



Classic LAN, Release 12.2.1

# Table of Contents

New and Changed Information .....	1
Creating a Classic LAN Fabric .....	2
General Parameters .....	2
Advanced .....	3
Resources .....	5
Configuration Backup .....	5
Bootstrap .....	6
Flow Monitor .....	8
Precision Time Protocol for Classic LAN Fabrics .....	11
Copyright .....	14

# 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
There were no major changes from the previous release.		

# Creating a Classic LAN Fabric

This topic describes how to create a new VXLAN EVPN fabric using the **Data Center VXLAN EVPN** template and contains descriptions for the IPv4 underlay. For information about IPv6 Underlay Support, see *IPv6 Underlay Support for Easy Fabric* in the *Cisco NDFC Fabric Controller Configuration Guide*.

1. Navigate to the **LAN Fabrics** page:

**Manage > Fabrics**

2. Click **Actions > Create Fabric**.

The **Create Fabric** window appears.

3. Enter a unique name for the fabric in the **Fabric Name** field, then click **Choose Fabric**.

A list of all available fabric templates are listed.

4. From the available list of fabric templates, choose the **Classic LAN** template, then click **Select**.
5. Enter the necessary field values to create a fabric.

The tabs and their fields in the screen are explained in the following sections. The overlay and underlay network parameters are included in these tabs.

- [General Parameters](#)
- [Advanced](#)
- [Resources](#)
- [Configuration Backup](#)
- [Bootstrap](#)
- [Flow Monitor](#)

6. When you have completed the necessary configurations, click **Save**.
  - Click on the fabric to display a summary in the slide-in pane.
  - Click on the Launch icon to display the Fabric Overview.

## General Parameters

The **General Parameters** tab is displayed by default. The fields in this tab are described in the following table.

Field	Description
<b>Fabric Monitor Mode</b>	Select this check box to only monitor the fabric, but not deploy the configuration.

Field	Description
<b>Enable Performance Monitoring</b>	<p>Select this check box to monitor the performance of the fabric.</p> <p>Ensure that you do not clear interface counters from the Command Line Interface of the switches. Clearing interface counters can cause the Performance Monitor to display incorrect data for traffic utilization. If you must clear the counters and the switch has both <b>clear counters</b> and <b>clear counters snmp</b> commands (not all switches have the <b>clear counters snmp</b> command), ensure that you run both the main and the SNMP commands simultaneously. For example, you must run the <b>clear counters interface ethernet slot/port</b> command followed by the <b>clear counters interface ethernet slot/port snmp</b> command. This can lead to a one time spike.</p>

**What's next:** Complete the configurations in another tab if necessary, or click **Save** when you have completed the necessary configurations for this fabric.

## Advanced

The fields in the **Advanced** tab are described in the following table. Most of the fields are automatically generated based on Cisco-recommended best practice configurations, but you can update the fields if needed.

Field	Description
<b>Power Supply Mode</b>	Choose the appropriate power supply mode.
<b>Enable MPLS Handoff</b>	Check the check box to enable the MPLS Handoff feature.
<b>Underlay MPLS Loopback Id</b>	Specifies the underlay MPLS loopback ID. The default value is 101.
<b>Enable AAA IP Authorization</b>	Enables AAA IP authorization, when IP Authorization is enabled in the remote authentication server. This is required to support Nexus Dashboard Fabric Controller in scenarios where customers have strict control of which IP addresses can have access to the switches.
<b>Enable NDFC as Trap Host</b>	Select this check box to enable Nexus Dashboard Fabric Controller as an SNMP trap destination. Typically, for a native HA Nexus Dashboard Fabric Controller deployment, the eth1 VIP IP address will be configured as SNMP trap destination on the switches. By default, this check box is enabled.
<b>Enable CDP for Bootstrapped Switch</b>	Enables CDP on management interface.
<b>Enable NX-API</b>	Specifies enabling of NX-API on HTTPS.
<b>NX-API HTTPS Port Number</b>	<p>Field becomes active if the <b>Enable NX-API</b> option is enabled.</p> <p>Enter the NX-API HTTPS port number. Default value is 443.</p>

Field	Description
<b>Enable HTTP NX-API</b>	<p>Specifies enabling of NX-API on HTTP. Enable this check box and the <b>Enable NX-API</b> check box to use HTTP. This check box is checked by default. If you uncheck this check box, the applications that use NX-API and supported by Cisco Nexus Dashboard Fabric Controller, such as Endpoint Locator (EPL), Layer 4-Layer 7 services (L4-L7 services), VXLAN OAM, and so on, start using the HTTPS instead of HTTP.</p> <div>  <p>If you check the <b>Enable NX-API</b> check box and the <b>Enable NX-API on HTTP</b> check box, applications use HTTP.</p> </div>
<b>NX-API HTTP Port Number</b>	<p>Field becomes active if the <b>Enable HTTP NX-API</b> option is enabled.</p> <p>Enter the NX-API HTTPS port number. Default value is 80.</p>
<b>Inband Mgmt</b>	<p>For Classic LAN fabrics, this knob enables Nexus Dashboard Fabric Controller to import and manage of switches with inband connectivity (reachable over switch loopback, routed, or SVI interfaces), in addition to management of switches with out-of-band connectivity (that is, reachable over switch mgmt0 interface). The only requirement is that for Inband managed switches, there should be IP reachability from Nexus Dashboard Fabric Controller to the switches through the Nexus Dashboard data interface. After enabling Inband management, during discovery, provide the IPs of all the switches to be imported using Inband Management and set maximum hops to 0. Nexus Dashboard Fabric Controller has a pre-check that validates that the Inband managed switch IPs are reachable over the Nexus Dashboard data interface. Once the pre-check has passed, Nexus Dashboard Fabric Controller then discovers and learns about the interface on that switch that has the specified discovery IP in addition to the VRF that the interface belongs to. As part of the process of switch import/discovery, this information is captured in the baseline intent that is populated on the Nexus Dashboard Fabric Controller. For more information, see <i>Inband Management in External Fabrics and LAN Classic Fabrics</i> in the <i>Cisco NDFC Fabric Controller Configuration Guide</i>.</p> <div>  <p>Bootstrap or POAP is only supported for switches that are reachable over out-of-band connectivity, that is, over switch mgmt0. The various POAP services on the Nexus Dashboard Fabric Controller are typically bound to the eth1 or out-of-band interface. In scenarios, where the Nexus Dashboard Fabric Controller eth0/eth1 interfaces reside in the same IP subnet, the POAP services are bound to both interfaces.</p> </div>
<b>Enable Precision Time Protocol (PTP)</b>	<p>Enables PTP across a fabric. When you check this check box, PTP is enabled globally and on core-facing interfaces. Additionally, the <b>PTP Source Loopback Id</b> and <b>PTP Domain Id</b> fields are editable. For more information, see <a href="#">[Precision Time Protocol]</a>.</p>

Field	Description
<b>PTP Source Loopback Id</b>	<p>Specifies the loopback interface ID Loopback that is used as the Source IP Address for all PTP packets. The valid values range from 0 to 1023. The PTP loopback ID cannot be the same as RP, Phantom RP, NVE, or MPLS loopback ID. Otherwise, an error will be generated. The PTP loopback ID can be the same as BGP loopback or user-defined loopback which is created from Nexus Dashboard Fabric Controller.</p> <p>If the PTP loopback ID is not found during <b>Deploy Config</b>, the following error is generated:</p> <p>Loopback interface to use for PTP source IP is not found. Create PTP loopback interface on all the devices to enable PTP feature.</p>
<b>PTP Domain Id</b>	Specifies the PTP domain ID on a single network. The valid values range from 0 to 127.
<b>Fabric Freeform</b>	You can apply configurations globally across all the devices discovered in the external fabric using this freeform field.
<b>AAA Freeform Config</b>	Specifies the AAA freeform configurations.

**What's next:** Complete the configurations in another tab if necessary, or click **Save** when you have completed the necessary configurations for this fabric.

## Resources


The fields in the **Resources** tab are described in the following table. Most of the fields are automatically generated based on Cisco-recommended best practice configurations, but you can update the fields if needed.

Field	Description
<b>Subinterface Range</b> <b>Dot1q</b>	Specifies the subinterface range when L3 sub interfaces are used.
<b>Underlay Loopback IP Range</b> <b>MPLS</b>	<p>Specifies the underlay MPLS loopback IP address range.</p> <p>Underlay routing loopback and Underlay MPLS loopback IP range must be a unique range. It should not overlap with IP ranges of the other fabrics, else VPNv4 peering will not come up.</p>

**What's next:** Complete the configurations in another tab if necessary, or click **Save** when you have completed the necessary configurations for this fabric.

## Configuration Backup

The fields in the **Configuration Backup** tab are described in the following table. Most of the fields are automatically generated based on Cisco-recommended best practice configurations, but you can update the fields if needed.



Field	Description
<b>Hourly Fabric Backup</b>	<p>Select the check box to enable an hourly backup of fabric configurations and the intent.</p> <p>The hourly backups are triggered during the first 10 minutes of the hour.</p>
<b>Scheduled Fabric Backup</b>	<p>Check the check box to enable a daily backup. This backup tracks changes in running configurations on the fabric devices that are not tracked by configuration compliance.</p>
<b>Scheduled Time</b>	<p>Specify the scheduled backup time in a 24-hour format. This field is enabled if you check the <b>Scheduled Fabric Backup</b> check box.</p> <p>Select both the check boxes to enable both back up processes.</p> <p>The backup process is initiated after you click <b>Save</b>.</p> <p>The scheduled backups are triggered exactly at the time you specify with a delay of up to two minutes. The scheduled backups are triggered regardless of the configuration deployment status.</p> <p>The number of fabric backups that will be retained on NDFC is decided by the <b>Admin &gt; System Settings &gt; Server Settings &gt; LAN Fabric &gt; Maximum Backups per Fabric</b>.</p> <p>The number of archived files that can be retained is set in the <b># Number of archived files per device to be retained:</b> field in the <b>Server Properties</b> window.</p> <div>  <p>To trigger an immediate backup, do the following:</p> <ol style="list-style-type: none"> <li>1. Choose <b>Overview &gt; Topology</b>.</li> <li>2. Click within the specific fabric box. The fabric topology screen comes up.</li> <li>3. From the <b>Actions</b> pane at the left part of the screen, click <b>Re-Sync Fabric</b>.</li> </ol> </div> <p>You can also initiate the fabric backup in the fabric topology window. Click <b>Backup Now</b> in the <b>Actions</b> pane.</p>

**What's next:** Complete the configurations in another tab if necessary, or click **Save** when you have completed the necessary configurations for this fabric.

## Bootstrap

The fields in the **Bootstrap** tab are described in the following table. Most of the fields are automatically generated based on Cisco-recommended best practice configurations, but you can update the fields if needed.




Field	Description
<b>Enable Bootstrap</b>	<p>Select this check box to enable the bootstrap feature. Bootstrap allows easy day-0 import and bring-up of new devices into an existing fabric. Bootstrap leverages the NX-OS POAP functionality.</p> <p>Starting from Cisco NDFC Release 12.1.1e, to add more switches and for POAP capability, chose check box for <b>Enable Bootstrap</b> and <b>Enable Local DHCP Server</b>. For more information, see <i>Inband Management and Inband POAP in Easy Fabrics</i> in the <i>Cisco NDFC-Fabric Controller Configuration Guide</i>.</p> <p>After you enable bootstrap, you can enable the DHCP server for automatic IP address assignment using one of the following methods:</p> <ul style="list-style-type: none"> <li>External DHCP Server: Enter information about the external DHCP server in the <b>Switch Mgmt Default Gateway</b> and <b>Switch Mgmt IP Subnet Prefix</b> fields.</li> <li>Local DHCP Server: Enable the <b>Local DHCP Server</b> check box and enter details for the remaining mandatory fields.</li> </ul>
<b>Enable Inband POAP</b>	<p>Choose this check box to enable Inband POAP.</p> <div>  <p>You must enable <b>Inband Mgmt</b> on the Advanced tab to enable this option.</p> </div>
<b>Enable Local DHCP Server</b>	<p>Select this check box to initiate enabling of automatic IP address assignment through the local DHCP server. When you select this check box, the <b>DHCP Scope Start Address</b> and <b>DHCP Scope End Address</b> fields become editable.</p> <p>If you do not select this check box, Nexus Dashboard Fabric Controller uses the remote or external DHCP server for automatic IP address assignment.</p>
<b>DHCP Version</b>	<p>Select DHCPv4 or DHCPv6 from this drop-down list. When you select DHCPv4, the <b>Switch Mgmt IPv6 Subnet Prefix</b> field is disabled. If you select DHCPv6, the <b>Switch Mgmt IP Subnet Prefix</b> is disabled.</p> <div>  <p>Cisco Nexus 9000 and 3000 Series Switches support IPv6 POAP only when switches are either Layer-2 adjacent (eth1 or out-of-band subnet must be a /64) or they are L3 adjacent residing in some IPv6 /64 subnet. Subnet prefixes other than /64 are not supported.</p> </div>
<b>DHCP Scope Start Address and DHCP Scope End Address</b>	Specifies the first and last IP addresses of the IP address range to be used for the switch out of band POAP.
<b>Switch Mgmt Default Gateway</b>	Specifies the default gateway for the management VRF on the switch.

Field	Description
<b>Switch Mgmt IP Subnet Prefix</b>	<p>Specifies the prefix for the Mgmt0 interface on the switch. The prefix should be between 8 and 30.</p> <p><i>DHCP scope and management default gateway IP address specification</i> – If you specify the management default gateway IP address 10.0.1.1 and subnet mask 24, ensure that the DHCP scope is within the specified subnet, between 10.0.1.2 and 10.0.1.254.</p>
<b>Enable AAA Config</b>	Select this check box to include AAA configurations from the Manageability tab as part of the device start-up config post bootstrap.
<b>Bootstrap Freeform Config</b>	<p>(Optional) Enter additional commands as needed. For example, if you require some additional configurations to be pushed to the device and be available post device bootstrap, they can be captured in this field, to save the desired intent. After the devices boot up, they will contain the configuration defined in the <b>Bootstrap Freeform Config</b> field.</p> <p>Copy-paste the running-config to a <b>freeform config</b> field with correct indentation, as seen in the running configuration on the NX-OS switches. The freeform config must match the running config. For more information, see <i>Enabling Freeform Configurations on Fabric Switches</i> in the <i>Cisco NDFC Fabric Controller Configuration Guide</i>.</p>
<b>DHCPv4 Multi Subnet Scope</b>	<p>Specifies the field to enter one subnet scope per line. This field is editable after you check the <b>Enable Local DHCP Server</b> check box.</p> <p>The format of the scope should be defined as:</p> <p><b>DHCP Scope Start Address, DHCP Scope End Address, Switch Management Default Gateway, Switch Management Subnet Prefix</b></p> <p>For example: 10.6.0.2, 10.6.0.9, 10.6.0.1, 24</p>

**What's next:** Complete the configurations in another tab if necessary, or click **Save** when you have completed the necessary configurations for this fabric.

## Flow Monitor

The fields in the **Flow Monitor** tab are described in the following table. Most of the fields are automatically generated based on Cisco-recommended best practice configurations, but you can update the fields if needed.

Field	Description
<b>Enable Netflow</b>	<p>Check this check box to enable Netflow on VTEPs for this Fabric. By default, Netflow is disabled. On Enable, NetFlow configuration will be applied to all VTEPS that support netflow.</p> <div>  <p>When Netflow is enabled on the fabric, you can choose not to have netflow on a particular switch by having a dummy no_netflow PTI.</p> </div> <p>If netflow is not enabled at the fabric level, an error message is generated when you enable netflow at the interface, network, or vrf level. For information about Netflow support for Cisco NDFC, see section "Netflow Support" in <a href="#">Understanding LAN Fabrics</a>.</p>

In the **Netflow Exporter** area, click **Actions > Add** to add one or more Netflow exporters. This exporter is the receiver of the netflow data. The fields on this screen are:

- **Exporter Name** - Specifies the name of the exporter.
- **IP** - Specifies the IP address of the exporter.
- **VRF** - Specifies the VRF over which the exporter is routed.
- **Source Interface** - Enter the source interface name.
- **UDP Port** - Specifies the UDP port over which the netflow data is exported.

Click **Save** to configure the exporter. Click **Cancel** to discard. You can also choose an existing exporter and select **Actions > Edit** or **Actions > Delete** to perform relevant actions.

In the **Netflow Record** area, click **Actions > Add** to add one or more Netflow records. The fields on this screen are:

- **Record Name** - Specifies the name of the record.
- **Record Template** - Specifies the template for the record. Enter one of the record templates names. In Release 12.0.2, the following two record templates are available for use. You can create custom netflow record templates. Custom record templates saved in the template library are available for use here.
  - **netflow\_ipv4\_record** - to use the IPv4 record template.
  - **netflow\_l2\_record** - to use the Layer 2 record template.
- **Is Layer2 Record** - Check this check box if the record is for Layer2 netflow.

Click **Save** to configure the report. Click **Cancel** to discard. You can also choose an existing record and select **Actions > Edit** or **Actions > Delete** to perform relevant actions.

In the **Netflow Monitor** area, click **Actions > Add** to add one or more Netflow monitors. The fields on this screen are:

- **Monitor Name** - Specifies the name of the monitor.
- **Record Name** - Specifies the name of the record for the monitor.
- **Exporter1 Name** - Specifies the name of the exporter for the netflow monitor.

- **Exporter2 Name** - (optional) Specifies the name of the secondary exporter for the netflow monitor.

The record name and exporters referred to in each netflow monitor must be defined in "**Netflow Record**" and "**Netflow Exporter**".

Click **Save** to configure the monitor. Click **Cancel** to discard. You can also choose an existing monitor and select **Actions > Edit** or **Actions > Delete** to perform relevant actions.

**What's next:** Complete the configurations in another tab if necessary, or click **Save** when you have completed the necessary configurations for this fabric.

# Precision Time Protocol for Classic LAN Fabrics

In the Fabric settings for the **Classic LAN** template, select the **Enable Precision Time Protocol (PTP)** check box to enable PTP across a fabric. When you select this check box, PTP is enabled globally and on core-facing interfaces. Additionally, the **PTP Loopback Id** and **PTP Domain Id** fields are editable.

The PTP feature is supported with Cisco Nexus 9000 Series cloud-scale switches, with NX-OS version 7.0(3)I7(1) or later. Warnings are displayed if there are non-cloud scale devices in the fabric, and PTP is not enabled. Examples of the cloud-scale devices are Cisco Nexus 93180YC-EX, Cisco Nexus 93180YC-FX, Cisco Nexus 93240YC-FX2, and Cisco Nexus 93360YC-FX2 switches. For more information, refer to <https://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html>.



PTP global configuration is supported with Cisco Nexus 3000 Series switches; however, PTP and TTAG configurations are not supported.

For more information, see the *Configuring PTP* chapter in *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide* and *Cisco Nexus Insights for Cisco User Guide*.

For Classic LAN fabric deployments, you have to enable PTP globally, and also enable PTP on core-facing interfaces. The interfaces could be configured to the external PTP server like a VM or Linux-based machine. Therefore, the interface should be edited to have a connection with the grandmaster clock. For PTP and TTAG configurations to be operational on Classic LAN Fabrics, you must sync up of Switch Configs to Nexus Dashboard Fabric Controller using the **host\_port\_resync** policy. For more information, see [Out-of-Band Switch Interface Configurations](#).

It is recommended that the grandmaster clock should be configured outside of Data Center VXLAN EVPN and it is IP reachable. The interfaces toward the grandmaster clock need to be enabled with PTP via the interface freeform config.

All core-facing interfaces are auto-enabled with the PTP configuration after you click **Deploy Config**. This action ensures that all devices are PTP synced to the grandmaster clock. Additionally, for any interfaces that are not core-facing, such as interfaces on the border devices and leafs that are connected to hosts, firewalls, service-nodes, or other routers, the TTAG related CLI must be added. The TTAG is added for all traffic entering the VXLAN EVPN fabric and the TTAG must be stripped when traffic is exiting this fabric.

Here is the sample PTP configuration:

```
feature ptp
```

```
ptp source 100.100.100.10 -> IP address of the loopback interface (loopback0)  
that is already created, or user-created loopback interface in the fabric settings
```

```
ptp domain 1 -> PTP domain ID specified in fabric settings
```

```
interface Ethernet1/59 -> Core facing interface
```

ptp

interface Ethernet1/50 -> Host facing interface

ttag

ttag-strip

The following guidelines are applicable for PTP:

- The PTP feature can be enabled in a fabric when all the switches in the fabric have Cisco NX-OS Release 7.0(3)I7(1) or a higher version. Otherwise, the following error message is displayed:

PTP feature can be enabled in the fabric, when all the switches have NX-OS Release 7.0(3)I7(1) or higher version. Please upgrade switches to NX-OS Release 7.0(3)I7(1) or higher version to enable PTP in this fabric.

- For hardware telemetry support in NIR, the PTP configuration is a prerequisite.
- If you are adding a non-cloud scale device to an existing fabric which contains PTP configuration, the following warning is displayed:

TTAG is enabled fabric wide, when all devices are cloud-scale switches so it cannot be enabled for newly added non cloud-scale device(s).

- If a fabric contains both cloud-scale and non-cloud scale devices, the following warning is displayed when you try to enable PTP:

TTAG is enabled fabric wide when all devices are cloud-scale switches and is not enabled due to non cloud-scale device(s).

- TTAG configuration is generated for all the devices if host configuration sync up is performed on all the devices. TTAG configuration will not be generated for any newly added devices if host configuration sync up is not performed on all newly added devices.

If the configuration is not synced, the following warning is displayed:

TTAG on interfaces with PTP feature can only be configured for cloud-scale devices. It will not be enabled on any newly added switches due to the presence of non cloud-scale devices.

- PTP and TTAG configurations are deployed on host interfaces.
- PTP and TTAG Configurations are supported between switches in the same fabric (intra-fabric links). PTP is created for inter-fabric links, and TTAG is created for the inter-fabric link if the other fabric (Switch) is not managed by Nexus Dashboard Fabric Controller. Inter-fabric links do not support PTP or TTAG configurations if both fabrics are managed by Nexus Dashboard Fabric Controller.

- TTAG configuration is configured by default after the breakout. After the links are discovered and connected post breakout, perform **Deploy Config** to generate the correct configuration based on the type of port (host, intra-fabric link, or inter fabric link).

# 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)

© 2017–2024 Cisco Systems, Inc. All rights reserved.