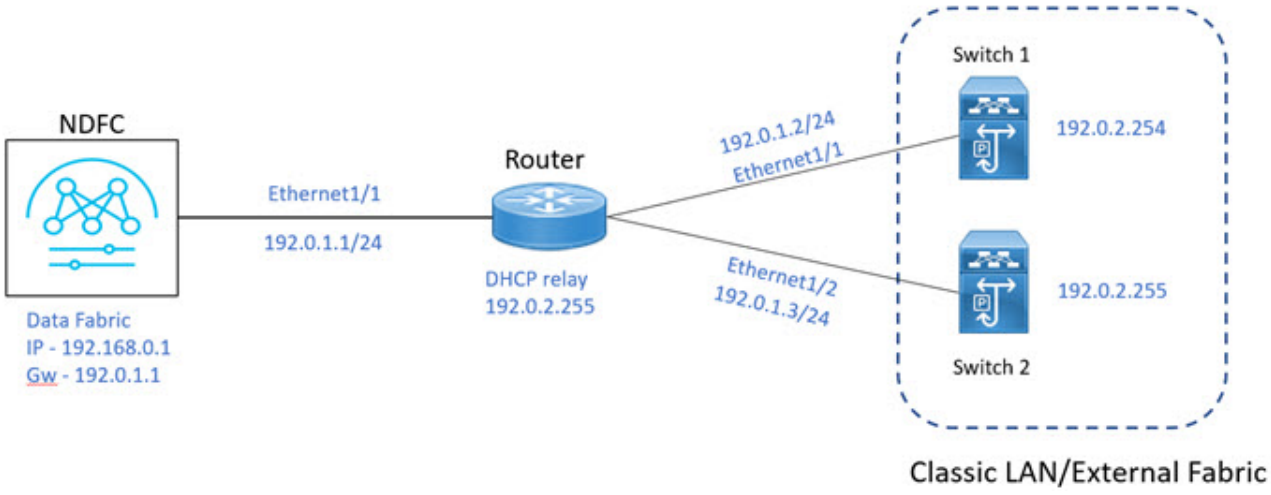
Create a policy for next-hop interfaces. Routes to Nexus Dashboard from 3rd party devices can contain multiple interfaces, which are known as ECMP routes. Find the next-hop interface and create an intent for the switch. Interface IP and VRF changes are not allowed.

If inband management is enabled, during Image management, the data interface of nexus dashboard is used to copy images on the switch, in ISSU, EPLD, RPM & SMU installation flows.

If you import the switches using inband connectivity in the fabric and later disable the inband Mgmt in the Fabric settings after deployment, the following error message is generated:

The fabric <<fabric name>> was updated with below message:
Fabric Settings cannot be changed for Inband Mgmt when switches are already imported using inband Ip.
Please remove the existing switches imported using Inband IP from the fabric, then change the Fabric Settings.

However, the same fabric can contain switches imported using both inband and out-of-band connectivity.



Prerequisites

The following are the prerequisites for using inband management:

- Configure the appropriate data network routes for reachability to the switch inband interfaces. Choose **Admin > System Settings > General**, locate the **Routes** area, then click **Edit** to enter route IP addresses in the **Data network routes** area.
- On the Nexus Dashboard Web UI, navigate to **Admin > System Settings > Fabric management > Advanced settings > Admin** and choose **Data** from the **LAN Device Management Connectivity** drop-down list to manage Data Center VXLAN EVPN fabrics through inband management, or an error message is displayed. If you choose **Data**, ensure that the required data service IP addresses are available in the Nexus Dashboard **External Service Pools** area (**Admin > System Settings > General > External pools**).



When server settings changed from **Data** to **Management** or vice-versa, allow some time for syslog or poap functionalities to be online and ensure that the IP addresses in Cluster configuration are moved to the appropriate pool.

Inband POAP management in External fabrics and Classic LAN fabrics

Inband POAP

Power On Auto Provisioning (POAP) automates the process of upgrading software images and installing configuration files on devices that are deployed on the network for the first time. POAP allows devices to bring up without performing any manual configuration.

When a POAP feature enabled device boots and does not find the startup configuration, the device enters POAP mode, locates a DHCP server, and bootstraps itself with its interface IP address, gateway, and DNS server IP addresses. The device obtains the IP address of a TFTP server and downloads a configuration script that enables the switch to download and install the appropriate software image and configuration file.

By using the POAP (Power On Auto Provisioning) feature of Nexus switches, Nexus Dashboard can automate the deployment of new datacenters reducing overall time and effort.

External Fabrics and Classic LAN fabrics support adding switches through POAP from inband interfaces.

The inband POAP is supported for all the roles for fabrics with External and Classic LAN templates.

Prerequisites

The following are the prerequisites for using inband poap:

- Configure the appropriate data network routes for reachability to the switch inband interfaces. Choose **Admin > System Settings > General**, locate the **Routes** area, then click **Edit** to enter route IP addresses in the **Data network routes** area.
- On the Nexus Dashboard Web UI, navigate to **Admin > System Settings > Fabric management > Advanced settings > Admin** and choose **Data** from the **LAN Device Management Connectivity** drop-down list to manage Data Center VXLAN EVPN fabrics through inband management, or an error message is displayed. If you choose **Data**, ensure that the required data service IP addresses are available in the Nexus Dashboard **External Service Pools** area (**Admin > System Settings > General > External pools**).

  When server settings changed from **Data** to **Management** or vice-versa, allow some time for syslog or poap functionalities to be online and ensure that the IP addresses in Cluster configuration are moved to the appropriate pool.

- Inband POAP on the Bootstrap tab is supported only when inband management is enabled on Advanced tab in the Fabric settings.

  Each subnet for the defined DHCP subnet scope that is mentioned in fabric settings must have a valid route for reverse traffic.

  Ensure that the DHCP relay functionality is set on intermediate routers.

Guidelines and limitations

- These are the guidelines and limitations for inband management:
  - Both inband and out-of-band switches in the same fabric is not supported.
  - When you add switches to fabric, ensure that the switches are not in maintenance mode.
- These are the guidelines and limitations for inband POAP:
  - Inband POAP is supported for NX-OS switches only.
  - You can enable inband POAP with Nexus Dashboard as a Local DHCP Server or on External DHCP Servers.
  - Inband POAP supports Multi Subnet scope.
  - Inband POAP requires the external router connected seed switches to have the following capabilities:
    - DHCP relay functionality
    - eBGP peering
- Enabling inband management and POAP is not supported in these situations:
  - When creating a new Classic LAN (Enhanced Classic LAN) fabric
  - When onboarding an existing Classic LAN (Enhanced) fabric
- However, enabling inband management and POAP is supported when onboarding an existing Classic LAN (Legacy) fabric.

Enable inband management and POAP on External fabrics and Classic LAN fabrics



For Classic LAN fabrics, enabling inband management and POAP is supported only when onboarding an existing Classic LAN (Legacy) fabric. For more information, see Inband management in External fabrics and Classic LAN fabrics and Guidelines and limitations.

To enable inband POAP on a fabric:

1. Navigate to **Manage > Fabrics**, then choose the appropriate fabric.
2. Click **Actions > Edit Fabric Settings**.
3. Click **Fabric Management**.
4. Click **Advanced**, then check the box in **Inband Mgmt**.
5. Click **Bootstrap**, then configure these settings:
   - Check the box in **Enable Bootstrap**.
   - Check the box in **Enable Local DHCP Server** and enter appropriate IP addresses in the required fields.

Add switches

To add or discover switches through inband POAP, follow these steps:

1. Pre-provision switches to a fabric
2. Add an interface
3. Add a policy to a fabric
4. Import switches using the bootstrap mechanism

Pre-provision switches to a fabric

To add switches to fabric:

1. Navigate to **Manage > Fabrics**, then click the appropriate fabric.

   The **Overview** window for that fabric appears.

2. Choose **Inventory > Switches** and click **Actions > Add Switches**.

   The **Add Switches** window appears.

3. Choose **Pre-provision** radio button.
4. Click **Actions** and add switches.

   You can add switches one at a time using the Add option or add multiple switches at the same time using the **Import** option.

   If you use the **Add** option, ensure you enter all the required details.

5. Choose a switch.
6. Enter the password in the **Admin password** field.
7. Click **Pre-provision**.

   The pre-provisioned switch is added.



For pre-provisioned switches, you can add dummy values for the serial number. After configuring the network successfully, you can change serial number with the appropriate number of the switch on the **Switches** tab. See the "Change Serial Number" section in "Performing Actions on Switches" in Working with Inventory in Your Nexus Dashboard LAN or IPFM Fabrics.

Import switches using the bootstrap mechanism



Ensure that you have pre-provisioned switches, added interface, and policy before importing the switches using the bootstrap mechanism.

To import switches using the bootstrap mechanism:

1. Navigate to **Manage > Fabrics**, then click the appropriate fabric.

The **Overview** window for that fabric appears.

2. Choose **Inventory > Switches** and click **Actions > Add Switches**.

   The **Add Switches** window appears.

   You can view the existing added switches in the **Switches to Bootstrap** area.

3. Choose **Bootstrap (POAP)** radio button and enter a password in **Admin password** field.
4. Choose the required switches and click **Import Selected Switches** to bootstrap switches.

Add an interface

Add an interface to configure the interface IP addresses on the required switch.

Before you begin:

Ensure that you have added the required configurations on the switches such as IP addresses and static routes.

To add an interface:

1. Navigate to **Manage > Fabrics**, then click the appropriate fabric.

   The **Overview** window for that fabric appears.

2. Choose **Connectivity > Interfaces** and click **Actions > Create interface**.

   The **Create New Interface** window appears.

3. Choose **Ethernet** from the **Type** drop-down list.
4. Choose the required switch from the **Select a device** drop-down list and enter a name in the **Interface name** field.
5. Select the **int_routed_host** policy from the list of policies .
6. Enter the required configuration details in the **Interface IP** and **IP Netmask Length** fields.
7. Enter appropriate details in all the mandatory fields and ensure that you check **Enable Interface** check box and then click **Save**.

Add a policy to a fabric

You can add a freeform policy to define external routes in the switch. To add a policy:

1. Navigate to **Manage > Fabrics**, then click the appropriate fabric.

   The **Overview** window for that fabric appears.

2. Choose **Configuration Policies > Policies** and click **Actions > Add policy**.
3. Choose an appropriate switch from the **Switch List** drop-down list and click **Choose Template**.
4. On **Select Policy Template** window, select the **switch_freeform** template and click **Select**.

   The **switch_freeform** policy type allows you to add configurations in CLI format.

Recalculate and deploy configurations on a switch

To push pending configurations to switches:

1. Navigate to **Manage > Fabrics**, then click the appropriate fabric.

   The **Overview** window for that fabric appears.

2. Choose **Inventory > Switches**.

   You can see that the **Config status** column displays **Pending** status.

3. Choose **Actions > Recalculate and deploy**.

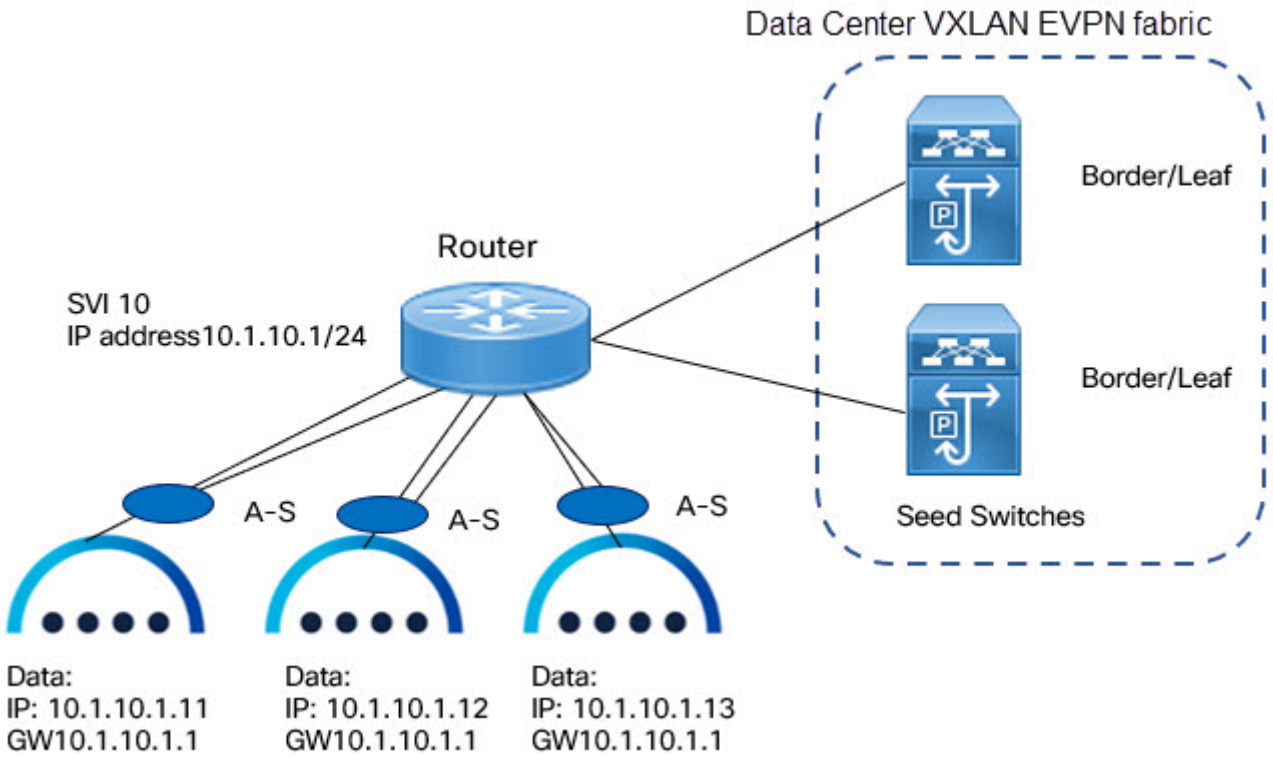
   The **Deploy Configuration** window appears. It displays the configuration status of the switches. You can also view the pending configurations by clicking the respective link in the **Pending Config** column.

   The **Pending Config** window appears. The **Pending Config** tab on this window displays the pending configurations on the switch. The **Side-by-Side Comparison** tab displays the running configuration and the expected configuration side-by-side.

4. Close the **Pending Config** window. When all the pending configuration is complete, the **Config status** column displays **In-Sync**.

Inband management and inband POAP in Data Center VXLAN EVPN fabrics

You can manage switches with inband connectivity and inband POAP for Data Center VXLAN EVPN fabrics. For inband management, the Loopback0 interface of the devices is used in the Fabric Settings.



If you want POAP Layer-3 adjacency to the switches, you must add the Nexus Dashboard node IP address as DHCP Relay address:

1. Navigate to **Admin > System Settings**.
2. Click **Fabric management**.
3. In the **Advanced settings** area, click **Admin**.
4. Note the setting in the **LAN Device Management Connectivity** field.
    - If the default value is set to **Management** in the **LAN Device Management Connectivity** field, then the DHCP Relay address must be set to the management interface IP (bond1br) in all Nexus Dashboard nodes.
    - If the default value is set to **Data** in the **LAN Device Management Connectivity** field, then the DHCP Relay address must be set to the data interface IP (bond0br) in all Nexus Dashboard nodes.

You can add switches with inband management enabled for Data Center VXLAN EVPN fabrics either in Greenfield or brownfield deployment with inband POAP or pre-provision and inband POAP.

- For Brownfield deployment, check **Preserve Config** check box.
- For Greenfield deployment, uncheck **Preserve Config** check box.

Importing switches with the **Preserve Config** option enabled will not work under the following conditions:

- You have more than 100 VRFs and 500 networks, and
- You are running on either of the following NX-OS images:
  - 7.0(3)I7(9)
  - 7.0(3)I7(10)

In these conditions, the switches will stay in migration mode. Upgrade to NX-OS release 9.x or later to resolve this issue.

The seed switches connect the external routers, and it provides management connectivity to the other switches in the fabric. Switches connected to external routers to provide connectivity to the fabrics are termed as seed switches. The interfaces on the seed switches which connects to the external routers are termed as bootstrap interfaces.

Prerequisites for inband and out-of-band management

1. Navigate to **Admin > System Settings**.
2. Click **Fabric management**.
3. In the **Advanced settings** area, click **Admin**.
4. In the **LAN Device Management Connectivity** field, choose **Data** to manage Data Center VXLAN EVPN fabrics through inband management.

   If you choose **Data**, ensure that the required persistent data IPs are available in the **External pools** area under **Admin > System Settings > General**.

When server settings changed from **Data** to **Management** or vice-versa, allow some time for syslog or poap functionalities to be online and ensure that the IP addresses in Cluster configuration are moved to the appropriate pool.

This server setting is required for both inband and out-of-band connectivity. Configure below static routes over data interface in Cisco Nexus Dashboard:

Enter static routes IP address required for external route and route over data interface in Cisco Nexus Dashboard.

Inband POAP requires the external router IP address connected to the seed switches to have the following capabilities:

- Routes for External router
- Route for Routing Loopback subnet range for Data Center VXLAN EVPN fabric
- Route for Underlay Routing subnet range for Data Center VXLAN EVPN fabric

Inband POAP requires the external router connected seed switches to have the following capabilities:

- DHCP relay functionality
- eBGP peering

To add switches for inband management and inband POAP, see the section "Discovering New Switches" in Working with Inventory in Your Nexus Dashboard LAN or IPFM Fabrics.

Guidelines and limitations

The following are the guidelines and limitations for inband management:

- Inband management is not supported when discovering or onboarding brownfield Data Center VXLAN EVPN fabrics.
- Ensure that the **Inband Management** is enabled for the inband interface. Both inband and out-of-band switches for a same fabric is not supported.
- It is supported only for IPv4 underlay and OSPF routing protocol.
- You can change switch management from inband to out-of-band and conversely after creating a fabric.
- For the inband managed switches, the following roles are supported:
  - Spine
  - Leaf
  - Border
  - Border Spine
  - Border Gateway
  - Border Gateway Spine
- Inband management is supported for both numbered and unnumbered fabric interface numbering
- Ensure that the same role switches are assigned as seed switches. If spine role switch is assigned as a seed switch, all the spine role switches in that fabric must be assigned as seed switches. It is recommended to assign switch as seed switches.
- When you add switches to fabric, ensure that the switches are not in maintenance mode.
- You can add switches in Brownfield deployment (check **Preserve Config** check box) only when the fabric is created. To add more switches, use inband POAP with import switches option.
- Set **vPC Peer Keep Alive** option to loopback if the vPC switches mgmt0 interfaces are not configured.

The following are the guidelines and limitations for inband POAP:

- Inband POAP for a fabric can be enabled only if **Inband Management** is enabled.
- Inband POAP requires the fabric or core facing interfaces to be cabled consistently for seed switches and spine switches.
- All spine switches in fabric must use same set of fabric interface numbers.
- If a fabric has set of leaf switches which are seed switches, then the switches must use same fabric interface number.
- The seed switches must have eBGP peering with the external router. Therefore, the external router must have the required eBGP route peering capabilities and display the configuration for External router for DHCP relay and Static routes configured for the Subnets used in Data Center VXLAN EVPN fabrics.

- DHCP relay must be configured on external routers interface which connects the seed switch in inband interfaces. Ensure that the DHCP relay destination configured is same for all cluster node data interface on Cisco Nexus Dashboard.
- DHCP server can be internal Nexus Dashboard or the external server.

Enable inband POAP on Data Center VXLAN EVPN fabrics

To enable inband POAP on Data Center VXLAN EVPN fabrics, perform the following steps:

1. Navigate to **Manage > Fabrics**, then click the appropriate fabric.

   The **Overview** window for that fabric appears.

2. Click **Actions > Edit Fabric Settings**.
3. Click **Fabric Management**.
4. Click **Manageability** and check the **Inband Management** box.
5. Click **Bootstrap**, then configure these settings:
   a. Check the **Enable Bootstrap** check box.
   b. Check the **Enable Local DHCP Server** checkbox to assign Nexus Dashboard as DHCP Server and enter the DHCP scopes for all the fabric seed switches bootstrap interfaces.

      If you choose **Enable Local DHCP Server**, and choose unnumbered in Fabric Interface Numbering drop-down list in the General Parameters tab, add details for:

      - Bootstrap Seed Switch Loopback Interface ID
      - Switch Loopback DHCP Scope Start Address
      - Switch Loopback DHCP Scope End Address

   c. Check the **External DHCP Server IP Addresses** check box to provide connectivity to Nexus Dashboard from the external router.

      If you choose **External DHCP Server IP Addresses**, you can add a maximum of three IPv4 addresses with a comma separated list.

      To have eBGP peering between seeds and an external router, add bootstrap seed switch loopback interface IP address, this IP must be a subset of the loopback id range.

   d. Enter Seed Switch interface in **Seed Switch Fabric Interfaces** text field.
   e. Enter Spine Switch interface in **Spine Switch Fabric Interfaces** text field.

      If the Spine switches are the seed switches, then the lists must be consistent in **Seed Switch Fabric Interfaces** text field.

6. For fabrics with unnumbered interface, do the following:
   a. Click **General Parameters**, then choose **unnumbered** from **Fabric Interface Numbering** drop-down list.

b. Click **Bootstrap** and configure these settings:

- **Bootstrap Seed Switch Loopback Interface ID** the loopback ID is the default router IP for the fabric. This loopback ID must not overlap with any of the existing fabric loopback IDs.
- **Switch Loopback DHCP Scope Start Address** this IP address is start address of the DHCP pool of the routing loopback addresses range to assign to the bootstrapping switch. This IP address must not overlap with any of the existing IP addresses of **Underlay Routing Loopback IP Range**.
- **Switch Loopback DHCP Scope End Address** is the end address of the DHCP pool.

Import switches in a Brownfield deployment

Before you begin:

Make sure that you follow prerequisites procedure before adding switches.

1. Create a fabric using the **Data Center VXLAN EVPN** template.

   See Creating LAN and ACI Fabrics and Fabric Groups.

   Ensure that you add switches in the order of Seed switches, Spine switches, and other switches. You can add spine switches as the seed switches.

2. Add the switches to the fabric with the **Preserve Config** check box.
3. Enter **hostname**, **Role**, enable **Seed Switch**, and enter appropriate IP address.
4. Enter the IP addresses for all the seed switches, click **Import Selected Switches** to add them to the fabric.
5. Navigate to **Policy** tab, click **Actions > Add policy**. Choose **ext_bgp_neighbor** policy so the seed switches establish eBGP peering. Enter the required details, and click **Save**.
6. Assign the appropriate switch roles.

   For more instructions, see the section " Adding Switches Using Bootstrap Mechanism" in Working with Inventory in Your Nexus Dashboard LAN or IPFM Fabrics.

Pre-provision switches through inband POAP

1. Navigate to **Manage > Fabrics**, then click the appropriate fabric.

   The **Overview** window for that fabric appears.

2. Choose **Inventory > Switches** and click **Actions > Add Switches**.

   The **Add Switches** window appears.

3. Choose **Pre-provision** radio button.
4. On **Switches to Pre-provision** table, click **Actions> Add**.

   The **Pre-provision a switch** window appears.

5. Enter appropriate details such as Serial Number, Model, IP Address, and click **Add**.

6. Enter single switch at once and enter the required information. If you have multiple switches.
7. Click **Import Switches to Fabric** to add switches.

Add a policy for Data Center VXLAN EVPN fabrics

1. Navigate to **Manage > Fabrics**, then click the appropriate fabric.

   The **Overview** window for that fabric appears.

2. Choose **Configuration Policies > Policies** and click **Actions > Add policy**.
3. Choose the appropriate switch from the **Switch** window and click **Choose Template**.
4. Choose **ext_bgp_neighbor policy** and click **Select**.

   The **Create Policy** window appears.

5. Click **Actions > Add policy**.

   The **Create Policy** window appears.

6. Enter the appropriate details in the window and click **Save**.
7. On **Fabric Overview** window, click **Actions > Recalculate and deploy**.

Change the fabric management mode

You can change the fabric from out-of-band to inband management and vice versa.

1. To change fabric management from out-of-band to inband management:
   a. Ensure that you followed the prerequisites for inband management.

      See Prerequisites for inband and out-of-band management.

   b. Navigate to **Manage > Fabrics**, then choose the appropriate fabric.

      The **Overview** window for that fabric appears.

   c. Click **Actions > Edit Fabric Settings**.
   d. Click **Fabric Management**.
   e. Click **Advanced**.
   f. Click the box for **Inband Mgmt** and click **Save**.
   g. Choose **Inventory > Switches**.
   h. Locate the switches that display **Migration** in the **Mode** column.
   i. Choose those switches, then click **Actions > Recalculate and deploy.**
      - The discovery IP address of the switches changes to the BGP routing loopback IP.
      - The discovery VRF displays default and discovery interface is updated to BGP routing loopback interface.
      - An error is generated displaying switch discovery is pending:

The discovery modes for switches have been updated but, discovery may not have completed. Please check to make sure Discovery Status is Ok and retry Recalculate & Deploy.

j. Click **OK**.

k. Ensure that the **Discovery Status** column displays **Ok** as the status, then click **Actions > Recalculate and deploy**.

2. To change fabric management from inband management to out-of-band:

a. Ensure that you followed the prerequisites for out-of-band management.

See Prerequisites for inband and out-of-band management.

b. Configure out-of-band IP addresses on the switch.

These IP addresses must be reachable from the Nexus Dashboard data or management interface.

c. Navigate to **Manage > Fabrics**, then choose the appropriate external/inter-fabric connectivity fabric.

The **Overview** window for that fabric appears.

d. Click **Actions > Edit Fabric Settings**.

e. Click **Fabric Management**.

f. Click **Advanced**.

g. Remove the check from the box in the **Inband Mgmt** field and click **Save**.

h. Choose **Inventory > Switches**.

i. Locate the switches that display **Migration** in the **Mode** column.

j. Choose those switches, then click **Actions > Recalculate and deploy.**

- The discovery IP address of the switches will be changed to the mgmt0 IP.
- The discovery VRF displays management and discovery interface will be updated to mgmt0. An error is generated displaying switch discovery is pending: The discovery modes for switches have been updated but, discovery may not have completed. Please check to make sure that Discovery Status is Ok and retry Recalculate & Deploy.

k. Click **OK**.

l. Ensure that the **Discovery Status** column displays **Ok** as the status, then click **Actions > Recalculate and deploy**.

Secure POAP

When you import switches through bootstrap or POAP in Nexus Dashboard, it locates a DHCP protocol and bootstraps with interface IP address, gateway, DNS server IP address, and POAP script path.

POAP uses an HTTPS server which is a secure protocol to encrypt traffic and validate Nexus Dashboard for network connection. You must configure Bench Router (BR) to host ®oot Certificate Authority (CA), which is a signed server certificate of POAP server that is hosted on Nexus Dashboard. In the DHCP response, BR is identified which acts as a trust for a new switch.



Secure POAP is not supported for inband connectivity with bench routers.

See the "CA Certificates" and "Bootstrap Certificates" sections in Managing Certificates in your Nexus Dashboard to upload the appropriate certificates on Nexus Dashboard.

Prerequisites for secure POAP

- Secure POAP is supported from Cisco NX-OS 9000 Release 10.2.3 or higher version switches.
- Navigate to **Admin > System Settings**, click **Edit** in the **Switch bootstrap** area, then choose **https** or **http&https** from the drop-down list for **Bootstrap Script Download Protocol** field.
- For the **http** or **http&https** option, you must enter the IP address of the bench router (BR), port number, and name for certificate bundle in **Bench Router URL with port and certificate file name** filed. Ensure that the certificates are uploaded on Nexus Dashboard server for values to autopopulate in this field.
- By default, for the **http** or **http&https** options, the **Bench router URL with port** field in the **Switch bootstrap** window will be blank. After you install the Root CA Certificate bundle on Bench routers, this field will be autopopulated.

  If these fields are autopopulated, with default port number 29151 and URL *https://10.10.10.1:29151/PoapCACertBundle.pem*, you must configure this URL before you install the BR with the Root CA certificate bundle.

- Make sure that the Fabric is in managed mode before configuring the BR.
- Ensure that you configure the DHCP option if the DHCP server is used.
- You must upload CA signed POAP server certificate on Nexus Dashboard and upload the corresponding CA certificate bundle for the BR. On Nexus Dashboard, navigate to **Admin > Certificate Management > Fabric Certificates** to upload the relevant certificates.

Out-of-Band PnP in Campus VXLAN EVPN fabrics

About Out-of-Band PnP in Campus VXLAN EVPN fabrics

Nexus Dashboard provides support for the Out-of-Band (OOB) Plug and Play (PnP) feature, which simplifies the process of onboarding new devices with a zero-touch deployment experience. PnP automates the day-zero provisioning of Cisco Catalyst 9000 Series switches using Nexus Dashboard. With OOB connectivity, the switch provides a separate dedicated network for management traffic over GigabitEthernet 0/0 interface which is always placed in mgmt-vrf.

When a Cisco Catalyst switch powers up and does not find the startup configuration, the device enters PnP mode and sends out a DHCP request, which is served by a DHCP server. The DHCP offer contains the PnP server address and other required configuration for the PnP client. The PnP client on the switch uses this information to connect to the appropriate PnP sever to finish the configuration of the switch. This is a multi-step process, and to provide additional security, the system prompts you to approve the addition of this switch to the fabric. The device then downloads a configuration script and installs the appropriate software image and configuration file.

Enable Out-of-Band PnP

Before you begin:

- You can use a local or external DHCP Server for IP address assignment.
- This release only supports DHCP for IPv4.
- This feature is supported only on Campus VXLAN EVPN fabric.

To enable Out-of-Band PnP in a fabric:

1. When creating a Campus VXLAN EVPN fabric, navigate to the **Bootstrap** tab of the **Create Fabric** window.
2. Check the **Enable Bootstrap** and **Enable Local DHCP Server** check boxes.
3. Enter the domain name of the DHCP server in the **Domain name** field.
4. Enter the start address and the end address of your subnet in the **DHCP Scope Start Address** and **DHCP Scope End Address** fields.
5. Enter the default gateway for the management VRF on the switch in the **Switch Mgmt Default Gateway** field.
6. Enter the prefix for the management interface on the switch in the **Switch Mgmt IP Subnet Prefix** field.

   The prefix should be between 8 and 30. The system assigns 24, by default.

7. Enter any other additional configuration CLIs in the **Bootstrap Freeform Config** field, as required and click **Save**.

Import switches using the bootstrap method

Before you begin:

Ensure you have uploaded the required SSL certificates for the switches. You can use CA-signed certificates or self-signed certificates. Nexus Dashboard does not mandate the signing; however, the security guidelines suggest you use the CA-signed certificates.

1. In the **Fabric Overview** window for a fabric, choose **Actions > Add Switches**.
2. In the **Switch Addition Mechanism** area, click the **Bootstrap** radio button.
3. Enter the Admin password in the **Admin Password** field.

   The **Switches to Bootstrap** table lists all the discovered switches.
4. Select the switches you want to add to the fabric and click **Import Selected Switches**.

Enable DHCP for PnP

If you are using an external DHCP server and not the Nexus Dashboard DHCP server, ensure you perform the following steps on the DHCP server to facilitate PnP server discovery using DHCP.

1. Define the following two DHCP options:
   - pnpserver code 43
   - vrf code 194
2. Define option vendor-class-identifier to use the value " ciscopnp" .
3. Assign values to option 43 and option 194.
4. Assign option pnpserver " 5A1D;K4;B2;I<EXT-IP-NDFC>;J9666" ;

   For <EXT-IP-NDFC>, enter the external POAP IP address on Nexus Dashboard.
5. Assign option vrf to use the value " Mgmt-vrf" .

   The following example shows a sample configuration.

```
option pnpserver code 43 = text;

option vrf code 194 = text;

class " ciscopnp"  {

match if option vendor-class-identifier = " ciscopnp" ;

option vendor-class-identifier " ciscopnp" ;

option pnpserver " 5A1D; K4; B2; I<EXT-IP-NDFC>; J9666" ;

option vrf " Mgmt-vrf" ;

option domain-name " cisco.com" ;
```

```
}
```

Copyright

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

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/go/trademarks. 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. (1110R)

© 2017-2025 Cisco Systems, Inc. All rights reserved.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

USA
https://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883