Cisco UCS Central Network Management Guide, Release 2.0

First Published: 2017-05-16

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

CONTENTS

Preface

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.

Text Type	Indication
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

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

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

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

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/ucs_rack_roadmap.html.

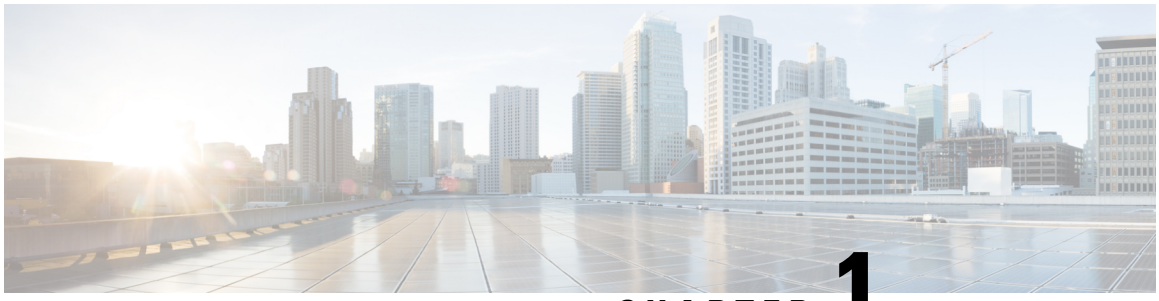
For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Other Documentation Resources

Follow Cisco UCS Docs on Twitter to receive document update notifications.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-docfeedback@external.cisco.com. We appreciate your feedback.



CHAPTER 1

Overview

This chapter includes the following sections:

Overview

This guide contains conceptual and procedural information on the following components that are intrinsic to Cisco UCS Central network management:

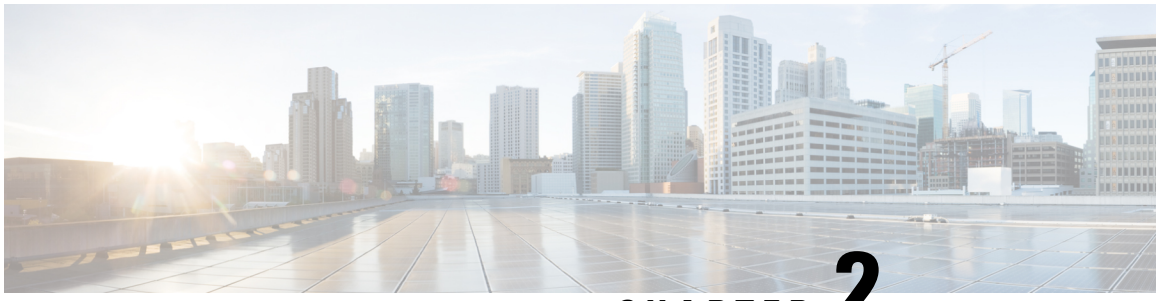
- Ports and port channels
- Global VLANs
- vNICs
- Network policies
- Traffic monitoring

Cisco UCS Central User Documentation Reference

The Cisco UCS Central following use case-based documents to understand and configure Cisco UCS Central:

Guide	Description
Cisco UCS Central Getting Started Guide	Provides a brief introduction to the Cisco UCS infrastructure, Cisco UCS Manager, and Cisco UCS Central. Includes an overview of the HTML5 UI, how to register Cisco UCS domains in Cisco UCS Central, and how to activate licenses.
Cisco UCS Central Administration Guide	Provides information on administrative tasks, such as user management, communication, firmware management, backup management, and Smart Call Home.

Guide	Description
Cisco UCS Central Authentication Guide	Provides information on authentication tasks, such as passwords, users and roles, RBAC, TACACS+, RADIUS, LDAP, and SNMP.
Cisco UCS Central Server Management Guide	Provides information on server management, such as equipment policies, physical inventory, service profiles and templates, server pools, server boot, and server policies.
Cisco UCS Central Storage Management Guide	Provides information on storage management, such as ports and port channels, VSAN and vHBA management, storage pools, storage policies, storage profiles, disk groups, and disk group configuration.
Cisco UCS Central Network Management Guide	Provides information on network management, such as ports and port channels, VLAN and vNIC management, network pools, and network policies.
Cisco UCS Central Operations Guide	Best practices for setting up, configuring, and managing domain groups for small, medium and large deployments.
Cisco UCS Central Troubleshooting Guide	Provides help for common issues in Cisco UCS Central.



CHAPTER 2

Ports and Port Channels

Server and Uplink Ports

Each fabric interconnect can include the following port types:

Server Ports

Server ports handle data traffic between the fabric interconnect and the adapter cards on the servers.

Uplink Ethernet Ports

Uplink Ethernet ports handle Ethernet traffic between the fabric interconnect and the next layer of the network. All network-bound Ethernet traffic is pinned to one of these ports.

By default, Ethernet ports are unconfigured. However, you can configure them to function in the following ways:

- Uplink
- FCoE
- Appliance

You can configure uplink Ethernet ports on either the fixed module or an expansion module.

Uplink Fibre Channel Ports

Uplink Fibre Channel ports handle FCoE traffic between the fabric interconnect and the next layer of the storage area network. All network-bound FCoE traffic is pinned to one of these ports.

By default, Fibre Channel ports are uplink. However, you can configure them to function as Fibre Channel storage ports. This is useful in cases where Cisco UCS requires a connection to a Direct-Attached Storage (DAS) device.

You can only configure uplink Fibre Channel ports on an expansion module. The fixed module does not include uplink Fibre Channel ports.

Unified Ports

Unified ports can be configured to carry either Ethernet or Fibre Channel traffic. These ports are not reserved. A Cisco UCS domain cannot use these ports until you configure them.

All ports on the following fabric interconnects are unified:

- Cisco UCS 6248 UP Fabric Interconnect
- Cisco UCS 6296 UP Fabric Interconnect
- Cisco UCS 6324 Fabric Interconnect
- Cisco UCS 6332-16UP Fabric Interconnect

Note When you configure a port on a fabric interconnect, the administrative state is automatically set to enabled. If the port is connected to another device, this may cause traffic disruption. You can disable the port after configuring it.

Unified Storage Ports

Unified storage is configuring the same physical port as an Ethernet storage interface and FCoE storage interface. You can configure any appliance port or FCoE storage port as a unified storage port on either a fixed module or an expansion module. To configure a unified storage port, the fabric interconnect must be in Fibre Channel switching mode.

In a unified storage port, you can enable/disable individual FCoE storage or appliance interfaces.

- In an unified storage port, if you do not specify a non default VLAN for the appliance port the fcoe-storage-native-vlan will be assigned as the native VLAN on the unified storage port. If the appliance port has a non default native VLAN specified as native VLAN, this will be assigned as the native VLAN for unified storage port.
- When you enable or disable the appliance interface, the corresponding physical port is enabled/disabled. So when you disable the appliance interface in a unified storage, even if the FCoE storage is enabled, it goes down with the physical port.

- When you enable or disable FCoE storage interface, the corresponding VFC is enabled or disabled. So when the FCoE storage interface is disabled in a unified storage port, the appliance interface will continue to function normally.

Unified Uplink Ports

When you configure an Ethernet uplink and an FCoE uplink on the same physical Ethernet port, it is called the unified uplink port. You can individually enable or disable either FCoE or Ethernet interfaces independently.

- Enabling or disabling the FCoE uplink results in corresponding VFC being enabled or disabled.
- Enabling or disabling an Ethernet uplink results in corresponding physical port being enabled or disabled.

If you disable an Ethernet uplink, it disables the underlying physical port in an unified uplink. So, even if the FCoE uplink is enabled, the FCoE uplink also goes down. But if you disable an FCoE uplink, only the VFC goes down. If the Ethernet uplink is enabled, it can still function properly in the unified uplink port.

Ports on the Cisco UCS 6300 Series Fabric Interconnects

The Cisco UCS 6300 Series Fabric Interconnect includes the Cisco UCS 6324 Fabric Interconnect for UCS Mini (Cisco UCS Manager Release 3.0), and the Cisco UCS 6332 and 6332-16UP Fabric Interconnects (Cisco UCS Manager Release 3.1).

The following table summarizes the port usage for the Cisco UCS 6300 Series Fabric Interconnects:

Fabric Interconnect Name:	Cisco UCS 6324 (Cisco UCS Mini)	Cisco UCS 6332	Cisco UCS 6332-16UP
Description:	Fabric Interconnect with 4 unified ports and 1 scalability port	32–Port Fabric Interconnect	40–Port Fabric Interconnect
Number of fixed 40 GB Interfaces:	—	6 (ports 17-32)	6 (ports 35-40)
Number of 1GB/10GB Interfaces (depending on the SFP module installed)	All	Ports 5–26 using breakout cable	Ports 17–34 using breakout cable
Unified Ports (8 Gb/s, FC, FCoE)	4	None	Ports 1–16

Note Cisco UCS 6300 Series Fabric Interconnects support breakout capability for ports. For more information on how the 40G ports can be converted into four 10G ports, see Scalability and Breakout Ports, on page 15.

Port Modes

The port mode determines whether a unified port on the fabric interconnect is configured to carry Ethernet or Fibre Channel traffic. The fabric interconnect does not automatically discover the port mode. You configure the port mode in Cisco UCS Central.

Changing the port mode deletes the existing port configuration and replaces it by a new logical port. Any objects associated with that port configuration, such as VLANs and VSANS, are removed. There is no restriction on the number of times you can change the port mode for a unified port.

Effect of Port Mode Changes on Data Traffic

Port mode changes can cause an interruption to the data traffic for the Cisco UCS domain. The length of the interruption and the traffic that is affected depend upon the configuration of the Cisco UCS domain and the module on which you made the port mode changes.

Tip To minimize the traffic disruption during system changes, form a Fibre Channel uplink port-channel across the fixed and expansion modules.

Impact of Port Mode Changes on an Expansion Module

After you make port mode changes on an expansion module, the module reboots. All traffic through ports on the expansion module is interrupted for approximately one minute while the module reboots.

Impact of Port Mode Changes on the Fixed Module in a Cluster Configuration

A cluster configuration has two fabric interconnects. After you make port changes to the fixed module, the fabric interconnect reboots. The impact on the data traffic depends upon whether or not you have configured the server vNICs to failover to the other fabric interconnect when one fails.

If you change the port modes on the expansion module of one fabric interconnect and then wait for that to reboot before changing the port modes on the second fabric interconnect, the following occurs:

- With server vNIC failover, traffic fails over to the other fabric interconnect and no interruption occurs.
- Without server vNIC failover, all data traffic through the fabric interconnect on which you changed the port modes is interrupted for approximately eight minutes while the fabric interconnect reboots.

If you change the port modes on the fixed modules of both fabric interconnects simultaneously, all data traffic through the fabric interconnects are interrupted for approximately eight minutes while the fabric interconnects reboot.

Impact of Port Mode Changes on the Fixed Module in a Standalone Configuration

A standalone configuration has only one fabric interconnect. After you make port changes to the fixed module, the fabric interconnect reboots. All data traffic through the fabric interconnect is interrupted for approximately eight minutes while the fabric interconnect reboots.

Port Roles

The port role defines the type of traffic carried over a unified port connection.

All of the port roles listed are configurable on both the fixed and expansion module, including server ports, which are configurable on the 6200 and later series fabric interconnect expansion modules.

By default, unified ports changed to Ethernet port mode are set to the uplink Ethernet port role. Unified ports changed to Fibre Channel (FC) port mode are set to the FC uplink port role. You cannot unconfigure FC ports.

Changing the port role does not require a reboot.

When you set the port mode to Ethernet, you can configure the following port roles:

- Server ports
- Ethernet uplink ports
- FCoE storage ports
- FCoE uplink ports
- Appliance ports

When you set the port mode to FC, you can configure the following port roles:

- FC uplink ports
- FC storage ports

Guidelines for Configuring Unified Ports

Consider the following guidelines and restrictions when configuring unified ports:

Hardware and Software Requirements

Unified ports are not supported on 6100 series fabric interconnects.

Port Mode Placement

Because the Cisco UCS Central GUI interface uses a slider to configure the port mode for unified ports on a fixed or expansion module, it automatically enforces the following restrictions which limits how port modes can be assigned to unified ports. When using the Cisco UCS Central CLI interface, these restrictions are enforced when you commit the transaction to the system configuration. If the port mode configuration violates any of the following restrictions, the Cisco UCS Central CLI displays an error:

- Ethernet ports must be grouped together in a block. For each module (fixed or expansion), the Ethernet port block must start with the first port and end with an even numbered port.
- Fibre Channel ports must be grouped together in a block. For each module (fixed or expansion), the first port in the Fibre Channel port block must follow the last Ethernet port and extend to include the rest of the ports in the module. For configurations that include only Fibre Channel ports, the Fibre Channel block must start with the first port on the fixed or expansion module.

- Alternating Ethernet and Fibre Channel ports is not supported on a single module.

Example of a valid configuration— Might include unified ports 1–16 on the fixed module configured in Ethernet port mode and ports 17–32 in Fibre Channel port mode. On the expansion module you could configure ports 1–4 in Ethernet port mode and then configure ports 5–16 in Fibre Channel mode. The rule about alternating Ethernet and Fibre Channel port types is not violated because this port arrangement complies with the rules on each individual module.

Example of an invalid configuration— Might include a block of Fibre Channel ports starting with port 16. Because each block of ports has to start with an odd-numbered port, you would have to start the block with port 17.

Note The total number of uplink Ethernet ports and uplink Ethernet port channel members that can be configured on each fabric interconnect is limited to 31. This limitation includes uplink Ethernet ports and uplink Ethernet port channel members configured on the expansion module.

The 40GB ports on the 6300 series fabric interconnects do not support expansion module configuration.

Cautions and Guidelines for Configuring Unified Uplink Ports and Unified Storage Ports

The following are cautions and guidelines to follow while working with unified uplink ports and unified storage ports:

- You must configure a non default native VLAN on FCoE and unified uplink ports. This VLAN is not used for any traffic. Cisco UCS Central will reuse an existing fcoe-storage-native-vlan for this purpose. This fcoe-storage-native-vlan will be used as a native VLAN on FCoE and unified uplinks.
- In an unified uplink port, if you do not specify a non default VLAN for the Ethernet uplink port the fcoe-storage-native-vlan will be assigned as the native VLAN on the unified uplink port. If the Ethernet port has a non default native VLAN specified as native VLAN, this will be assigned as the native VLAN for unified uplink port.
- When you create or delete a member port under an Ethernet port channel, Cisco UCS Central automatically creates or deletes the member port under FCoE port channel. The same happens when you create or delete a member port in FCoE port channel.
- When you configure an Ethernet port as a standalone port, such as server port, Ethernet uplink, FCoE uplink or FCoE storage and make it as a member port for an Ethernet or FCOE port channel, Cisco UCS Central automatically makes this port as a member of both Ethernet and FCoE port channels.
- When you remove the membership for a member port from being a member of server uplink, Ethernet uplink, FCoE uplink or FCoE storage, Cisco UCS Central deletes the corresponding members ports from Ethernet port channel and FCoE port channel and creates a new standalone port.
- For unified uplink ports and unified storage ports, when you create two interfaces, only one license is checked out. As long as either interface is enabled, the license remains checked out. The license will be released only if both the interfaces are disabled for a unified uplink port or a unified storage port.
- Cisco UCS 6100 series fabric interconnect switch can only support 1VF or 1VF-PO facing same downstream NPV switch.

Configuring Unified Ports

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click the **Tools** icon and choose **Unified Port Configuration**.

Step 4 Use your mouse to drag the slider along the bar until the displays shows the port mode configuration that you want to use.

The ports are displayed as follows:

- Ethernet ports are displayed in green.
- FC ports are displayed in purple.
- Disabled ports are displayed in faded green or purple.

Note Depending on the server, the Ethernet and FC port slider may be reversed.

Step 5 Click **Configure**.

Note Configuring unified ports reboots the FI, and can cause an interruption to the data traffic for the Cisco UCS domain.

Configuring Ports

Note Ports configured for Cisco UCS Manager releases prior to 3.1 were supported in Cisco UCS Central release 1.3, but are not supported in later releases of Cisco UCS Central. Any additional configuration of those ports must be done in Cisco UCS Manager.

Before you begin

- You must be running Cisco UCS Manager release 3.1 or above.
- All Cisco UCS Manager domains must be included in a Cisco UCS Central domain group.
- Port Configuration must be set to Global on the Policy Resolution Control page in Cisco UCS Manager.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click **Ports**.

Step 4 Choose the port that you want to configure.

Step 5 On the Ports page, click the **Tools** icon on the far right and select **Configure Port**.

The **Configure Port** page for the selected port displays.

Step 6 Select the **Role** for the port.

For Ethernet ports, this can be one of the following:

- Appliance
- FCoE Storage
- FCoE Uplink
- Server
- Uplink

For FC ports, this can be one of the following:

- FC Uplink
- FC Storage

Step 7 Complete the fields as required for your selection.

Step 8 Click **Save**.

Configuring an Appliance Port

Appliance ports are used to connect fabric interconnects to directly attached NFS storage.

Note If you are changing the configuration from an FCoE storage port to an appliance port, admin users have the option to make the port appliance only or unified storage.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click **Ports**.

Step 4 Choose the port that you want to configure.

Step 5 On the Ports page, click the **Tools** icon on the far right and select **Configure Port**.

The **Configure Port** page for the selected port displays.

Step 6 In the **Role** drop-down, select **Appliance**.

Step 7 On the **Basic** tab, do the following:

a) Enter the **Interface User Label**.
b) Select the port speed.
c) Select the quality of service setting associated with this interface. This can be one of the following:

- **Platinum**—Use this priority for vNIC traffic only.

- **Gold**—Use this priority for vNIC traffic only.
- **Silver**—Use this priority for vNIC traffic only.
- **Bronze**—Use this priority for vNIC traffic only.
- **Best Effort**—Do not use this priority. It is reserved for the Basic Ethernet traffic lane.
- **Fibre Channel**—Use this priority for vHBA traffic only.

Step 8 On the **Policies** tab, select the flow control policy, pin group, and network control policy.

Note Only network control policies of type Appliance are supported and available for appliance port configuration.

Step 9 On the **VLANs** tab, choose whether the port will be a **Truck** or **Access** port, and select the VLANs that you want to assign to the ports.

You can click **Search** and specify a VLAN name to filter the results of VLANs displayed. You can search with a partial or full name of the VLAN that you want to select. For example, you can search for *VLAN100* to filter the list of VLANs with names containing VLAN100.

- Trunk ports can have multiple VLANs and allow the VLANs to transport between switches over the trunk link.
- Access ports have one VLAN and is connected to an end point. If the VLAN is a primary VLAN, secondary VLANs are required.

The VLANs that you select are displayed in the **VLANs from System** column. VLANs that were created in Cisco UCS Manager are displayed in the **VLANs Configured on Domain** column.

Note Only VLANs of type Appliance are supported and available for appliance port configuration.

Step 10 On the **Ethernet Target Endpoint** tab, click **Enabled** to enter the **Name** and **MAC Address** for the endpoint.

The Ethernet target endpoint is disabled by default.

Step 11 Click **Save**.

Configuring an FCoE Storage Port

Fibre Channel over Ethernet (FCoE) Storage ports allow storage consolidation from two separate links to a single storage that carries both Fibre Channel (FC) and Ethernet traffic.

Note If you are changing the configuration from an appliance port to an FCoE storage port, admin users have the option to make the port FCoE storage only or unified storage.

Before you begin

The Fibre Channel switching mode must be set to Switching for these ports to be valid. The storage ports cannot function in end-host mode.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click **Ports**.

Step 4 Choose the port that you want to configure.

Step 5 On the Ports page, click the **Tools** icon on the far right and select **Configure Port**.

The **Configure Port** page for the selected port displays.

Step 6 In the **Role** drop-down, select **FCoE Storage**.

Step 7 On the **Basic** tab, enter the **Interface User Label**.

Step 8 On the **VSAN** tab, select the VSANs that you want to assign to the ports.

The VSANs that you select are displayed in the **VSAN** column. VSANs that were created in Cisco UCS Manager are displayed in the **VSAN on Domain** column.

Note Only VSANs of type Storage are supported and available for FCoE storage port configuration.

Step 9 Click **Save**.

Configuring an FCoE Uplink Port

FCoE Uplink ports are physical Ethernet interfaces between the fabric interconnects and the upstream Ethernet switch, used for carrying FCoE traffic. With this support, the same physical Ethernet port can carry both Ethernet traffic and Fibre Channel traffic.

Note If you are changing the configuration from an uplink port to an FCoE uplink port, admin users have the option to make the port FCoE uplink only or unified uplink.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click **Ports**.

Step 4 Choose the port that you want to configure.

Step 5 On the Ports page, click the **Tools** icon on the far right and select **Configure Port**.

The **Configure Port** page for the selected port displays.

Step 6 In the **Role** drop-down, select **FCoE Uplink**.

Step 7 On the **Basic** tab, enter the **Interface User Label**.

Step 8 On the **Policies** tab, select the link profile policy that you want to assign to the port.

Step 9 Click **Save**.

Configuring a Server Port

Server Ports handle data traffic between the Fabric Interconnect and the adapter cards on the servers. Server ports are only configurable on the 6200 series and 6300 series fabric interconnect expansion modules.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click **Ports**.

Step 4 Choose the port that you want to configure.

Step 5 On the Ports page, click the **Tools** icon on the far right and select **Configure Port**.

The **Configure Port** page for the selected port displays.

Step 6 In the **Role** drop-down, choose **Server**.

Step 7 In the **Server** field, enter the **Interface User Label**.

Step 8 Click **Save**.

Configuring an Uplink Port

Ethernet Uplink Ports connect to external LAN Switches. Network bound Ethernet traffic is pinned to one of these ports.

Note If you are changing the configuration from an FCoE uplink port to an uplink port, admin users have the option to make the port uplink only or unified uplink.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click **Ports**.

Step 4 Choose the port that you want to configure.

Step 5 On the Ports page, click the **Tools** icon on the far right and select **Configure Port**.

The **Configure Port** page for the selected port displays.

Step 6 In the **Role** drop-down, select **Uplink**.

Step 7 On the **Basic** tab, do the following:

a) Enter the **Interface User Label**.

b) Select the port speed.

Step 8 On the **VLANs** tab, select the VLANs that you want to assign to the ports.

The VLANs that you select are displayed in the **VLANs from System** column. VLANs that were created in Cisco UCS Manager are displayed in the **VLANs Configured on Domain** column.

You can click **Search** and specify a VLAN name to filter the results of VLANs displayed. You can search with a partial or full name of the VLAN that you want to select. For example, you can search for *VLAN100* to filter the list of VLANs with names containing VLAN100.

Note Only VLANs of type LAN are supported and available for uplink port configuration.

Step 9 From the **VLAN Groups** tab, select the VLAN groups you want to assign to the ports.

The VLAN Groups that you select are displayed in the **VLAN Groups from System** column. VLAN groups that were configured on the port in Cisco UCS Manager are displayed in the **VLAN Groups Configured on Domain** column.

Note Only LAN type VLAN groups are created and available in Cisco UCS Central.

Step 10 On the **Policies** tab, select the flow control policy and link profile.

Step 11 Click **Save**.

Configuring an FC Storage Port

FC Storage ports allow you to directly attach an FC storage device to a port on the FI.

Before you begin

The Fibre Channel switching mode must be set to Switching for these ports to be valid. The storage ports cannot function in end-host mode.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click **Ports**.

Step 4 Choose the port that you want to configure.

Step 5 On the Ports page, click the **Tools** icon on the far right and select **Configure Port**.

The **Configure Port** page for the selected port displays.

Step 6 In the **Role** drop-down, select **FC Storage**.

Step 7 On the **Basic** tab, enter the **Interface User Label** and select a fill pattern.

Step 8 On the **VSAN** tab, select the VSANs that you want to assign to the ports.

The VSANs that you select are displayed in the **VSAN** column. VSANs that were created in Cisco UCS Manager are displayed in the **VSAN on Domain** column.

Note Only VSANs of type Storage are supported and available for FC storage port configuration.

Step 9 Click **Save**.

Configuring an FC Uplink Port

FC uplink ports allow you to connect to external SAN switches.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click **Ports**.

Step 4 Choose the port that you want to configure.

Step 5 On the Ports page, click the **Tools** icon on the far right and select **Configure Port**.

The **Configure Port** page for the selected port displays.

Step 6 In the **Role** drop-down, select **FC Uplink**.

Step 7 On the **Basic** tab, enter the **Interface User Label** and select a fill pattern.

Step 8 On the **VSAN** tab, select the VSANs that you want to assign to the ports.

The VSANs that you select are displayed in the **VSAN from System** column. VSANs that were created in Cisco UCS Manager are displayed in the **VSAN Configured on Domain** column.

Note Only VSANs of type SAN are supported and available for FC uplink port configuration.

Step 9 Click **Save**.

Scalability and Breakout Ports

The Cisco UCS 6300 Series Fabric Interconnects contain scalability ports that can be broken out into groups of 4 10-Gigabit Ethernet ports. The configuration requires a Small Form-Factor Pluggable adapter (SPF) that has one 40GB QSFP+ on one end to connect to the Fabric Interconnect, and four 10 GB ports to connect to different end points supporting 10 GB connectivity.

- The Cisco UCS 6324 Fabric Interconnect contains one scalability port that can be used as a licensed server port for supported Cisco UCS rack servers, an appliance port, or a FCoE storage port.
- The Cisco UCS 6332 and Cisco UCS 6332-16 UP fabric interconnects contain multiple 40-Gigabet Ethernet ports that can be broken out into 10-Gigabit Ethernet ports.

Caution Configuring breakout ports requires rebooting the Fabric Interconnect. Any existing configuration on a port is erased. It is recommended to break out all required ports in a single transaction.

Once you configure a breakout port, you can configure each 10 GB sub-port as server, uplink, FCoE uplink, FCoE storage or appliance port as required.

The following table summarizes the constraints for breakout functionality for the Cisco UCS 6332 and 6332-16UP fabric interconnects:

Fabric Interconnect	Breakout Configurable Ports	Normal Ports with no Breakout Support
UCS-FI-6332	1-12,15-26	13-14,27-32 **Note** • Auto-negotiate behavior is not supported on ports 27–32. • A maximum of four ports are allowed as breakout ports if using QoS jumbo frames.
UCS-FI-6332-16UP	17-34	1-16,35-40 **Note** • Auto-negotiate behavior is not supported on ports 35-40. • A maximum of four ports are allowed as breakout ports if using QoS jumbo frames.

Managing Configured Ports

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click **Ports**.

Step 4 Choose the port that you want to configure.

Step 5 Click the Port **Tools** icon on the far right.

Step 6 Select one of the following:

- **Configuration Status**—Displays the status of the port.
- **Configure Port**—Enables you to change the configuration of the port.
- **Unconfigure Port**—Deletes the port configuration information. If you unconfigure a port, all traffic using the port will stop.
- **Enable Port**—Sets the administrative state of the port to Enabled. Only visible when the port is Disabled.
- **Disable Port**—Sets the administrative state of the port to Disabled. Only visible when the port is Enabled.

- **Unconfigure Breakout Port**—Combines the four 10GbE ports into a single 40GbE port.
- **Configure as Breakout Port**—Turns the port into a scalability port that can be broken out into four 10GbE ports.

Step 7 Complete the fields as required.

Creating a Port Channel

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 In the Fabric Interconnect page, click the **Tools** icon and choose **Create Port Channel**.

Step 4 In **Basic**, select the type of port channel that you want to create.

This can be one of the following:

Step 5 Complete the fields as required for your selection.

Step 6 Click **Save**.

Creating or Editing an Ethernet Port Channel

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 In the Fabric Interconnect page, click the **Tools** icon and choose **Create Port Channel**.

Step 4 In **Basic**, select **Ethernet** and complete the following:

a) Enter the **Port ID**, **Name**, and optional **Description**.
b) Select the admin speed and whether to enable auto negotiation.

Step 5 Click **Policies** and select the flow control and LACP policy that you want to assign to the ports.

Step 6 Click **VLANs** and select the VLANs that you want to assign to the ports.

The VLANs that you select are displayed in the **VLANs from System** column. VLANs that were created in Cisco UCS Manager are displayed in the **VLANs Configured on Domain** column.

Step 7 Click **Ports** and click the **Add** icon to add ports to the port channel.

Step 8 Click **Save**.

Creating or Editing an FC Port Channel

Note For Cisco UCS Manager release 3.1(2) and above, FC port channels must be disabled before you can delete them.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 In the Fabric Interconnect page, click the **Tools** icon and choose **Create Port Channel**.

Step 4 In **Basic**, select **FC** and complete the following:

a) Enter the **Port ID**, **Name**, and optional **Description**.

b) Select the **Admin Speed** for the port channel.

Step 5 Click **VLAN** and select the VLANs that you want to assign to the ports.

You can click **Search** and specify a VLAN name to filter the results of VLANs displayed. You can search with a partial or full name of the VLAN that you want to select. For example, you can search for *VLAN100* to filter the list of VLANs with names containing VLAN100.

The VLANs that you select are displayed in the **VLAN from System** column. VLANs that were created in Cisco UCS Manager are displayed in the **VLAN Configured on Domain** column.

Step 6 Click **Ports** and click the **Add** icon to add ports to the port channel.

Step 7 Click **Save**.

Creating or Editing an FCoE Port Channel

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 In the Fabric Interconnect page, click the **Tools** icon and choose **Create Port Channel**.

Step 4 In **Basic**, select **FCoE**.

Step 5 Enter the **Port Channel ID**, **Name**, and optional **Description**.

Step 6 Click **Policies** and select the LACP policy that you want to assign to the ports.

Step 7 Click **Ports** and click the Plus icon to add ports to the port channel.

Step 8 Click **Save**.

Creating or Editing an Appliance Port Channel

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 In the Fabric Interconnect page, click the **Tools** icon and choose **Create Port Channel**.

Step 4 **Basic**, select **Appliance** and complete the following:

a) Enter the **Port Channel ID**, **Name**, and optional **Description**.

b) Select the admin speed and whether to use **Static** mode or dynamic **LACP**.

c) Select the quality of service **Priority** associated with this interface. This can be one of the following:

- **Platinum**—Use this priority for vNIC traffic only.
- **Gold**—Use this priority for vNIC traffic only.
- **Silver**—Use this priority for vNIC traffic only.
- **Bronze**—Use this priority for vNIC traffic only.
- **Best Effort**—Do not use this priority. It is reserved for the Basic Ethernet traffic lane.
- **Fibre Channel**—Use this priority for vHBA traffic only.

Step 5 Click **Policies** and select the flow control policy, network control policy, and the pin group that you want to assign to the ports.

Step 6 Click **VLANs** and select the VLANs that you want to assign to the ports.

The VLANs that you select are displayed in the **VLANs from System** column. VLANs that were created in Cisco UCS Manager are displayed in the **VLANs Configured on Domain** column.

Step 7 Click **Ethernet Target Endpoint** and click **Enabled** to enter the **Name** and **MAC Address** for the endpoint.

The Ethernet target endpoint is disabled by default.

Step 8 Click **Ports** and click the **Add** icon to add ports to the port channel.

Step 9 Click **Save**.

Pin Groups

LAN Pin Groups

Cisco UCS uses LAN pin groups to pin Ethernet traffic from a vNIC on a server to an uplink Ethernet port or port channel on the fabric interconnect. You can use this pinning to manage the distribution of traffic from the servers.

To configure pinning for a server, you must include the LAN pin group in a vNIC policy. The vNIC policy is then included in the service profile assigned to that server. All traffic from the vNIC travels through the I/O module to the specified uplink Ethernet port.

Note If you do not assign a pin group to a server interface through a vNIC policy, Cisco UCS Central chooses an uplink Ethernet port or port channel for traffic from that server interface dynamically. This choice is not permanent. A different uplink Ethernet port or port channel may be used for traffic from that server interface after an interface flap or a server reboot.

If an uplink is part of a LAN pin group, the uplink is not necessarily reserved for only that LAN pin group. Other vNIC's policies that do not specify a LAN pin group can use the uplink as a dynamic uplink.

SAN Pin Groups

Cisco UCS uses SAN pin groups to pin Fibre Channel traffic from a vHBA on a server to an uplink Fibre Channel port on the fabric interconnect. You can use this pinning to manage the distribution of traffic from the servers.

Note In Fibre Channel switch mode, SAN pin groups are irrelevant. Any existing SAN pin groups will be ignored.

To configure pinning for a server, you must include the SAN pin group in a vHBA policy. The vHBA policy is then included in the service profile assigned to that server. All traffic from the vHBA will travel through the I/O module to the specified uplink Fibre Channel port.

You can assign the same pin group to multiple vHBA policies. As a result, you do not need to manually pin the traffic for each vHBA.

Important Changing the target interface for an existing SAN pin group disrupts traffic for all vHBAs which use that pin group. The fabric interconnect performs a log in and log out for the Fibre Channel protocols to re-pin the traffic.

Creating a Pin Group

You can create a pin group for either LAN or SAN.

Step 1 Click the **Browse Tables** icon and choose **Domains**.

Step 2 Click the domain in which you want to create a pin group.

Step 3 On the domain page, click the **Tools** icon and select **Create Pin Group**.

Step 4 In the **Create Pin Group** dialog box, click **Basic** and choose whether you want to create a LAN or a SAN pin group.

Step 5 Enter the **Name** and optional **Description**.

Step 6 In **Fabric A Target**, choose whether you want to manually select a port, or select an existing port channel.

Step 7 If you selected **Manual**, select the port.

For LAN pin groups, only ethernet uplink ports are shown. For SAN pin groups, only FC and FCoE uplink ports are shown.

Step 8 If you selected **Port Channel**, select an existing port channel.

For LAN pin groups, only ethernet port channels are shown. For SAN pin groups, only FC and FCoE port channels are shown.

Step 9 In **Fabric B Target**, select a port or a port channel.

Step 10 Click **Save**.

Fibre Channel Switching Mode

The Fibre Channel switching mode determines how the fabric interconnect behaves as a switching device between the servers and storage devices. The fabric interconnect operates in either of the following Fibre Channel switching modes:

End-Host Mode

End-host mode allows the fabric interconnect to act as an end host to the connected fibre channel networks, representing all servers (hosts) connected to it through virtual host bus adapters (vHBAs). This behavior is achieved by pinning (either dynamically pinned or hard pinned) vHBAs to Fibre Channel uplink ports, which makes the Fibre Channel ports appear as server ports (N-ports) to the rest of the fabric. When in end-host mode, the fabric interconnect avoids loops by denying uplink ports from receiving traffic from one another.

End-host mode is synonymous with N Port Virtualization (NPV) mode. This mode is the default Fibre Channel Switching mode.

Note When you enable end-host mode, if a vHBA is hard pinned to an uplink Fibre Channel port and this uplink port goes down, the system cannot repin the vHBA, and the vHBA remains down.

Switch Mode

Switch mode is the traditional Fibre Channel switching mode. Switch mode allows the fabric interconnect to connect directly to a storage device. Enabling Fibre Channel switch mode is useful in Pod models where there is no SAN (for example, a single Cisco UCS domain that is connected directly to storage), or where a SAN exists (with an upstream MDS).

Switch mode is not the default Fibre Channel switching mode.

Note In Fibre Channel switch mode, SAN pin groups are irrelevant. Any existing SAN pin groups are ignored.

Configuring Fibre Channel Switching Mode

You can configure your fabric interconnect to use either FC End-Host Mode or FC Switch Mode. By default, the FI is set to end-host mode.

Note When you change the Fibre Channel switching mode, Cisco UCS Central logs you out and restarts the fabric interconnect. For a cluster configuration, Cisco UCS Central restarts both fabric interconnects sequentially. The second fabric interconnect can take several minutes to complete the change in Fibre Channel switching mode and become system ready.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 On the fabric interconnect page, click the **Tools** icon and select the **FC switching mode**.

If you are using end-host mode, **Set FC Switching Mode** displays. If you are using FC switching mode, **Set FC End-Host Mode** displays.

Step 4 Click **Yes** on the warning page to change the configuration and restart the FI.

Viewing Port Configuration Status

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click the Tools icon on the far right and select **Configuration Status**.

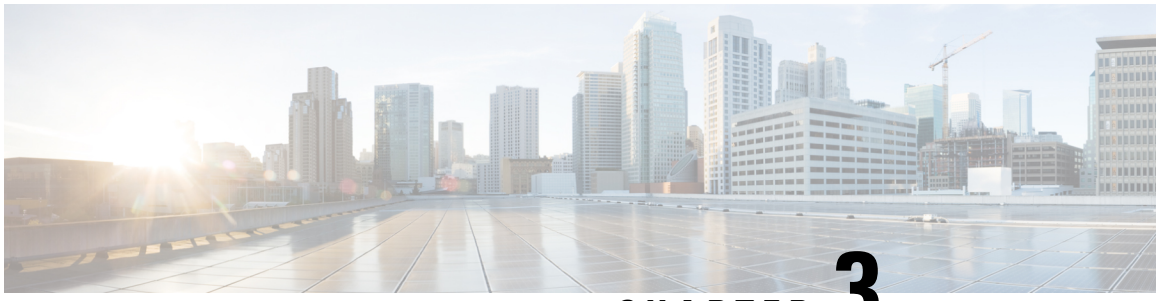
The Configuration Status page for the selected port displays.

Step 4 Click **Close** to close the window.

Port Configuration Faults

The port faults page displays the following information for each fault:

- **Code**—The ID associated with the fault
- **Timestamp**—Date and time at which the fault occurred
- **Cause**—Cause of the fault
- **Affected Object**—The component that is affected by this fault
- **Fault Details**—The details of the fault.
- **Severity**—The severity of the fault
- **Action**—Any action required by the fault



CHAPTER 3

Global VLANs

Global VLANs

Cisco UCS Central enables you to define global VLANs in a LAN cloud at the domain group root, or at the domain group level. You can create a single VLAN or multiple VLANs in one operation.

Global VLAN resolution takes place in Cisco UCS Central prior to global service profiles deployment. If a global service profile references a global VLAN, and that VLAN does not exist, the global service profile deployment fails in the Cisco UCS domain due to insufficient resources. All global VLANs created in Cisco UCS Central must be resolved before deploying that global service profile.

Global VLANs are pushed to Cisco UCS domain along with the global service profiles that reference them. Global VLAN information is visible to Cisco UCS Manager only if a global service profile with reference to a global VLAN is deployed in that Cisco UCS domain. When a global VLAN is deployed and becomes available in the Cisco UCS domain, locally-defined service profiles and policies can reference the global VLAN. A global VLAN is not deleted when a global service profile that references it is deleted.

If a global VLAN is part of a global service profile, or a global port configuration, automatic VLAN resolution takes place when the service profile is pushed down, and the VLANs are available for local consumption in the Cisco UCS domain. If the global VLANs are not associated to a global service profile, or a global port configuration, you must manually publish them to deploy them to Cisco UCS Manager. Cisco UCS Central provides a command to manually publish the global VLAN to sync with Cisco UCS Manager. For more information on Publishing VLANs see Cisco UCS Central CLI Reference Manual.

Note You must have created the VLAN in Cisco UCS Central prior to publishing it to push it down to Cisco UCS Manager.

Note If a VLAN group is used to allow VLANs on a Fabric Interconnect's uplink, the global VLAN must be manually published to Cisco UCS Manager and added to the VLAN group, prior to adding to the service profile assigned to the Cisco UCS domain. If the global VLAN is not published and added to the VLAN group, the vNIC will shut down as the uplink will not allow the global VLAN to pass through.

Note A global VLAN is not deleted when a global service profile that references it is deleted.

You cannot delete a global VLAN from Cisco UCS Manager. If you want to delete a global VLAN from Cisco UCS Manager, you have to localize the VLAN and then delete it.

VLAN Org Permission

All VLANs configured in Cisco UCS Central are common to the orgs in which they are created. You must assign organization permissions before the Cisco UCS Manager instances that are part of the organizations can consume the resources. When you assign org permission to a VLAN, the VLAN is visible to those organizations, and available to be referenced in service profiles maintained by the Cisco UCS Manager instances that are part of the organization.

VLAN name resolution takes place within the hierarchy of each domain group. If a VLAN with the same name exists in multiple domain groups, the organization permissions are applied to all VLANs with the same name across the domain groups.

You can create, modify or delete VLAN org permission.

Note Make sure to delete the VLAN org permission from the same org you created it in. On Cisco UCS Central GUI you can view the org structure where this VLAN is associated. But at the sub org level on the Cisco UCS Central CLI, you cannot view the VLAN org permission association hierarchy, so if you try to delete the VLAN at the sub org level on the Cisco UCS Central CLI the delete operation will fail.

Creating or Editing a VLAN

You can create a VLAN at the domain group root or at a specific domain group level, and specify the orgs that can access the VLAN.

You can edit the**VLAN ID**, **Multicast Policy** and access for control for any selected VLANs. After creating a VLAN in a domain group, you can not change the **Domain Group Location** or the **VLAN Name**.

To watch a video on creating a VLAN, see Video: Creating a VLAN and Assigning Org Permission.

Step 1 In the **Actions** bar, type **Create VLAN** and press Enter.

Step 2 In the **VLAN** dialog box, choose the type of VLAN that you want to create.

This can be one of the following:

- **LAN**—The VLAN is used for communication with an external LAN.

- **Appliance**—The VLAN is used for appliance ports and port channels only.

Step 3 In **Basic**, click **Domain Group Location** and select the location in which you want to create this VLAN.

Step 4 Enter a **Name** for this VLAN.

The VLAN name is case sensitive.

Important Do not use the name **default** when you create a VLAN in Cisco UCS Central. If you want to create a global default VLAN, you may use **globalDefault** for the name.

Step 5 Enter the **VLAN ID**.

A VLAN ID can:

- Be between 1 and 3967

  Note If the registeredCisco UCS Domain has Cisco UCS Manager version 2.2(4) or above the ID range can be between 1 an 4027.

- Be between 4048 and 4093
- Overlap with other VLAN IDs already defined in other domain groups

Step 6 (Optional) Choose whether to enable **Check VLAN Name Overlap** and **Check VLAN ID Overlap** to identify any overlaps.

Step 7 (Optional) If you want to associate a **Multicast Policy** with this VLAN, enter the multicast policy name.

Cisco UCS Central identifies the multicast policy and attaches it to the VLAN in the back end.

Step 8 In **Private VLAN**, click the **Sharing Type** to determine whether the VLAN is subdivided into private or secondary VLANs. This can be one of the following:

- **None**—This VLAN does not have any secondary or private VLANs.
- **Primary**—This VLAN can be associated with one or more secondary VLANs.
- **Isolated**—This is a private VLAN. Select the primary VLAN with which it is associated in the Primary VLAN drop-down list.
- **Community**—This VLAN can communicate with other ports on the same PVLAN as well as the promiscuous port. Select the primary VLAN with which it is associated in the Primary VLAN drop-down list.

Step 9 In **Access Control**, click the plus sign to display available orgs.

Step 10 Select the organizations and click the checkmark to apply the selected orgs as **Permitted Orgs** for this VLAN.

Step 11 In **Aliased VLANs**, you can view the existing VLANs to see if a VLAN of the same name already exists.

Step 12 In**Multicast Policy**, click **Manually Provision** and enter the specific multicast policy name that you want to associate with this VLAN.

Cisco UCS Central attaches it to the VLAN in the back end. If the multicast policy is associated with a global service profile, the Cisco UCS Central displays a Policy Conflict message when a multicast policy of the same name exists in Cisco UCS Manager.

Step 13 (Optional) Click **Global Policy** and then select the global multicast policy that you want to assign to this VLAN.

Step 14 Click **Create**.

Creating or Editing a VLAN Range

Step 1 In the **Actions** bar, type **Create VLAN Range** and press Enter.

Step 2 In the **VLAN Range** dialog box, click **Basic** and choose the **Domain Group Location** in which you want to create this VLAN.

Step 3 Enter a **Name Prefix** for this VLAN range.

Step 4 Enter **VLAN ID**.

A VLAN ID can:

- Be between 1 and 3967
- Be between 4048 and 4093
- Overlap with other VLAN IDs already defined in other domain groups

Example:

For example, to create six VLANs with IDs 4, 22, 40, 41, 42, and 43, you would enter 4, 22, 40-43.

Step 5 (Optional) Choose whether to enable **Check VLAN Name Overlap** and **Check VLAN ID Overlap** to identify any overlaps.

Step 6 (Optional) if you want to associate a **Multicast Policy** with this VLAN range, enter the multicast policy name.

Cisco UCS Central identifies the multicast policy and attaches it to the VLAN range in the back end.

Step 7 In **Private VLAN**, click the **Sharing Type** to determine whether the VLAN is subdivided into private or secondary VLANs. This can be one of the following:

- **None**—This VLAN does not have any secondary or private VLANs.
- **Primary**—This VLAN can be associated with one or more secondary VLANs.
- **Isolated**—This is a private VLAN. Select the primary VLAN with which it is associated in the Primary VLAN drop-down list.
- **Community**—This VLAN can communicate with other ports on the same PVLAN as well as the promiscuous port. Select the primary VLAN with which it is associated in the Primary VLAN drop-down list.

Step 8 In **Access Control**, click the plus sign display available orgs.

Step 9 Select the orgs and click the checkmark to apply the selected orgs as **Permitted Orgs** for this VLAN.

Step 10 In **Aliased VLANs**, you can view the existing VLANs to see if a VLAN of the same name already exists.

Step 11 In**Multicast Policy**, click **Manually Provision** and enter the specific multicast policy name that you want to associate with this VLAN.

Cisco UCS Central associates it to the VLAN in the back end. If the multicast policy is associated with a global service profile, the Cisco UCS Central displays a Policy Conflict message when a multicast policy of the same name exists in Cisco UCS Manager.

This feature is supported with the Cisco UCS Manager release 3.1(3) and later.

Step 12 (Optional) Click **Global Policy** and then select the global multicast policy that you want to assign to this VLAN.

Step 13 Click **Create**.

Managing VLAN Access

From the **Manage VLAN Access** dialog box, you can add or remove permissions to one or more VLANs at the same time.

Note You can only add or remove access each time you open the dialog box. If you want to do both actions, you will need to relaunch the dialog box.

Step 1 In the **Actions** bar, type **Manage VLAN Access** and press Enter.

Step 2 To add access permissions to VLANs, do the following in the **VLAN Access** dialog box:

a) Click **Add Org Permissions**.

b) Select the VLAN name or range that you want to use to filter the VLANs and click **Search**.

You can click specify a VLAN name to filter the results of VLANs displayed. You can search with a partial or full name of the VLAN that you want to select. For example, you can search for *VLAN100* to filter the list of VLANs with names containing VLAN100.

c) Click the check boxes for the VLANs that you want to change the permissions for, or select the top check box to select all VLANs on the page.

d) Click the Plus icon, and select the organizations for which you want to grant permissions.

Step 3 To remove access permissions to VLANs, do the following:

a) Click **Remove Org Permissions**.

b) Select the organization for which you want to remove access permissions.

c) Select the VLAN name or range that you want to use to filter the VLANs and click **Search**.

d) Click the check boxes for the VLANs that you want to remove the permissions for, or select the top check box to select all VLANs on the page.

Step 4 Click **Apply** to save and apply your changes.

VLAN Groups

A VLAN Group is a logical entity created to configure VLANs on uplink ports and port channels, and vNICs in a Global Service Profile. Starting Cisco UCS Central 2.0, you can create a VLAN Group to logically group VLANs on Ethernet uplink ports by function, or by VLANs that belong to a specific network. You can apply these VLAN Groups to Ethernet uplink ports or service profile vNICs. VLAN Groups for Ports and Service Profiles are supported for Cisco UCS Manager 3.1(3) and later releases. However, Global VLAN Groups are

not supported on Cisco UCS Manager releases prior to 3.1(3) even though they are supported locally in Cisco UCS Central.

Creating or Editing a VLAN Group

You can create a VLAN Group under **LAN Cloud** per Domain-Group.

- For a Global Service profile, all associated VLAN Groups are resolved when the service profile is associated to a server. Depending on the server location in Cisco UCS Central, the VLANs get dynamically resolved and get deployed to the domain.
- For VLAN Groups on a Port, all associated VLANs are resolved when you save the port configuration depending on the domain group membership of the domain in **Cisco UCS Central**.

VLAN Groups have Org permission configured, and are accessible only from those Global Service Profiles that are created under the **Orgs** with the corresponding org permission. After you assign a VLAN to a VLAN group, all changes you make are applied to all Ethernet uplink ports and vNICs that are configured in the VLAN Group. You can configure multiple VLAN Groups for a vNIC (in the case of the Global Service Profile), and for uplink ports or port-channels. More than one VLAN Group can co-exist with other ungrouped VLANs that are configured on a vNIC or a port or port-channel.

When you add a VLAN Group to an uplink port, all the VLANs assigned before to the port are removed and re-added once the configuration is complete. Also, the uplink port allows the newly added VLANs instead. An uplink port on a particular Cisco UCS Domain that is not associated with the VLAN Group does not support the VLANs that are part of the configured VLAN Group.

You can configure VLAN Groups on the vNICs in the following ways:

- Directly modifying the vNIC
- Modifying through the LAN Connectivity Policy
- Modifying through the vNIC template

Step 1 In the **Actions** bar, type **Create VLAN Group** and press Enter.

Step 2 In the **VLAN Group** dialog box, choose the domain group to create the VLAN group.

Step 3 Choose the **Organization** where you want to create the VLAN group, and enter the **Name** and optional **Description**.

The name is case-sensitive.

Step 4 In **VLANs**, select the VLAN you want to add to the VLAN group. Optionally, you can choose any VLAN from the following VLAN types and **Set as Native** VLAN by checking the **Set as Native** check box:

- Primary
- Community
- isolated
- *Name*-VLAN

Step 5 In **Access Controls**, select the Organization permission.

Step 6 Click **Create**.

Step 7 In **Access Control**, click the plus sign to display available organizations.

Step 8 Select the organizations and click the checkmark to apply the selected organizations as **Permitted Orgs** for this VLAN.

You must configure the permitted Orgs for VLAN Groups for a Global Service Profile. Configuring Access controls is optional for Port groups.

Viewing a VLAN Group

Step 1 From **VLAN Groups Container** view, select a **VLAN Group** you want to view and press Enter.

Step 2 The VLAN Group view displays the following details:

- VLANs associated with the VLAN group, and native VLANs configured on the VLAN group
- Size of the VLAN group
- Permitted organizations and Location of the VLAN group

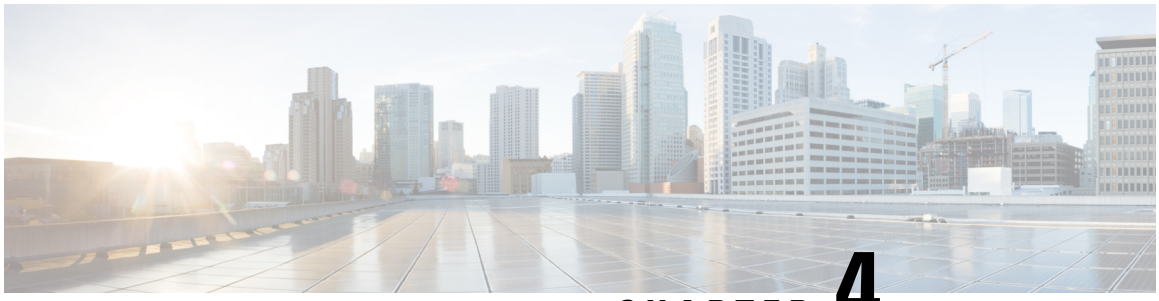
From the **VLAN Group** view, you can **Edit**, **Delete**, **Share**, **Favorite**, and **Tag** the VLAN Group you created.

VLAN Group Container View

A **VLAN Group Container** view displays a list of all VLAN groups in a domain. You can view the following details in the VLAN Group Container view:

- **Name**—Lists the VLAN group names present in a domain group
- **Native VLAN**—Lists the Native VLANs associated with the VLAN groups

You can filter the VLAN group Containers by Domain Group, **Export**, **Delete**, **Tag**, and **Search** for a specific VLAN group on this page.



CHAPTER 4

vNICs

vNIC Templates

Use vNIC templates to define how a vNIC on a server connects to the LAN. You can view all existing vNIC templates on the **Templates** page.

vNIC Redundancy Template Pairs

Creating vNIC template pairs enables you to group vNICs that belong to a specific server. For example, you can create a vNIC template and specify it as the primary template, then create a different vNIC template and specify it as the secondary template. You can link the two templates to create a pair that share attributes that you define in the primary template. The secondary template inherits the attributes from the primary template. If you select **Updating Template**, any changes made to the primary template are propagated to the secondary template in the template pair. You can also modify any non-shared configurations on each individual template in the pair.

When creating the pair, you can assign one template to each fabric. For example you could assign the primary template to fabric A, and the secondary template to fabric B. This eliminates the need to configure vNIC pairs independently using one or more templates. The number of vNIC pairs that can be created using a template pair is only limited by the adapter's maximum capabilities.

The following configurations are shared when using template pairs:

- Network Control Policy
- QoS Policy
- Template Type
- Connection Policies
- VLANs
- MTU
- Statistics Threshold Policy

The following configurations are not shared when using template pairs:

- Fabric ID
- CDN Source
- MAC Pool
- Description
- Pin Group Policy

Note If you plan to use a global vNIC redundancy template pair in a local service profile in Cisco UCS Manager, you cannot assign the vNIC template for the primary and the secondary of the redundancy template pair at the same time. You will need to assign the vNIC template for the primary vNIC and set the peer name for the second vNIC, then modify the second vNIC and manually assign the secondary vNIC template.

Creating or Editing a vNIC Template

Note Global vNICs can be used in local service profiles created in Cisco UCS Manager.

Step 1 In the **Actions** bar, type **Create vNIC Template** and press Enter.

Step 2 In the **vNIC Template** dialog box, click **Basic** and complete the following:

a) Choose the **Organization** where you want to create the vNIC template.
b) Enter a **Name** and **Description**.
c) Choose the **Redundancy Type** to enable vNIC pairing.

This can be one of the following:

- **None**—Creates a standard vNIC template without vNIC pairing.
- **Primary**—Creates the primary vNIC template.
- **Secondary**—Creates the secondary vNIC template.

d) Select the options for **Type**, **Fabric ID**, **Fabric Failover** and enter the **MTU**.
e) Select the **CDN Source**. If you choose to use a user defined name, you must also enter the **User Defined CDN Name**.

Step 3 If you enabled vNIC pairing, click **Peer Redundancy Template** and choose the primary or secondary vNIC template.

Step 4 Click **MAC Address** and select the MAC address.

If you do not assign a MAC address pool, the system assigns the default.

Step 5 Click **VLANs** and add the VLANs that you want to use for this vNIC template.

You can click **Search** and specify a VLAN name to filter the results of VLANs displayed. You can search with a partial or full name of the VLAN that you want to select. For example, you can search for *VLAN100* to filter the list of VLANs

with names containing VLAN100. You cannot set multiple native VLANs for a vNIC in a Service Profile. When you click on **Set as Native**, a **Configuration Error** results.

Step 6 Click **VLAN Groups** and specify the VLAN group name and choose the **Organization** you want to create the vNIC template.
The VLAN group is resolved only if the service profile referencing the template is associated. Once the service profile is associated, the VLAN group gets resolved based on the name on the Domain on the associated server.

Step 7 Click **Policies** and assign the policies that you want to use for this vNIC template.

If the policies are not assigned, click on each of the policies. On the right, click the drop-down to display related policies and select the one you want for this vNIC template.

Step 8 Click **Create**.

Default vNIC Behavior Policy

Default vNIC behavior policy allows you to configure how vNICs are created for a service profile. You can choose to create vNICS manually, or you can create them automatically.

You can configure the default vNIC behavior policy to define how vNICs are created. This can be one of the following:

- **None**— does not create default vNICs for a service profile. All vNICs must be explicitly created.
- **HW Inherit**—If a service profile requires vNICs and none have been explicitly defined, creates the required vNICs based on the adapter installed in the server associated with the service profile.

Note If you do not specify a default behavior policy for vNICs, **HW Inherit** is used by default.

Configuring Default vNIC Behavior

If you do not specify a default behavior policy for vNICs, **HWInherit** is used by default.

Step 1 On the menu bar, click **Network**.

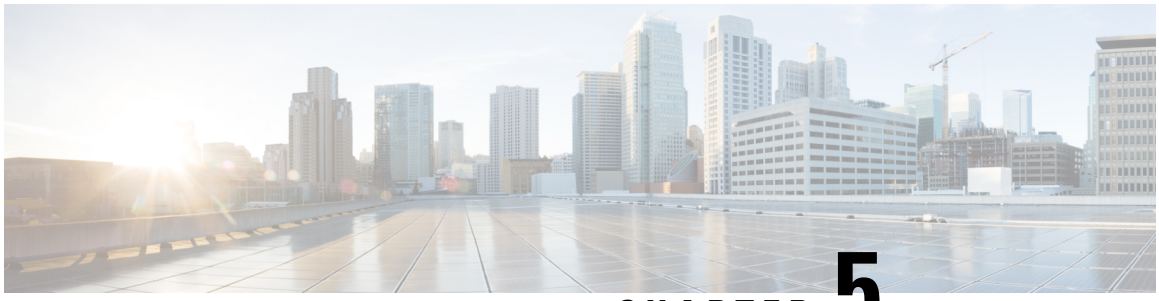
Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.

You can only configure the default vNIC behavior policy in the root organization. You cannot configure the default vNIC behavior policy in a sub-organization.

Step 3 Right-click **Default vNIC Behavior** and choose **Properties**.

Step 4 In the **Properties (Default vNIC Behavior)** dialog box, choose the **Action** and the optional **vNIC Template**.

Step 5 Click **OK**.



CHAPTER 5

Network Pools

MAC Pools

A MAC pool is a collection of network identities or MAC addresses that are unique in their layer 2 environment and are available to be assigned to vNICs on a server. MAC pools created in Cisco UCS Central can be shared between Cisco UCS domains. If you use MAC pools in service profiles, you do not have to manually configure the MAC addresses to be used by the server associated with the service profile.

In a system that implements multi-tenancy, you can use the organizational hierarchy to ensure that MAC pools can only be used by specific applications or business services. Cisco UCS Central uses the name resolution policy to assign MAC addresses from the pool.

To assign a MAC address to a server, you must include the MAC pool in a vNIC policy. The vNIC policy is then included in the service profile assigned to that server.

You can specify your own MAC addresses or use a group of MAC addresses provided by Cisco.

Creating and Editing a MAC Pool

After creating a MAC pool you can edit it by selecting the **Edit** icon on the overall summary page of the selected MAC pool. To select a MAC pool, go to **All Pools** page and select the MAC pool that you want to edit. The page redirects you to the overall summary page of the selected MAC pool.

Step 1 In the Actions bar, type **Create MAC Pool** and press **Enter**.

This launches the **Create MAC Pool** dialog box.

Step 2 In **Basic**, complete the following:

a) From the **Organization** drop-down list, select an organization or a sub-organization in which you want to create or access a MAC pool.

b) Enter name and description of the pool.

Step 3 In **MAC Blocks**, complete the following:

a) Click the **Plus** icon to create a block of MAC addresses.

b) In the **MAC Block Start** column, enter the first MAC address in the block.

c) In the **Size** column, enter the number of MAC addresses in the block.
d) Click the **Apply** icon.

Additional fields related to the MAC pools are displayed.

e) In **MAC Addresses**, you can view a graphical representation of the number if MAC addresses in the pool, the number of assigned MAC addresses, duplicate MAC addresses, and MAC summary.
f) In **Access Control**, select the ID range access control policy to apply to this block. If you do not have a policy, you can create one by typing **Create ID Range Access Control Policy** in the task bar.

Step 4 Click **Create**.

What to do next

Include the MAC pool in a vNIC template.

Deleting a Pool

If you delete a pool, Cisco UCS Central does not reallocate any addresses from that pool that have been assigned to vNICs or vHBAs in Cisco UCS Manager. All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until one of the following occurs:

- The associated service profiles are deleted.
- The vNIC or vHBA to which the address is assigned is deleted.
- The vNIC or vHBA is assigned to a different pool.

Step 1 Click the **Browse Tables** icon and choose **Pools**.

Step 2 In the **Pool Name** column, locate the pool that you want to delete.

You can search for the pool in one of the following ways:

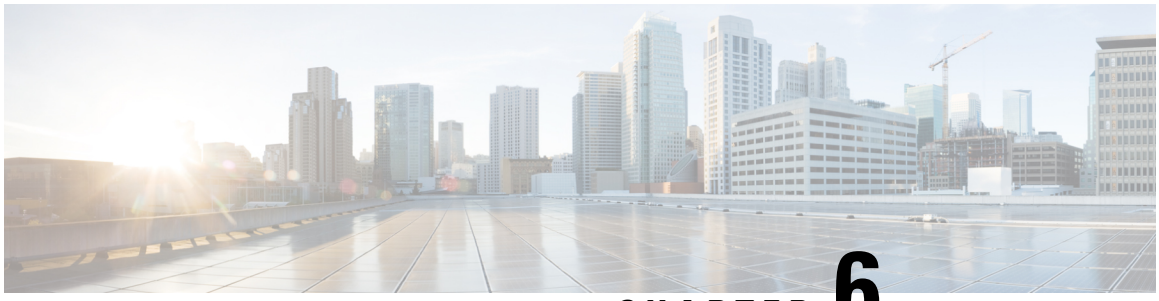
- Browse through the list of pools.
- Click the **Search** icon and enter the pool name.
- Select a pool type from the **Filters** column.

Step 3 Click the pool.

This launches the overall summary page of the selected pool.

Step 4 Click the **Delete** icon.

If Cisco UCS Central displays a confirmation dialog box, click **Delete**.



CHAPTER 6

Network Policies

Network Control Policy

This policy configures the network control settings for the Cisco UCS domain, including the following:

- Whether the Cisco Discovery Protocol (CDP) is enabled or disabled
- How the virtual interface (VIF) behaves if no uplink port is available in end-host mode
- The action that Cisco UCS Central takes on the remote Ethernet interface, vEthernet interface , or vFibre Channel interface when the associated border port fails
- Whether the server can use different MAC addresses when sending packets to the fabric interconnect
- Whether MAC registration occurs on a per-VNIC basis or for all VLANs

Action on Uplink Fail

By default, the **Action on Uplink Fail** property in the network control policy is configured with a value of link-down. For adapters such as the Cisco UCS M81KR Virtual Interface Card, this default behavior directs Cisco UCS Central to bring the vEthernet or vFibre Channel interface down if the associated border port fails. For Cisco UCS systems using a non-VM-FEX capable converged network adapter that supports both Ethernet and FCoE traffic, such as Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, this default

behavior directs Cisco UCS Central to bring the remote Ethernet interface down if the associated border port fails. In this scenario, any vFibre Channel interfaces that are bound to the remote Ethernet interface are brought down as well.

Note if your implementation includes those types of non-VM-FEX capable converged network adapters mentioned in this section and the adapter is expected to handle both Ethernet and FCoE traffic, we recommend that you configure the **Action on Uplink Fail** property with a value of warning. Note that this configuration might result in an Ethernet teaming driver not being able to detect a link failure when the border port goes down.

MAC Registration Mode

MAC addresses are installed only on the native VLAN by default, which maximizes the VLAN port count in most implementations.

Note If a trunking driver is being run on the host and the interface is in promiscuous mode, we recommend that you set the Mac Registration Mode to All VLANs.

Creating or Editing a Network Control Policy

Step 1 In the **Actions** bar, type **Create Network Control Policy** and press Enter.

Step 2 In the **Network Control Policy** dialog box, choose whether to create a default or appliance network control policy.

Step 3 Choose the **Organization** where you want to create the policy, and enter the **Name** and optional **Description**.

The name is case sensitive.

Step 4 Choose whether to enable **Cisco Discovery Protocol (CDP)**.

Step 5 Select values for **Action on Uplink Failure**, **MAC Address Registration**, and **MAC Address Forging**.

Step 6 Choose whether to enable or disable **Link Layer Discovery Protocol (LLDP) Transmit** and **Link Layer Discovery Protocol (LLDP) Receive**.

Step 7 Click **Create**.

Deleting a Network Control Policy

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.

If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Network Control Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Ethernet Adapter Policy

Ethernet adapter policies govern the host-side behavior of the adapter, including how the adapter handles traffic. For example, you can use these policies to change default settings for the following:

- Queues
- Interrupt handling
- Performance enhancement
- RSS hash
- Failover in an cluster configuration with two fabric interconnects

Operating System Specific Adapter Policies

By default, Cisco UCS provides a set of Ethernet adapter policies. These policies include the recommended settings for each supported server operating system. Operating systems are sensitive to the settings in these policies. Storage vendors typically require non-default adapter settings. You can find the details of these required settings on the support list provided by those vendors.

Note We recommend that you use the values in these policies for the applicable operating system. Do not modify any of the values in the default policies unless directed to do so by Cisco Technical Support.

If you are creating an Ethernet adapter policy (instead of using the default Windows adapter policy) for a Windows operating system, you must use the following formulas to calculate values that work with Windows:

Completion Queues = Transmit Queues + Receive Queues

Interrupt Count = (Completion Queues + 2) rounded up to nearest power of 2

For example, if Transmit Queues = 1 and Receive Queues = 8 then:

Completion Queues = 1 + 8 = 9

Interrupt Count = (9 + 2) rounded up to the nearest power of 2 = 16

Creating and Editing an Ethernet Adapter Policy

Step 1 In the **Actions** bar, type **Create Ethernet Adapter Policy** and press Enter.

Step 2 In the **Ethernet Adapter Policy** dialog box, In **Basic**, choose the **Organization** where you want to create the ethernet adapter policy.

Step 3 Enter the **Name** and optional **Description**.

Step 4 In **Resources**, complete the following:

a) In **Transmit Queues**, enter the number of transmit queue resources to allocate.

b) In **Transmit Queue Ring Size**, enter the number of descriptors in each transmit queue.
c) In **Receive Queues**, enter the number of receive queue resources to allocate.
d) In **Receive Queues Ring Size**, enter the number of descriptors in each receive queue.
e) In **Completion Queues**, enter the number of completion queue resources to allocate. In general, the number of completion queue resources you allocate should be equal to the number of transmit queue resources, plus the number of receive queue resources.
f) In **Interrupts**, enter the number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources.

Step 5 In **Settings**, complete the following:

a) Choose whether to enable **Transmit Checksum Offloading**, **Receive Checksum Offloading**, **TCP Segmentation Offloading**, **Large TCP Receive Offloading**, **Receive Side Scaling**, **Virtual Extensible LAN (VXLAN)**, **RDMA over Converged Ethernet (RoCE)**, **Accelerated Receive Flow Steering (ARF)**, and **NVGRE**.
b) Select an **Interrupt Mode**.
c) Enter the **Interrupt Timer** value in microseconds.
d) Select the **Interrupt Coalescing Type**.
e) Enter the **Failback Timeout** in seconds.

Step 6 Click **Create**.

Dynamic vNIC Connection Policy

The dynamic vNIC connection policy determines how the connectivity between VMs and dynamic vNICs is configured. This policy is required for Cisco UCS domains that include servers with VIC adapters on which you have installed VMs and configured dynamic vNICs.

Each dynamic vNIC connection policy includes an Ethernet adapter policy and designates the number of vNICs that can be configured for any server associated with a service profile that includes the policy.

Note Server Migration:

- If you migrate a server that is configured with dynamic vNICs or another migration tool, the dynamic interface used by the vNICs fails and Cisco UCS Central notifies you of that failure.
- When the server comes back up, Cisco UCS Central assigns new dynamic vNICs to the server. If you are monitoring traffic on the dynamic vNIC, you must reconfigure the monitoring source.

Creating or Editing a Dynamic vNIC Connection Policy

Step 1 In the **Actions** bar, type **Create Dynamic vNIC Connection Policy** and press Enter.

Step 2 In the **Dynamic vNIC Connection Policy** dialog box, choose the **Organization** in which you want to create the dynamic vNIC connection policy.

Step 3 Enter a **Name** and optional **Description**.

The policy name is case sensitive.

Step 4 Enter the number of dynamic vNICS that you want to create.

Step 5 Select the protection mode that you want to use.

Step 6 Select the adapter profile to be associated with this policy.

The profile must already exist to be included in the **Ethernet Adapter** drop-down list.

Step 7 Click **Create**.

usNIC Connection Policy

The Cisco user-space NIC (Cisco usNIC) connection policy page displays the details of your usNIC connection policy and what service profiles it is associated with.

Creating or Editing a usNIC Connection Policy

Step 1 In the **Actions** bar, type **Create usNIC Connection Policy** and press Enter.

Step 2 In the **usNIC Connection Policy** dialog box, choose the **Organization** in which you want to create the policy.

Step 3 Enter a **Name** and optional **Description**.

The policy name is case sensitive.

Step 4 Enter the **Number of usNICs** that you want to create.

Step 5 Select the **Adapter Policy** that you want to specify for the usNIC.

We recommend that you use the global-usNIC adapter policy, which is created by default.

Step 6 Click **Create**.

VMQ Connection Policy

VMQ provides improved network performance to the entire management operating system. From Cisco UCS Central you can create a VMQ connection policy for a vNIC on a service profile. To configure the VMQ vNIC on a service profile for a server, at least one adapter in the server must support VMQ. Make sure the servers have at least one the following adapters installed:

- UCS-VIC-M82-8P
- UCSB-MLOM-40G-01
- UCSC-PCIE-CSC-02

You must have one of the following Operating systems to use VMQ:

- Windows 2012
- Windows 2012R2

When you select the vNIC connection policy for a service profile, make sure to select one of the three options such as Dynamic, usNIC or VMQ connection policy for the vNIC. You can apply only any one of the vNIC connection policies on a service profile at any one time.

When you have selected VMQ policy on the vNIC for a service profile, you must also have the following settings in the service profile:

- Select SRIOV in the BIOS policy.
- Select Windows in the Adapter policy.

Configuring a VMQ vNIC connection policy involves the following:

- Creating a VMQ connection policy
- Creating a static vNIC in a service profile
- Applying the VMQ connection policy to the vNIC

Creating or Editing a VMQ Connection Policy

Step 1 In the **Actions** bar, type **Create VMQ Connection Policy** and press Enter.

Step 2 In the **VMC Connection Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.

Step 3 Enter the **Name** and optional **Description**.

The name is case sensitive.

Step 4 In **Number of VMQs** filed, enter a number between 1 to 128.

Step 5 In the Number of Interrupts field, enter a number between 1 to 128.

Step 6 Click **Create**.

What to do next

Associate the VMQ connection policy with a vNIC, vNIC template, or LAN connectivity policy.

LAN Connectivity Policy

LAN connectivity policies determine the connections and the network communication resources between the server and the LAN on the network. These policies use pools to assign MAC addresses to servers and to identify the vNICs that the servers use to communicate with the network.

Note These policies are included in service profiles and service profile templates, and can be used to configure multiple servers. So, using static IDs in connectivity policies is not recommended.

Privileges Required for LAN and SAN Connectivity Policies

Connectivity policies enable users without network or storage privileges to create and modify service profiles and service profile templates with network and storage connections. However, users must have the appropriate network and storage privileges to create connectivity policies.

Privileges Required to Create Connectivity Policies

Connectivity policies require the same privileges as other network and storage configurations. For example, you must have at least one of the following privileges to create connectivity policies:

- admin—Can create LAN and SAN connectivity policies
- ls-server—Can create LAN and SAN connectivity policies
- ls-network—Can create LAN connectivity policies
- ls-storage—Can create SAN connectivity policies

Privileges Required to Add Connectivity Policies to Service Profiles

After the connectivity policies have been created, a user with ls-compute privileges can include them in a service profile or service profile template. However, a user with only ls-compute privileges cannot create connectivity policies.

Creating or Editing a LAN Connectivity Policy

Step 1 In the **Actions** bar, type **Create LAN Connectivity Policy** and press Enter.

Step 2 In the **LAN Connectivity Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.

Step 3 Enter the **Name** and optional **Description**.

The name is case sensitive.

Step 4 In **vNICs**, create one or more vNICs and select these properties:

- **Basic**— Select the **Fabric Interconnect**, **Fabric Failover** option (Enabled or diasabled), **MTU**, and the **CDN Source** (vNIC Name or User Defined Name for the CDN source.
- **MAC Address**— Select the MAC address from a pool.
- **VLANs**— Specify or search for the VLAN name. You can click **Search** and specify a VLAN name to filter the results of VLANs displayed. You can search with a partial or full name of the VLAN that you want to select. For example, you can search for *VLAN100* to filter the list of VLANs with names containing VLAN100. You cannot set multiple native VLANs for a vNIC in a Service Profile. When you click on **Set as Native**, a **Configuration Error** results.
- **VLAN Groups**— Specify the VLAN group name that you have created to group the VLANs. You can add multiple VLAN groups and VLANs you want to associate with the policy.

  Note A VALN group is resolved only if the service profile referencing the template is associated. Once the service profile is associated, the VLAN group gets resolved based on the name on the Domain on the associated server.

- **Policies**— Select the policy that you want to assign to the vNIC.

You can manually create the vNIC, use a vNIC template, or create a redundancy template pair. For more information, see vNIC Templates, on page 31.

Step 5 In **iSCSI vNICs**, enter the **iSCSI vNIC** and enter the appropriate properties values.

Note If you create a LAN Connectivity Policy in the HTML5 GUI, any iSCSI vNIC parameters that you set on the iSCSI vNICS in the policy can only be updated in the HTML5 GUI.

Step 6 Click **Create**.

Creating a vNIC for a LAN Connectivity Policy

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.

If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Select the LAN connectivity policy for which you want to create a vNIC.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **vNICs** area, click **Create vNIC**.

Step 7 In the **Create vNIC** dialog box, enter the name, select a **MAC Address Assignment**, and check the **Use vNIC Template** check box if you want to use an existing vNIC template.

You can also create a MAC pool from this area.

Step 8 In the **Details** area, choose the **Fabric ID**, select the VLANs you want to use, and enter the **MTU**.

You can click **Search** and specify a VLAN name to filter the results of VLANs displayed. You can search with a partial or full name of the VLAN that you want to select. For example, you can search for *VLAN100* to filter the list of VLANs with names containing VLAN100.

Step 9 In the **Pin Group** area, choose a **Pin Group Name**.

Step 10 In the **Operational Parameters** area, choose a **Stats Threshold Policy**.

You can also create a threshold policy from this area.

Step 11 In the **Adapter Performance Profile** area, choose an **Adapter Policy**, **QoS Policy**, and a **Network Control Policy**.

You can also create an ethernet adapter policy, a QoS policy, and a network control policy from this area.

Step 12 Click **OK**.

Creating an iSCSI vNIC for a LAN Connectivity Policy

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.

If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Select the LAN connectivity policy for which you want to create an iSCSI vNIC.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **iSCSI vNICs** area, click **Create iSCSI vNIC**.

Step 7 In the **Create iSCSI vNIC** dialog box, enter the name, choose the **Overlay vNIC**, **iSCSI Adapter Policy**, and **VLAN** from the drop-down lists, and select a **MAC Address Assignment**.

You can also create an iSCSI adapter policy and a MAC pool from this dialog box.

You can click **Search** and specify a VLAN name to filter the results of VLANs displayed. You can search with a partial or full name of the VLAN that you want to select. For example, you can search for *VLAN100* to filter the list of VLANs with names containing VLAN100.

Step 8 Click **OK**.

Deleting a LAN Connectivity Policy

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.

If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Deleting a vNIC from a LAN Connectivity Policy

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.

If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Select the policy for which you want to delete the vNIC.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **vNICs** table, click the vNIC you want to delete.

Step 7 On the **vNICs** table icon bar, click **Delete**.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Deleting an iSCSI vNIC from a LAN Connectivity Policy

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.

If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Select the policy for which you want to delete the iSCSI vNIC.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **iSCSI vNICs** table, click the vNIC you want to delete.

Step 7 On the **iSCSI vNICs** table icon bar, click **Delete**.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

UniDirectional Link Detection (UDLD)

UniDirectional Link Detection (UDLD) is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. All connected devices must support UDLD for the protocol to successfully identify and disable unidirectional links. When UDLD detects a unidirectional link, it marks the link as unidirectional. Unidirectional links can cause a variety of problems, including spanning-tree topology loops.

UDLD works with the Layer 1 mechanisms to determine the physical status of a link. At Layer 1, autonegotiation takes care of physical signaling and fault detection. UDLD performs tasks that autonegotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected interfaces. When you enable both autonegotiation and UDLD, the Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols.

A unidirectional link occurs whenever traffic sent by a local device is received by its neighbor but traffic from the neighbor is not received by the local device.

Modes of Operation

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD can detect unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD can also detect unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and to misconnected interfaces on fiber-optic links.

In normal mode, UDLD detects a unidirectional link when fiber strands in a fiber-optic interface are misconnected and the Layer 1 mechanisms do not detect this misconnection. If the interfaces are connected correctly but the traffic is one way, UDLD does not detect the unidirectional link because the Layer 1 mechanism, which is supposed to detect this condition, does not do so. In case, the logical link is considered undetermined, and UDLD does not disable the interface. When UDLD is in normal mode, if one of the fiber strands in a pair is disconnected and autonegotiation is active, the link does not stay up because the Layer 1 mechanisms did not detect a physical problem with the link. In this case, UDLD does not take any action, and the logical link is considered undetermined.

UDLD aggressive mode is disabled by default. Configure UDLD aggressive mode only on point-to-point links between network devices that support UDLD aggressive mode. With UDLD aggressive mode enabled, when a port on a bidirectional link that has a UDLD neighbor relationship established stops receiving UDLD packets, UDLD tries to reestablish the connection with the neighbor and administratively shuts down the affected port. UDLD in aggressive mode can also detect a unidirectional link on a point-to-point link on which no failure between the two devices is allowed. It can also detect a unidirectional link when one of the following problems exists:

- On fiber-optic or twisted-pair links, one of the interfaces cannot send or receive traffic.
- On fiber-optic or twisted-pair links, one of the interfaces is down while the other is up.
- One of the fiber strands in the cable is disconnected.

Methods to Detect Unidirectional Links

UDLD operates by using two mechanisms:

- Neighbor database maintenance

  UDLD learns about other UDLD-capable neighbors by periodically sending a hello packet (also called an advertisement or probe) on every active interface to keep each device informed about its neighbors. When the switch receives a hello message, it caches the information until the age time (hold time or time-to-live) expires. If the switch receives a new hello message before an older cache entry ages, the switch replaces the older entry with the new one.

  UDLD clears all existing cache entries for the interfaces affected by the configuration change whenever an interface is disabled and UDLD is running, whenever UDLD is disabled on an interface, or whenever the switch is reset. UDLD sends at least one message to inform the neighbors to flush the part of their caches affected by the status change. The message is intended to keep the caches synchronized.

- Event-driven detection and echoing

  UDLD relies on echoing as its detection mechanism. Whenever a UDLD device learns about a new neighbor or receives a resynchronization request from an out-of-sync neighbor, it restarts the detection window on its side of the connection and sends echo messages in reply. Because this behavior is the same on all UDLD neighbors, the sender of the echoes expects to receive an echo in reply.

  If the detection window ends and no valid reply message is received, the link might shut down, depending on the UDLD mode. When UDLD is in normal mode, the link might be considered undetermined and might not be shut down. When UDLD is in aggressive mode, the link is considered unidirectional, and the interface is shut down.

If UDLD in normal mode is in the advertisement or in the detection phase and all the neighbor cache entries are aged out, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbors.

If you enable aggressive mode when all the neighbors of a port have aged out either in the advertisement or in the detection phase, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbor. UDLD shuts down the port if, after the fast train of messages, the link state is still undetermined.

UDLD Configuration Guidelines

The following guidelines and recommendations apply when you configure UDLD:

- A UDLD-capable interface also cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch.

- When configuring the mode (normal or aggressive), make sure that the same mode is configured on both sides of the link.
- UDLD should be enabled only on interfaces that are connected to UDLD capable devices. The following interface types are supported:
  - Ethernet uplink
  - FCoE uplink
  - Ethernet uplink port channel member
  - FCoE uplink port channel member

Creating or Editing a UDLD Link Policy

Step 1 In the **Actions** bar, type **Create UDLD Link Policy** and press Enter.

Step 2 In the **UDLD Link Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.

Step 3 Enter a **Name** and optional **Description**.

The policy name is case sensitive.

Step 4 Choose whether to enable **Admin State**.

Step 5 Choose the **Mode**. This can be one of the following:

- **Normal**—UDLD can detect unidirectional links due to misconnected interfaces on fibre-optic connections.
- **Aggressive**—UDLD can detect unidirectional links due to one-way traffic on fiber-optic and twisted-pair links, as well as misconnected interfaces on fiber-optic links.

Step 6 Click **Create**.

Creating or Editing a Link Profile

Step 1 In the **Actions** bar, type **Create Link Profile** and press Enter.

Step 2 In the **Link Profile** dialog box, click **Basic** and choose the **Domain Group Location** in which you want to create the link profile.

Step 3 Enter a **Name** and optional **Description**.

The policy name is case sensitive.

Step 4 In **UDLD Link**, select the UDLD link policy that you want to associate with the link profile.

Step 5 Click **Save**.

LACP Policy

Link Aggregation combines multiple network connections in parallel to increase throughput and to provide redundancy. Cisco UCS uses Link Aggregation Control Protocol (LACP) to group uplink ethernet ports into a port channel. You can create an LACP policy in Cisco UCS Central to manage how a particular port channel uses LACP. The following port channel types support LACP:

- Ethernet Port Channels
- FCoE Port Channels
- Appliance Port Channels

A default LACP policy is automatically assigned to all port channels that you create. You can edit this LACP policy or create a new one and assign it to a port channel. The LACP policy controls the following:

- **Suspend Individual**—When enabled, the ports in the port channel go into suspended mode if they do not receive LACP PDUs.
- **LACP Rate**—Modifies the duration of the LACP timeout. The normal timeout rate is 30 seconds, and the fast timeout rate is 1 second.

Creating or Editing a LACP Policy

Step 1 In the **Actions** bar, type **Create Link Aggression Control Protocol (LACP) Policy** and press Enter.

Step 2 In the **Link Aggression Control Protocol (LACP) Policy** dialog box, click **Domain Group Location** and select where you want to create the policy.

Step 3 Enter the **Name**.

The name is case sensitive.

Step 4 Choose whether to enable **Suspend Individual**.

Step 5 Choose the **LACP Rate** that you want to use.

Step 6 Click **Create**.

Flow Control Policy

Flow control policies determine whether the uplink Ethernet ports in a Cisco UCS domain send and receive IEEE 802.3x pause frames when the receive buffer for a port fills. These pause frames request that the transmitting port stop sending data for a few milliseconds until the buffer clears.

For flow control to work between a LAN port and an uplink Ethernet port, you must enable the corresponding receive and send flow control parameters for both ports. For Cisco UCS, the flow control policies configure these parameters.

When you enable the send function, the uplink Ethernet port sends a pause request to the network port if the incoming packet rate becomes too high. The pause remains in effect for a few milliseconds before traffic is

reset to normal levels. If you enable the receive function, the uplink Ethernet port honors all pause requests from the network port. All traffic is halted on that uplink port until the network port cancels the pause request.

Because you assign the flow control policy to the port, changes to the policy have an immediate effect on how the port reacts to a pause frame or a full receive buffer.

Creating or Editing a Flow Control Policy

Note If you have selected global port configuration for **Policy Resolution Control** in Cisco UCS Manager, then all local flow control policies will be deleted, and global flow control policies belonging to the same domain group in Cisco UCS Central will be created in Cisco UCS Manager.

Step 1 Click **Domain Group Location** and select the domain group for which you want to create the policy.

Step 2 Enter a **Name**.

The policy name is case sensitive.

Step 3 Select the **Priority**. This can be one of the following:

- **On**—PPP is enabled on this fabric interconnect.
- **Auto**—Cisco UCS and the network negotiate whether PPP is used on this fabric interconnect.

Step 4 Choose whether to enable or disable **Receive**. This can be one of the following:

- **Enabled**—Pause requests are honored and all traffic is halted on that uplink port until the network cancels the pause request.
- **Disabled**—Pause requests from the network are ignored and traffic flow continues as normal.

Step 5 Choose whether to enable or disable **Send**. This can be one of the following:

- **Enabled**—Cisco UCS sends a pause request to the network if the incoming packet rate becomes too high. The pause remains in effect for a few milliseconds before traffic is reset to normal levels.
- **Disabled**—Traffic on the port flows normally regardless of the packet load.

Step 6 Click **Save**.

Quality of Service Policy

A quality of service (QoS) policy assigns a system class to the outgoing traffic for a vNIC or vHBA. This system class determines the quality of service for that traffic. For certain adapters, you can also specify additional controls on the outgoing traffic, such as burst and rate.

You must include a QoS policy in a vNIC policy or vHBA policy and then include that policy in a service profile to configure the vNIC or vHBA.

Creating or Editing a Quality of Service Policy

Step 1 In the **Actions** bar, type **Create Quality of Service (QoS) Policy** and press Enter.

Step 2 In the **Create Quality of Service (QoS) Policy** dialog box, click **Organization** and select the location in which you want to create the policy.

Step 3 Enter the **Name** and optional **Description**.

The name is case sensitive.

Step 4 Select an **Egress Priority**.

Step 5 Choose whether to enable **Host Control Class of Service (CoS)**.

Step 6 Enter an **Egress Burst Size**, and select the egress average traffic rate.

Step 7 Click **Create**.

Deleting a QoS Policy

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.

If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **QoS Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

QoS System Classes

Cisco UCS uses Data Center Ethernet (DCE) to handle all traffic inside a Cisco UCS domain. This industry standard enhancement to Ethernet divides the bandwidth of the Ethernet pipe into eight virtual lanes. Two virtual lanes are reserved for internal system and management traffic. You can configure quality of service (QoS) for the other six virtual lanes. System classes determine how the DCE bandwidth in these six virtual lanes is allocated across the entire Cisco UCS domain.

Each system class reserves a specific segment of the bandwidth for a specific type of traffic, which provides a level of traffic management, even in an oversubscribed system. For example, you can configure the Fibre Channel Priority system class to determine the percentage of DCE bandwidth allocated to FCoE traffic.

Creating QoS System Class Settings

Step 1 In the **Actions** bar, type **Create QoS System Class Settings** and press Enter.

Step 2 In the **Create QoS System Class Settings** dialog box, choose the **Organization** in which you want to create the policy.

Step 3 Enter the **Name** and optional **Description**.

The name is case sensitive.

Step 4 Click **Create**.

To understand the impact of the policy, click **Evaluate**.

Step 5 In **System Classes**, define the following:

Table 1: System Classes

System Class	Description
Platinum Gold Silver Bronze	A configurable set of system classes that you can include in the QoS policy for a service profile. Each system class manages one lane of traffic. All properties of these system classes are available for you to assign custom settings and policies.
Best Effort	A system class that sets the quality of service for the lane reserved for basic Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a drop policy that allows it to drop data packets if required. You cannot disable this system class.
Fibre Channel	A system class that sets the quality of service for the lane reserved for Fibre Channel over Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a no-drop policy that ensures it never drops data packets. You cannot disable this system class. **Note** FCoE traffic has a reserved QoS system class that should not be used by any other type of traffic. If any other type of traffic has a CoS value that is used by FCoE, the value is remarked to 0.

ID Range Access Control Policy

Use the ID range access control policy to limit what pools can be utilized in a specific domain group. When you apply the access control policy to a pool, only the domain groups selected can access those pools.

Creating or Editing an ID Range Access Control Policy

Step 1 In the **Actions** bar, type **Create ID Range Access Control Policy** and press Enter.

Step 2 In the **ID Range Access Control Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.

Step 3 Enter the **Name** and optional **Description**.

The name is case sensitive.

Step 4 In **Domain Groups**, click **Add** to select the **Permitted Domain Groups** associated with this policy.

Step 5 Click **Create**.

Multicast Policy

Multicast Policy is used to configure Internet Group Management Protocol (IGMP) snooping and IGMP querier. IGMP snooping dynamically determines hosts in a VLAN that should be included in particular multicast transmissions. You can create, modify, and delete a Multicast Policy that can be associated with one or more VLANs. When a Multicast Policy is modified, all VLANs associated with that Multicast Policy are reprocessed to apply the changes. By default, IGMP snooping is enabled and IGMP querier is disabled. For private VLANs, you can set a Multicast Policy for primary VLANs but not for their associated isolated VLANs. This is due to a Cisco NX-OS forwarding implementation.

The **Multicast Policy** view displays the IGMP Snooping State, IGMP Snooping Querier State, and the FI-A and FI-B Querier IPv4 Addresses for the specific policy.

Creating a Multicast Policy

Step 1 In the **Actions** bar, type **Multicast Policy** and press Enter.

Step 2 In the **Multicast Policy** dialog box, choose the **Domain Group Location** in which you want to create the policy.

Step 3 Enter a **Name** for the Multicast Policy.

The name is case sensitive.

Step 4 Select the **IGMP Snooping State** that determines if IGMP snooping examines IGMP protocol messages within a VLAN to discover which interfaces are connected to hosts or other devices interested in receiving multicast traffic:

- If **Enabled**, IGMP snooping is used for VLANs associated with this policy. IGMP snooping is **Enabled** by default.
- If **Disabled**, IGMP snooping is not used for associated VLANs.

Step 5 Select the **IGMP Snooping Querier State** that determines if the IGMP snooping querier sends out periodic IGMP queries that trigger IGMP report messages from hosts that want to receive IP multicast traffic. This can be one of the following:

- If **Enabled** periodic IGMP queries are sent out.
- If **Disabled** no IGMP queries are sent out.

IGMP querier is **Disabled** by default.

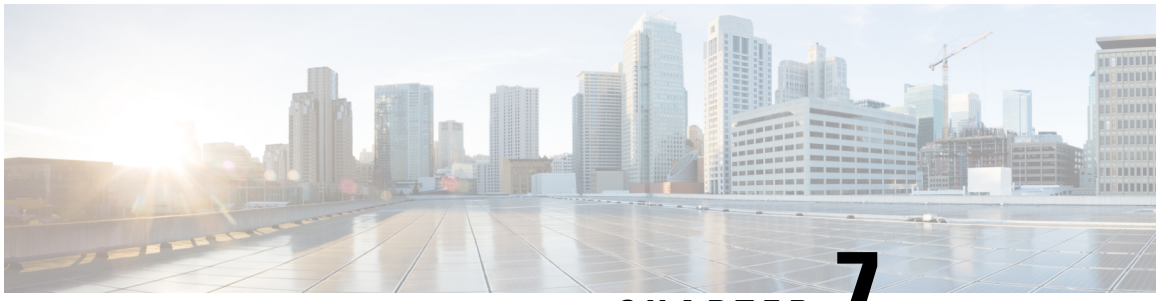
Step 6 Specify the IPv4 addresses for the IGMP snooping querier interfaces on the designated fabric interconnects in the **FI A Querier IPv4 Addresses** field. These fields are displayed only if the **IGMP Snooping Querier State** is **Enabled**.

Step 7 Click **Create**.

- Cisco UCS Central supports Multicast Policy for Cisco UCS Manager release 3.1(3) and later.
- You cannot create a create policy with the same name on Cisco UCS Manager. A global service profile displays a conflict when the multicast policy already exists in Cisco UCS Manager.

Step 8 On the **Multicast policy** page, click the **Delete** icon.

A dialog box prompting you to confirm the deletion of the policy appears.



CHAPTER 7

Traffic Monitoring

Traffic Monitoring

Traffic monitoring copies traffic, from one or more source ports, and sends it to a dedicated destination port for analysis by a network analyzer. This feature is also known as Switched Port Analyzer (SPAN).

Important For FC port channels on Cisco UCS 6200 Fabric Interconnects, you can monitor only egress traffic.

For FC port channels on Cisco UCS 6300 Fabric Interconnects, you can monitor only ingress traffic.

Traffic Monitoring Session Types

When you create a traffic monitoring session, you can choose either an Ethernet or Fibre Channel destination port to receive the traffic. The type of destination port determines the type of session, which in turn determines the types of available traffic sources. For an Ethernet traffic monitoring session, the destination port must be an unconfigured physical port. For a Fibre Channel traffic monitoring session, the destination port must be a Fibre Channel uplink port.

Note For Cisco UCS 6300 Fabric Interconnects, the destination port must also be an unconfigured physical Ethernet port. For Cisco UCS 6332 and Cisco UCS 6332-16UP Fabric Interconnects, you cannot choose Fibre Channel destination ports, but can use unconfigured ethernet ports as a destination for FC traffic monitoring sessions.

Traffic Monitoring Across Ethernet

An Ethernet traffic monitoring session can monitor any of the following traffic source and destination ports:

Source Ports	Destination Ports
• Uplink Ethernet port • Ethernet port channel • VLAN • Service profile vNIC • Service profile vHBA • FCoE port • Port channels • Unified uplink port • VSAN • Unified storage port • Appliance storage port	• Unconfigured Ethernet Port

Traffic Monitoring for UCS 6300 Interconnects

- Cisco UCS 6300 Fabric Interconnect supports port-based mirroring.
- Cisco UCS 6300 Fabric Interconnect supports VLAN SPAN only in the receive (rx) direction.
- Ethernet SPAN is port based on the Cisco UCS 6300 Fabric Interconnect.

Traffic Monitoring for UCS 6200 Interconnects

- Cisco UCS 6200 and 6324 supports monitoring traffic in the transmit (tx) direction for up to two sources per Fabric Interconnect.
- Cisco UCS 6200 SPAN traffic is rate-limited by the SPAN destination port speed. This can be either 1 Gbps or 10 Gbps.

Traffic Monitoring Across Fibre Channel

You can monitor Fibre Channel traffic using either a Fibre Channel traffic analyzer or an Ethernet traffic analyzer. When Fibre Channel traffic is monitored with an Ethernet traffic monitoring session, the destination traffic is FCoE. The Cisco UCS 6300 Fabric Interconnect supports FC SPAN only on the ingress side. You cannot configure a Fibre Channel port on a Cisco Cisco UCS 6248 Fabric Interconnect as a source port.

A Fibre Channel traffic monitoring session can monitor any of the following traffic source and destination ports:

Source Ports	Destination Ports
• FC Port • FC Port Channel • Uplink Fibre Channel port • SAN port channel • VSAN • Service profile vHBA • Fibre Channel storage port	• Fibre Channel uplink port • Ethernet Port (only for Cisco UCS 6300 Fabric Interconnects)

Guidelines and Recommendations for Traffic Monitoring

When configuring or activating traffic monitoring, consider the following guidelines:

Traffic Monitoring Sessions

A traffic monitoring session is disabled by default when created. To begin monitoring traffic, you must activate the session.

- Create a unique traffic monitoring session on any fabric interconnect within the Cisco UCS pod.
- Create each monitoring session with a unique name and unique source.
- Add all vNICs from the service profile of a server to monitor traffic from a server.
- Locate all traffic sources within the same switch as the destination port.
- Do not add the same source in multiple traffic monitoring sessions.
- Do not configure a port as a destination port and a source port.
- Do not configure a member port, of a port channel, individually as a source. If you configure the port channel as a source, all member ports are source ports.

Maximum Supported Active Traffic Monitoring Sessions

You can only monitor up to four traffic directions for each Cisco UCS 6300 Fabric Interconnect. You can create and store up to 16 traffic monitoring sessions, but only four can be active at the same time for each Fabric Interconnect. The receive and transmit directions each count separately as one active session, while the bidirectional is counted as two active sessions. For example:

- Four active sessions—If each session is configured to monitor traffic in only one direction.
- Two active sessions—If each session is configured to monitor traffic bidirectionally.
- Three active sessions—If one session is unidirectional and the second session is bidirectional.

Note Traffic monitoring can impose a significant load on your system resources. To minimize the load, select sources that carry as little unwanted traffic as possible and disable traffic monitoring when it is not needed.

vNIC

Because a traffic monitoring destination is a single physical port, a traffic monitoring session can monitor only a single fabric. To monitor uninterrupted vNIC traffic across a fabric failover, create two sessions, one per fabric, and connect two analyzers. Add the vNIC as the traffic source using the exact same name for both sessions. If you change the port profile of a virtual machine, you must reconfigure the monitoring session. All associated vNICs used as source ports are removed from monitoring.

vHBA

You can use a vHBA as a source for either an Ethernet or Fibre Channel monitoring session, but it cannot be a source for both simultaneously. When a VHBA is set as the SPAN source, the SPAN destination only receives VN-tagged frames. It does not receive direct FC frames.

SPAN Ports Support Matrix

Note For Cisco UCS 6200 and 6324 FIs, you can only set the source mode to transmit for two sources per Cisco UCS domain.

Ethernet Span Port Sources

Source Ethernet SPAN ports are supported in the following configurations:

Source Type	Source Mode		
	on Cisco UCS 6200 FI	on Cisco UCS 6324 FI	on Cisco UCS 6332 FI
Ethernet Uplink	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both
Ethernet Port-Channel	Receive	Receive	Receive, Transmit, Both
FCoE Uplink	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both
FCoE Port-Channel	Receive	Receive	Receive, Transmit, Both
Appliance Port	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both
FCoE Storage	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both
Unified Ports	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both
VLAN	Receive	Receive	Receive
Static vNIC	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both
vHBA	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both

Ethernet Span Port Destinations

Destination Ethernet SPAN ports are supported in the following configurations:

Session Type	Admin Speed		
	on Cisco UCS 6200 FI	on Cisco UCS 6324 FI	on Cisco UCS 6332 FI
Ethernet SPAN Ports	Ethernet Unconfigured at 1 Gbps, 10 Gbps	Ethernet Unconfigured at 1 Gbps, 10 Gbps	Ethernet Unconfigured at 1Gbps, 10 Gbps, 40 Gbps

FC Span Port Sources

Source FC SPAN ports are supported in the following configurations:

Source Type	Source Mode		
	on Cisco UCS 6200 FI	on Cisco UCS 6324 FI	on Cisco UCS 6332 FI
FC Uplink	Transmit	Not Supported	Receive
FC Port-Channel	Transmit	Not Supported	Receive
FC Storage	Transmit	Not Supported	Receive
VSAN	Not Supported	Not Supported	Receive
vHBA	Receive, Transmit, Both	Not Supported	Receive, Transmit, Both

FC Span Port Destinations

Destination FC SPAN ports are supported in the following configurations:

Session Type	Admin Speed		
	on Cisco UCS 6200 FI	on Cisco UCS 6324 FI	on Cisco UCS 6332 FI
FC SPAN Ports	FC Uplink at 1 Gbps, 2 Gbps, 4 Gbps, 8 Gbps, Auto	Not Supported	FC Unconfigured at 1 Gbps, 2 Gbps, 4 Gbps, 8 Gbps, 16 Gbps, Auto
FC SPAN Ports	FC Monitor at 1 Gbps, 2 Gbps, 4 Gbps, 8 Gbps, Auto	Not Supported	FC Monitor at 1 Gbps, 2 Gbps, 4 Gbps, 8 Gbps, 16 Gbps, Auto

Creating a Traffic Monitoring Session

You can choose multiple sources from more than one source type to be monitored by a traffic monitoring session. The available sources depend on the existing components configured.

Before you begin

Before creating a traffic monitoring session in Cisco UCS Central, ensure that port configuration is set to **Global** on the **Policy Resolution Control** page for the Cisco UCS.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 On the **Fabric Interconnects** page, select the fabric interconnect to which you want to add a traffic monitoring session.

Step 3 On the **Fabric Interconnect** page, click the Tools icon and choose **Create Traffic Monitoring**.

Step 4 In the **Traffic Monitoring** dialog box, on the **Basic** tab, do the following:

a) Choose whether to create an **Ethernet** or **FC** traffic monitoring session.

You cannot modify the type after creation.

b) Enter the **Name** for your traffic monitoring session.

You cannot modify the name after creation.

c) Choose the **Admin State**:

- **Disabled**—Creates the session, but does not activate traffic monitoring.
- **Enabled**—Immediately activates the traffic monitoring session upon creation.

d) Select the **Destination Port** that you want to monitor.

Step 5 On the **Sources** tab, add the sources that you want to monitor.

For Ethernet traffic monitoring, you can monitor ports, port channels, VLANs, vNICs or vHBAs.

For FC traffic monitoring, you can monitor ports, port channels, VSANs, or vHBAs.

Step 6 Click **Create**.

Editing an Existing Traffic Monitoring Session

Modify the **Admin State** to activate or deactivate the traffic monitoring session.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 On the **Fabric Interconnects** page, select the fabric interconnect with the traffic monitoring session that you want to modify.

Step 3 On the **Fabric Interconnect** page, click the **Traffic Monitoring** tab.

Step 4 Select the traffic monitoring session that you want to modify, and click the **Edit** icon.

Note You cannot modify the name or the type of traffic monitoring.

Step 5 On the **Basic** tab, in Admin State, choose one of the following:

- **Disabled**—Deactivates traffic monitoring.
- **Enabled**—Activates the traffic monitoring session.

Step 6 Modify the **Destination Port**, if necessary.

Step 7 On the **Sources** tab, make any necessary changes to the sources that you want to monitor.

Step 8 Click **Save**.

Activating or Deactivating a Traffic Monitoring Session

Existing traffic monitoring sessions can be activated or deactivated.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.
Step 2 Choose the fabric interconnect where you want to update traffic monitoring.
Step 3 On the fabric interconnect page, click **Traffic Monitoring**.
Step 4 Click on the traffic monitoring session that you want to edit.
Step 5 Click the **Edit** icon.
Step 6 Modify the Admin State:

- **Enabled**—Immediately activates the traffic monitoring session.
- **Disabled**—Deactivates the active traffic monitoring session.

Step 7 Click **Save**.

Deleting a Traffic Monitoring Session

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.
Step 2 Choose the fabric interconnect where you want to update traffic monitoring.
Step 3 On the fabric interconnect page, click **Traffic Monitoring**.
Step 4 Click on the traffic monitoring session that you want to delete.
Step 5 Click the **Delete** icon.