Cisco UCS Manager Network Management Guide, Release 6.0

First Published: 2025-09-02

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

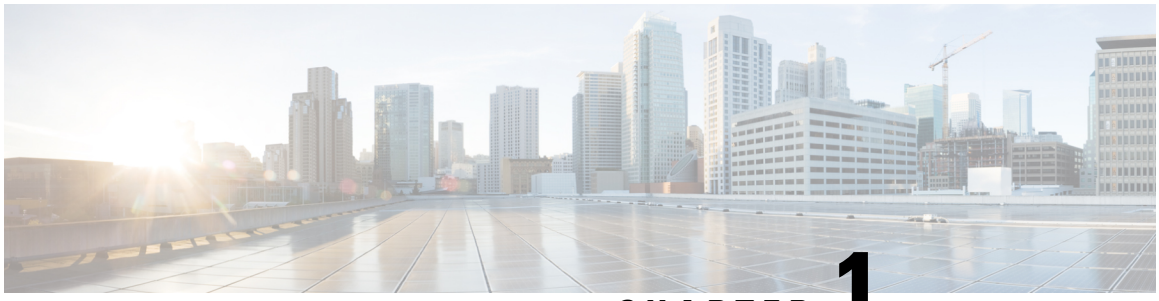
For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmapdoc 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.

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

New and Changed Information

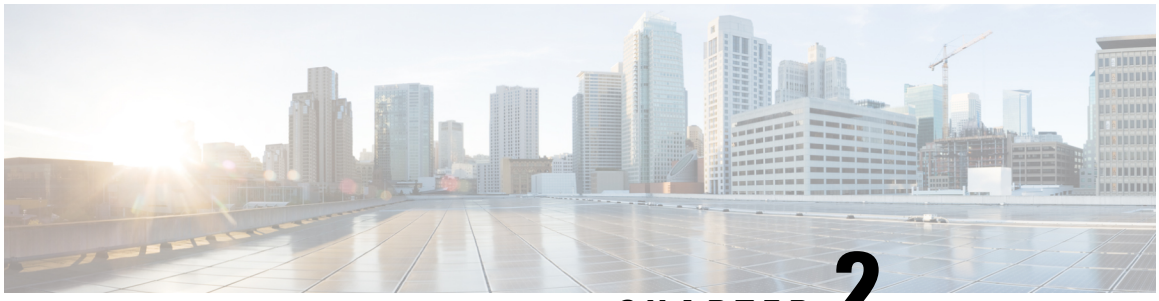
New and Changed Information

This section provides information on new features and changed behavior in Cisco UCS Manager, Release 6.0.

Table 1: New Features and Changed Behavior in Cisco UCS Manager, Release 6.0(1b)

Feature	Description	Where Documented
Support for Cisco UCS 6600 Series Fabric Interconnect	Cisco UCS Manager supports Cisco UCS 6664 Fabric Interconnect	• Fabric Interconnect Port Types, on page 15 • Default Open Ports, on page 19 • TCP and UDP Ports, on page 20 • Configuring Port Modes for Cisco UCS 6600 Series Fabric Interconnect, on page 23 • VLAN Port Count Optimization, on page 111 • Quality of Service, on page 127 • Configuring Port Modes for Cisco UCS 6600 Series Fabric Interconnect, on page 23

Feature	Description	Where Documented
Support for Cisco UCS C-Series rack servers in Cisco UCS X-Series Direct	Cisco UCS Manager now supports Cisco UCS C-Series rack servers in Cisco UCS Fabric Interconnect 9108 100G (Cisco UCS X-Series Direct), enabling you to manage both UCS X-Series compute nodes (M6, M7, and M8) and C-Series (M7 and M8) rack servers together in the same domain.	Port Breakout Functionality on Cisco UCS Fabric Interconnects 9108 100G (Cisco UCS X-Series Direct), on page 24
MACsec support for Cisco UCS 6664 Fabric Interconnect and Cisco UCS X-Series Direct	Cisco UCS Manager 6.0(1b) adds MACsec support for the Cisco UCS 6664 Fabric Interconnect and Cisco UCS Fabric Interconnect 9108 100G (Cisco UCS X-Series Direct).	Guidelines and Limitations for MACsec, on page 224
A warning for Native VLAN changes on vNICs	Cisco UCS Manager now supports an enhanced Native VLAN Configuration on vNICs, providing a warning message for Native VLAN changes that highlights the required port flap and brief connectivity impact (approximately 20–40 seconds).	About the Native VLAN, on page 94
Deprecated support for Cisco UCS 6300 series Fabric Interconnect	Cisco UCS Manager support for Cisco UCS 6300 Series Fabric Interconnect is deprecated.	-



CHAPTER 2

Overview

Overview

This guide includes the following information:

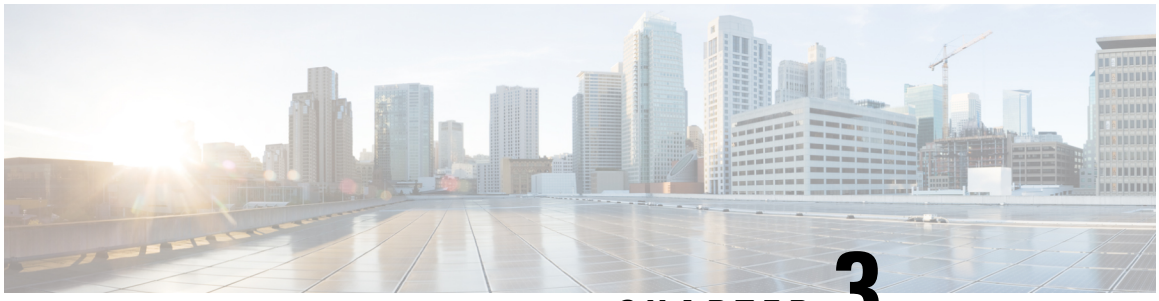
- Configure/Enable Server Ports; Configure/Enable Uplink Ports; Configure/Enable FC Ports.
- Create LAN Pin Groups
- Create VLANs and VLAN groups
- Create Server Links
- Configure QoS System Class
- Configure Global Policies
- Monitor Network Health
- Traffic Monitoring

Cisco UCS Manager User Documentation

Cisco UCS Manager offers you a new set of smaller, use-case based documentation described in the following table:

Guide	Description
Cisco UCS Manager Getting Started Guide	Discusses Cisco UCS architecture and Day 0 operations, including Cisco UCS Manager initial configuration, and configuration best practices.

Guide	Description
Cisco UCS Manager Administration Guide	Discusses password management, role-based access configuration, remote authentication, communication services, CIMC session management, organizations, backup and restore, scheduling options, BIOS tokens and deferred deployments.
Cisco UCS Manager Infrastructure Management Guide	Discusses physical and virtual infrastructure components used and managed by Cisco UCS Manager.
Cisco UCS Manager Firmware Management Guide	Discusses downloading and managing firmware, upgrading through Auto Install, upgrading through service profiles, directly upgrading at endpoints using firmware auto sync, managing the capability catalog, deployment scenarios, and troubleshooting.
Cisco UCS Manager Server Management Guide	Discusses the new licenses, registering Cisco UCS domains with Cisco UCS Central, power capping, server boot, server profiles and server-related policies.
Cisco UCS Manager Storage Management Guide	Discusses all aspects of storage management such as SAN and VSAN in Cisco UCS Manager.
Cisco UCS Manager Network Management Guide	Discusses all aspects of network management such as LAN and VLAN connectivity in Cisco UCS Manager.
Cisco UCS Manager System Monitoring Guide	Discusses all aspects of system and health monitoring including system statistics in Cisco UCS Manager.
Cisco UCS S3260 Server Integration with Cisco UCS Manager	Discusses all aspects of management of UCS S-Series servers that are managed through Cisco UCS Manager.



CHAPTER 3

LAN Connectivity

Fabric Interconnect Overview

The fabric interconnect is the core component of Cisco UCS. The Cisco UCS Fabric Interconnects provide uplink access to LAN, SAN, and out-of-band management segment. Cisco UCS infrastructure management is through the embedded management software, Cisco UCS Manager, for both hardware and software management. The Cisco UCS Fabric Interconnects are Top-of-Rack devices, and provide unified access to the Cisco UCS domain.

The Cisco UCS FIs provide network connectivity and management for the connected servers. The Cisco UCS Fabric Interconnects run the Cisco UCS Manager control software and consist of expansion modules for the Cisco UCS Manager software.

For more information about Cisco UCS Fabric Interconnects, see the *Cisco UCS Manager Getting Started Guide*.

IOMs and Fabric Interconnects Connectivity

Each chassis is equipped with two IOMs: IOM 1 should be connected to Fabric Interconnect A. IOM 2 should be connected to Fabric Interconnect B. This configuration provides redundant paths, ensuring uninterrupted operation of the Cisco UCS system even in the event of a failure in one of the Fabric Interconnects or IOMs. Additionally, this configuration enables traffic load distribution across both Fabric Interconnects, enhancing load balancing and increasing throughput. As a result, the Cisco UCS system achieves high availability, reliability, and optimal performance, making it ideal for data center environments.

Uplink Connectivity

Use fabric interconnect ports configured as uplink ports to connect to uplink upstream network switches. Connect these uplink ports to upstream switch ports as individual links, or as links configured as port channels. Port channel configurations provide bandwidth aggregation as well as link redundancy.

You can achieve northbound connectivity from the fabric interconnect through a standard uplink, a port channel, or a virtual port channel configuration. The port channel name and ID configured on fabric interconnect should match the name and ID configuration on the upstream Ethernet switch.

It is also possible to configure a port channel as a vPC, where port channel uplink ports from a fabric interconnect are connected to different upstream switches. After all uplink ports are configured, create a port channel for these ports.

Downlink Connectivity

Beginning with release 4.3(2a), Cisco UCS Manager supports Cisco UCS X9508 server chassis with Cisco UCS X-Series servers. Cisco UCS X-Series servers support Intelligent Fabric Modules (IFM), which function similarly to the Input/Output Module (IOM) in Cisco UCS B-Series servers. This guide uses the term IOM to refer both IOM and IFM.

Each fabric interconnect is connected to IOMs in the UCS chassis, which provides connectivity to each blade server. Internal connectivity from blade servers to IOMs is transparently provided by Cisco UCS Manager using 10BASE-KR Ethernet standard for backplane implementations, and no additional configuration is required. You must configure the connectivity between the fabric interconnect server ports and IOMs. Each IOM, when connected with the fabric interconnect server port, behaves as a line card to fabric interconnect, hence IOMs should never be cross-connected to the fabric interconnect. Each IOM is connected directly to a single fabric interconnect.

The Fabric Extender (also referred to as the IOM, or FEX) logically extends the fabric interconnects to the blade server. The best analogy is to think of it as a remote line card that's embedded in the blade server chassis, allowing connectivity to the external world. IOM settings are pushed via Cisco UCS Manager and are not managed directly. The primary functions of this module are to facilitate blade server I/O connectivity (internal and external), multiplex all I/O traffic up to the fabric interconnects, and help monitor and manage the Cisco UCS infrastructure.

Configure Fabric interconnect ports that should be connected to downlink IOM cards as server ports. Make sure there is physical connectivity between the fabric interconnect and IOMs. You must also configure the IOM ports and the global chassis discovery policy.

Note For UCS 2200 I/O modules, you can also select the Port Channel option and all I/O module-connected server ports will be automatically added to a port channel.

Configuring the Fabric Interconnects

Fabric Interconnect Information Policy

Fabric Interconnect Information Policy enables you to display the uplink switches that are connected to fabric interconnect.

Important You must enable the information policy on the fabric interconnect to view the details of SAN, LAN, and LLDP neighbours of the fabric interconnect.

Configuring the Information Policy on the Fabric Interconnect

Procedure

Step 1 Navigate to **Equipment** > **Policies** > **Global Policies**

Step 2 In the **Info Policy** group, choose one of the following:

- **Disabled**: Click to disable the information policy on the fabric interconnect. This is the default option.
- **Enabled**: Click to enable the information policy on the fabric interconnect.

Step 3 Click **Save Changes**.

Installing Secure FPGA

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click **Install Secure FPGA**.

Step 5 In the dialog box, click **OK**.

Warning
This procedure will upgrade the FPGA and automatically reboot the system after completion of the FPGA upgrade. Kindly refrain from reloading or power-cycling the system during the upgrade, as the manual reboot will result in failure of Fabric Interconnect.

Cisco UCS Manager restarts the fabric interconnect, logs you out, and disconnects Cisco UCS Manager GUI on choosing **Yes** in the warning message.

Viewing the LAN Neighbors of a Fabric Interconnect

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.
Step 2 In the **Equipment** tab, expand **Equipment** > **Fabric Interconnects**.
Step 3 Click the fabric interconnect for which you want to view the LAN neighbors.
Step 4 In the **Work** pane, click the **Neighbors** tab.
Step 5 Click the **LAN** subtab.

This subtab lists all the LAN neighbors of the specified Fabric Interconnect.

Viewing the SAN Neighbors of a Fabric Interconnect

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.
Step 2 In the **Equipment** tab, expand **Equipment** > **Fabric Interconnects**.
Step 3 Click the fabric interconnect for which you want to view the SAN neighbors.
Step 4 In the **Work** pane, click the **Neighbors** tab.
Step 5 Click the **SAN** subtab.

This subtab lists all the SAN neighbors of the specified Fabric Interconnect.

Viewing the LLDP Neighbors of a Fabric Interconnect

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.
Step 2 Expand **Equipment** > **Fabric Interconnects**.
Step 3 Click the fabric interconnect for which you want to view the LLDP neighbors.
Step 4 In the **Work** pane, click the **Neighbors** tab.
Step 5 Click the **LLDP** subtab.

This subtab lists all the LLDP neighbors of the specified Fabric Interconnect.

Fabric Evacuation

Cisco UCS Manager introduces fabric evacuation, which is the ability to evacuate all traffic that flows through a fabric interconnect from all servers attached to it through an IOM or FEX while upgrading a system. Fabric evacuation is not supported on direct-attached rack servers.

Upgrading the secondary fabric interconnect in a system disrupts active traffic on the fabric interconnect. This traffic fails over to the primary fabric interconnect. You can use fabric evacuation during the upgrade process as follows:

1. Stop all the traffic that is active through a fabric interconnect.
2. For vNICs configured with failover, verify that the traffic has failed over by using Cisco UCS Manager, or tools such as vCenter.
3. Upgrade the secondary fabric interconnect.
4. Restart all the stopped traffic flows.
5. Change the cluster lead to the secondary fabric interconnect.
6. Repeat steps 1 to 4 and upgrade the primary fabric interconnect.

Note

- Fabric interconnect traffic evacuation is supported only in a cluster configuration.
- You can evacuate traffic only from the subordinate fabric interconnect.
- The IOM or FEX backplane ports of the fabric interconnect on which evacuation is configured will go down, and their state will appear as **Admin down**. During the manual upgrade process, to move these backplane ports back to the Up state and resume traffic flow, you must explicitly configure **Admin Evac Mode** as **Off**.
- Starting with Cisco UCS Manager Release 3.1(3), you can use fabric evacuation during Auto Install.
- If you use fabric evacuation outside of the upgrade process, you must re-acknowledge the FEX to get the VIFs back to the online state.

Configuring Fabric Evacuation

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click **Configure Evacuation**.
The Configure Evacuation dialog box appears.

Step 5 To configure fabric evacuation on the specified Fabric Interconnect, click one of the following radio buttons in the **Admin Evac Mode** field:

- **On**—Stops all the traffic that is active through the specified Fabric Interconnect.
- **Off**—Restarts traffic through the specified Fabric Interconnect.

Step 6 (Optional) To evacuate a Fabric Interconnect irrespective of its current evacuation state, check the **Force** check box.

Step 7 Click **Apply**.
A warning dialog box appears.

```
Enabling fabric evacuation will stop all traffic through this Fabric Interconnect from
servers attached through IOM/FEX.
The traffic will fail over to the Primary Fabric Interconnect for fail over vnics.
Are you sure you want to continue?
```

Step 8 Click **OK** to confirm fabric evacuation and continue.

Displaying the Status of Fabric Evacuation on a Fabric Interconnect

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 The Status area displays

Fabric Interconnect Switching Modes

The Cisco UCS Fabric Interconnects operate in two main switching modes: Ethernet or Fibre Channel. These modes are independent of each other. They determine how the fabric interconnect behaves as a device between the server and network/server and storage device.

Ethernet Switching Mode

The Ethernet switching mode determines how the fabric interconnect behaves as a switching device between the servers and the network. The fabric interconnect operates in either of the following Ethernet switching modes:

End-Host Mode

End-host mode allows the fabric interconnect to act as an end host to the network, representing all servers (hosts) connected to it through vNICs. This behavior is achieved by pinning (either dynamically pinning or hard pinning) vNICs to uplink ports, which provides redundancy to the network, and makes the uplink ports appear as server ports to the rest of the fabric.

In end-host mode, the fabric interconnect does not run the Spanning Tree Protocol (STP), but it avoids loops by denying uplink ports from forwarding traffic to each other and by denying egress server traffic on more than one uplink port at a time. End-host mode is the default Ethernet switching mode and should be used if either of the following is used upstream:

- Layer 2 switching for Layer 2 aggregation
- Virtual Switching System (VSS) aggregation layer

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

Switch Mode

Switch mode is the traditional Ethernet switching mode. The fabric interconnect runs STP to avoid loops, and broadcast and multicast packets are handled in the traditional way. Use the switch mode only if the fabric interconnect is directly connected to a router, or if either of the following is used upstream:

- Layer 3 aggregation
- VLAN in a box

Note For both Ethernet switching modes, even when vNICs are hard-pinned to uplink ports, all server-to-server unicast traffic in the server array is sent only through the fabric interconnect and is never sent through uplink ports. Server-to-server multicast and broadcast traffic is sent through all uplink ports in the same VLAN.

Cisco UCS Fabric Interconnect in Switch Mode with Cisco MDS 9000 Family Fibre Channel Switching Modules

While creating a port channel between a Cisco MDS 9000 family FC switching module and a Cisco UCS Fabric Interconnect in switch mode, use the following order:

1. Create the port channel on the MDS side.
2. Add the port channel member ports.
3. Create the port channel on the Fabric Interconnect side.
4. Add the port channel member ports.

If you create the port channel on the Fabric Interconnect side first, the ports will go into a suspended state.

When the Cisco UCS Fabric Interconnect is in switch mode, the port channel mode can only be in **ON** mode and not **Active**. However, to get the peer wwn information for the Fabric Interconnect, the port channel must be in **Active** mode.

Configuring Ethernet Switching Mode

Important When you change the Ethernet switching mode, Cisco UCS Manager logs you out and restarts the fabric interconnect. For a cluster configuration, Cisco UCS Manager restarts both fabric interconnects. The subordinate fabric interconnect reboots first as a result of the change in switching mode. The primary fabric interconnect reboots only after you acknowledge it in **Pending Activities**. The primary fabric interconnect can take several minutes to complete the change in Ethernet switching mode and become system ready. The existing configuration is retained.

While the fabric interconnects are rebooting, all blade servers lose LAN and SAN connectivity, causing a complete outage of all services on the blades. This might cause the operating system to fail.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click one of the following links:

- **Set Ethernet Switching Mode**
- **Set Ethernet End-Host Mode**

The link for the current mode is dimmed.

Step 5 In the dialog box, click **Yes**.

Cisco UCS Manager restarts the fabric interconnect, logs you out, and disconnects Cisco UCS Manager GUI.

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 is synonymous with N Port Virtualization (NPV) mode. This mode is the default Fibre Channel Switching 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 pinning or hard-pinning) 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 preventing uplink ports from receiving traffic from one another.

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 not the default 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). In Fibre Channel switch mode, SAN pin groups are irrelevant. Any existing SAN pin groups are ignored.

Configuring Fibre Channel Switching Mode

Important When you change the Fibre Channel switching mode, Cisco UCS Manager logs you out and restarts the fabric interconnect. For a cluster configuration, Cisco UCS Manager restarts both fabric interconnects simultaneously in Cisco UCS Manager Release 3.1(1) and earlier releases. In Cisco UCS Manager Release 3.1(2), when the Fibre Channel switching mode is changed, the UCS fabric interconnects reload sequentially. In Cisco UCS Manager Release 3.1(3), and later releases, the subordinate fabric interconnect reboots first as a result of the change in switching mode. The primary fabric interconnect reboots only after you acknowledge it in **Pending Activities**. The primary fabric interconnect can take several minutes to complete the change in Fibre Channel switching mode and become system ready.

Note When the Fibre Channel switching mode is changed, both UCS fabric interconnects will reload simultaneously. Reloading of fabric interconnects will cause a system-wide downtime lasting approximately 10-15 minutes.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click one of the following links:

- **Set Fibre Channel Switching Mode**
- **Set Fibre Channel End-Host Mode**

The link for the current mode is dimmed.

Step 5 In the dialog box, click **Yes**.

Cisco UCS Manager restarts the fabric interconnect, logs you out, and disconnects Cisco UCS Manager GUI.

Changing the Properties of the Fabric Interconnects

Note To change the subnet or network prefix for a Cisco UCS domain, you must simultaneously change all subnets or prefixes, the virtual IPv4 or IPv6 address used to access Cisco UCS Manager, and the IPv4 or IPv6 addresses for both fabric interconnects.

Both fabric interconnects must maintain the same management address type, either IPv4 or IPv6. You cannot change the management address type for Fabric A without changing the management address type for Fabric B.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **Admin** > **All**.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Management Interfaces** to open the **Management Interfaces** dialog box.

Step 5 In the **Management Interfaces** dialog box, modify the values as necessary.

Step 6 To change only the virtual IP address that you use to access Cisco UCS Manager, enter the desired IP address in either the **IPv4 Address** or the **IPv6 Address** field in the **Virtual IP** area.

Step 7 To change only the name assigned to the Cisco UCS domain, enter the desired name in the **Name** field in the **Virtual IP** area.

Step 8 To change the subnet and IPv4 address, or the network prefix and IPv6 address, and default gateway assigned to the fabric interconnects, update the following fields:

a) In the **Virtual IP** area, change the IP address used to access Cisco UCS Manager in the **IPv4 Address** or **IPv6 Address** field.

b) In the **Fabric Interconnect** area for each fabric interconnect, click either the IPv4 or IPv6 tab.

c) On the IPv4 tab, update the IP address, subnet mask, and default gateway.

d) On the IPv6 tab, update the IP address, prefix, and default gateway.

Step 9 Click **OK**.

Step 10 Log out of Cisco UCS Manager GUI and log back in again to see your changes.

Determining the Primary Fabric Interconnect

Important If the admin password is lost, you can determine the primary and secondary roles of the fabric interconnects in a cluster by opening the Cisco UCS Manager GUI from the IP addresses of both fabric interconnects. The subordinate fabric interconnect fails with the following message:

```
UCSM GUI is not available on secondary node.
```

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects**.

Step 3 Click the fabric interconnect for which you want to identify the role.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **General** tab, click the down arrows on the **High Availability Details** bar to expand that area.

Step 6 View the **Leadership** field to determine whether the fabric interconnect is primary or subordinate.

Fabric Interconnect Port Types

By default, all fabric interconnect ports are unconfigured. For Ethernet LAN connectivity, fabric interconnect ports can be in the following states:

- **Unconfigured**—Port is not configured and cannot be used.
- **Server Port**—Port is configured for downlink connection to an IOM Fabric Extender (FEX) module in a blade chassis.
- **Uplink Port**—Port is configured for uplink connection to the upstream Ethernet switch. Uplink ports are always configured as trunk ports.
- **Disabled**—Port is configured either as an uplink or server port and is currently disabled by the administrator.

On Cisco UCS 6454 and 64108 Fabric Interconnects, ports 1 to 16 are unified ports. These ports can be configured as either Ethernet or Fibre Channel ports.

On Cisco UCS 6536 Fabric Interconnects, ports 33 to 36 are unified ports. These ports can be configured as either Ethernet or Fibre Channel ports.

On Cisco UCS X-Series Direct, also referred as Cisco UCS Fabric Interconnects 9108 100G (UCSX-S9108-100G), supports port breakout for Ethernet Ports (1-8) and Unified Ports (1 & 2).

On Cisco UCS 6600 Series Fabric Interconnects, ports 25-40 are unified ports. These ports can be configured as either Ethernet or Fibre Channel ports.

Note For detailed information on each type of Fabric Interconnect port, see Cisco UCS Manager Getting Started Guide.

vNICs

Once the connectivity between upstream uplink switches and downstream IOMs is established, we can connect vNICs from blade servers configuring vNICs. We recommended that you create a vNIC template to provide ease of management .

vNICs can be created within server profiles or by using a vNIC template. Using a vNIC template is the recommended method for configuring the NIC settings once, for each template, and then quickly creating new vNICs with the desired configuration. The vNIC configuration settings can be optimized for various operating systems, storage devices, and hypervisors.

A vNIC template can be configured as either of the following:

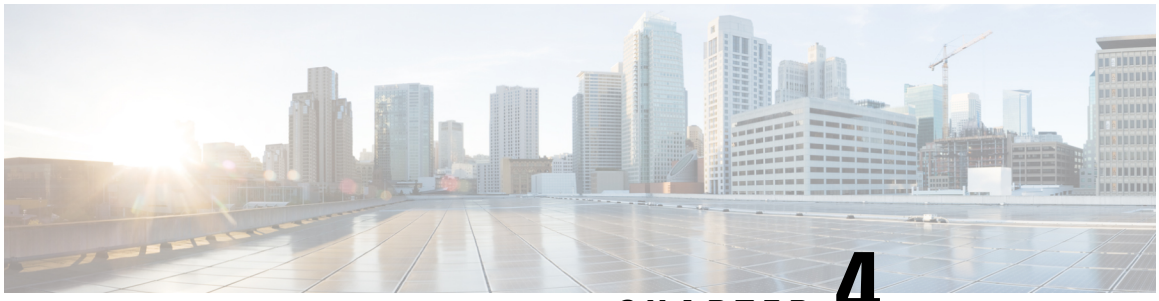
- Initiating template: This vNIC template will provide one-time configuration for the vNICs created using this template. Any subsequent changes to the template are not propagated to abstracted vNICs.
- Updating template: This vNIC template will provide initial configuration for the vNICs created using this template. Any subsequent changes to the template will also be propagated to abstracted vNICs. We recommend that you to create an updating vNIC template for production environments.

vNIC MAC addresses can be assigned manually or by configuring a MAC address pool. It is possible to either use the burned-in MAC addresses or abstract MAC addresses from an identity pool with system-defined prefixes. Stateless computing is the salient feature of the Cisco UCS platform. Therefore we recommend to you abstract vNIC MAC addresses for server profiles, and consequently use server vNIC MAC addresses from MAC address identity pools instead of using burned-in NIC MAC addresses. The benefit of abstracting the MAC identity is that in case of physical server failure, the server profile can be easily associated with the replacement server. The new server will acquire all the identities associated with the old server including the vNIC MAC addresses. From the operating system perspective, there is no change at all.

We recommend that you create vNIC templates with different configurations and create individual vNICs from vNIC templates as required. Also, define MAC address pools and assign MAC addresses to individual vNICs using those MAC address pools.

A vNIC is typically abstracted from the physical mezzanine card. Older Emulex, QLogic, and Intel NIC cards have fixed ports. The Cisco mezzanine NIC card, also known as a Palo card or Virtual Interface Card (VIC), provides dynamic server interfaces. Cisco VIC cards provide up to 256 dynamic interfaces. vNICs can be created within server profiles or by using a vNIC template. Using a vNIC template is the recommended method for configuring the NIC settings, doing so once for each template and then quickly creating additional vNICs with the desired configurations. The vNIC configuration settings can be optimized for various operating systems, storage devices, and hypervisors.

The vNIC creation for servers is part of the server profile, or server profile template creation. Once **Create Service Profile Template** or **Service Profile (Expert)** is started for the blade servers, creating the vNIC is the second step in the configuration wizard.



CHAPTER 4

LAN Ports and Port Channels

Port Modes

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

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

Port Types

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

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

Changing the port type does not require a reboot.

Ethernet Port Mode

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

- Server ports
- Ethernet uplink ports
- Ethernet port channel members
- FCoE ports
- Appliance ports
- Appliance port channel members
- SPAN destination ports
- SPAN source ports

Note For SPAN source ports, configure one of the port types and then configure the port as SPAN source.

Fibre Channel Port Mode

When you set the port mode to Fibre Channel, you can configure the following port types:

- Fibre Channel uplink ports
- Fibre Channel port channel members
- Fibre Channel storage ports
- SPAN source ports

Note For SPAN source ports, configure one of the port types and then configure the port as SPAN source.

Default Open Ports

The following table lists the default open ports used in Cisco UCS Manager.

Port	Interface	Protocol	Traffic Type	Fabric Interconnect	Usage
22	CLI	SSH	TCP	UCS 6400 Series UCS 6500 Series Cisco UCS Fabric Interconnects 9108 100G (Cisco UCS X-Series Direct) Cisco UCS 6600 Series Fabric Interconnect	Cisco UCS Manager CLI access
80	XML	HTTP	TCP	UCS 6400 Series UCS 6500 Series Cisco UCS Fabric Interconnects 9108 100G (Cisco UCS X-Series Direct) Cisco UCS 6600 Series Fabric Interconnect	Cisco UCS Manager GUI and third party management stations. Client download

Port	Interface	Protocol	Traffic Type	Fabric Interconnect	Usage
443	XML	HTTP	TCP	UCS 6400 Series UCS 6500 Series Cisco UCS Fabric Interconnects 9108 100G (Cisco UCS X-Series Direct) Cisco UCS 6600 Series Fabric Interconnect	Cisco UCS Manager login page access Cisco UCS Manager XML API access
743	KVM	HTTP	TCP	UCS 6400 Series	CIMC Web Service / Direct KVM
7546	CFS	CFSD	TCP	UCS 6400 Series UCS 6500 Series Cisco UCS Fabric Interconnects 9108 100G (Cisco UCS X-Series Direct) Cisco UCS 6600 Series Fabric Interconnect	Cisco Fabric Service

TCP and UDP Ports

The tables below list the incoming and outgoing TCP and UDP ports used in Cisco UCS for management access.

Table 2: Incoming ports

Port	Interface	Protocol	Traffic type	Usage
23	CLI	Telnet	TCP	Cisco UCS Manager CLI access
22	CLI	SSH	TCP	Cisco UCS Manager CLI access
443	Static HTML	HTTPS	TCP	Cisco UCS Manager login page access
80	Static HTML	HTTP	TCP	Client download

Port	Interface	Protocol	Traffic type	Usage
443	XML	HTTPS	TCP	Cisco UCS Manager XML API access
80	XML	HTTP	TCP	Ports used by Cisco UCS Manager GUI and third party management stations.
23	Serial-over-LAN	Telnet	TCP	COM1 port access on a specified server
22	Serial-over-LAN	SSH	TCP	COM1 port access on a specified server
161	SNMP	SNMP	UDP	SNMP MIBs exposed for monitoring
623	IPMI-over-LAN	RMCP	UDP	IPMI access to BMCs
2068	KVM	HTTPS	TCP	Data path for the BMCs
5988	CIMC XML	HTTP	TCP	Send CIMC messages over HTTP
743	KVM	HTTP	TCP	CIMC Web Service / Direct KVM
5661		HTTPD	TCP	Internal communication This port is applicable only to UCS 6400 Series Fabric Interconnects, 6500 Series Fabric Interconnect, Cisco UCS Fabric Interconnects 9108 100G, and Cisco UCS 6600 Series Fabric Interconnect.
7162		HTTPD	TCP	Internal communication This port is applicable only to UCS 6400 Series Fabric Interconnects, 6500 Series Fabric Interconnect, Cisco UCS Fabric Interconnects 9108 100G, and Cisco UCS 6600 Series Fabric Interconnect.
7546	CFS	CFSD	TCP	Cisco Fabric Service This port is applicable only to UCS 6400 Series Fabric Interconnects, 6500 Series Fabric Interconnect, Cisco UCS Fabric Interconnects 9108 100G, and Cisco UCS 6600 Series Fabric Interconnect.

Table 3: Outgoing ports

Port	Service	Protocol	Traffic type	Usage
1812	AAA	RADIUS	UDP	AAA server authentication requests
1813	AAA	RADIUS	UDP	AAA server authentication requests
49	AAA	TACACS	TCP	AAA server authentication requests
389	AAA	LDAP	UDP	
123	Time Sync	NTP	UDP	Synchronize the time with global time servers
162	SNMP Traps	SNMP	UDP	Send traps to a remote network management system.
25	Call Home	SMTP	TCP	Email-based and web-based notifications for critical system events
514	Syslog	SYSLOG	UDP	Cisco UCS Manager generated Syslog messages
53	Name resolution	DNS	UDP	DNS queries
69	TFTP	TFTP	UDP	File transfers
115	SFTP	SFTP	TCP	File transfers
20-21	FTP	FTP	TCP	File transfers
21	SCP	SCP	TCP	File transfers

Port Functionality and Configuring Port Modes for Cisco UCS Fabric Interconnects

Cisco UCS 6600 Series Fabric Interconnects

Configuring Port Modes for Cisco UCS 6600 Series Fabric Interconnect

This procedure includes steps for port mode configuration while managing traffic impact in high availability environments. In Cisco UCS 6600 Series Fabric Interconnect, port breakout functionality is currently not supported.

Caution Changing the port mode can cause an interruption in data traffic and lead to immediate Fabric Interconnect reboot.

If the Cisco UCS domain has a cluster configuration that is set up for high availability and servers with service profiles that are configured for failover, traffic fails over to the other fabric interconnect and data traffic is not interrupted when the port mode is changed on the fixed module.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > *Fabric_Interconnect_Name*.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click **Configure Unified Ports**.

Step 5 Review the confirmation message and click one of the following:

- **Yes**—To continue with configuring the port mode.
- **No**—To exit without configuring the port mode, and, wait for an appropriate maintenance window.

Step 6 In the **Configure Unified Ports** dialog box, use your mouse to drag the slider along the bar, from right to left, until the display shows the port-mode configuration that you want for the module.

To unconfigure Unified Ports, use your mouse to drag the slider along the bar, from left to right. When you unconfigure the unified port, it defaults to Ethernet Uplink port.

Step 7 Click **OK** to save your port-mode configuration.

The fabric interconnect reboots. All data traffic through that fabric interconnect is interrupted. If this occurs in a cluster configuration that provides high availability and includes servers with vNICs that are configured for failover, traffic fails over to the other fabric interconnect and no interruption occurs.

What to do next

Configure the port types for the ports. You can right-click on any port in the module display above the slider and configure that port for an available port type.

Cisco UCS X-Series Direct Fabric Interconnect

Port Breakout Functionality on Cisco UCS Fabric Interconnects 9108 100G (Cisco UCS X-Series Direct)

The Cisco UCS Fabric Interconnects 9108 100G is equipped with advanced port breakout functionality, which allows network administrators to subdivide a single high-bandwidth port into multiple lower-bandwidth ports. This feature is particularly beneficial for optimizing port utilization, managing cabling complexity, and adapting to various bandwidth requirements.

Physical Port	Breakout Options	Logical Ports After Breakout	Supported Speeds through breakout cables
Ethernet 1/1 - Ethernet 1/8	4x25G	Ethernet 1/1/1 to Ethernet 1/8/4	Up to 8x100 Gbps
Fibre Channel 1/1 and 1/2	4x8G, 4x16G, 4x32G	Fibre Channel 1/1/1 to Fibre Channel 1/2/4	Up to 8x32Gbps

Breakout Port Guidelines

Breakout ports are supported as destinations for traffic monitoring. The following are the guidelines for breakout functionality for Cisco UCS Fabric Interconnects 9108 100G:

- **Breakout Availability:** Breakout functionality is available for physical ports 1-8.
- **Ethernet Breakout:** Ethernet breakout ports can be configured on physical ports 1 through 8, resulting in 32 logical ports.
- **Fibre Channel Breakout:** Fibre Channel breakout ports can be configured on unified ports 1/1 and 1/2, resulting in 8 logical ports.
- **Port Configurations:** Physical Ports 1-8 can be configured as Uplink Ports, FCoE Uplink Ports, FCoE Storage Ports, and Appliance Ports.
- **Port Conversions:** All port conversions support up to 8 standard ports or 8 breakout ports.
- **Server Ports:** Configuration of server ports is supported only on ports 1–8, which are 100G ports. However, configuring a server port as a breakout port is not supported.
- **Fibre Channel Direct Ports:** Direct ports for Fibre Channel are not supported.
- **Traffic Monitoring:** Breakout ports can be utilized as destinations for traffic monitoring.

Configuring Ethernet Breakout Ports on Cisco UCS Fabric Interconnects 9108 100G

Procedure

Step 1 On the **Equipment** tab, expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

The Fabric Interconnect **General** tab appears, providing at-a-glance status, actions, physical display, properties, and firmware information for the selected fabric interconnect.

Step 2 View the available port(s) to break out.

Ensure that the port overall status is up and admin status is available. Do one of the following:

- In the **Work** pane, click the **Physical Ports** tab. The **Ethernet Ports** and **FC Ports** subtabs appear.
- In the **Work** pane, click the **Physical Display** tab. The Physical Display shows a graphical representation of the base fabric interconnect with a legend to help you identify port admin status.
- In the **Navigation** pane, expand ***Fabric_Interconnect_Name*** > **Fixed Module** > **Ethernet Ports.** this action displays ports in a tree view.

Step 3 Select one or more ports that you can break out. On the Cisco UCS Fabric Interconnects 9108 100G, ports 1 to 8 support breakout. Do one of the following:

- On the **Physical Display**, click a port or Ctrl-click to select multiple ports.
- On the **Ethernet Ports** tab, click a port or Ctrl-click to select multiple ports.
- On the **Ethernet Ports** tree view, click a port or Ctrl-click to select multiple ports.

Step 4 Configure the selected port(s) as breakout ports.

- On the **Ethernet Ports** tab, right-click the selected port(s) and choose **Configure 4x10G Breakout Port** or **Configure 4x25G Breakout Port** from the pop-up menu.
- On the **Ethernet Ports** tree view, right-click the selected port(s) and choose **Configure 4x10G Breakout Port** or **Configure 4x25G Breakout Port** from the pop-up menu. You can also select ports in the **Ethernet Ports** tree view and select **Configure Breakout Port** from the **Work** pane **Actions** Area. From the drop-down list, choose whether you want to configure the breakout port as a **4x10G port** or a **4x25G** port.

Step 5 Click **OK**.

Step 6 Configure the breakout ports according to your requirements.

Right-click one or more ports and select one of the following options. This table describes the actions that occur when you select the option. If a option is disabled, the port is already configured as such.

Configure Option	Action
Configure as Uplink Port	You confirm your action. Configuration takes place. The system displays a successful message. Click **Yes**.
Configure as FCoE Uplink Port	You confirm your action. Configuration takes place. The system displays a successful message. Click **Yes**.
Configure as FCoE Storage Port	You confirm your action. Configuration takes place. The system displays a successful message. Click **Yes**.

Configure Option	Action
Configure as Appliance Port	You confirm your action. Configuration takes place. The system displays a successful message. Click **Yes**.

Note
The **Configure as Server Port** option is supported on Cisco UCS Fabric Interconnects 9108 100G (Cisco UCS X-Series Direct). However, configuring a server port as a breakout port is not supported.

Step 7 The confirmation dialog box displays. Click **Yes**.

Note
Ethernet breakout port configuration will not lead to Fabric Interconnect reboot.

Configuring Port Modes for Cisco UCS Fabric Interconnects 9108 100G

The Cisco UCS X-Series Direct, also referred as Cisco UCS Fabric Interconnects 9108 100G (UCSX-S9108-100G), supports port breakout for Ethernet Ports (1-8) and Unified Ports (1 & 2). These unified ports can function as Ethernet or Fibre Channel (FC) ports, accommodating up to 8 sub-ports configured in groups of four.

Caution Changing the port mode can cause an interruption in data traffic and lead to immediate Fabric Interconnect reboot.

If the Cisco UCS domain has a cluster configuration that is set up for high availability and servers with service profiles that are configured for failover, traffic fails over to the other fabric interconnect and data traffic is not interrupted when the port mode is changed on the fixed module.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click **Configure Unified Ports**.

Step 5 Review the confirmation message and click one of the following:

- **Yes**—To continue with configuring the port mode.
- **No**—To exit without configuring the port mode, and, wait for an appropriate maintenance window.

Step 6 In the **Configure Unified Ports** dialog box, use your mouse to drag the slider along the bar, from right to left, until the display shows the port-mode configuration that you want for the module.

To unconfigure Unified Ports, use your mouse to drag the slider along the bar, from left to right. When you unconfigure the unified port, it defaults to Ethernet Uplink port.

Step 7 Click **OK** to save your port-mode configuration.

The fabric interconnect reboots. All data traffic through that fabric interconnect is interrupted. If this occurs in a cluster configuration that provides high availability and includes servers with vNICs that are configured for failover, traffic fails over to the other fabric interconnect and no interruption occurs.

What to do next

Configure the port types for the ports. You can right-click on any port in the module display above the slider and configure that port for an available port type.

Cisco UCS 6536 Fabric Interconnects

Port Breakout Functionality on Cisco UCS 6536 Fabric Interconnects

The Cisco UCS 6536 36-Port Fabric Interconnect is a One-Rack-Unit (1RU) 1/10/25/40/100 Gigabit Ethernet, FCoE, and Fibre Channel switch offering up to 7.42 Tbps throughput and up to 36 ports.

Cisco UCS 6536 Fabric Interconnect supports splitting a single 40 Gigabit(G)/100G Quad Small Form-factor Pluggable (QSFP) port into four 10G/25G ports using a supported breakout cable. The switch has 32 40/100-Gbps Ethernet ports and four unified ports that can support 40/100-Gbps Ethernet ports or 16 Fiber Channel (FC) ports after breakout at 8/16/32-Gbps FC speeds. The 16 FC ports after breakout can operate as an FC Uplink or FC storage port. The switch also supports two ports (Port 9 and Port 10) at 1-Gbps speed using QSA, and all 36 ports can breakout for 10 or 25 Gbps Ethernet connectivity. All Ethernet ports can support FCoE.

Port breakout is supported for Ethernet ports (1-32) and Unified ports (33-36). These 40/100G ports are numbered in a 2-tuple naming convention. The process of changing the configuration from 40G to 10G, or from 100G to 25G is called breakout, and the process of changing the configuration from [4X]10G to 40G or from [4X]25G to 100G is called unconfigure.

When you break out a 40G port into 10G ports or a 100G port into 25G ports, the resulting ports are numbered using a 3-tuple naming convention. For example, the breakout ports of the second 40-Gigabit Ethernet port are numbered as 1/31/1, 1/31/2, 1/31/3, and 1/31/4.

FC breakout is supported on ports 36 through 33 when each port is configured with a four-port breakout cable. For example: Four FC breakout ports on the physical port 33 are numbered as 1/33/1, 1/33/2, 1/33/3, and 1/33/4.

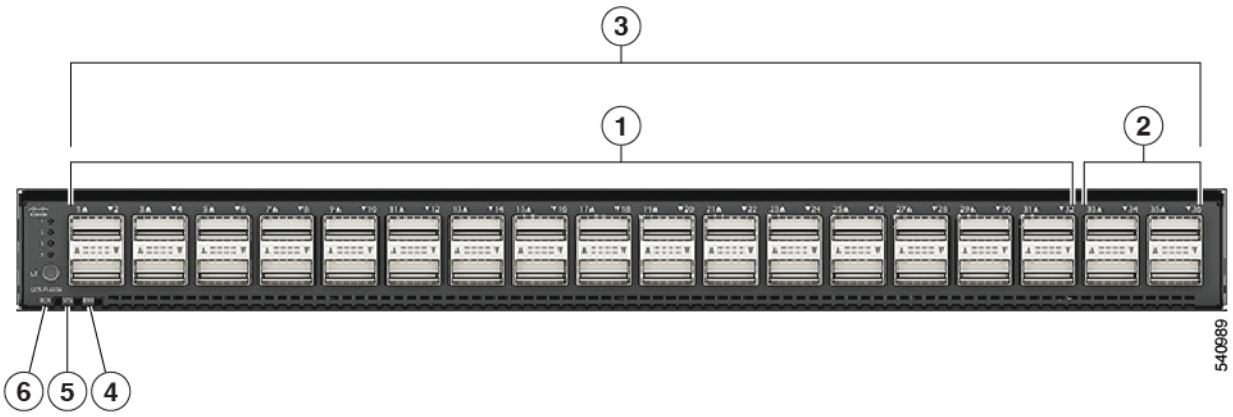
Note Fibre Channel support is only available through the configuration of the Unified Ports (36-33) as Fibre Channel breakout port.

The following image shows the rear view of the Cisco UCS 6536 fabric interconnect:

Figure 1: Cisco UCS 6536 Fabric Interconnect Rear View

The following image shows the rear view of the Cisco UCS 6536 fabric interconnect that include Ports and LEDs:

Figure 2: Cisco UCS 6536 Fabric Interconnect Rear View



1	Ports 1-32. Uplink ports are Ethernet port that can operate with the port speed of 10 Gbps/25 Gbps/40 Gbps/100 Gbps. When using a breakout cable, each of these ports can operate as: 4 x 10 Gbps/4x 25 Gbps/1 x 40 Gbps/1 x 100 Gbps Ethernet or FCoE ports.	2	Ports 33-36. Unified Ports can operate with port speed of 10 Gbps/25 Gbps/ 40 Gbps/100 Gbps Ethernet. or 8 Gbps/16 Gbps/32 Gbps Fibre Channel (FC). When using a breakout cable, each of these ports can operate as 4 x 10 Gbps/4 x 25 Gbps Ethernet or 4x8Gbps/4x16Gbps/4x32Gbps FC ports.
3	Ports 1-36. Uplink ports and Unified ports that can be configured as Ethernet Breakout Port and can operate with the port speed of 10 Gbps/25 Gbps/40 Gbps/100 Gbps. When using a breakout cable, each of these ports can operate as: 4 x 10 Gbps/4x 25 Gbps/1 x 40 Gbps/1 x 100 Gbps Ethernet or FCoE ports.	4	System environment (fan fault) LED
5	System status (STS) LED	6	Beacon (BCN) LED

Breakout Port Guidelines

The following are the guidelines for breakout functionality for Cisco UCS 6536 Fabric Interconnects:

- The configurable breakout ports are from port 1-36.

- You can configure the speed for each breakout port. Each breakout port can be configured at the speed of 4 x 8 Gbps/ 4 x 16 Gbps/ 4 x 32 Gbps for Fibre Channel.
  - For Fibre Channel breakout, each breakout port can be configured at the speed of 4 x 8 Gbps/ 4 x 16 Gbps/ 4 x 32 Gbps.
  - For Ethernet breakout, each breakout port can be configured at the speed of 4 x 10 Gbps/4 x 25 Gbps.
- Fibre Channel breakout ports are supported, and Fiber Channel direct ports are not supported.
- FC breakout port can be configured from 1/36 through 1/33. FC breakout ports (36-33) cannot be configured unless the previous ports are FC breakout ports. Configuration of a single (individual) FC breakout port is also supported.
- If the breakout mode for any of the supported Fabric Interconnect ports (1-36) is an Ethernet breakout, the Fabric Interconnect does not lead to a reboot.
- If the breakout mode for any of the supported Fabric Interconnect ports (36-33) is a Fibre Channel uplink breakout, the Fabric Interconnect leads to a reboot.
- Breakout ports are supported as destinations for traffic monitoring.
- Ports 1-36 can be configured as Server Port, FCoE Uplink Port, Appliance Port, and Monitor Port.
- Port 36-33 can be configured also as FC Uplink Port or FC Storage Port when configured as unified port.

Configuring Ethernet Breakout Ports on UCS 6536 Fabric Interconnects

Procedure

Step 1 On the **Equipment** tab, expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

The Fabric Interconnect **General** tab appears, providing at-a-glance status, actions, physical display, properties, and firmware information for the selected fabric interconnect.

Step 2 View the available port(s) to break out.

Ensure that the port overall status is up and admin status is available. Do one of the following:

- In the **Work** pane, click the **Physical Ports** tab. The **Ethernet Ports** and **FC Ports** subtabs appear.
- In the **Work** pane, click the **Physical Display** tab. The Physical Display shows a graphical representation of the base fabric interconnect with a legend to help you identify port admin status.
- In the **Navigation** pane, expand ***Fabric_Interconnect_Name*** > **Fixed Module** > **Ethernet Ports.** this action displays ports in a tree view.

Step 3 Select one or more ports that you can break out. On the UCS 6536 fabric interconnect, ports 1 to 36 support breakout. Do one of the following:

- On the **Physical Display**, click a port or Ctrl-click to select multiple ports.
- On the **Ethernet Ports** tab, click a port or Ctrl-click to select multiple ports.
- On the **Ethernet Ports** tree view, click a port or Ctrl-click to select multiple ports.

Step 4 Configure the selected port(s) as breakout ports.

- On the **Ethernet Ports** tab, right-click the selected port(s) and choose **Configure 4x10G Breakout Port** or **Configure 4x25G Breakout Port** from the pop-up menu.
- On the **Ethernet Ports** tree view, right-click the selected port(s) and choose **Configure 4x10G Breakout Port** or **Configure 4x25G Breakout Port** from the pop-up menu. You can also select ports in the **Ethernet Ports** tree view and select **Configure Breakout Port** from the **Work** pane **Actions** Area. From the drop-down list, choose whether you want to configure the breakout port as a **4x10G port** or a **4x25G** port.

Step 5 Click **OK**.

Step 6 Configure the breakout ports according to your requirements.

Right-click one or more ports and select one of the following options. This table describes the actions that occur when you select the option. If a option is disabled, the port is already configured as such.

Configure Option	Action
Configure as Server Port	You confirm your action. Configuration takes place. The system displays a successful message. Click **Yes**.
Configure as Uplink Port	You confirm your action. Configuration takes place. The system displays a successful message. Click **Yes**.
Configure as FCoE Uplink Port	You confirm your action. Configuration takes place. The system displays a successful message. Click **Yes**.
Configure as FCoE Storage Port	You confirm your action. Configuration takes place. The system displays a successful message. Click **Yes**.
Configure as Appliance Port	You confirm your action. Configuration takes place. The system displays a successful message. Click **Yes**.

Step 7 The confirmation dialog box displays. Click **Yes**.

Note
Ethernet breakout port configuration will not lead to Fabric Interconnect reboot.

Configuring a 10/25G Port with QSA on Cisco UCS FI 6536

When a port on UCS FI 6536 is operating at the default 40/100G port speed, Cisco UCS Manager does not let you choose port speeds of 1G, 10G, or 25G. To use a 40/100G port on UCS FI 6536 as a 10/25 G port with a QSFP+Adapter (QSA) transceiver on the other end, you must configure it in the breakout mode.

Note When you try to change port speeds to 10G or 25G, Cisco UCS Manager displays a prompt to configure the port in breakout mode. After you configure a breakout port, you can configure each 10/25G GB sub-port as an uplink, or FCoE uplink port as required.

When you break out the port, use a breakout cable to split a single port into four 10G or 25G ports, and configure the ports in breakout mode, you can use all lanes as 10 G or 25G ports. If you break out the port without a breakout cable, only the first lane becomes usable as a 10G or 25G interface.

Procedure

Step 1 Configure breakout feature on the port that you want to use as a 10/25G port on the Cisco UCS FI 64108. For more information about configuring the break out feature, see *Configuring Fabric Interconnect Ethernet Breakout Ports*.

Step 2 In Cisco UCS Manager, the first tuple interface is enabled after the QSA transceiver is plugged into the FI port. You can configure this interface based on your requirements.

The resulting ports after a break out of the 40/100G port are numbered using a 3-tuple naming convention. For example, the breakout ports of the second 40-Gigabit Ethernet port are numbered as 1/36/1, 1/36/2, 1/36/3, 1/36/4, and only the first port becomes usable as a 10 GB port.

Cisco UCS 6400 Series Fabric Interconnects

Port Breakout Functionality on Cisco UCS 64108 Fabric Interconnects

About Breakout Ports

Cisco UCS 64108 fabric interconnects support splitting a single 40/100G QSFP port into four 10/25G ports using a supported breakout cable. On the UCS 64108 fabric interconnect, by default, there are 12 ports in the 40/100G mode. These are ports 97 to 108. These 40/100G ports are numbered in a 2-tuple naming convention. For example, the second 40G port is numbered as 1/99. The process of changing the configuration from 40G to 10 G, or from 100G to 25G is called breakout, and the process of changing the configuration from [4X]10G to 40G or from [4X]25G to 100G is called unconfigure. These ports can be used as uplink port, appliance port, server port (using FEX), and FCoE storage port.

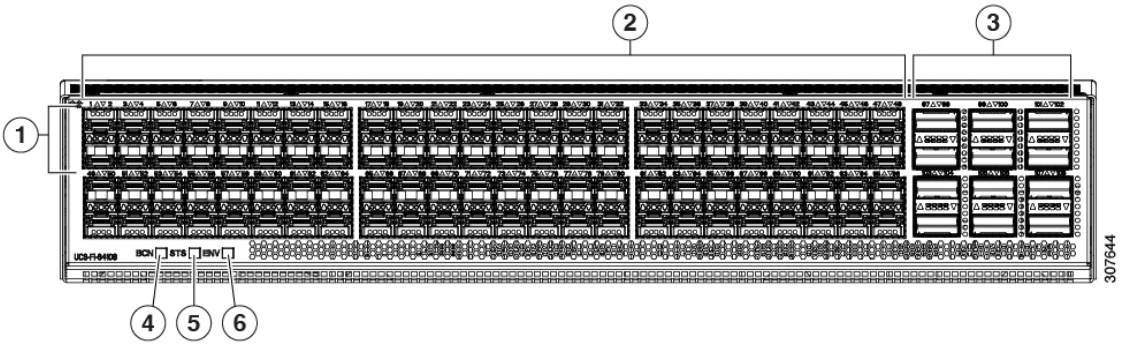
When you break out a 40G port into 10G ports or a 100G port into 25G ports, the resulting ports are numbered using a 3-tuple naming convention. For example, the breakout ports of the second 40-Gigabit Ethernet port are numbered as 1/99/1, 1/99/2, 1/99/3, 1/99/4.

Note Cisco UCS Manager does not support connection of FEX, chassis, blade, IOM, or adapters (other than VIC adapters) to the uplink ports of Fabric Interconnect.

Starting with Cisco UCS Manager Release 4.2(3b), configuring the Ethernet breakout ports will not lead to Fabric Interconnect reboot.

The following image shows the rear view of the Cisco UCS 64108 fabric interconnect, and includes the ports that support breakout port functionality:

Figure 3: Cisco UCS 64108 Fabric Interconnect Rear View



1	Ports 1-16. Unified Ports can operate as 10/25 Gbps Ethernet or 8/16/32 Gbps Fibre Channel. FC ports are converted in groups of four. Unified ports: • 10/25 Gbps Ethernet or FCoE • 8/16/32 Gbps Fibre Channel	2	Ports 1-96. Each port can operate as either a 10 Gbps or 25 Gbps Ethernet or FCoE SFP28 port.
3	Uplink Ports 97-108. Each port can operate as either a 40 Gbps or 100 Gbps Ethernet or FCoE port. When using a breakout cable, each of these ports can operate as 4 x 10 Gbps or 4 x 25 Gbps Ethernet or FCoE ports. Ports 97 - 108 can be used to connect to Ethernet or FCoE uplink ports, and not to UCS server ports.	4	Ports 89-96 • 10/25 Gbps Ethernet or FCoE • 1 Gbps Ethernet
5	System environment (fan fault) LED	6	System status LED
7	Beacon LED		

Breakout Port Guidelines

The following are the guidelines for breakout functionality for Cisco UCS 64108 fabric interconnects:

- The breakout configurable ports are ports 97-108.
- You cannot configure the speed for each breakout port. Each breakout port is in auto mode.
- Breakout ports are not supported as destinations for traffic monitoring.
- Ports 97-108 at 40/100G can be configured as uplink, FCoE, or appliance port. Ports 97-108 after breakout to 10/25G can be configured as uplink, appliance, FCoE, or for direct-connect rack server connectivity.

Configuring Ethernet Breakout Ports on UCS 64108 Fabric Interconnects

Beginning with Cisco UCS Manager Release 4.2(3p), Ethernet breakout port configuration will not lead to Fabric Interconnect reboot.

After you configure a breakout port, you can configure each 10/25G GB sub-port as an uplink, or FCoE uplink port as required.

Procedure

Step 1 On the **Equipment** tab, expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

The Fabric Interconnect **General** tab appears, providing at-a-glance status, actions, physical display, properties, and firmware information for the selected fabric interconnect.

Step 2 View the available port(s) to break out.

Ensure that the port overall status is up and admin status is available. Do one of the following:

- In the **Work** pane, click the **Physical Ports** tab. The **Ethernet Ports** and **FC Ports** subtabs appear.
- In the **Work** pane, click the **Physical Display** tab. The Physical Display shows a graphical representation of the base fabric interconnect with a legend to help you identify port admin status.
- In the **Navigation** pane, expand ***Fabric_Interconnect_Name*** > **Fixed Module** > **Ethernet Ports.** this action displays ports in a tree view.

Step 3 Select one or more ports that you can break out. On the UCS 64108 fabric interconnect, ports 97 to 108 support breakout. Do one of the following:

- On the **Physical Display**, click a port or Ctrl-click to select multiple ports.
- On the **Ethernet Ports** tab, click a port or Ctrl-click to select multiple ports.
- On the **Ethernet Ports** tree view, click a port or Ctrl-click to select multiple ports.

Step 4 Configure the selected ports as breakout ports.

- On the **Ethernet Ports** tab, right-click the selected port(s) and choose **Configure 4x10G Breakout Port** or **Configure 4x25G Breakout Port** from the pop-up menu. This command is disabled if the port does not support breakout.
- On the **Ethernet Ports** tree view, right-click the selected port(s) and choose **Configure 4x10G Breakout Port** or **Configure 4x25G Breakout Port** from the pop-up menu. This command is disabled if the port does not support breakout. You can also select ports in the **Ethernet Ports** tree view and select **Configure Breakout Port** from the **Work** pane **Actions** Area. From the drop-down list, choose whether you want to configure the breakout port as a **4x10G port** or a **4x25G** port.

Step 5 Click **OK**.

Step 6 Configure the breakout ports according to your requirements.

Right-click one or more ports and select one of the following commands. This table describes the actions that occur when you select the command. If a command is disabled, the port is already configured as such.

Configure Command	Action
Configure as Server Port	You confirm your action. Configuration takes place. The system displays a successful message. Click **Yes**.

Configure Command	Action
Configure as Uplink Port	You confirm your action. Configuration takes place. The system displays a successful message. Click **Yes**.
Configure as FCoE Uplink Port	You confirm your action. Configuration takes place. The system displays a successful message. Click **Yes**.
Configure as FCoE Storage Port	Not supported on UCS 64108.
Configure as Appliance Port	Not supported on UCS 64108.

Step 7 The confirmation dialog box displays. Click **Yes**.

Configuring a 10/25G Port with QSA on Cisco UCS FI 64108

When a port on UCS FI 64108 is operating at the default 40/100G port speed, Cisco UCS Manager does not let you choose port speeds of 1G, 10G, or 25G. To use a 40/100G port on UCS FI 6454 as a 10/25 G port with a QSFP+Adapter (QSA) transceiver on the other end, you must configure it in the breakout mode.

Note When you try to change port speeds to 10G or 25G, Cisco UCS Manager displays a prompt to configure the port in breakout mode. After you configure a breakout port, you can configure each 10/25G GB sub-port as an uplink, or FCoE uplink port as required.

When you break out the port, use a breakout cable to split a single port into four 10G or 25G ports, and configure the ports in breakout mode, you can use all lanes as 10 G or 25G ports. If you break out the port without a breakout cable, only the first lane becomes usable as a 10G or 25G interface.

Procedure

Step 1 Configure breakout feature on the port that you want to use as a 10/25G port on the Cisco UCS FI 64108. For more information about configuring the break out feature, see *Configuring Fabric Interconnect Ethernet Breakout Ports*.

Step 2 In Cisco UCS Manager, the first tuple interface is enabled after the QSA transceiver is plugged into the FI port. You can configure this interface based on your requirements.

The resulting ports after a break out of the 40/100G port are numbered using a 3-tuple naming convention. For example, the breakout ports of the second 40-Gigabit Ethernet port are numbered as 1/50/1, 1/50/2, 1/50/3, 1/50/4, and only the first port becomes usable as a 10 GB port.

Port Breakout Functionality on Cisco UCS 6454 Fabric Interconnects

About Breakout Ports

Cisco UCS 6454 fabric interconnects support splitting a single 40/100G QSFP port into four 10/25G ports using a supported breakout cable. These ports can be used only as uplink ports connecting to a 10/25G switch. On the UCS 6454 fabric interconnect, by default, there are 6 ports in the 40/100G mode. These are ports 49 to 54. These 40/100G ports are numbered in a 2-tuple naming convention. For example, the second 40G port is numbered as 1/50. The process of changing the configuration from 40G to 10 G, or from 100G to 25G is called breakout, and the process of changing the configuration from [4X]10G to 40G or from [4X]25G to 100G is called unconfigure.

When you break out a 40G port into 10G ports or a 100G port into 25G ports, the resulting ports are numbered using a 3-tuple naming convention. For example, the breakout ports of the second 40-Gigabit Ethernet port are numbered as 1/50/1, 1/50/2, 1/50/3, 1/50/4.

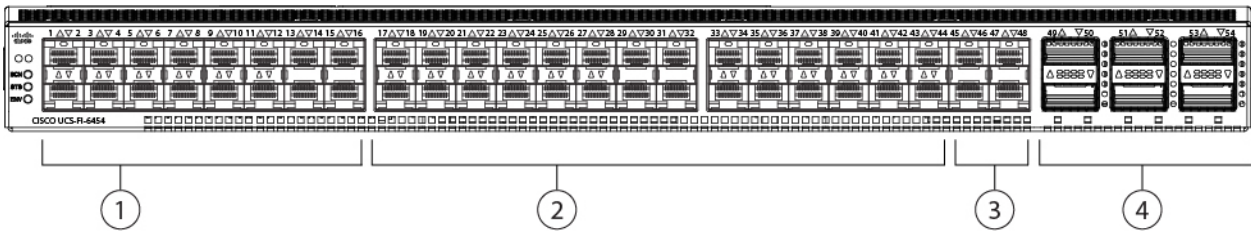
Starting with Cisco UCS Manager Release 4.2(3b), Ethernet breakout ports configuration will not lead to Fabric Interconnect reboot.

Starting with Cisco UCS Manager Release 4.1(3a), you can connect Cisco UCS Rack servers with VIC 1455 and 1457 adapters, to the uplink ports 49 to 54 (40/100 Gbps Ethernet or FCoE) in Cisco UCS 6454 Fabric Interconnects.

Note Cisco UCS Manager does not support connection of FEX, chassis, blade, IOM, or adapters (other than VIC 1455 and 1457 adapters) to the uplink ports of Fabric Interconnect.

The following image shows the rear view of the Cisco UCS 6454 fabric interconnect, and includes the ports that support breakout port functionality:

Figure 4: Cisco UCS 6454 Fabric Interconnect Rear View



1	Ports 1-16 (Unified Ports 10/25 Gbps Ethernet or FCoE or 8/16/32 Gbps Fibre Channel)	2	Ports 17-44 (10/25 Gbps Ethernet or FCoE)
3	Ports 45-48 (1/10/25 Gbps Ethernet or FCoE)	4	Uplink Ports 49-54 (40/100 Gbps Ethernet or FCoE)

Breakout Port Guidelines

The following are the guidelines for breakout functionality for Cisco UCS 6454 fabric interconnects:

- The breakout configurable ports are ports 49-54.

- You cannot configure the speed for each breakout port. Each breakout port is in auto mode.
- In Cisco UCS Manager Release 4.0(2), breakout ports are not supported as destinations for traffic monitoring.
- Ports 49-54 at 40/100G can be configured as uplink, FCoE, or appliance port. Ports 49-54 after breakout to 10/25G can be configured as uplink, appliance, FCoE, or for direct-connect rack server connectivity.

Configuring Ethernet Breakout Ports on UCS 6454 Fabric Interconnects

Caution Beginning with Cisco UCS Manager Release 4.2(3p), Ethernet breakout ports configuration will not lead to Fabric Interconnect reboot.

Procedure

Step 1 On the **Equipment** tab, expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

The Fabric Interconnect **General** tab appears, providing at-a-glance status, actions, physical display, properties, and firmware information for the selected fabric interconnect.

Step 2 View the available port(s) to break out.

Ensure that the port overall status is up and admin status is available. Do one of the following:

- In the **Work** pane, click the **Physical Ports** tab. The **Ethernet Ports** and **FC Ports** subtabs appear.
- In the **Work** pane, click the **Physical Display** tab. The Physical Display shows a graphical representation of the base fabric interconnect with a legend to help you identify port admin status.
- In the **Navigation** pane, expand ***Fabric_Interconnect_Name*** > **Fixed Module** > **Ethernet Ports.** this action displays ports in a tree view.

Step 3 Select one or more ports that you can break out. On the UCS 6454 fabric interconnect, ports 49 to 54 support breakout. Do one of the following:

- On the **Physical Display**, click a port or Ctrl-click to select multiple ports.
- On the **Ethernet Ports** tab, click a port or Ctrl-click to select multiple ports.
- On the **Ethernet Ports** tree view, click a port or Ctrl-click to select multiple ports.

Step 4 Configure the selected port(s) as breakout ports.

- On the **Ethernet Ports** tab, right-click the selected port(s) and choose **Configure 4x10G Breakout Port** or **Configure 4x25G Breakout Port** from the pop-up menu. This command is disabled if the port does not support breakout.
- On the **Ethernet Ports** tree view, right-click the selected port(s) and choose **Configure 4x10G Breakout Port** or **Configure 4x25G Breakout Port** from the pop-up menu. This command is disabled if the port does not support breakout. You can also select ports in the **Ethernet Ports** tree view and select **Configure Breakout Port** from the **Work** pane **Actions** Area. From the drop-down list, choose whether you want to configure the breakout port as a **4x10G port** or a **4x25G** port.

Step 5 Click **OK**.

Step 6 Configure the breakout ports according to your requirements.

Right-click one or more ports and select one of the following commands. This table describes the actions that occur when you select the command. If a command is disabled, the port is already configured as such.

Configure Command	Action
Configure as Server Port	You confirm your action. Configuration takes place. The system displays a successful message. Click **Yes**.
Configure as Uplink Port	You confirm your action. Configuration takes place. The system displays a successful message. Click **Yes**.
Configure as FCoE Uplink Port	You confirm your action. Configuration takes place. The system displays a successful message. Click **Yes**.
Configure as FCoE Storage Port	Not supported on Cisco UCS 6454.
Configure as Appliance Port	Not supported on Cisco UCS 6454.

Step 7 The confirmation dialog box displays. Click **Yes**.

Configuring a 10/25G Port with QSA Adapter on Cisco UCS FI 6454

When a port on UCS FI 6454 is operating at the default 40/100G port speed, Cisco UCS Manager does not let you choose port speeds of 1G, 10G, or 25G. To use a 40/100G port on UCS FI 6454 as a 10/25 G port with a QSFP+Adapter (QSA) transceiver on the other end, you must configure it in the breakout mode.

Note When you try to change port speeds to 10G or 25G, Cisco UCS Manager displays a prompt to configure the port in breakout mode. After you configure a breakout port, you can configure each 10/25G GB sub-port as an uplink, or FCoE uplink port as required.

When you break out the port, use a breakout cable to split a single port into four 10G or 25G ports, and configure the ports in breakout mode, you can use all lanes as 10 G or 25G ports. If you break out the port without a breakout cable, only the first lane becomes usable as a 10G or 25G interface.

Procedure

Step 1 Configure breakout feature on the port that you want to use as a 10/25G port on the Cisco UCS FI 6454. For more information about configuring the break out feature, see *Configuring Fabric Interconnect Ethernet Breakout Ports*.

Step 2 In Cisco UCS Manager, the first tuple interface is enabled after the QSA transceiver is plugged into the FI port. You can configure this interface based on your requirements.

The resulting ports after a break out of the 40/100G port are numbered using a 3-tuple naming convention. For example, the breakout ports of the second 40-Gigabit Ethernet port are numbered as 1/50/1, 1/50/2, 1/50/3, 1/50/4, and only the first port becomes usable as a 10 GB port.

Reconfiguring an Ethernet Breakout Port

You can reconfigure an unconfigured breakout port in a particular role, such as Server, Uplink, or Appliance. Reconfiguring the breakout port allows you to modify the existing port configuration to your current requirements.

An unconfigured Cisco UCS 6400 Series Fabric Interconnect breakout port can be reconfigured only as an Uplink or FCoE Uplink port.

Procedure

Step 1 On the **Equipment** tab, expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name*** > **Fixed Module**.

Step 2 Select one or more ports that you have broken out. Do one of the following:

- On the **Physical Display**, click a port or Ctrl-click to select multiple ports.
- On the **Ethernet Ports** tab, click a port or Ctrl-click to select multiple ports.
- On the **Ethernet Ports** tree view, click a port or Ctrl-click to select multiple ports.

Step 3 Reconfigure the port(s)

On the **General** Tab **Actions** area, click **Reconfigure** from the pop-up menu.

Step 4 The confirmation dialog box displays.

Click **Yes**. The fabric interconnect reboots and all traffic stops.

Step 5 The system displays a success message.

Click **OK**.

Note
Starting with Cisco UCS Manager Release 4.2(3b), configuring the Ethernet breakout ports will not lead to Fabric Interconnect reboot.

Unconfiguring a Breakout Port

If you want to configure a breakout port back to a 40 GB Ethernet port on a Cisco UCS 6400 Series , or Cisco UCS 6500 Series Fabric Interconnect, you must first unconfigure it.

This procedure does not apply to Cisco UCS 6600 Series Fabric Interconnect, as breakout ports are currently not supported on this model.

Procedure

Step 1 On the **Equipment** tab, expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name*** > **Fixed Module**.

Step 2 On the **General Tab**, right-click a port in the physical display area and select **Unconfigure**.

Step 3 Click **Yes** in the confirmation box.

The fabric interconnect reboots and all traffic stops.

Note
Starting with Cisco UCS Manager Release 4.2(3b), configuring the Ethernet breakout ports will not lead to Fabric Interconnect reboot.

Unified Ports

Beacon LEDs for Unified Ports

Each port fabric interconnect has a corresponding beacon LED. When the **Beacon LED** property is configured, the beacon LEDs illuminate, showing you which ports are configured in a given port mode.

You can configure the **Beacon LED** property to show you which ports are grouped in one port mode: either Ethernet or Fibre Channel. By default, the Beacon LED property is set to Off.

Note For unified ports on the expansion module, you can reset the **Beacon LED** property to the default value of **Off** during expansion module reboot.

Guidelines for Configuring Unified Ports

Consider the following guidelines and restrictions when configuring unified ports:

Hardware and Software Requirements

Unified ports are supported on the following:

- Cisco UCS 6664 Fabric Interconnect with Cisco UCS Manager Release 6.0(1b)and later releases
- Cisco UCS Fabric Interconnects 9108 100G (Cisco UCS X-Series Direct) with Cisco UCS Manager Release 4.3(4b) and later releases
- Cisco UCS 6536 Fabric Interconnect with Cisco UCS Manager Release 4.2(3b) and later releases
- Cisco UCS 64108 Fabric Interconnect with Cisco UCS Manager Release 4.1 and later releases
- Cisco UCS 6454 Fabric Interconnect with Cisco UCS Manager Release 4.0 and later releases

Port Mode Placement

Because the Cisco UCS Manager 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 Manager 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 Manager 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.

Note

- On the Cisco UCS Fabric Interconnects 9108 100G, the ports 1 & 2 are unified ports and can be configured as Ethernet or Fibre Channel ports.
- On the Cisco UCS 6536 Fabric Interconnect, the Unified Port capability is restricted to the first 16 ports. Only ports 1/1-1/16 can be configured as FC. The Fibre Channel ports must be contiguous, followed by contiguous Ethernet ports.
- On the Cisco UCS 6400 Series Fabric Interconnect, the Unified Port capability is restricted to first 16 ports. Only ports 1/1-1/16 can be configured as FC. The Fibre Channel ports must be contiguous, followed by contiguous Ethernet ports. The Cisco UCS 6400 Series Fabric Interconnect connected to a Cisco UCS server, connecting more than 16 ports will result in an error.
- 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.

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:

- In an unified uplink port, if you enable one component as a SPAN source, the other component will automatically become a SPAN source.

Note If you create or delete a SPAN source under the Ethernet uplink port, Cisco UCS Manager automatically creates or deletes a SPAN source under the FCoE uplink port. The same happens when you create a SPAN source on the FCOE uplink port.

- You must configure a non default native VLAN on FCoE and unified uplink ports. This VLAN is not used for any traffic. Cisco UCS Manager 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 Manager 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 Manager 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 Manager deletes the corresponding members ports from Ethernet port channel and FCoE port channel and creates a new standalone port.
- If you downgrade Cisco UCS Manager from release 2.1 to any of the prior releases, all unified uplink ports and port channels will be converted to Ethernet ports and Ethernet port channels when the downgrade is complete. Similarly, all the unified storage ports will be converted to appliance ports.
- 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.
- In Cisco UCS 6536 Fabric Interconnect to configure FC breakout port, you have to configure ports from the sequence from 1/36 through 1/33. FC breakout ports (36 - 33) cannot be configured unless the previous ports are FC breakout ports. Also, configuring a single (individual) FC breakout port is supported.

  Ports 33-36 can be configured only as FC Uplink Port or FC Storage Port when it is configured as unified port.
- The Cisco UCS Fabric Interconnects 9108 100G (Cisco UCS X-Series Direct) supports port breakout for Ethernet Ports (1-8) and Unified Ports (1 and 2). These unified ports can function as Ethernet or Fibre Channel (FC) ports, accommodating up to 8 sub-ports configured in groups of four. The FC breakout ports can be configured as FC Uplink Port or FC Storage Port.

Configuring the Beacon LEDs for Unified Ports

Complete the following task for each module for which you want to configure beacon LEDs.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 Depending upon the location of the unified ports for which you want to configure the beacon LEDs, click on one of the following:

- **Fixed Module**
- **Expansion Module**

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Properties** area, click one of the following radio buttons in the **Beacon LED** field:

- **Off**—All physical LEDs are off.
- **Eth**—The physical LEDs next to all Ethernet ports are on.
- **Fc**—The physical LEDs next to all Fibre Channel ports are on.

Step 6 Click **Save Changes**.

Changing Port Modes

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 Non-Cluster Configuration

A non-cluster 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.

Configuring Port Modes for Cisco UCS X-Series Direct Fabric Interconnect

In Cisco UCS X-Series Direct Fabric Interconnects, port breakout is supported for Ethernet Ports (1-8) and Unified Ports (1-2). The unified ports can be configured as FC uplink ports (with sub-group of 4 in each unified port, a maximum 16 sub-ports can be configured as FC port).

Caution Changing the port mode can cause an interruption in data traffic and lead to immediate Fabric Interconnect reboot.

If the Cisco UCS domain has a cluster configuration that is set up for high availability and servers with service profiles that are configured for failover, traffic fails over to the other fabric interconnect and data traffic is not interrupted when the port mode is changed on the fixed module.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click **Configure Unified Ports**.

Step 5 Review the confirmation message and click one of the following:

- **Yes**—To continue with configuring the port mode.
- **No**—To exit without configuring the port mode, and, wait for an appropriate maintenance window.

Step 6 In the **Configure Unified Ports** dialog box, use your mouse to drag the slider along the bar, from right to left, until the display shows the port-mode configuration that you want for the module.

To unconfigure Unified Ports, use your mouse to drag the slider along the bar, from left to right. When you unconfigure the unified port, it defaults to Ethernet Uplink port.

Step 7 Click **OK** to save your port-mode configuration.

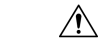
The fabric interconnect reboots. All data traffic through that fabric interconnect is interrupted. If this occurs in a cluster configuration that provides high availability and includes servers with vNICs that are configured for failover, traffic fails over to the other fabric interconnect and no interruption occurs.

What to do next

Configure the port types for the ports. You can right-click on any port in the module display above the slider and configure that port for an available port type.

Configuring Port Modes for Cisco UCS X-Series Direct Fabric Interconnect

In Cisco UCS X-Series Direct Fabric Interconnects, port breakout is supported for Ethernet Ports (1-8) and Unified Ports (1-2). The unified ports can be configured as FC uplink ports (with sub-group of 4 in each unified port, a maximum 16 sub-ports can be configured as FC port).



Caution Changing the port mode can cause an interruption in data traffic and lead to immediate Fabric Interconnect reboot.

If the Cisco UCS domain has a cluster configuration that is set up for high availability and servers with service profiles that are configured for failover, traffic fails over to the other fabric interconnect and data traffic is not interrupted when the port mode is changed on the fixed module.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click **Configure Unified Ports**.

Step 5 Review the confirmation message and click one of the following:

- **Yes**—To continue with configuring the port mode.
- **No**—To exit without configuring the port mode, and, wait for an appropriate maintenance window.

Step 6 In the **Configure Unified Ports** dialog box, use your mouse to drag the slider along the bar, from right to left, until the display shows the port-mode configuration that you want for the module.

To unconfigure Unified Ports, use your mouse to drag the slider along the bar, from left to right. When you unconfigure the unified port, it defaults to Ethernet Uplink port.

Step 7 Click **OK** to save your port-mode configuration.

The fabric interconnect reboots. All data traffic through that fabric interconnect is interrupted. If this occurs in a cluster configuration that provides high availability and includes servers with vNICs that are configured for failover, traffic fails over to the other fabric interconnect and no interruption occurs.

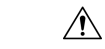
What to do next

Configure the port types for the ports. You can right-click on any port in the module display above the slider and configure that port for an available port type.

Configuring Port Modes for a 64108 Fabric Interconnect

On the UCS 64108 Fabric Interconnect, the first 16 ports are unified ports and can be configured as FC ports in groups of 4 or 8 ports by one of the following ways:

- First 4 ports - Ports 1 to 4 on the Fabric Interconnect
- First 8 ports - Ports 1 to 8 on the Fabric Interconnect



Caution Changing the port mode can cause an interruption in data traffic and lead to immediate Fabric Interconnect reboot.

If the Cisco UCS domain has a cluster configuration that is set up for high availability and servers with service profiles that are configured for failover, traffic fails over to the other fabric interconnect and data traffic is not interrupted when the port mode is changed on the fixed module.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click **Configure Unified Ports**.

Step 5 Review the confirmation message and click one of the following:

- **Yes**—To continue with configuring the port mode.
- **No**—To exit without configuring the port mode, and, wait for an appropriate maintenance window.

Step 6 In the **Configure Unified Ports** dialog box, use your mouse to drag the slider along the bar, from left to right, until the display shows the port-mode configuration that you want for the module.

To unconfigure Unified Ports, use your mouse to drag the slider along the bar, from right to left. When you unconfigure the unified port, it defaults to Ethernet Uplink port.

Step 7 If you need to configure port modes for the other module, repeat Steps 5 and 6.

Step 8 Click **OK** to save your port-mode configuration.

The fabric interconnect reboots. All data traffic through that fabric interconnect is interrupted. If this occurs in a cluster configuration that provides high availability and includes servers with vNICs that are configured for failover, traffic fails over to the other fabric interconnect and no interruption occurs.

What to do next

Configure the port types for the ports. You can right-click on any port in the module display above the slider and configure that port for an available port type.

Configuring Port Modes for a 6454 Fabric Interconnect

On the 6454 Fabric Interconnect, the first 16 ports are unified ports and can be configured as FC ports in groups of 4 or 8 ports by one of the following ways:

- First 4 ports - Ports 1 to 4 on the Fabric Interconnect
- First 8 ports - Ports 1 to 8 on the Fabric Interconnect

Caution Changing the port mode can cause an interruption in data traffic and lead to immediate Fabric Interconnect reboot.

If the Cisco UCS domain has a cluster configuration that is set up for high availability and servers with service profiles that are configured for failover, traffic fails over to the other fabric interconnect and data traffic is not interrupted when the port mode is changed on the fixed module.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click **Configure Unified Ports**.

Step 5 Review the confirmation message and click one of the following:

- **Yes**—To continue with configuring the port mode.
- **No**—To exit without configuring the port mode, and, wait for an appropriate maintenance window.

Step 6 In the **Configure Unified Ports** dialog box, use your mouse to drag the slider along the bar, from left to right, until the display shows the port-mode configuration that you want for the module.

To unconfigure Unified Ports, use your mouse to drag the slider along the bar, from right to left. When you unconfigure the unified port, it defaults to Ethernet Uplink port.

Step 7 If you need to configure port modes for the other module, repeat Steps 5 and 6.

Step 8 Click **OK** to save your port-mode configuration.

The fabric interconnect reboots. All data traffic through that fabric interconnect is interrupted. If this occurs in a cluster configuration that provides high availability and includes servers with vNICs that are configured for failover, traffic fails over to the other fabric interconnect and no interruption occurs.

What to do next

Configure the port types for the ports. You can right-click on any port in the module display above the slider and configure that port for an available port type.

Reconfiguring a Port on a Fabric Interconnect

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.
Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.
Step 3 Expand the node for the ports that you want to reconfigure.
Step 4 Click the port or ports that you want to reconfigure.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 In the **Actions** area, click **Reconfigure**.
Step 7 From the drop-down list, choose which way you want the port reconfigured.

Example: Reconfiguring an Uplink Ethernet Port as a Server Port

1. Expand the **Ethernet Ports** node and select the port you want to reconfigure.
2. Follow steps 5 and 6 above.
3. From the drop-down list choose **Configure as Server Port**.

Enabling or Disabling a Port on a Fabric Interconnect

After you enable or disable a port on a fabric interconnect, wait for at least 1 minute before you re-acknowledge the chassis. If you re-acknowledge the chassis too soon, the pinning of server traffic from the chassis might not get updated with the changes to the port that you enabled or disabled.

You can enable or disable a port only when it is configured. If the port is unconfigured, the enable and disable options are not active.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.
Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.
Step 3 Expand the node for the ports that you want to enable or disable.
Step 4 Under the **Ethernet Ports** node, select a port.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 In the **Actions** area, click **Enable Port** or **Disable Port**.

Step 7 If a confirmation dialog box displays, click **Yes**.

Step 8 Click **OK**.

Unconfiguring a Port on a Fabric Interconnect

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 Expand the node for the ports that you want to unconfigure.

Step 4 Under the **Ethernet Ports** node, select a port.

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

Step 6 In the **Actions** area, click **Unconfigure**.

Step 7 If a confirmation dialog box displays, click **Yes**.

Step 8 Click **OK**.

Server Ports

Automatic Configuration of Fabric Interconnect Server Ports

Starting with Cisco UCS Manager release 3.1(3), you can automatically configure the fabric interconnect server ports. The server **Port Auto-Discovery Policy** determines how the system reacts when a new rack server, chassis, or FEX is added. By enabling this policy, Cisco UCS Manager automatically determines the type of device connected to the switch port and configures the switch port accordingly.

Note

- If you do not want a Cisco UCS C-Series appliance to be UCS Managed, pre-configure the appliance ports before connecting VIC ports to the Cisco UCS Fabric Interconnects.
- The **Port Auto-Discovery Policy** is not applicable for servers connected through direct 25G port or 4x25g breakout on Cisco UCS 6454, UCS 64108, and 6536 Fabric Interconnects.

Automatically Configuring Server Ports

Procedure

Step 1 In the Navigation pane, click **Equipment**.

Step 2 Expand **Equipment** > **Policies** > **Port Auto-Discovery Policy**.

Step 3 In the **Port Auto-Discovery Policy** actions area, by default the policy is set to **Local**. The policy is determined and managed by Cisco UCS Manager. In this case, **Use Global** is visible in Cisco UCS Manager.

To have the port auto-discovery policy managed by Cisco UCS Central, refer *Registering a Cisco UCS Domain with Cisco UCS Central* in the Cisco UCS Manager Server Management Guide.

Step 4 In the **Properties** area complete the following fields:

Name	Description
Owner field	If set to local, the policy is determined and managed by Cisco UCS Manager. If set to global, the policy is determined and managed by Cisco UCS Central.
Auto Configure Server Port	• **Enabled** - Cisco UCS Manager automatically determines the type of server connected to a switch port and configures the switch port accordingly. • **Disabled** - Disables automatic configuration of fabric interconnect server ports.

Configuring Server Ports

All of the port types listed are configurable on both the fixed module and expansion module, including the server ports.

This task describes only one method of configuring ports. You can also configure ports from a right-click menu, or in the LAN Uplinks Manager.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name*** > **Fixed Module** > **Ethernet Ports**.

Step 3 Click a port under the **Ethernet Ports** node.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Reconfigure**.

Step 6 From the drop-down list, choose **Configure as Server Port**.

Modifying the Properties of a Server Port

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 Expand the node for the server port that you want to modify.

Step 4 Expand **Ethernet Ports**.

Step 5 Click the server port for which you want to modify the properties.

Step 6 In the **Work** pane, click the **General** tab.

Step 7 In the **Actions** area, click **Show Interface**.

You may need to expand the pane or use the scroll bars in the **Properties** dialog box to see all the fields.

Step 8 In the **Properties** dialog box, modify the values as needed.

Step 9 Click **OK**.

Configuring a Server Port for Forward Error Correction

The N9K-C93180YC-FX3 in FEX mode connects to 25Gbps or 100Gbps server port on the Cisco UCS 6400 series Fabric Interconnects. To have the link-up at 25Gbps, the server port on Cisco UCS 6400 series Fabric Interconnect requires forward error correction (FEC) of CL-74. This CL-74 configuration on the server port is required only for connecting N9K-C93180YC-FX3 to Cisco UCS 6400 series Fabric Interconnects.

For Cisco UCS 6500 Series Fabric Interconnect, the N9K-C93180YC-FX3 in FEX mode connects to Fabric Interconnect at 100Gbps server port. To have the link at 100Gbps, the server port and Cisco UCS 6500 Series Fabric Interconnect requires forward error correction (FEC) of CL-91.

Note The CL-74 configuration is not applicable for other server port connectivity such as I/O module or direct-attached rack server.

Table 4: FEC CL-74 Support Matrix

Port Speed	FEC CL-74
1 Gbps	Not supported
10 Gbps	Not supported
25 Gbps	Supported
40 Gbps	Not supported

Port Speed	FEC CL-74
100 Gbps	Supported
Auto	Based on inserted tranceiver's maximum supported speed

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 Expand the node for the server ports that you want to configure.

Step 4 Select **Show Interface**.

Step 5 Choose **Eth Server**.

Step 6 Select **Auto** or **Cl74** to set the forward error correction mode as for the server port. **Auto** is the default option.

Step 7 Select **Enabled** or **Disabled** to set the auto negotiation for the server port. **Enabled** is the default option.

Step 8 Click **OK**.

Note
Following are the mandatory configuration parameters on the server port for connecting to N9K-C93180YC-FX3:

- The FEC must be **Auto** for 100Gps server port.
- The FEC must be **Cl74** for 25Gps server port.
- The auto-negotiation must be **Disabled** for 100Gps server port.

Uplink Ethernet Ports

Configuring Uplink Ethernet Ports

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

This task describes only one method of configuring uplink Ethernet ports. You can also configure uplink Ethernet ports from a right-click menu.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 Expand the node for the ports that you want to configure.

Step 4 Click on one of the ports under the **Ethernet Ports** node.

If you want to reconfigure a server port, appliance port, or FCoE storage port, expand the appropriate node.

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

Step 6 In the **Actions** area, click **Reconfigure**.

Step 7 From the drop-down list choose **Configure as Uplink Port**.

What to do next

If desired, change the properties for the default flow control policy and admin speed of the uplink Ethernet port.

Changing the Properties of an Uplink Ethernet Port

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 Expand the node for the ports that you want to configure.

Step 4 In the **Ethernet Ports** node, click the uplink Ethernet port that you want to change.

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

Step 6 In the **Actions** area, click **Show Interface**.

Step 7 In the **Properties** dialog box, complete the following fields:

a) (Optional) In the **User Label** field, enter a label to identify the port.

b) From the **Flow Control Policy** drop-down list, select a flow control policy to determine how the port sends and receives IEEE 802.3x pause frames when the receive buffer fills.

c) In the **Admin Speed** field, click one of the following radio buttons:

- 1 Gbps
- 10 Gbps
- 25 Gbps
- 40 Gbps
- 100 Gbps

Note
25 Gbps can be selected for ports 1 to 48 only on Cisco UCS 6454 Fabric Interconnects. 40 Gbps and 100 Gbps speeds are only for ports 49 to 54 on Cisco UCS 6454 Fabric Interconnects.

25 Gbps can be selected for ports 1 to 96 only on Cisco UCS 64108 Fabric Interconnects. 40 Gbps and 100 Gbps speeds are only for ports 97 to 108 on Cisco UCS 64108 Fabric Interconnects.

25 Gbp, 40 Gbps and 100 Gbpss can be selected for ports 1 to 36 only on Cisco UCS 6500 series Fabric Interconnects.

Step 8 Click **OK**.

Configuring an Ethernet Port for Forward Error Correction

You can configure forward error correction (FEC) for uplink Ethernet ports, Ethernet appliances, and FCoE uplinks for transceiver modules.

Table 5: Supported Port Speed and FEC Matrix

Port Speed	FEC CL-74	FEC CL-91	RS Cons 16	RS 1eee
1 Gbps	Not supported	Not supported	-	-
10 Gbps	Not supported	Not supported	Not supported	Not supported
25 Gbps	Supported	Supported	Supported	Supported
40 Gbps	Not supported	Not supported	Not supported	Not supported
100 Gbps	Not supported	Supported	Not supported	Not supported
Auto	Automatically selects the optimal FEC mode based on the transceiver's maximum supported speed.	Automatically selects the optimal FEC mode based on the transceiver's maximum supported speed.	Automatically selects the optimal FEC mode based on the transceiver's maximum supported speed.	Automatically selects the optimal FEC mode based on the transceiver's maximum supported speed.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > *Fabric_Interconnect_Name*.

Step 3 Expand the node for the ports that you want to configure.

Step 4 Click on one of the ports under the **Ethernet Ports** node.

If you want to reconfigure a server port, appliance port, or FCoE storage port, expand the appropriate node.

Step 5 Select **Show Interface**.

Step 6 Choose **Uplink Eth Interface** or **Uplink FCoE Interface**.

Step 7 Select **Auto, Cl74, or CL91, RS Cons 16, or RS 1eee** for the forward error correction mode. **Auto** is the default option.

Note

- The Forward Error Correction (FEC) modes for **RS Cons 16** and **RS 1eee** are supported only on 25 Gbps speed.
- The FEC is not supported in breakout port mode or in Ethernet port channels.

Step 8 Click **OK**.

This sets the forward error correction setting for the Ethernet uplink port.

Note
For Cisco UCS 6400and 6500 Series Fabric Interconnects, the FEC is only configurable for 25 Gbps or 100 Gbps port speed.

Q-in-Q Forwarding

QinQ is defined by IEEE 802.1ad. QinQ is also known as 802.1Q-in-802.1Q that helps to expand the VLAN space through the addition of 802.1Q tag to 802.1Q-tagged packets. This expansion is also termed as VLAN stacking or double VLAN.

In general, the QinQ packets have a standard format. In a VLAN stacking, one 802.11Q tagged packet is encapsulated in another 802.1Q tag. During transmission, packets are forwarded on the outer VLAN tag on the public network and on the inner VLAN tag for private network.

Note The 802.1Q supports 4096 VLANs.

Configuring Q-in-Q Forwarding

You can configure Q-in-Q Forwarding on Cisco UCS 6400 Series Fabric Interconnects, Cisco UCS 6536 Fabric InterconnectCisco UCS Fabric Interconnects 9108 100G, and Cisco UCS 6664 Fabric Interconnect.

To configure Q-in-Q Forwarding, do the following:

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud**.

Step 3 In the **Work** pane, click the **Global Policies** tab.

Step 4 In the **Q-in-Q Forwarding** section, click to select **Enabled** radio button.

Step 5 Click **Save Changes**.

Step 6 If the **Q-in-Q Forwarding** option is successfully selected, a confirmation message displays. Click **OK** to close the dialog box.

Note
Q-in-Q Forwarding is a prerequisite for **Enable QinQ** and **QinQ VLAN**. If you want to choose **Enable QinQ** on a vLAN, ensure **Q-in-Q Forwarding** field enabled.

Unconfiguring Q-in-Q Forwarding

You can unconfigure Q-in-Q Forwarding on Cisco UCS 6400 Series Fabric Interconnects, Cisco UCS 6536 Fabric InterconnectCisco UCS Fabric Interconnects 9108 100G, and Cisco UCS 6664 Fabric Interconnect. By default, Q-in-Q Forwarding is disabled.

To unconfigure Q-in-Q Forwarding, do the following:

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud**.

Step 3 In the **Work** pane, click the **Global Policies** tab.

Step 4 In the **Q-in-Q Forwarding** section, choose **Disabled**.

Step 5 Click **Save Changes**.

Step 6 If the **Q-in-Q Forwarding** option is successfully disabled, a confirmation message displays. Click **OK** to close the dialog box.

Appliance Ports

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

Note When you create a new appliance VLAN, its IEEE VLAN ID is not added to the LAN Cloud. Therefore, appliance ports that are configured with the new VLAN remain down, by default, due to a pinning failure. To bring up these appliance ports, you have to configure a VLAN in the LAN Cloud with the same IEEE VLAN ID.

Cisco UCS Manager supports up to four appliance ports per fabric interconnect.

Configuring an Appliance Port

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

This task describes only one method of configuring appliance ports. You can also configure appliance ports from the **General** tab for the port.

Note If you configure an appliance port when the uplink port is down, Cisco UCS Manager may display an error message stating that the appliance port has failed. This message is controlled by the **Action on Uplink Fail** option in the associated Network Control Policy.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 Expand the node for the ports that you want to configure.

Step 4 Under the **Ethernet Ports** node, select a port.

If you want to reconfigure a server port, uplink Ethernet port, or FCoE storage port, expand the appropriate node.

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

Step 6 In the **Actions** area, click **Reconfigure**.

Step 7 From the drop-down list, click **Configure as Appliance Port**.

Step 8 If a confirmation dialog box displays, click **Yes**.

Step 9 In the **Configure as Appliance Port** dialog box, complete the required fields.

Step 10 In the **VLANs** area, do the following:

a) In the **Port Mode** field, click one of the following radio buttons to select the mode you want to use for the port channel:

- **Trunk**—Cisco UCS Manager GUI displays the VLANs Table that lets you choose the VLANs you want to use.
- **Access**—Cisco UCS Manager GUI displays the **Select VLAN** drop-down list that allows you to choose a VLAN to associate with this port or port channel.

With either mode, you can click the **Create VLAN** link to create a new VLAN.

Note
If traffic for the appliance port needs to traverse the uplink ports, you must also define each VLAN used by this port in the LAN cloud. For example, you need the traffic to traverse the uplink ports if the storage is also used by other servers, or if you want to ensure that traffic fails over to the secondary fabric interconnect if the storage controller for the primary fabric interconnect fails.

b) If you clicked the **Trunk** radio button, complete the required fields in the VLANs table.

c) If you clicked the **Access** radio button, choose a VLAN from the **Select VLAN** drop-down list.

Step 11 (Optional) If you want to add an endpoint, check the **Ethernet Target Endpoint** check box and specify the name and MAC address.

Step 12 Click **OK**.

Modifying the Properties of an Appliance Port

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > *Fabric_Interconnect_Name*.

Step 3 Expand the node for the appliance port that you want to modify.

Step 4 Expand **Ethernet Ports**.

Step 5 Click the appliance port for which you want to modify the properties.

Step 6 In the **Work** pane, click the **General** tab.

Step 7 In the **Actions** area, click **Show Interface**.

You may need to expand the pane or use the scroll bars in the **Properties** dialog box to see all the fields.

Step 8 In the **Properties** dialog box, modify the values as needed.

Step 9 Click **OK**.

Configuring an Appliance Port for Forward Error Correction

You can configure forward error correction (FEC) for appliance ports that operate at 25 Gbps and 100 Gbps speeds that support this feature.

Table 6: Supported Port Speed and FEC Matrix

Port Speed	FEC CL-74	FEC CL-91	RS Cons 16	RS 1eee
1 Gbps	Not supported	Not supported	-	-
10 Gbps	Not supported	Not supported	Not supported	Not supported
25 Gbps	Supported	Supported	Supported	Supported
40 Gbps	Not supported	Not supported	Not supported	Not supported
100 Gbps	Not supported	Supported	Not supported	Not supported
Auto	Automatically selects the optimal FEC mode based on the transceiver's maximum supported speed.	Automatically selects the optimal FEC mode based on the transceiver's maximum supported speed.	Automatically selects the optimal FEC mode based on the transceiver's maximum supported speed.	Automatically selects the optimal FEC mode based on the transceiver's maximum supported speed.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.
Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.
Step 3 Expand the node for the Appliance ports that you want to configure.
Step 4 Select **Show Interface**.
Step 5 Choose **Appliance Port**.
Step 6 Select **Auto, CL-74, CL-91, Rs Cons 16, or Rs 1eee** to set the forward error correction mode. **Auto** is the default option.
Step 7 Select **Enabled** or **Disabled** to set the auto negotiation for the Appliance port. **Enabled** is the default option.
Step 8 Click **OK**.

Modifying an Appliance Breakout Port for Forward Error Correction

You can configure forward error correction (FEC) for appliance breakout ports.

Table 7: FEC CL-74 and FEC CL-91 Support Matrix

BreakoutType	Port Speed	Forward Error Correction	Allowed
25x4	25 Gbps	Auto	Yes
25x4	25 Gbps	CL74	Yes
25x4	25 Gbps	CL91	Yes
25x4	Auto	Auto	Yes
v	Auto	CL74	No
25x4	Auto	CL91	No

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.
Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.
Step 3 Expand the node for the Appliance ports that you want to configure.
Step 4 Select **Show Interface**.
Step 5 Choose **Appliance Port**.
Step 6 Select **Auto** or **CL-74** or **CL-91**to set the forward error correction mode as for the Appliance port. **Auto** is the default option.
Step 7 Select **Enabled** or **Disabled** to set the auto negotiation for the Appliance port. **Enabled** is the default option.

Step 8 Click **OK**.

FCoE and Fibre Channel Storage Ports

Configuring an Ethernet Port as an FCoE Storage Port

You can configure FCoE storage ports on either the fixed module or an expansion module.

This task describes only one method of configuring FCoE storage ports. You can also configure FCoE storage ports from the **General** tab for the port.

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.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > *Fabric_Interconnect_Name*.

Step 3 Depending upon the location of the ports you want to configure, expand one of the following:

- **Fixed Module**
- **Expansion Module**

Step 4 Click one or more of the ports under the **Ethernet Ports** node.

If you want to reconfigure an uplink Ethernet port, server port, or appliance port, expand the appropriate node.

Step 5 Right-click the selected port or ports and choose **Configure as FCoE Storage Port**.

On Cisco UCS 6454 Fabric Interconnects, ports 49-54 cannot be configured as FCoE storage ports.

On Cisco UCS 64108 Fabric Interconnects, ports 97-108 cannot be configured as FCoE storage ports.

On Cisco UCS 6536 Fabric Interconnects, ports 1-32 cannot be configured as FCoE storage ports.

On Cisco UCS Fabric Interconnects 9108 100G, ports 3-8 cannot be configured as FCoE storage ports.

Step 6 If a confirmation dialog box displays, click **Yes**.

Step 7 Click **OK**.

Configuring a Fibre Channel Storage Port

This task describes only one method of configuring FC storage ports. You can also configure FC storage ports from the **General** tab for the port.

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.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.
Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.
Step 3 Expand the **Expansion Module** node.
Step 4 Click one or more of the ports under the **FC Ports** node.
Step 5 Right-click the selected port or ports and choose **Configure as FC Storage Port**.
Step 6 If a confirmation dialog box displays, click **Yes**.
Step 7 Click **OK**.

Restoring an Uplink Fibre Channel Port

This task describes only one method of restoring an FC storage port to function as an uplink FC port. You can also reconfigure FC storage ports from the **General** tab for the port.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.
Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.
Step 3 Expand the **Expansion Module** node.
Step 4 Click one or more of the ports under the **FC Ports** node.
Step 5 Right-click the selected port or ports and choose **Configure as Uplink Port**.
Step 6 If a confirmation dialog box displays, click **Yes**.
Step 7 Click **OK**.

Note
During the initial bring-up of a Fibre Channel (FC) uplink, such as when enabling a port or after a Fabric Interconnect reboot, it is normal to observe transient discards or cyclic redundancy check (CRC) errors on the peer interface, such as a Cisco MDS switch. These errors may occur during the link negotiation and stabilization process. If the error count stops incrementing once the uplink is operational and normal traffic is flowing, these transient errors are considered normal behavior and do not require further action.

Converting FC Storage Port to FC Uplink Port

You can configure an FC Uplink port on either a fixed module or an expansion module.

This task describes only one method of configuring FC Uplink ports. You can also configure FC uplink ports from a right-click menu for the port.

Important The fill pattern is greyed out and is automatically set to IDLE on Cisco UCS Fabric Interconnects 9108 100G (Cisco UCS X-Series Direct), Cisco UCS 6500 Series Fabric Interconnects and Cisco UCS 6400 Series Fabric Interconnect.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 Expand the node for the ports that you want to configure.

Step 4 Under the **FC Ports** node, select any **Storage** port.

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

Step 6 From the **Actions** area, select **Configure as Uplink Port**.

Step 7 If a confirmation dialog box displays, click **Yes**.

Step 8 The Cisco UCS Manager GUI displays a success message.

In the **Actions** area, **Configure as Uplink Port** becomes grayed out and **Configure as FC Storage Port** becomes active.

Configuring FCoE Uplink for Forward Error Correction

Cisco UCS Manager Release 4.3(4b) introduces support for FCoE uplink ports in Fibre Channel switch mode on the Cisco UCS Fabric Interconnects 9108 100G.

Cisco UCS Manager Release 4.2(3b) introduces support for FCoE uplink ports in Fibre Channel switch mode on the Cisco UCS 6536 Fabric Interconnect.

You can configure forward error correction (FEC) for FCoE uplinks that operate at 25 Gbps and 100 Gpbs speeds that support this feature.

Table 8: FEC CL-74 and FEC CL-91 Support Matrix

Port Speed	FEC CL-74	FEC CL-91
1 Gbps	Not supported	Not supported
10 Gbps	Not supported	Not supported

Port Speed	FEC CL-74	FEC CL-91
25 Gbps	Supported	Supported
40 Gbps	Not supported	Not supported
100 Gbps	Not supported	Supported
Auto	Based on inserted tranceiver's maximum supported speed	Based on inserted tranceiver's maximum supported speed

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope fc-uplink**	Enters FCoE uplink mode.
Step 2	UCS-A /fc-uplink # **scope fabric a** | **b**}	Enters fabric mode for the specified fabric.
Step 3	UCS-A /fc-uplink/fabric # **scope fcoeinterface** *slot-id port-id*	Enters FCoE interface mode for the specified interface.
Step 4	Required: UCS-A /fc-uplink/fabric/fcoeinterface # **set fec** {**auto** |**cl74** | **cl91**}	Sets the forward error correction setting as auto, cl74, or cl91 for the FCoE uplink. For the UCS 6400 Series Fabric Interconnect, Cisco UCS 6536 Fabric Interconnect, and Cisco UCS Fabric Interconnects 9108 100G fabric interconnects, the forward error correction is only configurable for 25 Gbps or 100 Gbps port speeds.
Step 5	UCS-A /fc-uplink/fabric/fcoeinterface # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to enable forward error correction cl74 on an interface for FCoE uplink 35 on slot 1 of fabric A, and commits the transaction:

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope fcoeinterface 1 35
UCS-A /fc-uplink/fabric/fcoeinterface # set fec cl74
UCS-A /fc-uplink/fabric/fcoeinterface # commit-buffer
```

FCoE Uplink Ports

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.

FCoE uplink ports connect to upstream Ethernet switches using the FCoE protocol for Fibre Channel traffic. This allows both the Fibre Channel traffic and Ethernet traffic to flow on the same physical Ethernet link.

Note FCoE uplinks and unified uplinks enable the multi-hop FCoE feature, by extending the unified fabric up to the distribution layer switch.

You can configure the same Ethernet port as any of the following:

- **FCoE uplink port**—As an FCoE uplink port for only Fibre Channel traffic.
- **Uplink port**—As an Ethernet port for only Ethernet traffic.
- **Unified uplink port**—As a unified uplink port to carry both Ethernet and Fibre Channel traffic.

Configuring FCoE Uplink Ports

You can configure an FCoE Uplink port on either a fixed module or an expansion module.

This task describes only one method of configuring FCoE Uplink ports. You can also configure FCoE uplink ports from a right-click menu or from the General tab for the port.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 Expand the node for the ports that you want to configure.

Step 4 Under the **Ethernet Ports** node, select any **Unconfigured** port.

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

Step 6 In the **Actions** area, click **Reconfigure**.

Step 7 From the drop down options, select **Configure as FCoE Uplink Port**.

Step 8 If a confirmation dialog box displays, click **Yes**.

Step 9 The Cisco UCS Manager GUI displays a success message.

In the **Properties** area, the **Role** changes to **Fcoe Uplink**.

Unified Storage Ports

Unified storage involves configuring the same physical port as both an Ethernet storage interface and an FCoE storage interface. You can configure any appliance port or FCoE storage port as a unified storage port. To configure a unified storage port, you must have the fabric interconnect in Fibre Channel switching mode.

In a unified storage port, you can enable or 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 the unified storage port.
- When you enable or disable the appliance interface, the corresponding physical port is enabled or disabled. So when you disable the appliance interface in unified storage, even if the FCoE storage is enabled, it goes down with the physical port.
- When you enable or disable the 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.

Configuring an Appliance Port as a Unified Storage Port

You can configure a unified storage port either from an appliance port or from an FCoE storage port. You can also configure the unified storage port from an unconfigured port. If you start from an unconfigured port, you will assign either an appliance configuration or an FCoE storage configuration to the port, and then will add another configuration to enable it as a unified storage port.

Important Make sure the fabric interconnect is in Fibre Channel switching mode.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 Depending on the location of the ports you want to configure, expand one of the following:

- **Fixed Module**
- **Expansion Module**

Step 4 Under the **Ethernet Ports** node, select any the port that is already configured as an appliance port.

In the **Work** pane, under the **General** tab, in the **Properties** area, the **Role** will show as **Appliance Storage**.

Step 5 In the **Actions** area, click **Reconfigure**.

Step 6 From the pop-up menu, select **Configure as FCoE Storage** port.

Step 7 If a confirmation dialog box displays, click **Yes**.

Step 8 The Cisco UCS Manager GUI displays a success message. In the **Properties** area, the **Role** changes to **Unified Storage**.

Unconfiguring a Unified Storage Port

You can unconfigure and remove both configurations from the unified connect port. Or you can unconfigure either of them and retain the other on the port.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 Expand the node for the ports that you want to unconfigure.

Step 4 Under the **Ethernet Ports** node, select the port that you want to unconfigure.

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

Step 6 In the **Actions** area, click **Unconfigure**. You will see the following options:

- **Unconfigure FCoE Storage Port**
- **Unconfigure Appliance Port**
- **Unconfigure both**

Step 7 Select one of the unconfigure options.

Step 8 If a confirmation dialog box displays, click **Yes**.

Step 9 The Cisco UCS Manager GUI displays a success message. In the **Properties** area, the **Role** changes to based on your unconfigure selection.

Unified Uplink Ports

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

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

If you disable an Ethernet uplink, it disables the underlying physical port in a unified uplink. Therefore, even when 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.

Configuring Unified Uplink Ports

You can configure the unified uplink port from either of the following:

- From an existing FCoE uplink port or Ethernet uplink port
- From an unconfigured uplink port

You can configure the unified uplink port on either a fixed module or on an expansion module.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.
Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.
Step 3 Expand the node for the ports that you want to configure.
Step 4 Under the **Ethernet Ports** node, select a port.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 In the **Properties** area, make sure the **Role** shows as **Fcoe Uplink**.
Step 7 In the **Actions** area, click **Reconfigure**.
Step 8 From the drop-down options, select **Configure as Uplink Port**.
Step 9 If a confirmation dialog box displays, click **Yes**.
Step 10 The Cisco UCS Manager GUI displays a success message.

In the **Properties** area, the **Role** changes to **Unified Uplink**.

Unconfiguring a Unified Storage Port

You can unconfigure and remove both configurations from the unified connect port. Or you can unconfigure either of them and retain the other on the port.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.
Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.
Step 3 Expand the node for the ports that you want to unconfigure.
Step 4 Under the **Ethernet Ports** node, select the port that you want to unconfigure.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 In the **Actions** area, click **Unconfigure**. You will see the following options:

- **Unconfigure FCoE Storage Port**
- **Unconfigure Appliance Port**
- **Unconfigure both**

Step 7 Select one of the unconfigure options.
Step 8 If a confirmation dialog box displays, click **Yes**.
Step 9 The Cisco UCS Manager GUI displays a success message. In the **Properties** area, the **Role** changes to based on your unconfigure selection.

Uplink Ethernet Port Channels

An uplink Ethernet port channel allows you to group several physical uplink Ethernet ports (link aggregation) to create one logical Ethernet link to provide fault-tolerance and high-speed connectivity. In Cisco UCS Manager, you create a port channel first and then add uplink Ethernet ports to the port channel. You can add up to 16 uplink Ethernet ports to a port channel.

Important The state of a configured port changes to unconfigured in the following scenarios:

- The port is deleted or removed from a port channel. The port channel can be of any type, such as, uplink or storage.
- A port channel is deleted.

Note Cisco UCS uses Link Aggregation Control Protocol (LACP), not Port Aggregation Protocol (PAgP), to group the uplink Ethernet ports into a port channel. If the ports on the upstream switch are not configured for LACP, the fabric interconnects treat all ports in an uplink Ethernet port channel as individual ports, and therefore forward packets.

Creating an Uplink Ethernet Port Channel

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud**.

Step 3 Expand the node for the fabric interconnect where you want to add the port channel.

Step 4 Right-click the **Port Channels** node and choose **Create Port Channel**.

Step 5 In the **Set Port Channel Name** panel, specify the ID and name, then click **Next**.

Step 6 In the **Add Ports** panel, specify the ports that you want to add.

Note
Cisco UCS Manager warns you if you select a port that has been configured as a server port. You can click **Yes** in the dialog box to reconfigure that port as an uplink Ethernet port and include it in the port channel.

Step 7 Click **Finish**.

Enabling an Uplink Ethernet Port Channel

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **LAN** > **LAN Cloud**.
Step 3 Expand the node for the fabric interconnect that includes the port channel you want to enable.
Step 4 Expand the **Port Channels** node.
Step 5 Right-click the port channel you want to enable and choose **Enable Port Channel**.
Step 6 If a confirmation dialog box displays, click **Yes**.

Disabling an Uplink Ethernet Port Channel

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **LAN** > **LAN Cloud**.
Step 3 Expand the node for the fabric interconnect that includes the port channel you want to disable.
Step 4 Expand the **Port Channels** node.
Step 5 Right-click the port channel you want to disable and choose **Disable Port Channel**.

Adding Ports to and Removing Ports from an Uplink Ethernet Port Channel

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **LAN** > **LAN Cloud** > ***Fabric*** > **Port Channels**.
Step 3 Click the port channel to which you want to add or remove ports.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Actions** area, click **Add Ports**.
Step 6 In the **Add Ports** dialog box, do one of the following:

- To add ports, choose one or more ports in the **Ports** table, and then click the >> button to add the ports to the **Ports in the port channel** table.
- To remove ports, choose one or more ports in the **Ports in the port channel** table, and then click the << button to remove the ports from the port channel and add them to the **Ports** table.

Step 7 Click **OK**.

Deleting an Uplink Ethernet Port Channel

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **LAN** > **LAN Cloud**.
Step 3 Expand the node for the fabric interconnect where you want to delete the port channel.
Step 4 Click the **Port Channels** node.
Step 5 In the **General** tab for the **Port Channels** node, choose the port channel that you want to delete.
Step 6 Right-click the port channel and choose **Delete**.

Appliance Ports

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

Note When you create a new appliance VLAN, its IEEE VLAN ID is not added to the LAN Cloud. Therefore, appliance ports that are configured with the new VLAN remain down, by default, due to a pinning failure. To bring up these appliance ports, you have to configure a VLAN in the LAN Cloud with the same IEEE VLAN ID.

Cisco UCS Manager supports up to four appliance ports per fabric interconnect.

Creating an Appliance Port Channel

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **LAN** > **Appliances**.
Step 3 Expand the node for the fabric interconnect where you want to add the port channel.
Step 4 Right-click the **Port Channels** node and choose **Create Port Channel**.
Step 5 In the **Set Port Channel Name** panel of the **Create Port Channel** wizard, complete the required fields to specify the identity and other properties of the port channel.

You can create a LAN pin group, network control policy, and flow control policy from this panel.

Step 6 In the **VLANs** area, specify the **Port Mode** and other information for the VLANs.

You can create a VLAN from this panel.

Step 7 (Optional) If you want to add an endpoint, click the **Ethernet Target Endpoint** check box to specify the name and MAC address.

Step 8 Click **Next**.

Step 9 In the **Add Ports** panel of the **Create Port Channel** wizard, specify the ports that you want to add.

Note
Cisco UCS Manager warns you if your configuration could cause issues with service profiles or port configurations. You can click **Yes** in the dialog box if you want to create the port channel despite those potential issues.

Step 10 Click **Finish**.

Enabling an Appliance Port Channel

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Appliances**.

Step 3 Expand the node for the fabric interconnect that includes the port channel you want to enable.

Step 4 Expand the **Port Channels** node.

Step 5 Right-click the port channel you want to enable and choose **Enable Port Channel**.

Step 6 If a confirmation dialog box displays, click **Yes**.

Disabling an Appliance Port Channel

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Appliances**.

Step 3 Expand the node for the fabric interconnect that includes the port channel you want to disable.

Step 4 Expand the **Port Channels** node.

Step 5 Right-click the port channel that you want to disable and choose **Disable Port Channel**.

Step 6 If a confirmation dialog box displays, click **Yes**.

Deleting an Appliance Port Channel

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **LAN** > **Appliances**.
Step 3 Expand the node for the fabric interconnect that includes the port channel you want to delete.
Step 4 Expand the **Port Channels** node.
Step 5 Right-click the port channel you want to enable and choose **Delete**.
Step 6 If a confirmation dialog box displays, click **Yes**.

Adding Ports and Removing Ports within an Appliance Port Channel

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **LAN** > **Appliances** > *Fabric* > **Port Channels**.
Step 3 Click the port channel to which you want to add ports, or from which to remove ports.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Actions** area, click **Add Ports**.
Step 6 In the **Add Ports** dialog box, do one of the following:

- To add ports, choose one or more ports in the **Ports** table, and then click the >> button to add the ports to the **Ports in the port channel** table.
- To remove ports, choose one or more ports in the **Ports in the port channel** table, and then click the << button to remove the ports from the port channel and add them to the **Ports** table.

Step 7 Click **OK**.

Creating a Threshold Definition

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 In the **Admin** tab, expand **All** > **Stats Management** > **fabric** > **Internal LAN** > **thr-policy-default**.
Step 3 Click **Create Threshold Class**.

Step 4 In the **Choose Statistics Class** > **Create Threshold Class**, choose **NI Ether Error Stats** statistics class to monitor network interface ports. You can configure a custom threshold for these ports from the **Stat Class** drop-down list.

Step 5 Click **Next**.

Step 6 In the **Threshold Definitions** screen of the **Create Threshold Class** wizard, click **Add**.

The **Create Threshold Definition** dialog box opens.

a) From the **Property Type** field, choose the threshold property that you want to define for the class.
b) In the **Normal Value** field, enter the desired value for the property type.
c) In the **Alarm Triggers (Above Normal Value)** fields, check one or more of the following check boxes:

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Condition**
- **Info**

d) In the **Up and Down** fields, enter the range of values that should trigger the alarm.
e) In the **Alarm Triggers (Below Normal Value)** fields, click one or more of the following check boxes:

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Condition**
- **Info**

f) In the **Up and Down** fields, enter the range of values that should trigger the alarm.
g) Click **Ok**.

Monitoring a Fabric Port

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 On the **Equipment** tab, expand **Chassis** > **IO Modules** > **IO Module 1** > **Fabric Ports**.

Step 3 Click the fabric port that you want to monitor.

Step 4 Click one of the following tabs to view the status of the fabric:

Option	Description
General	Provides an overview of the status of the fabric, including a summary of any faults, a summary of the fabric properties, and a physical display of the fabric and its components.
Faults	Provides details of the faults generated by the fabric.
Events	Provides details of the events generated by the fabric.
Statistics	Provides statistics about the fabric and its components. You can view these statistics in tabular format or in chart format.

Policy-Based Port Error Handling

If Cisco UCS Manager detects any errors on active network interface (NI) ports, and if the error-disable feature has been implemented, Cisco UCS Manager automatically disables the respective fabric interconnect port that is connected to the NI port that had errors. When a fabric interconnect port is error disabled, it is effectively shut down and no traffic is sent or received on that port.

The error-disable function serves two purposes:

- It lets you know which fabric interconnect port is error-disabled and that the connected NI Port has errors.
- It eliminates the possibility that this port can cause the failure of other ports other ports connected to the same Chassis/FEX. Such a failure can occur when the NI port has errors, which can ultimately cause serious network issues. The error-disable function helps prevent these situations.

Configuring Error-Based Action

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **Admin** > **All** > **Stats Management** > **fabric** > **Internal LAN** > **thr-policy-default** > **etherNiErrStats**.

Step 3 Select a delta property.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 To implement an error-disable state on a fabric interconnect port, check the **Disable FI port when fault is raised** check box.

Step 6 To enable auto recovery, in the **Enable Auto Recovery** field, select **Enable**.

Step 7 To specify the time after which the port can automatically be re-enabled, in the **Time (in minutes)** field, type the desired value.

Step 8 Click **Save Changes**.

FCoE Port Channels

An FCoE port channel allows you to group several physical FCoE ports to create one logical FCoE port channel. At a physical level, the FCoE port channel carries FCoE traffic over an Ethernet port channel. So an FCoE port channel with a set of members is essentially an Ethernet port channel with the same members. This Ethernet port channel is used as a physical transport for FCoE traffic.

For each FCoE port channel, Cisco UCS Manager creates a VFC internally and binds it to an Ethernet port channel. FCoE traffic received from the hosts is sent over the VFC the same way as the FCoE traffic is sent over Fibre Channel uplinks.

Creating an FCoE Port Channel

Procedure

Step 1 In the **Navigation** pane, click **SAN**.

Step 2 Expand **SAN** > **SAN Cloud**.

Step 3 Expand the node for the fabric where you want to create the port channel.

Step 4 Right-click the **FCoE Port Channels** node and choose **Create FCoE Port Channel**.

Step 5 In the **Set Port Channel Name** panel of the **Create FCoE Port Channel** wizard, specify the ID and name, then click **Next**.

Step 6 In the **Add Ports** panel of the **Create FCoE Port Channel** wizard, specify the ports that you want to add.

Step 7 Click **Finish**.

Deleting an FCoE Port Channel

Procedure

Step 1 In the **Navigation** pane, click **SAN**.

Step 2 On the **SAN** tab, expand **SAN** > **SAN Cloud** > ***Fabric*** > **FCoE Port Channels**.

Step 3 Right-click the port channel you want to delete and choose **Delete**.

Step 4 If a confirmation dialog box displays, click **Yes**.

Unified Uplink Port Channel

When you create an Ethernet port channel and an FCoE port channel with the same ID, it is called a unified uplink port channel. When the unified port channel is created, a physical Ethernet port channel and a VFC

are created on the fabric interconnect with the specified members. The physical Ethernet port channel is used to carry both Ethernet and FCoE traffic. The VFC binds FCoE traffic to the Ethernet port channel.

The following rules will apply to the member port sets of the unified uplink port channel:

- The Ethernet port channel and FCoE port channel on the same ID, must have the same set of member ports.
- When you add a member port channel to the Ethernet port channel, Cisco UCS Manager adds the same port channel to FCoE port channel as well. Similarly, adding a member to the FCoE port channel adds the member port to the Ethernet port channel.
- When you delete a member port from one of the port channels, Cisco UCS Manager automatically deletes the member port from the other port channel.

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

Adapter Port Channels

An adapter port channel groups into one logical link all the physical links going from a Cisco UCS Virtual Interface Card (VIC) into an I/O.

Adapter port channels are created and managed internally by Cisco UCS Manager when it detects that the correct hardware is present. Adapter port channels cannot be configured manually. Adapter port channels are viewable using the Cisco UCS Manager GUI or the Cisco UCS Manager CLI.

Viewing Adapter Port Channels

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > ***Chassis_Number*** > **Servers** > ***Server_Number*** > **Interface Cards**

Step 3 Click the adapter for which you want to view the adapter port channels.

Step 4 In the **Work** pane, click the **DCE Interfaces** tab.

Step 5 To view details of the adapter port channel, click the link in the **Port Channel** column.

Fabric Port Channels

Fabric port channels allow you to group several of the physical links from an IOM and IFM (IOM for Cisco UCS X-Series Servers) to a fabric interconnect into one logical link for redundancy and bandwidth sharing. As long as one link in the fabric port channel remains active, the fabric port channel continues to operate.

If the correct hardware is connected, fabric port channels are created by Cisco UCS Manager in the following ways:

- During chassis discovery according to the settings configured in the chassis discovery policy.
- After chassis discovery according to the settings configured in the chassis connectivity policy for a specific chassis.

For each IOM and IFM (IOM for Cisco UCS X-Series Servers) there is a single fabric port channel. Each uplink connecting an IOM and IFM (IOM for Cisco UCS X-Series Servers) to a fabric interconnect can be configured as a discrete link or included in the port channel, but an uplink cannot belong to more than one fabric port channel. For example, if a chassis with two IOMs is discovered and the chassis discovery policy is configured to create fabric port channels, Cisco UCS Manager creates two separate fabric port channels: one for the uplinks connecting IOM-1 and another for the uplinks connecting IOM-2. No other chassis can join these fabric port channels. Similarly, uplinks belonging to the fabric port channel for IOM-1 cannot join the fabric port channel for IOM-2.

Load Balancing Over Ports

Load balancing traffic among ports between IOMs and fabric interconnects uses the following criteria for hashing.

- For Ethernet traffic:

  Layer 2 source and destination address

  Layer 3 source and destination address

  Layer 4 source and destination ports

- For FCoE traffic:

  Layer 2 source and destination address

  Source and destination IDs (SID and DID) and Originator Exchange ID (OXID)

In this example, a 2200 Series IOM module is verified by connecting iom *X* (where *X* is the chassis number).

```
show platform software fwmctrl nifport
(....)
 Hash Parameters:
   l2_da: 1 l2_sa: 1 l2_vlan: 0
   l3_da: 1 l3_sa: 1
   l4_da: 1 l4_sa: 1
   FCoE l2_da: 1 l2_sa: 1 l2_vlan: 0
   FCoE l3_did: 1 l3_sid: 1 l3_oxid: 1
```

Configuring a Fabric Port Channel

Procedure

Step 1 To include all links from the IOM to the fabric interconnect in a fabric port channel during chassis discovery, set the link grouping preference in the chassis discovery policy to port channel.

See the *Configuring the Chassis/FEX Discovery Policy* section in *Cisco UCS Manager Infrastructure Management Guide, Release 3.2*.

Step 2 To include links from an individual chassis in a fabric port channel during chassis discovery, set the link grouping preference in the chassis connectivity policy to port channel.

See the *Configuring a Chassis Connectivity Policy* section in *Cisco UCS Manager Infrastructure Management Guide, Release 3.2*.

Step 3 After chassis discovery, enable or disable additional fabric port channel member ports.

See Enabling or Disabling a Fabric Port Channel Member Port, on page 77

What to do next

To add or remove chassis links from a fabric port channel after making a change to the chassis discovery policy or the chassis connectivity policy, reacknowledge the chassis. Chassis reacknowledgement is not required to enable or disable chassis member ports from a fabric port channel.

Viewing Fabric Port Channels

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **IO Modules**.

Step 3 Click the IOM for which you want to view the fabric port channels.

Step 4 In the **Work** pane, click the **Fabric Ports** tab.

Step 5 To view details of the fabric port channel, click the link in the **Port Channel** column.

Enabling or Disabling a Fabric Port Channel Member Port

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Internal LAN** > ***Fabric*** > **Port Channels**.

Step 3 Expand the port channel for which you want to enable or disable a member port.

Step 4 Click the Ethernet interface for the member port that you want to enable or disable.

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

Step 6 In the **Actions** area, click one of the following:

- **Enable Interface**
- **Disable Interface**

Step 7 If a confirmation dialog box displays, click **Yes**.

Configuring Server Ports with the Internal Fabric Manager

Internal Fabric Manager

The Internal Fabric Manager provides a single interface through which you can configure server ports for a fabric interconnect in a Cisco UCS domain. The Internal Fabric Manager is accessible from the **General** tab for that fabric interconnect.

Some of the configuration that you can do in the Internal Fabric Manager can also be done in nodes on the **Equipment** tab, on the **LAN** tab, or in the LAN Uplinks Manager.

Note Server port configuration are not supported on Cisco UCS X-Series Direct (UCSX-S9108-100G) Fabric Interconnects.

Launching the Internal Fabric Manager

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 Click **Fixed Module**.

Step 4 In the **Work** pane, click **Internal Fabric Manager** in the **Actions** area.

The Internal Fabric Manager opens in a separate window.

Configuring a Server Port with the Internal Fabric Manager

Procedure

Step 1 In the Internal Fabric Manager, click the down arrows to expand the **Unconfigured Ports** area.

Step 2 Right-click the port that you want to configure and choose **Configure as Server Port**.

Step 3 If a confirmation dialog box displays, click **Yes**.

Step 4 If you complete all of the tasks in the Internal Fabric Manager, click **OK**.

Unconfiguring a Server Port with the Internal Fabric Manager

Procedure

Step 1 In the Internal Fabric Manager, click the server port in the **Server Ports** table.
Step 2 Click **Unconfigure Port**.
Step 3 If a confirmation dialog box displays, click **Yes**.
Step 4 If you complete all of the tasks in the Internal Fabric Manager, click **OK**.

Enabling a Server Port with the Internal Fabric Manager

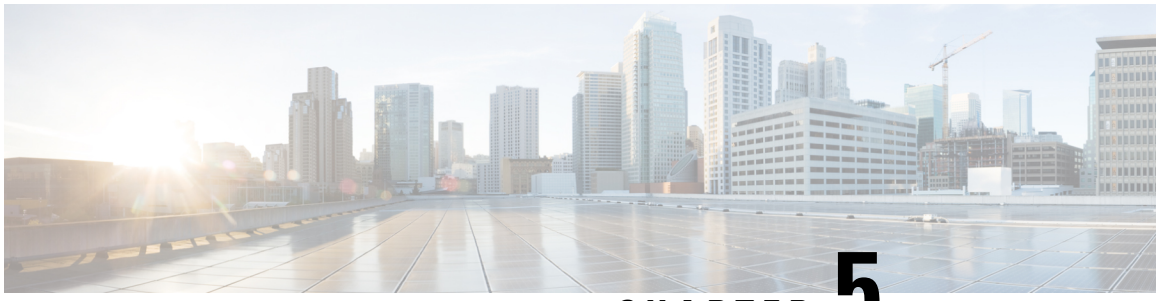
Procedure

Step 1 In the Internal Fabric Manager, click the server port in the **Server Ports** table.
Step 2 Click **Enable Port**.
Step 3 If a confirmation dialog box displays, click **Yes**.
Step 4 If you complete all of the tasks in the Internal Fabric Manager, click **OK**.

Disabling a Server Port with the Internal Fabric Manager

Procedure

Step 1 In the Internal Fabric Manager, click the server port in the **Server Ports** table.
Step 2 Click **Disable Port**.
Step 3 If a confirmation dialog box displays, click **Yes**.
Step 4 If you complete all of the tasks in the Internal Fabric Manager, click **OK**.



CHAPTER 5

LAN Uplinks Manager

LAN Uplinks Manager

The LAN Uplinks Manager provides a single interface where you can configure the connections between Cisco UCS and the LAN. You can use the LAN Uplinks Manager to create and configure the following:

- Ethernet switching mode
- Uplink Ethernet ports
- Port channels
- LAN pin groups
- Named VLANs
- Server ports
- QoS system classes
- You can view Ethernet related events, faults, and FSM status using the tab available at the top in LAN Uplinks Manager.

Some of the configuration that you do in the LAN Uplinks Manager can also be done in nodes on other tabs, such as the **Equipment** tab or the **LAN** tab.

Launching the LAN Uplinks Manager

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 On the **LAN** tab, click the **LAN** node.

Step 3 In the **Work** pane, click the **LAN Uplinks Manager** link on the **LAN Uplinks** tab.

The LAN Uplinks Manager opens in a separate window.

Changing the Ethernet Switching Mode with the LAN Uplinks Manager

Warning When you change the Ethernet switching mode, Cisco UCS Managerlogs you out and restarts the fabric interconnect. For a cluster configuration, Cisco UCS Manager restarts both fabric interconnects. The second fabric interconnect may take several minutes to complete the change in Ethernet switching mode and become system ready. The system retains the configuration.

While the fabric interconnects are booting, all blade servers lose all LAN and SAN connectivity, causing a complete outage of all services on the blades. This action may cause the operating system to crash.

Procedure

Step 1 In the LAN Uplinks Manager, click **LAN Uplinks**.

Step 2 In the **Uplink Mode** area, click one of the following buttons:

- Set **Ethernet Switching Mode**
- Set **Ethernet End-Host Switching Mode**

The button for the current switching mode is dimmed.

Step 3 In the dialog box, click **Yes**.

Cisco UCS Manager restarts the fabric interconnect, logs you out, and disconnects the Cisco UCS Manager GUI.

Configuring a Port with the LAN Uplinks Manager

All port types listed are configurable on both the fixed and expansion module, including server ports.

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Ports** area, click the down arrows to expand the **Unconfigured Ports** section.

Step 3 Expand **Fabric Interconnects** > ***Fabric_Interconnect_Name*** .

Step 4 Expand the node where you want to configure ports.

If no ports are listed below the node that you expanded, all ports in that module have already been configured.

Step 5 Right-click the port that you want to configure and choose one of the following:

- **Configure as Server Port**
- **Configure as Uplink Port**

Step 6 If a confirmation dialog box displays, click **Yes**.

Configuring Server Ports

Enabling a Server Port with the LAN Uplinks Manager

This procedure assumes that the port has been configured as a server port, but is disabled.

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Ports** area, click the down arrows to expand the **Server Ports** section.

Step 3 Expand **Fabric Interconnects** > ***Fabric_Interconnect_Name*** .

Step 4 Right-click the port that you want to enable and choose **Enable**.

Disabling a Server Port with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.
Step 2 In the **Ports** area, click the down arrows to expand the **Server Ports** section.
Step 3 Expand **Fabric Interconnects** > ***Fabric_Interconnect_Name*** .
Step 4 Right-click the port that you want to disable and choose **Disable**.
Step 5 If a confirmation dialog box displays, click **Yes**.

Configuring Uplink Ethernet Ports

Enabling an Uplink Ethernet Port with the LAN Uplinks Manager

This procedure assumes that the port has been configured as an uplink Ethernet port, but is disabled.

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.
Step 2 In the **Port Channels and Uplinks** area, expand **Interfaces** > **Fabric Interconnects** > ***Fabric_Interconnect_Name*** .
Step 3 Right-click the port that you want to enable and choose **Enable Interface**.
Step 4 If a confirmation dialog box displays, click **Yes**.

Disabling an Uplink Ethernet Port with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.
Step 2 In the **Port Channels and Uplinks** area, expand **Interfaces** > **Fabric Interconnects** > ***Fabric_Interconnect_Name*** .
Step 3 Right-click the port that you want to disable and choose **Disable Interfaces**.

You can select multiple ports if you want to disable more than one uplink Ethernet port.

Step 4 If a confirmation dialog box displays, click **Yes**.

The disabled port is removed from the list of enabled interfaces and returned to the **Unconfigured Ports** list.

Configuring Uplink Ethernet Port Channels

Creating a Port Channel with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Port Channels and Uplinks** area, click **Create Port Channel**.

Step 3 From the pop-up menu, select one of the following fabric interconnects where you want to create the port channel:

- **Fabric Interconnect A**
- **Fabric Interconnect B**

Step 4 In the **Set Port Channel Name** panel, specify the ID and name, then click **Next**.

Step 5 In the **Add Ports** panel, specify the ports you want to add.

Note
Cisco UCS Manager warns you if you select a port that has been configured as a server port. You can reconfigure that port as an uplink Ethernet port, and include it in the port channel by clicking **Yes** in the dialog box.

Step 6 Click **Finish**.

Enabling a Port Channel with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Port Channels and Uplinks** area, expand **Port Channels** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 Right-click the port channel that you want to enable and choose **Enable Port Channel**.

Step 4 If a confirmation dialog box displays, click **Yes**.

Disabling a Port Channel with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Port Channels and Uplinks** area, expand **Port Channels** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 Right-click the port channel that you want to disable and choose **Disable Port Channel**.

Step 4 If a confirmation dialog box displays, click **Yes**.

Adding Ports to a Port Channel with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Port Channels and Uplinks** area, expand **Port Channels** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 Right-click the port channel to which you want to add ports and choose **Add Ports**.

Step 4 In the **Add Ports** dialog box, specify the ports that you want to add.

Note
Cisco UCS Manager warns you if you select a port that has been configured as a server port. You can click **Yes** in the dialog box to reconfigure that port as an uplink Ethernet port and include it in the port channel.

Step 5 Click **OK**.

Removing Ports from a Port Channel with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Port Channels and Uplinks** area, expand **Port Channels** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 Expand the port channel from which you want to remove ports.

Step 4 Right-click the port that you want to remove from the port channel and choose **Delete**.

Step 5 If a confirmation dialog box displays, click **Yes**.

Deleting a Port Channel with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Port Channels and Uplinks** area, expand **Port Channels** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 Right-click the port channel you want to delete and choose **Delete**.

Step 4 If a confirmation dialog box displays, click **Yes**.

Configuring LAN Pin Groups

Creating a Pin Group with the LAN Uplinks Manager

In a system with two fabric interconnects, you can associate the pin group with only one fabric interconnect or with both fabric interconnects.

Before you begin

Configure the ports and port channels with which you want to configure the pin group. You can only include ports and port channels configured as uplink ports in a LAN pin group.

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Port Channels and Uplinks** area, click **Create Pin Group**.

Step 3 In the **Create LAN Pin Group** dialog box, enter a unique name and description for the pin group.

Step 4 To pin traffic for fabric interconnect A, do the following in the **Targets** area:

a) Check the **Fabric Interconnect A** checkbox.

b) Click the drop-down arrow on the **Interface** field and navigate through the tree browser to select the port or port channel you want to associate with the pin group.

Step 5 To pin traffic for fabric interconnect B, do the following in the **Targets** area:

a) Check the **Fabric Interconnect B** checkbox.

b) Click the drop-down arrow on the **Interface** field and navigate through the tree browser to select the port or port channel you want to associate with the pin group.

Step 6 Click **OK**.

What to do next

Include the pin group in a vNIC template.

Deleting a Port Channel with the LAN Uplinks Manager

Procedure

Step 1 In the LAN Uplinks Manager, click the **LAN Uplinks** tab.

Step 2 In the **Port Channels and Uplinks** area, expand **Port Channels** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 Right-click the port channel you want to delete and choose **Delete**.

Step 4 If a confirmation dialog box displays, click **Yes**.

Configuring Named VLANs

Creating a Named VLAN with the LAN Uplinks Manager

In a Cisco UCS domain with two switches, you can create a named VLAN that is accessible to both switches or to only one switch.

Table 9: Cisco UCS and fabric interconnect reserved VLANs

Cisco UCS 6400 Series Fabric Interconnects	Cisco UCS 6500 Series Fabric Interconnects	Cisco UCS Fabric Interconnects 9108 100G
VLANs 3915 to 4042 (reserved for Cisco NX-OS)	VLANs 1002 to 1005 (reserved for Cisco NX-OS)	VLANs 1002 to 1005 (reserved for Cisco NX-OS)
VLANs 4043 to 4047 (reserved for Cisco UCS Manager)		
VLANs 4094 to 4098 (reserved for Cisco NX-OS)		

Important VLANs with IDs from 4043 to 4047 and from 4094 to 4095 are reserved. You cannot create VLANs with IDs from this range. Until Cisco UCS Manager Release 4.0(1d), VLAN ID 4093 was in the list of reserved VLANs. VLAN 4093 has been removed from the list of reserved VLANs and is available for configuration.

For Cisco UCS 6600 Series Fabric Interconnect, Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 and 6400 Series Fabric Interconnects, VLAN IDs from 1002 to 1005 are reserved for VLAN Trunking Protocol (VTP).

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

Procedure

Step 1 In the LAN Uplinks Manager, click the **VLANs** tab.

Step 2 On the icon bar to the right of the table, click **+**.

If the **+** icon is disabled, click an entry in the table to enable it.

Step 3 In the **Create VLANs** dialog box, specify the required fields and then click **OK**.

Private VLANs are not supported for Cisco UCS Mini.

Step 4 Click **OK**.

Cisco UCS Manager adds the VLAN to one of the following **VLANs** nodes:

- The **LAN Cloud** > **VLANs** node for a VLAN accessible to both fabric interconnects.
- The ***Fabric_Interconnect_Name*** > **VLANs** node for a VLAN accessible to only one fabric interconnect.

Deleting a Named VLAN with the LAN Uplinks Manager

If Cisco UCS Manager includes a named VLAN with the same VLAN ID as the one you delete, the VLAN is not removed from the fabric interconnect configuration until all named VLANs with that ID are deleted.

Procedure

Step 1 In the LAN Uplinks Manager, click the **VLANs** tab.

Step 2 Click one of the following subtabs, based on the VLAN that you want to delete:

Subtab	Description
All	Displays all VLANs in the Cisco UCS domain.
Dual Mode	Displays the VLANs that are accessible to both fabric interconnects.
Fabric A	Displays the VLANs that are accessible to only fabric interconnect A.
Fabric B	Displays the VLANs that are accessible to only fabric interconnect B.

Step 3 In the table, click the VLAN you want to delete.

You can use the **Shift** key or **Ctrl** key to select multiple entries.

Step 4 Right-click the highlighted VLAN or VLANs and select **Delete**.

Step 5 If a confirmation dialog box displays, click **Yes**.

Configuring QoS System Classes with the LAN Uplinks Manager

The type of adapter in a server might limit the maximum MTU supported. For example, network MTU above the maximums might cause the packet to be dropped for the following adapters:

- The Cisco UCS M71KR CNA adapter, which supports a maximum MTU of 9000.
- The Cisco UCS 82598KR-CI adapter, which supports a maximum MTU of 14000.

Procedure

Step 1 In the LAN Uplinks Manager, click the **QoS** tab.

Step 2 Update the following properties for the system class you want to configure, to meet the traffic management needs of the system:

Note
Some properties may not be configurable for all system classes.

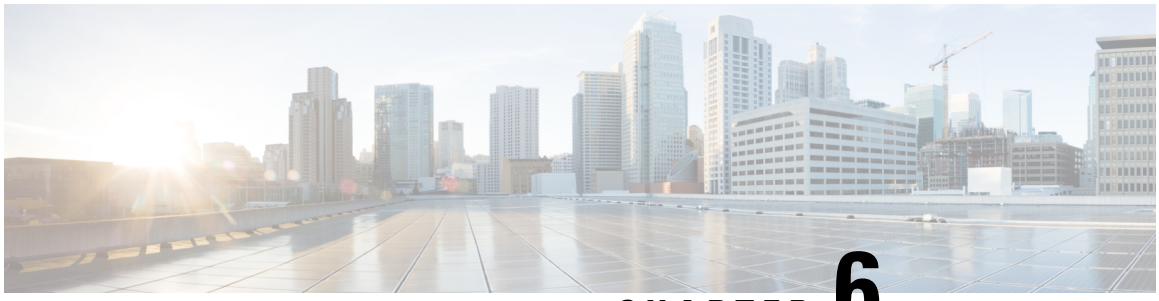
Name	Description
Enabled check box	If checked, the associated QoS class is configured on the fabric interconnect and can be assigned to a QoS policy. If unchecked, the class is not configured on the fabric interconnect and any QoS policies associated with this class default to **Best Effort** or, if a system class is configured with a Cos of 0, to the Cos 0 system class. **Note** This field is always checked for **Best Effort** and **Fibre Channel**.

Name	Description
CoS field	The class of service. You can enter an integer value between 0 and 6, with 0 being the lowest priority and 6 being the highest priority. We recommend that you do not set the value to 0, unless you want that system class to be the default system class for traffic if the QoS policy is deleted or the assigned system class is disabled. **Note** This field is set to 7 for internal traffic and to **any** for **Best Effort**. Both of these values are reserved and cannot be assigned to any other priority.
Packet Drop check box	If checked, packet drop is allowed for this class. If unchecked, packets cannot be dropped during transmission. MTU configuration for drop classes is ignored. This field is always unchecked for the **Fibre Channel** class, which never allows dropped packets, and always checked for **Best Effort**, which always allows dropped packets. **Note** When you save changes to the Packet Drop, the following warning message displays: You are making changes to the QOS system class, which may cause momentary disruption to traffic forwarding. Are you sure you want to apply the changes?
Weight drop-down list	This can be one of the following: • An integer between 1 and 10. If you enter an integer, Cisco UCS determines the percentage of network bandwidth assigned to the priority level as described in the **Weight (%)** field. • **best-effort**. • **none**.
Weight (%) field	To determine the bandwidth allocated to a channel, Cisco UCS: **a.** Adds the weights for all the channels **b.** Divides the channel weight by the sum of all weights to get a percentage **c.** Allocates that percentage of the bandwidth to the channel

Name	Description
MTU drop-down list	The maximum transmission unit for the channel. This can be one of the following: • An integer between 1500 and 9000. This value corresponds to the maximum packet size. **Note** When you save changes to the MTU, the following warning message displays: You are making changes to the QOS system class, which may cause momentary disruption to traffic forwarding. Are you sure you want to apply the changes? • **fc**—A predefined packet size of 2240. • **normal**—A predefined packet size of 1500. **Note** This field is always set to **fc** for **Fibre Channel**. **Note** Under the network QoS policy, the MTU is used only for buffer carving when no-drop classes are configured. No additional MTU adjustments are required under the network QoS policy to support jumbo MTU.
Multicast Optimized check box	If checked, the class is optimized to send packets to multiple destinations simultaneously. **Note** This option is not applicable to the **Fibre Channel**. **Note** Cisco UCS 6400 Series and Cisco UCS 6500 Series Fabric InterconnectFabric Interconnects do not support Multicast Optimized.

Step 3 Do one of the following:

- Click **OK** to save your changes and exit from the LAN Uplinks Manager.
- Click **Apply** to save your changes without exiting from the LAN Uplinks Manager.



CHAPTER 6

VLANs

About VLANs

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment.

Any switch port can belong to a VLAN. Unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or bridge.

VLANs are typically associated with IP subnetworks. For example, all of the end stations in a particular IP subnet belong to the same VLAN. To communicate between VLANs, you must route the traffic. By default, a newly created VLAN is operational. Additionally, you can configure VLANs to be in the active state, which is passing traffic, or in the suspended state, in which the VLANs are not passing packets. By default, the VLANs are in the active state and pass traffic.

You can use the Cisco UCS Manager to manage VLANS. You can do the following:

- Configure named VLANs.
- Assign VLANS to an access or trunk port.

- Create, delete and modify VLANs.

Guidelines for Creating, Deleting, and Modifying VLANs

VLANs are numbered from 1 to 4094. All configured ports belong to the default VLAN when you first bring up a switch. The default VLAN (VLAN1) uses only default values. You cannot create, delete, or suspend activity in the default VLAN.

You configure a VLAN by assigning a number to it. You can delete VLANs or move them from the active operational state to the suspended operational state. If you attempt to create a VLAN with an existing VLAN ID, the switch goes into the VLAN submode, but does not create the same VLAN again. Newly created VLANs remain unused until you assign ports to the specific VLAN. All of the ports are assigned to VLAN1 by default. Depending on the range of the VLAN, you can configure the following parameters for VLANs (except for the default VLAN):

- VLAN name
- Shutdown or not shutdown

When you delete a specified VLAN, the ports associated to that VLAN are shut down and no traffic flows. However, the system retains all of the VLAN-to-port mappings for that VLAN. When you re-enable or recreate the specified VLAN, the system automatically re-instates all of the original ports to that VLAN.

If a vLAN group is used on a vNIC and also on a port-channel assigned to an uplink, then you cannot delete and add vLANs in the same transaction. Deleting and adding vLANs in the same transaction causes ENM pinning failure on the vNIC. vNIC configurations are done first and vLAN is deleted from the vNIC and a new vLAN is added, but this vLAN is not yet configured on the uplink. Hence, the transaction causes the pinning failure. You must add and delete a vLAN from a vLAN group in separate transactions.

If more than 500 VLANs are created or deleted in a single operation, the UCSM GUI automatically logs out to maintain system stability. However, the VLAN create or delete operation succeeds, and you can re-login to verify.

About the Native VLAN

The Native VLAN and the default VLAN serve different purposes within a network. Native VLAN refers to the VLAN that handles untagged traffic—Ethernet frames transmitted without an 802.1Q VLAN tag. Native VLAN traffic is untagged, and its frames are transmitted without modification. The Native VLAN can either be assigned to a specific VLAN or left unconfigured.

It is possible to tag all VLAN traffic and eliminate the use of a Native VLAN across your network. By default, VLAN 1 is assigned as the Native VLAN on switches, but this setting can be modified to meet specific network requirements.

The UCS Manager LAN Uplink Manager allows you to configure VLANs and change the Native VLAN setting.

Changing the Native VLAN triggers a single port flap, resulting in a temporary connectivity loss of approximately 20–40 seconds. This port flap is necessary for the change to take effect. However, continuous port flapping is not expected and may indicate underlying configuration issues that require troubleshooting.

Native VLAN Guidelines

- Native VLANs can only be configured on trunk ports.
- When changing the native VLAN on a UCS vNIC, a port flap will occur, leading to brief traffic interruptions.
- Cisco recommends using the Native VLAN 1 setting to minimize traffic interruptions, particularly when using the Cisco Nexus 1000v switches. Ensure the Native VLAN configuration is consistent between the Nexus 1000v port profiles and the UCS vNIC definition.
- If there is a continuous port flapping, incorrect traffic routing, or outages, verify the configuration of your disjoint Layer 2 network for potential issues.
- Using VLAN 1 for management access across all devices can lead to potential security risks if another switch is connected to the same VLAN as your management devices.

About the Access and Trunk Ports

Access Ports on a Cisco Switch

Access ports only sends untagged frames and belongs to and carries the traffic of only one VLAN. Traffic is received and sent in native formats with no VLAN tagging. Anything arriving on an access port is assumed to belong to the VLAN assigned to the port.

You can configure a port in access mode and specify the VLAN to carry the traffic for that interface. If you do not configure the VLAN for a port in access mode, or an access port, the interface carries the traffic for the default VLAN, which is VLAN 1. You can change the access port membership in a VLAN by configuring the VLAN. You must create the VLAN before you can assign it as an access VLAN for an access port. If you change the access VLAN on an access port to a VLAN that is not yet created, the UCS Manager shuts down that access port.

If an access port receives a packet with an 802.1Q tag in the header other than the access VLAN value, that port drops the packet without learning its MAC source address.

Trunk Ports on a Cisco Switch

Trunk ports allow multiple VLANs to transport between switches over that trunk link. A trunk port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default port VLAN ID to the trunk port, all untagged traffic travels on the default port VLAN ID for the trunk port, and all untagged traffic is assumed to belong to this VLAN. This VLAN is referred to as the native VLAN ID for a trunk port. The native VLAN ID is the VLAN that carries untagged traffic on trunk ports.

The trunk port sends an egressing packet with a VLAN that is equal to the default port VLAN ID as untagged; all the other egressing packets are tagged by the trunk port. If you do not configure a native VLAN ID, the trunk port uses the default VLAN.

Note Changing the native VLAN on a trunk port, or an access VLAN of an access port flaps the switch interface.

Named VLANs

A named VLAN creates a connection to a specific external LAN. The VLAN isolates traffic to that external LAN, including broadcast traffic.

The name that you assign to a VLAN ID adds a layer of abstraction that allows you to globally update all servers associated with service profiles that use the named VLAN. You do not need to reconfigure the servers individually to maintain communication with the external LAN.

You can create more than one named VLAN with the same VLAN ID. For example, if servers that host business services for HR and Finance need to access the same external LAN, you can create VLANs named HR and Finance with the same VLAN ID. Then, if the network is reconfigured and Finance is assigned to a different LAN, you only have to change the VLAN ID for the named VLAN for Finance.

In a cluster configuration, you can configure a named VLAN to be accessible only to one fabric interconnect or to both fabric interconnects.

Guidelines for VLAN IDs

Important VLANs with IDs from 4043 to 4047 and from 4094 to 4095 are reserved. You cannot create VLANs with IDs from this range. Until Cisco UCS Manager Release 4.0(1d), VLAN ID 4093 was in the list of reserved VLANs. VLAN 4093 has been removed from the list of reserved VLANs and is available for configuration.

For Cisco UCS 6600 Series Fabric Interconnect, Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 and 6400 Series Fabric Interconnects, VLAN IDs from 1002 to 1005 are reserved for VLAN Trunking Protocol (VTP).

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

VLAN 4048 is user configurable. However, Cisco UCS Manager uses VLAN 4048 for the following default values. If you want to assign 4048 to a VLAN, you must reconfigure these values:

- After an upgrade to Cisco UCS, Release 2.0—The FCoE storage port native VLAN uses VLAN 4048 by default. If the default FCoE VSAN was set to use VLAN 1 before the upgrade, you must change it to a VLAN ID that is not used or reserved. For example, consider changing the default to 4049 if that VLAN ID is not in use.
- After a fresh install of Cisco UCS, Release 2.0—The FCoE VLAN for the default VSAN uses VLAN 4048 by default. The FCoE storage port native VLAN uses VLAN 4049.

The VLAN name is case sensitive.

Private VLANs

A private VLAN (PVLAN) partitions the Ethernet broadcast domain of a VLAN into subdomains, and allows you to isolate some ports. Each subdomain in a PVLAN includes a primary VLAN and one or more secondary VLANs. All secondary VLANs in a PVLAN must share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another.

Isolated and Community VLANs

All secondary VLANs in a Cisco UCS domain can be Isolated or Community VLANs.

Note You cannot configure an isolated VLAN to use with a regular VLAN.

Ports on Isolated VLANs

Communications on an isolated VLAN can only use the associated port in the primary VLAN. These ports are isolated ports and are not configurable in Cisco UCS Manager. A primary VLAN can have only one isolated VLAN, but multiple isolated ports on the same isolated VLAN are allowed. These isolated ports cannot communicate with each other. The isolated ports can communicate only with a regular trunk port or promiscuous port that allows the isolated VLAN.

An isolated port is a host port that belongs to an isolated secondary VLAN. This port has complete isolation from other ports within the same private VLAN domain. PVLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports. You can have more than one isolated port in a specified isolated VLAN. Each port is completely isolated from all other ports in the isolated VLAN.

Guidelines for Uplink Ports

When you create PVLANs, use the following guidelines:

- The uplink Ethernet port channel cannot be in promiscuous mode.
- Each primary VLAN can have only one isolated VLAN.
- VIFs on VNTAG adapters can have only one isolated VLAN.

Guidelines for VLAN IDs

Note You cannot create VLANs with IDs from 3915 to 4042. These ranges of VLAN IDs are reserved.

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

VLAN 4048 is user configurable. However, Cisco UCS Manager uses VLAN 4048 for the following default values. If you want to assign 4048 to a VLAN, you must reconfigure these values:

- After an upgrade to Cisco UCS, Release 2.0—The FCoE storage port native VLAN uses VLAN 4048 by default. If the default FCoE VSAN was set to use VLAN 1 before the upgrade, you must change it to a VLAN ID that is not used or reserved. For example, consider changing the default to 4049 if that VLAN ID is not in use.
- After a fresh install of Cisco UCS, Release 2.0—The FCoE VLAN for the default VSAN uses VLAN 4048 by default. The FCoE storage port native VLAN uses VLAN 4049.

The VLAN name is case sensitive.

VLAN Port Limitations

Cisco UCS Manager limits the number of VLAN port instances that you can configure under border and server domains on a fabric interconnect.

Types of Ports Included in the VLAN Port Count

The following types of ports are counted in the VLAN port calculation:

- Border uplink Ethernet ports
- Border uplink Ether-channel member ports
- FCoE ports in a SAN cloud
- Ethernet ports in a NAS cloud
- Static and dynamic vNICs created through service profiles
- VM vNICs created as part of a port profile in a hypervisor in hypervisor domain

Based on the number of VLANs configured for these ports, Cisco UCS Manager tracks the cumulative count of VLAN port instances and enforces the VLAN port limit during validation. Cisco UCS Manager reserves some pre-defined VLAN port resources for control traffic. These include management VLANs configured under HIF and NIF ports.

VLAN Port Limit Enforcement

Cisco UCS Manager validates VLAN port availability during the following operations:

- Configuring and unconfiguring border ports and border port channels
- Adding or removing VLANs from a cloud
- Configuring or unconfiguring SAN or NAS ports
- Associating or disassociating service profiles that contain configuration changes
- Configuring or unconfiguring VLANs under vNICs or vHBAs
- Receiving creation or deletion notifications from a VMWare vNIC and from an ESX hypervisor

Note This is outside the control of the Cisco UCS Manager.

- Fabric interconnect reboot
- Cisco UCS Manager upgrade or downgrade

Cisco UCS Manager strictly enforces the VLAN port limit on service profile operations. If Cisco UCS Manager detects that the VLAN port limit is exceeded, the service profile configuration fails during deployment.

Exceeding the VLAN port count in a border domain is less disruptive. When the VLAN port count is exceeded in a border domain Cisco UCS Manager changes the allocation status to Exceeded. To change the status back to **Available**, complete one of the following actions:

- Unconfigure one or more border ports
- Remove VLANs from the LAN cloud
- Unconfigure one or more vNICs or vHBAs

Configuring Named VLANs

Creating a Named VLAN

In a Cisco UCS domain that is configured for high availability, you can create a named VLAN that is accessible to both fabric interconnects or to only one fabric interconnect.

Important VLANs with IDs from 4043 to 4047 and from 4094 to 4095 are reserved. You cannot create VLANs with IDs from this range. Until Cisco UCS Manager Release 4.0(1d), VLAN ID 4093 was in the list of reserved VLANs. VLAN 4093 has been removed from the list of reserved VLANs and is available for configuration.

For Cisco UCS 6600 Series Fabric Interconnect, Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 and 6400 Series Fabric Interconnects, VLAN IDs from 1002 to 1005 are reserved for VLAN Trunking Protocol (VTP).

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 On the **LAN** tab, click the **LAN** node.

Step 3 In the **Work** pane, click the **VLANs** tab.

Step 4 On the icon bar to the right of the table, click +.

If the + icon is disabled, click an entry in the table to enable it.

Step 5 In the **Create VLANs** dialog box, complete the required fields.

Step 6 If you clicked the **Check Overlap** button, do the following:

a) Click the **Overlapping VLANs** tab and review the fields to verify that the VLAN ID does not overlap with any IDs assigned to existing VLANs.

b) Click the **Overlapping VSANs** tab and review the fields to verify that the VLAN ID does not overlap with any FCoE VLAN IDs assigned to existing VSANs.

c) Click **OK**.

d) If Cisco UCS Manager identified any overlapping VLAN IDs or FCoE VLAN IDs, change the VLAN ID to one that does not overlap with an existing VLAN.

Step 7 Click **OK**.

Cisco UCS Manager adds the VLAN to one of the following **VLANs** nodes:

- The **LAN Cloud** > **VLANs** node for a VLAN accessible to both fabric interconnects.
- The ***Fabric_Interconnect_Name*** > **VLANs** node for a VLAN accessible to only one fabric interconnect.

Deleting a Named VLAN

If Cisco UCS Manager includes a named VLAN with the same VLAN ID as the one you delete, the VLAN is not removed from the fabric interconnect configuration until all named VLANs with that ID are deleted.

If you are deleting a private primary VLAN, ensure that you reassign the secondary VLANs to another working primary VLAN.

Before you begin

Before you delete a VLAN from a fabric interconnect, ensure that the VLAN was removed from all vNICs and vNIC templates.

Note If you delete a VLAN that is assigned to a vNIC or vNIC template, the vNIC might allow that VLAN to flap.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 On the **LAN** tab, click the **LAN** node.

Step 3 In the **Work** pane, click the **VLANs** tab.

Step 4 Click one of the following subtabs, based on the VLAN that you want to delete:

Subtab	Description
All	Displays all VLANs in the Cisco UCS domain.
Dual Mode	Displays the VLANs that are accessible to both fabric interconnects.
Fabric A	Displays the VLANs that are accessible to only fabric interconnect A.
Fabric B	Displays the VLANs that are accessible to only fabric interconnect B.

Step 5 In the table, click the VLAN that you want to delete.

You can use the **Shift** key or **Ctrl** key to select multiple entries.

Step 6 Right-click the highlighted VLAN or VLANs and click **Delete**.

Step 7 If a confirmation dialog box displays, click **Yes**.

Configuring Private VLANs

Creating a Primary VLAN for a Private VLAN

In a Cisco UCS domain that is configured for high availability, you can create a primary VLAN that is accessible to both fabric interconnects or to only one fabric interconnect.

Important VLANs with IDs from 4043 to 4047 and from 4094 to 4095 are reserved. You cannot create VLANs with IDs from this range. Until Cisco UCS Manager Release 4.0(1d), VLAN ID 4093 was in the list of reserved VLANs. VLAN 4093 has been removed from the list of reserved VLANs and is available for configuration.

For Cisco UCS 6600 Series Fabric Interconnect, Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 and 6400 Series Fabric Interconnects, VLAN IDs from 1002 to 1005 are reserved for VLAN Trunking Protocol (VTP).

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 On the **LAN** tab, click the **LAN** node.

Step 3 In the **Work** pane, click the **VLANs** tab.

Step 4 On the icon bar to the right of the table, click +.

If the + icon is disabled, click an entry in the table to enable it.

Step 5 In the **Create VLANs** dialog box, complete the required fields.

Step 6 If you clicked the **Check Overlap** button, do the following:

a) Click the **Overlapping VLANs** tab and review the fields to verify that the VLAN ID does not overlap with any IDs assigned to existing VLANs.

b) Click the **Overlapping VSANs** tab and review the fields to verify that the VLAN ID does not overlap with any FCoE VLAN IDs assigned to existing VSANs.

c) Click **OK**.

d) If Cisco UCS Manager identified any overlapping VLAN IDs or FCoE VLAN IDs, change the VLAN ID to one that does not overlap with an existing VLAN.

Step 7 Click **OK**.

Cisco UCS Manager adds the primary VLAN to one of the following **VLANs** nodes:

- The **LAN Cloud** > **VLANs** node for a primary VLAN accessible to both fabric interconnects.
- The ***Fabric_Interconnect_Name*** > **VLANs** node for a primary VLAN accessible to only one fabric interconnect.

Creating a Secondary VLAN for a Private VLAN

In a Cisco UCS domain that is configured for high availability, you can create a secondary VLAN that is accessible to both fabric interconnects or to only one fabric interconnect.

Important VLANs with IDs from 4043 to 4047 and from 4094 to 4095 are reserved. You cannot create VLANs with IDs from this range. Until Cisco UCS Manager Release 4.0(1d), VLAN ID 4093 was in the list of reserved VLANs. VLAN 4093 has been removed from the list of reserved VLANs and is available for configuration.

For Cisco UCS 6600 Series Fabric Interconnect, Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 and 6400 Series Fabric Interconnects, VLAN IDs from 1002 to 1005 are reserved for VLAN Trunking Protocol (VTP).

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

Before you begin

Create the primary VLAN.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 On the **LAN** tab, click the **LAN** node.

Step 3 In the **Work** pane, click the **VLANs** tab.

Step 4 On the icon bar to the right of the table, click +.

If the + icon is disabled, click an entry in the table to enable it.

Step 5 In the **Create VLANs** dialog box, specify the required fields.

Note
The multicast policy is associated to the primary VLAN, not the secondary VLAN.

Step 6 If you clicked the **Check Overlap** button, do the following:

a) Click the **Overlapping VLANs** tab and review the fields to verify that the VLAN ID does not overlap with any IDs assigned to existing VLANs.
b) Click the **Overlapping VSANs** tab and review the fields to verify that the VLAN ID does not overlap with any FCoE VLAN IDs assigned to existing VSANs.
c) Click **OK**.
d) If Cisco UCS Manager identified any overlapping VLAN IDs or FCoE VLAN IDs, change the VLAN ID to one that does not overlap with an existing VLAN.

Step 7 Click **OK**.

Cisco UCS Manager adds the primary VLAN to one of the following **VLANs** nodes:

- The **LAN Cloud** > **VLANs** node for a primary VLAN accessible to both fabric interconnects.
- The ***Fabric_Interconnect_Name*** > **VLANs** node for a primary VLAN accessible to only one fabric interconnect.

Community VLANs

Cisco UCS Manager supports Community VLANs in UCS Fabric Interconnects. Community ports communicate with each other and with promiscuous ports. Community ports have Layer 2 isolation from all other ports in other communities. A promiscuous port can communicate with all interfaces.

Creating a Community VLAN

In a Cisco UCS domain configured for high availability, you can create a Community VLAN accessible to both fabric interconnects or to only one fabric interconnect.

Important VLANs with IDs from 4043 to 4047 and from 4094 to 4095 are reserved. You cannot create VLANs with IDs from this range. Until Cisco UCS Manager Release 4.0(1d), VLAN ID 4093 was in the list of reserved VLANs. VLAN 4093 has been removed from the list of reserved VLANs and is available for configuration.

For Cisco UCS 6600 Series Fabric Interconnect, Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 and 6400 Series Fabric Interconnects, VLAN IDs from 1002 to 1005 are reserved for VLAN Trunking Protocol (VTP).

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 On the **LAN** tab, click the **LAN** node.

Step 3 In the **Work** pane, click the **VLANs** tab.

Step 4 On the icon bar to the right of the table, click **+**.

If the **+** icon is disabled, click an entry in the table to enable it.

Step 5 In the **Create VLANs** dialog box, complete the following fields:

Name	Description
VLAN Name/Prefix field	For a single VLAN, this is the VLAN name. For a range of VLANs, this is the prefix that the system uses for each VLAN name. The VLAN name is case sensitive. This name can be between 1 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Multicast Policy drop-down list	The multicast policy associated with this VLAN.
Create Multicast Policy link	Click this link to create a new multicast policy that will be available to all VLANs.
Configuration options	You can choose one of the following: • **Common/Global**—The VLANs apply to both fabrics and use the same configuration parameters in both cases. • **Fabric A**—The VLANs only apply to fabric A. • **Fabric B**—The VLAN only apply to fabric B. • **Both Fabrics Configured Differently**—The VLANs apply to both fabrics, but you can specify different VLAN IDs for each fabric. For upstream disjoint L2 networks, Cisco recommends that you choose **Common/Global** to create VLANs that apply to both fabrics.

Name	Description
VLAN IDs field	To create one VLAN, enter a single numeric ID. To create multiple VLANs, enter individual IDs or ranges of IDs separated by commas. A VLAN ID can: • Be between 1 and 3967 • Be between 4048 and 4093 • Overlap with other VLAN IDs already defined on the system For example, to create six VLANs with the IDs 4, 22, 40, 41, 42, and 43, enter **`4, 22, 40-43`**. **Important** VLANs with IDs from 4043 to 4047 and from 4094 to 4095 are reserved. You cannot create VLANs with IDs from this range. Until Cisco UCS Manager Release 4.0(1d), VLAN ID 4093 was in the list of reserved VLANs. VLAN 4093 has been removed from the list of reserved VLANs and is available for configuration. For Cisco UCS 6600 Series Fabric Interconnect, Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 and 6400 Series Fabric Interconnects, VLAN IDs from 1002 to 1005 are reserved for VLAN Trunking Protocol (VTP). The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch. VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.
Sharing Type field	Whether this 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 have one or more secondary VLANs, as shown in the **Secondary VLANs** area. • **Isolated**—This is a private VLAN. The primary VLAN with which it is associated is shown in the **Primary VLAN** drop-down list.
Primary VLAN drop-down list	If the **Sharing Type** field is set to **Isolated**, this is the primary VLAN associated with the IsolatedVLAN.
Permitted Orgs for VLAN(s)	Select the organization from the list for the VLAN. This VLAN will be available for the organizations that you select.

Name	Description
Check Overlap button	Click this button to determine whether the VLAN ID overlaps with any other IDs on the system.

Step 6 If you clicked the **Check Overlap** button, do the following:

a) Click the **Overlapping VLANs** tab and review the following fields to verify that the VLAN ID does not overlap with any IDs assigned to existing VLANs.

Name	Description
Fabric ID column	This can be one of the following: • **A** • **B** • **Dual**—The component is accessible to either fabric interconnect. This setting applies to virtual LAN and SAN networks created at the system level as opposed to the fabric-interconnect level.
Name column	The name of the VLAN.
VLAN column	The numeric id for the VLAN.
DN column	The full path to the VLAN. Click the link in this column to view the properties for the VLAN.

b) Click the **Overlapping VSANs** tab and review the following fields to verify that the VLAN ID does not overlap with any FCoE VLAN IDs assigned to existing VSANs:

Name	Description
Fabric ID column	This can be one of the following: • **A** • **B** • **Dual**—The component is accessible to either fabric interconnect. This setting applies to virtual LAN and SAN networks created at the system level as opposed to the fabric-interconnect level.
Name column	The name of the VSAN.
ID column	The numeric id for the VSAN.
FCoE VLAN ID column	The unique identifier assigned to the VLAN used for Fibre Channel connections.
DN column	The full path to the VSAN. Click the link in this column to view the properties for the VSAN.

c) Click **OK**.

d) If Cisco UCS Manager identified any overlapping VLAN IDs or FCoE VLAN IDs, change the VLAN ID to one that does not overlap with an existing VLAN.

Step 7 Click **OK**.

Cisco UCS Manager adds the Community VLAN to one of the following **VLANs** nodes:

- The **LAN Cloud** > **VLANs** node for a VLAN accessible to both fabric interconnects.
- The ***Fabric_Interconnect_Name*** > **VLANs** node for a VLAN accessible to only one fabric interconnect.

Creating Promiscuous Access on Appliance Port

Cisco UCS Manager supports Promiscuous access on appliance ports. The following procedure details the configurations steps.

Before you begin

Create the PVLANs in Appliance Cloud.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **LAN** > **Appliances** > ***Fabric*** > **Interfaces**.
The Interfaces pane displays.

Step 3 In the **Interfaces** pane on the icon bar to the right of the table, click **+** .
The **Appliance Links** pane displays.

Step 4 In the **Appliance Links** pane, click the **Unconfigured Ethernet Ports** to expand the **Unconfigured Ethernet Ports**.
All available Unconfigured Ethernet Ports display.

Step 5 Click the **Unconfigured Ethernet Ports** that you want to make an Appliance Port.

Step 6 Click **Make Appliance Port**.
The **Configure as Appliance Port** confirmation box displays.

Step 7 Click **Yes** to configure the appliance port.
The **Configure Appliance Port** dialog box opens.

Step 8 On the **LAN** tab, expand **LAN** > **Appliances** > ***Fabric*** > **Interfaces**.

Step 9 Expand **Appliance Ports**.

Step 10 Click the appliance port for which you want to modify the properties.

Step 11 In the **Interfaces** pane on the icon bar to the right of the table, click **Modify**.
The **Properties for Appliance Interface** dialog box displays.

Step 12 In the **VLANs** pane, click the **Access** radio button.

Step 13 Select a Primary VLAN from the **Select VLAN** drop-down list to assign to the appliance port.
A list of secondary VLANs associated with the primary VLAN displays.

Step 14 Select a set of secondary VLANs allowed on the port.

Selecting an **Isolated** or **Community** VLAN turns the **VLAN** into a **Promiscuous Port**. If you select the Primary VLAN from the **Select VLAN** drop-down list, you must select the required secondary VLAN.

Step 15 Click **Apply** to configure **Promiscuous Access on Appliance Port**.

Creating a Promiscuous Trunk on Appliance Port

Cisco UCS Manager supports Promiscuous Trunks on appliance ports. The following procedure details the configurations steps.

Before you begin

Create the Private VLANs in the Appliance Cloud.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **LAN** > **Appliances** > ***Fabric*** > **Interfaces**.
The **Interfaces** pane displays.

Step 3 In the **Interfaces** pane on the icon bar to the right of the table, click **+** .
The **Appliance Links** pane displays.

Step 4 In the **Appliance Links** pane, click the **Unconfigured Ethernet Ports** to expand the **Unconfigured Ethernet Ports**.
All available Unconfigured Ethernet Ports display.

Step 5 Click the **Unconfigured Ethernet Ports** that you to want make an Appliance Port.

Step 6 Click **Make Appliance Port**.
The **Configure as Appliance Port** confirmation box displays.

Step 7 Click **Yes** to configure the appliance port.

Step 8 On the **LAN** tab, expand **LAN** > **Appliances** > ***Fabric*** > **Interfaces**.

Step 9 Expand **Appliance Ports**.

Step 10 Click the appliance port for which you want to modify the properties.

Step 11 In the **Interfaces** pane on the icon bar to the right of the table, click the **Modify** icon.
The **Properties for Appliance Interface** dialog box displays.

Step 12 In the **VLANs** pane, click the **Trunk** radio button.

Step 13 Select a **VLAN** from the available VLANs.

From the list of VLANs, you can select multiple **Isolated**,**Community**, **Primary** and **Regular** VLANs to apply on the port to make it a promiscuous trunk port.

Step 14 Click **Apply** to configure **Promiscuous on Trunk on Appliance Port**.

Viewing VLAN Optimization Sets

Cisco UCS Manager automatically creates VLAN port count optimization groups based on the VLAN IDs in the system. All of the VLANs in the group share the same IGMP policy. The following VLANs are not included in the VLAN port count optimization group:

- FCoE VLANs
- Primary PVLANs and secondary PVLANs
- VLANs that are specified as a SPAN source
- VLANs configured as a single allowed VLAN on an interface and port profiles with a single VLAN

Cisco UCS Manager GUI automatically groups the optimized VLANs.

Note It is recommended to keep the VLAN optimization set to be not more than 32. If the VLAN optimization set exceeds 32, you may observe latency during VLAN configuration changes and in bringing up all the server connections upon switch reboot.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud**.

Step 3 In the **Navigation** pane, click **Fabric A** or **Fabric B** to expand the list.

Step 4 Click **VLAN Optimization Sets**.

The **Work** pane displays the list of VLAN optimization groups with **Name** and **Size**.

Viewing the VLAN Port Count

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects**.

Step 3 Click the fabric interconnect for which you want to view the VLAN port count.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **General** tab, click the down arrows on the **VLAN Port Count** bar to expand that area.

Cisco UCS Manager GUI displays the following details:

Name	Description
VLAN Port Limit field	The maximum number of VLAN ports allowed on this fabric interconnect.
Access VLAN Port Count field	The number of available VLAN access ports.
Border VLAN Port Count field	The number of available VLAN border ports.
Allocation Status field	The VLAN port allocation status.

VLAN Port Count Optimization

VLAN port count optimization enables mapping the state of multiple VLANs into a single internal state. When you enable the VLAN port count optimization, Cisco UCS Manager logically groups VLANs based on the port VLAN membership. This grouping increases the port VLAN count limit. VLAN port count optimization also compresses the VLAN state and reduces the CPU load on the fabric interconnect. This reduction in the CPU load enables you to deploy more VLANs over more vNICs. Optimizing VLAN port count does not change any of the existing VLAN configuration on the vNICs.

VLAN port count optimization is disabled by default. You can enable or disable the option based on your requirements.

Important

- Enabling VLAN port count optimization increases the number of available VLAN ports for use. If the port VLAN count exceeds the maximum number of VLANs in a non-optimized state, you cannot disable the VLAN port count optimization.
- On the Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 Series Fabric Interconnects and Cisco UCS 6400 Series Fabric Interconnect, the VLAN port count optimization is performed when the PV count exceeds 16000.

When the Cisco UCS 6400 Series Fabric Interconnect is in Ethernet switching mode:

- The FI does not support **VLAN Port Count Optimization Enabled**
- The FI supports 16000 PVs, similar to EHM mode, when **VLAN Port Count Optimization** is **Disabled**.

The following table illustrates the Port VLAN (PV) Count with VLAN port count optimization enabled and disabled:

Fabric Interconnect Model	PV Count with VLAN Port Count Optimization Disabled	PV Count with VLAN Port Count Optimization Enabled
Cisco UCS 6400 Series FI (6454 FI & 64108 FI)	16000	108000
Cisco UCS 6500 Series FI (6536 FI)	16000	108000

Fabric Interconnect Model	PV Count with VLAN Port Count Optimization Disabled	PV Count with VLAN Port Count Optimization Enabled
Cisco UCS Fabric Interconnects 9108 100G (UCS X-Series Direct/UCSX-S9108-100G)	16000	108000
Cisco UCS 6600 Series Fabric Interconnect (6664 FI)	16000	108000

The following table illustrates the PV Count with VLAN port count optimization enabled and disabled:.

	Cisco UCS 6300 Series FI	Cisco UCS 6400 Series FI	Cisco UCS 6500 Series FI (6536 FI)	Cisco UCS Fabric Interconnects 9108 100G (UCS X-Series Direct/UCSX-S9108-100G)
PV Count with VLAN Port Count Optimization Disabled	16000	16000	16000	16000
PV Count with VLAN Port Count Optimization Enabled	64000	108000	108000	108000

Enabling Port VLAN Count Optimization

By default, the port VLAN count optimization is disabled. You can enable the port VLAN count optimization to optimize the CPU usage and to increase the port VLAN count.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud**.

Step 3 In the **Work** pane, click the **Global Policies** tab.

Step 4 In the **Port, VLAN Count Optimization** section, choose **Enabled**.

Step 5 Click **Save Changes**.

Step 6 If the **Port, VLAN Count Optimization** option is successfully enabled, a confirmation message displays. Click **OK** to close the dialog box.

Disabling Port VLAN Count Optimization

By default, the port VLAN count optimization is disabled. You can disable the port VLAN count optimization option if you enabled it to increase the port VLAN count and to optimize the CPU usage.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud**.

Step 3 In the **Work** pane, click the **Global Policies** tab.

Step 4 In the **Port, VLAN Count Optimization** section, choose **Disabled**.

Step 5 Click **Save Changes**.

Step 6 If the **Port, VLAN Count Optimization** option is successfully disabled, a confirmation message displays. Click **OK** to close the dialog box.

Viewing VLAN Optimization Sets

Cisco UCS Manager automatically creates VLAN port count optimization groups based on the VLAN IDs in the system. All of the VLANs in the group share the same IGMP policy. The following VLANs are not included in the VLAN port count optimization group:

- FCoE VLANs
- Primary PVLANs and secondary PVLANs
- VLANs that are specified as a SPAN source
- VLANs configured as a single allowed VLAN on an interface and port profiles with a single VLAN

Cisco UCS Manager GUI automatically groups the optimized VLANs.

Note It is recommended to keep the VLAN optimization set to be not more than 32. If the VLAN optimization set exceeds 32, you may observe latency during VLAN configuration changes and in bringing up all the server connections upon switch reboot.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud**.

Step 3 In the **Navigation** pane, click **Fabric A** or **Fabric B** to expand the list.

Step 4 Click **VLAN Optimization Sets**.

The **Work** pane displays the list of VLAN optimization groups with **Name** and **Size**.

VLAN Groups

VLAN groups allow you to group VLANs on Ethernet uplink ports, by function or by VLANs that belong to a specific network. You can define VLAN membership and apply the membership to multiple Ethernet uplink ports on the fabric interconnect.

Note Cisco UCS Manager supports a maximum of 200 VLAN Groups. If Cisco UCS Manager determines that you create more than 200 VLAN groups, the system disables VLAN compression.

You can configure inband and out-of-band (OOB) VLAN groups to use to access the Cisco Integrated Management Interface (CIMC) on blade and rack servers. Cisco UCS Manager supports OOB IPv4 and inband IPv4 and IPv6 VLAN groups for use with the uplink interfaces or uplink port channels.

Note Inband Management is not supported on VLAN 2 or VLAN 3.

After you assign a VLAN to a VLAN group, any changes to the VLAN group are applied to all Ethernet uplink ports that are configured with the VLAN group. The VLAN group also enables you to identify VLAN overlaps between disjoint VLANs.

You can configure uplink ports under a VLAN group. When you configure an uplink port for a VLAN group, that uplink port will support all the VLANs that are part of the associated VLAN groups and individual VLANs that are associated with the uplink using LAN Uplinks Manager, if any. Further, any uplink that is not selected for association with that VLAN group will stop supporting the VLANs that are part of that VLAN group.

You can create VLAN groups from the **LAN Cloud** or from the **LAN Uplinks Manager**.

Creating a VLAN Group

You can create a **VLAN Group** from **LAN Cloud** or the **LAN Uplinks Manager**. This procedure explains creating a VLAN group from the **LAN Cloud**. You can create separate VLAN groups to use for inband and out-of-band access using service profiles.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud**.

Step 3 Right-click **LAN Cloud** and choose **Create VLAN Group** from the drop-down list.

The **Create VLAN Group** wizard launches.

Step 4 In the **Select VLANs** dialog box, specify the name and VLANs, then click **Next**.

Step 5 (Optional) In **Add Uplink Ports** dialog box, select the **Uplink Ports** from the list and add the ports to the **Selected Uplink Ports**, then click **Next**.

Step 6 (Optional) In **Add Port Channels** dialog box, select the **Port Channels**, and add the port channels to the **Selected Port Channels**, then click **Next**.

Step 7 (Optional) In the **Org Permissions** dialog box, select the appropriate groups from the list, then click **Next**.

The VLANs that belong to the group that you are creating can only access the groups that you select.

Step 8 Click **Finish**.

This VLAN group is added to the list of **VLAN Groups** under **LAN** > **LAN Cloud** > **VLAN Groups**.

Editing the Members of a VLAN Group

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud**.

Step 3 In the **Navigation** pane, click **VLAN Groups** to expand the VLAN group list.

Step 4 From the list of VLAN groups, choose the VLAN group name to edit the group member VLANs.

You can use the **Shift** key or **Ctrl** key to select multiple entries.

Step 5 Right-click the highlighted VLAN group or VLAN groups and choose **Edit VLAN Group Members**.

The **Modify VLAN Group** *VLAN Group Name* dialog box opens.

Step 6 In the **Modify VLAN Group** *VLAN Group Name* dialog box, select the VLANs that you want to remove or add from the list and click **Next**.

Step 7 (Optional) In **Add Port Channels** pane, choose the **Port Channels**, and add them to the **Selected Port Channels**.

Step 8 (Optional) In the **Org Permissions** pane, choose the appropriate groups from the list.

The VLANs that belong to the group that you are creating can only access the groups that you select.

Step 9 Click **Finish**.

Step 10 This VLAN group is modified based on your selections.

Modifying the Organization Access Permissions for a VLAN Group

When you modify the organization access permissions for a VLAN group, the change in permissions applies to all VLANs that are in that VLAN group.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud** > **VLAN Group**, select *VLAN group name*.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In **Actions**, click **Modify VLAN Groups Org Permissions**.

The **Modify VLAN Groups Org Permissions** dialog box opens.

Step 5 In **Org Permissions**, do the following:

- To add organizations, select the organizations.
- To remove access permission from an organization, click to remove the selection.

Step 6 Click **OK**.

Deleting a VLAN Group

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud**.

Step 3 In the **Navigation** pane, click **VLAN Groups** to expand the VLAN group list.

Step 4 From the displayed list of VLAN groups, choose the VLAN group name you want to delete.

You can use the **Shift** key or **Ctrl** key to select multiple entries.

Step 5 Right-click the highlighted VLAN group or VLAN groups and choose **Delete**.

Step 6 If a confirmation dialog box displays, click **Yes**.

VLAN Permissions

VLAN permissions restrict access to VLANs based on specified organizations and on the service profile organizations to which the VLANs belong. VLAN permissions also restrict the set of VLANs that you can assign to service profile vNICs. VLAN permissions is an optional feature and is disabled by default. You can enable or disable the feature based on your requirements. If you disable the feature, all of the VLANs are globally accessible to all organizations.

Note If you enable the org permission in **LAN** > **LAN Cloud** > **Global Policies** > **Org Permissions**, when you create a VLAN, the **Permitted Orgs for VLAN(s)** option displays in the **Create VLANs** dialog box. If you do not enable the **Org Permissions**, the **Permitted Orgs for VLAN(s)** option does not display.

Enabling the org permission allows you to specify the organizations for the VLAN. When you specify the organizations, the VLAN becomes available to that specific organization and all of the sub organizations below the structure. Users from other organizations cannot access this VLAN. You can also modify the VLAN permission anytime based on changes to your VLAN access requirements.

Caution When you assign the VLAN org permission to an organization at the root level, all sub organizations can access the VLANs. After assigning the org permission at the root level, and you change the permission for a VLAN that belongs to a sub organization, that VLAN becomes unavailable to the root level organization.

Enabling VLAN Permissions

By default, VLAN permissions are disabled. If you want to restrict VLAN access by creating permissions for different organizations, you must enable the org permission option.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud**.

Step 3 In the **Work** pane, click the **Global Policies** tab.

Step 4 In the **Org Permissions** section, choose **Enabled**.

Step 5 Click **Save Changes**.

Step 6 If the **Org Permissions** option is successfully enabled, a confirmation message displays. Click **OK** to close the dialog box.

Disabling VLAN Permissions

By default, VLAN permissions are disabled. You can enable VLAN permissions and assign a VLAN to a different network group or organization. You can also disable the VLAN permission globally; however, the permissions assigned to the VLANs continue to exist in the system, but are not enforced. If you want to use the org permissions later, you can enable the feature to use the assigned permissions.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud**.

Step 3 In the **Work** pane, click the **Global Policies** tab.

Step 4 In the **Org Permissions** section, choose **Disabled**.

Step 5 Click **Save Changes**.

Step 6 If the **Org Permissions** option is successfully disabled, a confirmation message displays. Click **OK** to close the dialog box.

Adding or Modifying VLAN Permissions

You can add or delete the permitted organization for a VLAN.

Note When you add an organization as a permitted organization for a VLAN, all of the descendant organizations can access the VLAN. When you remove the permission to access a VLAN from an organization, the descendant organizations no longer have access to the VLAN.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud** > **VLANs**, select *VLAN name*.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In **Actions**, click **Modify VLAN Org Permissions**.

The **Modify VLAN Org Permissions** dialog box opens.

Step 5 In **Permitted Orgs for VLAN(s)**,

- To add organizations, select the organizations.
- To remove access permission from an organization, click to remove the selection.

Step 6 Click **OK**.

Modifying Reserved VLANs

This task describes how to modify the reserved VLAN ID.

For Cisco UCS 6500 FI Series, VLAN IDs from 1002 to 1005 are reserved for NX-OS.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 In the **Work** pane, click the **Global Policies** tab.

Step 3 Specify a new value in the Reserved VLAN Start ID field. The reserved VLAN range ID can be specified from 2-3915.

Step 4 Click **Save Changes**.

VIC QinQ Tunneling

Starting with release 4.3(2a), Cisco UCS Manager introduces support for VIC Q-in-Q tunneling configuration. A Q-in-Q (802.1Q-in-802.1Q) tunnel allows to segregate the traffic in the infrastructure and helps to expand the VLAN space through the addition of 802.1Q tag to 802.1Q-tagged packets.

To configure VIC QinQ Tunneling, ensure **Q-in-Q Forwarding** is enabled. For more information, see Q-in-Q Forwarding, on page 54.

To know more about supported combinations and limitations of VIC QinQ Tunneling: see VIC QinQ Tunneling - Supported Combinations and Limitations, on page 121.

Enabling QinQ on a vNIC in a LAN Connectivity Policy

To enable VIC QinQ Tunneling on a vNIC in a LAN Connectivity Policy, do the following:

1. In the **Navigation** pane, click **LAN** and expand **LAN** > **Policies**.
2. Expand the node for the organization where you want to create the policy. If the system does not include multi tenancy, expand the **root** node.
3. Right-click **LAN Connectivity Policies** and choose **Create LAN Connectivity Policy**.
4. In the **Create LAN Connectivity Policy** dialog box, enter a name and optional description.
5. To add vNICs, click **Add** next to the plus sign and complete the following fields in the **Create vNIC** dialog box:
   a. Enter a name for the vNIC.
   b. Check the **Enable QinQ** check box.
   c. In the **VLANs** table, click the **QinQ VLAN** radio button. The supported QinQ VLAN ID range is 2 to 4094.

      QinQ VLAN can be a Native or a Non-Native VLAN. You can configure a Native VLAN and a Non-Native VLAN as a QinQ VLAN on the vNIC. When using the Native VLAN as QinQ VLAN, no additional VLAN can be configured on the vNIC.
   d. Select or update other fields for any necessary configurations on the vNIC. For more information, see Creating a vNIC for a LAN Connectivity Policy, on page 190
   e. Click **OK**

Note This QinQ VLAN selection is considered only when the **Enable QinQ** check box is selected on the vNIC.

6. Click **Save Changes**.

Note VIC QinQ Tunneling can also be configured on any of the following ways:

- vNIC Template - For more information, see Creating a vNIC Template, on page 150.
- Creating a vNIC option on a Service Profile of a Policy - For more information, see Enabling QinQ on a vNIC of a Service Profile, on page 120.

Enabling QinQ on a vNIC of a Service Profile

To enable VIC QinQ Tunneling on a vNIC of a Service Profile, do the following:

1. In the **Navigation** pane, click **Servers**.
2. On the **Servers** tab, expand **Servers** > **Service Profile** > **root**.
3. Expand the service profile that you want to configure QinQ Tunneling and then click **vNICs**.
4. Choose the desired vNIC.
5. In the **Work Pane**, click the **General** tab.
6. In the **Fabric Interconnect** area, do the following:
   a. Check the **Enable QinQ** check box.
   b. In the **VLANs** table, click the **QinQ VLAN** radio button. The supported QinQ VLAN ID range is 2 to 4094.

      QinQ VLAN can be a Native or a Non-Native VLAN. You can configure a Native VLAN and a Non-Native VLAN as a QinQ VLAN on the vNIC. When using the Native VLAN as QinQ VLAN, no additional VLAN can be configured on the vNIC.

Note This QinQ VLAN selection is considered only when the **Enable QinQ** check box is selected on the vNIC.

7. Click **OK**.
8. Click **Save Changes**.

Note VIC QinQ Tunneling can also be configured on any of the following ways:

- vNIC Template - For more information, see Creating a vNIC Template, on page 150.
- Creating a vNIC option on a LAN Connectivity Policy - For more information, see Enabling QinQ on a vNIC in a LAN Connectivity Policy, on page 119.

Viewing QinQ VLAN

The VLANs tab displays the QinQ VLAN selection.

Name	Description
VLAN column	The vNIC network name.
VLAN ID column	The identifier for the VLAN associated with this network.
Oper VLAN column	The full path to the network. Click the link in this column to view the network properties in a pop-up window.
Native ID column	This column displays an icon if this is the native VLAN for the vNIC.
QinQ VLAN	This column displays the VIC QinQ Tunneling for the VLAN.

Note VLANs are not supported with Microsoft Hyper-V dynamic vNICs.

VIC QinQ Tunneling - Supported Combinations and Limitations

Following are the supported combinations for VIC QinQ Tunneling:

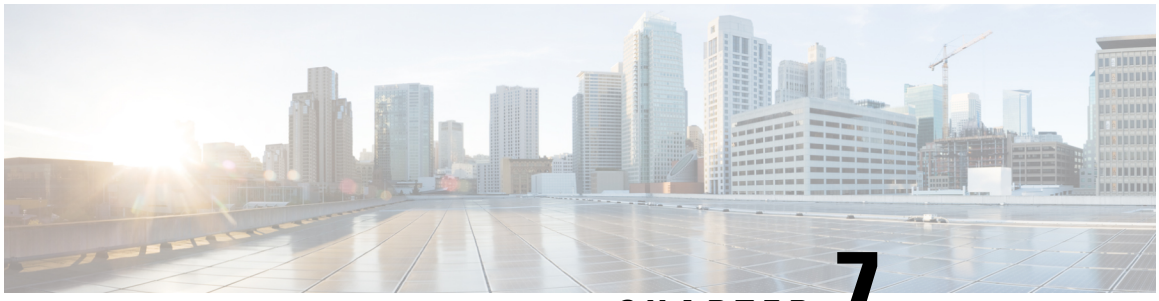
- QinQ VLAN selection is considered only when the **Enable QinQ** check box is selected on a vNIC Interface.
- QinQ Configuration supports a maximum of two VLANs on a vNIC Interface. A QinQ VLAN can be a Native or a non-Native VLAN. You can configure a Native VLAN and a Non-Native VLAN as a QinQ VLAN on the vNIC.

  When using the Native VLAN as QinQ VLAN, no additional VLAN can be configured on the vNIC.
- For Cisco UCS VIC 15000 series adapters, QinQ and Geneve Offload can be enabled on a vNIC Interface.

Following are the limitations of VIC QinQ Tunneling:

- QinQ configuration on a vNIC Interface is not supported on Cisco UCS VIC 1300 series adapters.
- The default VLAN (VLAN ID: 1) is not supported as a QinQ VLAN on a vNIC Interface.
- When a Native VLAN and a QinQ VLAN are configured on a vNIC Interface, a new VLAN configuration is not supported and results in Server Profile association failures when selected. To accommodate a new VLAN, either the Native VLAN or QinQ VLAN must be removed.
- When the QinQ VLAN is the same as the Native VLAN on a vNIC Interface, a new VLAN configuration is not supported and results in Server Profile association failures when selected. To accommodate a new VLAN, either the Native VLAN or QinQ VLAN must be modified.
- For Cisco UCS VIC 1400, 14000, and 15000 series adapters, LAN (or PXE) Boot and QinQ cannot be configured on a vNIC interface and result in configuration failures when enabled.
- For Cisco UCS VIC 1400, 14000, and 15000 series adapters, iSCSI Boot and QinQ cannot be configured on a vNIC interface and result in configuration failures when enabled.

- For Cisco UCS VIC 1400 and 14000 series adapters, QinQ and Geneve Offload cannot be configured on a vNIC interface and result in configuration failures when enabled.
- For Cisco UCS VIC 1400, 14000, and 15000 series adapters, QinQ and VMMQ cannot be configured on a vNIC interface and result in configuration failures when enabled.
- For Cisco UCS VIC 1400, 14000, and 15000 series adapters, QinQ and RDMA V2 cannot be configured on a vNIC interface and result in configuration failures when enabled.
- For Cisco UCS 6454, 64108, 6536 Fabric InterconnectsCisco UCS Fabric Interconnects 9108 100G, and Cisco UCS 6664 Fabric Interconnect, QinQ must be enabled at LAN > Global Policies to support QinQ VLAN on a VIC adapter.
- For Cisco UCS VIC 1400, 14000, and 15000 series adapters, QinQ and SR-IOV cannot be configured on a vNIC interface and result in configuration failures when enabled.
- When the Service Profile is already associated, you cannot enable or disable QinQ on a B-Series server.
- For Cisco UCS 6454, Cisco UCS 64108, Cisco UCS 6536 Fabric InterconnectsCisco UCS Fabric Interconnects 9108 100G, and Cisco UCS 6664 Fabric Interconnect, QinQ configuration for Fabric Interconnects in Global Policy > LAN Connectivity Policy must be enabled to configure QinQ on a vNIC interface.
- QinQ and usNIC cannot be enabled together on a vNIC interface.
- When VIC QinQ Tunneling is enabled, you cannot downgrade to lower release versions.



CHAPTER 7

MAC 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. 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 multitenancy, you can use the organizational hierarchy to ensure that MAC pools can be used only by specific applications or business services. Cisco UCS 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 a MAC Pool

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Pools**.

Step 3 Expand the node for the organization where you want to create the pool.

If the system does not include multi tenancy, expand the **root** node.

Step 4 Right-click **MAC Pools** and select **Create MAC Pool**.

Step 5 In the **Define Name and Description** page of the **Create MAC Pool** wizard, complete the following fields:

Name	Description
Name field	The name of the MAC pool. This name can be between 1 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Description field	A description of the MAC pool. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).
Assignment Order field	This can be one of the following: • **Default**—Cisco UCS Manager selects a random identity from the pool. • **Sequential**—Cisco UCS Manager selects the lowest available identity from the pool.

Step 6 Click **Next**.

Step 7 In the **Add MAC Addresses** page of the **Create MAC Pool** wizard, click **Add**.

Step 8 In the **Create a Block of MAC Addresses** dialog box, complete the following fields:

Name	Description
First MAC Address field	Enter the first MAC address for the block. A MAC address is 6 bytes (48 bits) long, typically displayed as 12 hexadecimal digits separated by colons. It is recommended to use the prefix 00:25:b5 to ensure unique MAC addresses in the LAN fabric. Example, 00:25:b5:xx:xx:xx.
Size field	Specify the number of MAC addresses in the block. This determines how many consecutive addresses will be generated starting from the first MAC address. The size can range from 1 to 1000 per block.

Step 9 Click **OK**.

Step 10 Click **Finish**.

What to do next

Include the MAC pool in a vNIC template.

Deleting a MAC Pool

If you delete a pool, Cisco UCS Manager does not reallocate any addresses from that pool that were assigned to vNICs or vHBAs. 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.

Procedure

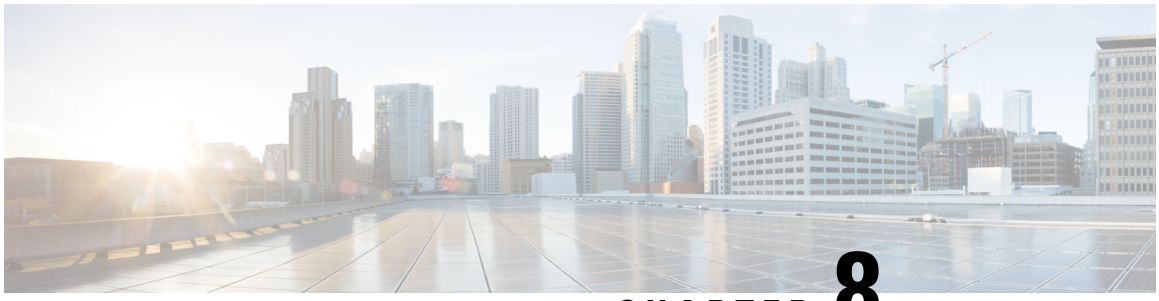
Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN** > **Pools** > ***Organization_Name*** .

Step 3 Expand the **MAC Pools** node.

Step 4 Right-click the MAC pool you want to delete and select **Delete**.

Step 5 If a confirmation dialog box displays, click **Yes**.



CHAPTER 8

Quality of Service

Quality of Service

Cisco UCS provides the following methods to implement quality of service:

- System classes that specify the global configuration for certain types of traffic across the entire system
- QoS policies that assign system classes for individual vNICs
- Flow control policies that determine how uplink Ethernet ports handle pause frames

Global QoS changes made to the QoS system class may result in brief data-plane interruptions for all traffic. Some examples of such changes are:

- Changing the MTU size for an enabled class
- Changing packet drop for an enabled class
- Changing the CoS value for an enabled class

Guidelines and Limitations for Quality of Service on Cisco UCS 6600 Series Fabric Interconnect, Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6536 Fabric Interconnects, Cisco UCS 6400 Series Fabric Interconnects

- Multicast optimization is not supported.
- For all QoS system classes except for Fibre Channel, the default MTU is 1500 bytes. The MTU for Fiber Channel class is not configurable and is set to 2240 bytes internally. All classes (excluding Fibre Channel) allow for MTU configuration up to a maximum of 9216 bytes.

Note The maximum MTU for a QoS class on the Fabric Interconnect is 9216 bytes, while the maximum MTU that can be set on a vNIC is 9000 bytes. The vNIC MTU is configured through the adapter policy.

- The MTU size for fibre channel is always 2240 bytes.
- Multicast is not supported on any no-drop QoS class.

Configuring System Classes

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.

The following table describes the system classes that you can configure.

Table 10: 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. The default MTU for the Best Effort class is 1500. You cannot disable this system class.

System Class	Description
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.

Configuring QoS System Classes

Note

- Under the Network QoS policy, MTU settings primarily affect buffer allocation for both drop and no-drop classes, which support configurations up to 9216 bytes. While Fabric Interconnects (FI) are capable of forwarding packets with an MTU of up to 9216 bytes (a limit determined by the overall QoS configuration), the maximum configurable MTU for vNICs remains 9000 bytes.
- For Cisco VIC 1400 series, 14000 series, and later adapters, vNIC MTU can be adjusted directly from host interface settings. When configuring an Overlay network, it is crucial to ensure the overall MTU does not surpass the QoS system class MTU to prevent packet drops during data transmission.

Important Use the same CoS (Class of Service) values on UCS and N5K/N9K for all the no-drop policies. To insure that end-to-end PFC works correctly, have the same QoS policy configured on all intermediate switches.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud**.

Step 3 Select the **QoS System Class** node. MTU is configurable for both drop and no-drop type QoS system classes.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 Update the properties for the system class that you want to configure to meet the traffic management needs of the system.

Note
Some properties may not be configurable for all system classes. The maximum configurable MTU for a QoS system class is 9216 bytes. However, the Fabric Interconnects can forward packets with an MTU of up to 9216 bytes, as determined by the overall QoS configuration.

Step 6 Click **Save Changes**.

Enabling a QoS System Class

The Best Effort or Fibre Channel system classes are enabled by default.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **LAN** > **LAN Cloud**.
Step 3 Select the **QoS System Class** node.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 Check the **Enabled** check box for the QoS system that you want to enable.
Step 6 Click **Save Changes**.

Disabling a QoS System Class

You cannot disable the Best Effort or Fibre Channel system classes.

All QoS policies that are associated with a disabled system class default to Best Effort or, if the disabled system class is configured with a Cos of 0, to the Cos 0 system class.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **LAN** > **LAN Cloud**.
Step 3 Select the **QoS System Class** node.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 Uncheck the **Enabled** check box for the QoS system that you want to disable.
Step 6 Click **Save Changes**.

Configuring Quality of Service Policies

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 a QoS Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies**.

Step 3 Expand the node for the organization where you want to create the pool.

If the system does not include multi tenancy, expand the **root** node.

Step 4 Right-click **QoS Policy** and select **Create QoS Policy**.

Step 5 In the **Create QoS Policy** dialog box, complete the required fields.

Step 6 Click **OK**.

What to do next

Include the QoS policy in a vNIC or vHBA template.

Deleting a QoS Policy

If you delete a QoS policy that is in use or you disable a system class that is used in a QoS policy, any vNIC or vHBA that uses that QoS policy is assigned to the Best Effort system class or to the system class with a CoS of 0. In a system that implements multitenancy, Cisco UCS Manager first attempts to find a matching QoS policy in the organization hierarchy.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **Servers** > **Policies** > ***Organization_Name***.

Step 3 Expand the **QoS Policies** node.

Step 4 Right-click the QoS policy you want to delete and select **Delete**.

Step 5 If a confirmation dialog box displays, click **Yes**.

Configuring Flow Control Policies

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 a Flow Control Policy

Before you begin

Configure the network port with the corresponding setting for the flow control that you need. For example, if you enable the send setting for flow-control pause frames in the policy, ensure that the receive parameter in the network port is set to on or to desired. If you want the Cisco UCS port to receive flow-control frames, ensure that the send parameter is set to on or to desire on the network port. If you do not want to use flow control, you can set the send and receive parameters on the network port to off.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies**.

Step 3 Expand the **root** node.

You can only create a flow control policy in the root organization. You cannot create a flow control policy in a sub-organization.

Step 4 Right-click the **Flow Control Policies** node and select **Create Flow Control Policy**.

Step 5 In the **Create Flow Control Policy** wizard, complete the required fields.

Step 6 Click **OK**.

What to do next

Associate the flow control policy with an uplink Ethernet port or port channel.

Deleting a Flow Control Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **LAN** > **Policies** > ***Organization_Name***.
Step 3 Expand the **Flow Control Policies** node.
Step 4 Right-click the policy you want to delete and select **Delete**.
Step 5 If a confirmation dialog box displays, click **Yes**.

Configuring Slow Drain

QoS Slow Drain Device Detection and Mitigation

All data traffic between end devices in the fabric is carried by Fibre Channel services that use link-level, per-hop-based, and buffer-to-buffer flow control. These classes of service do not support end-to-end flow control. When slow devices are attached to the fabric, the end devices do not accept the frames at the configured or negotiated rate. The slow devices lead to an Inter-Switch Link (ISL) credit shortage in the traffic that is destined for these devices, and they congest the links. The credit shortage affects the unrelated flows in the fabric that use the same ISL link even though destination devices do not experience a slow drain.

Similarly, in End-Host Mode, if a server that is directly attached to the Fabric Interconnect receives traffic slowly, it may congest the uplink port shared by other servers. If a slow server is attached to a HIF port on FEX/IOM, it may congest the fabric port and/or uplink port.

Cisco UCS Manager Release 4.0(2) introduces the QoS Slow Drain Detection and Mitigation feature on Cisco UCS 6454 Fabric Interconnects. This feature provides various enhancements that enable you to detect slow drain devices that cause congestion in the network, and also mitigate it. The enhancements are mainly on the edge ports and core ports that connect to the slow drain devices. This is done to minimize the frames stuck condition in the edge and core ports due to slow drain devices that are causing an ISL blockage. To avoid or minimize the stuck condition, you can configure smaller frame timeout for the ports. A smaller frame timeout value helps to alleviate the slow drain condition that affects the fabric by dropping the packets on the edge ports sooner than the time they actually get timed out. This function frees the buffer space in ISL, which can be used by other unrelated flows that do not experience the slow drain condition. Cisco UCS Manager Release 4.1 extends support of this feature to Cisco UCS 64108 Fabric Interconnects.

Note Another way of mitigating network congestion is to use the watchdog timer function, supported on Cisco UCS 6400 Series Fabric Interconnects starting with Cisco UCS Manager 4.2. However, the slow drain and watchdog timer functions are mutually exclusive.

In this release, slow drain detection and mitigation is supported on the following ports:

- FCoE
- Back-plane

Configuring Slow Drain

While configuring slow drain timeout timers, you can select the timeout value from the list of allowed values. You cannot configure custom timeout values.

Note

- In Cisco UCS Manager Release 4.1(3a), the slow drain timeout timer is enabled on the FCoE port by default with a 500ms timeout value. Starting with Cisco UCS Manager Release 4.2(1), the slow drain timeout timer is disabled and the watchdog timer is enabled by default.
- We recommend to change the default timeout values of the Core FCoE port and Edge FCoE Port only when the current default timeout values result in the dropping of packets during high traffic load.
- Slow drain and the watchdog timer cannot be used simultaneously. Attempting to do so will result in an error.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud**.

Step 3 Starting in UCS Manager 4.2.1 click on the **QoS System Class** entry. in earlier releases, go to the **QoS** entry and click to go to the **Work** pane.

Step 4 In the **Work** pane, click the **QoS** tab.

Step 5 Click **Configure Slow Drain**.

Step 6 In the **Configure Slow Drain Timers** dialog box that appears, configure the following fields:

Name	Description
FCoE Port radio button	Whether slow drain timers are enabled on FCoE ports. • **Disabled**—Configuration of slow drain timers is disabled. This is the default option till the previous version of Cisco UCS Manager Release 4.1(3a). • **Enabled**—Configuration of slow drain timers is enabled. Starting with Cisco UCS Manager Release 4.1(3a), this is the default option.
Core FCoE port (ms) drop-down list	The time in milliseconds (ms) after which frames timeout on core FCoE ports. You can select from the following values: • 100 • 200 • 300 • 400 • 500—This is the default value • 600 • 700 • 800 • 900 • 1000

Name	Description
Edge FCoE Port (ms) drop-down list	The time in milliseconds (ms) after which frames timeout on edge FCoE ports. You can select from the following values: • 100 • 200 • 300 • 400 • 500—This is the default value • 600 • 700 • 800 • 900 • 1000

Step 7 Click **OK**.

Step 8 Click **Save Changes**.

Correcting a Slow Drain Condition

Correcting a slow drain condition will work only on those ports that are designated to be in the 'error-disabled' state because of 'slow-drain'.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **IO Modules**.

Step 3 Choose the I/O module on which you want to recover backplane ports that are in the **error-disabled** state.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Correct Slow Drain Condition**.

Step 6 If a confirmation dialog box displays, click **Yes**.

Configuring the Watchdog Timer

The Watchdog Timer

Cisco UCS Manager 4.2 supports the watchdog timer function on Cisco 6400 Series Fabric Interconnects with switch ports that are PFC mode enabled.

Priority flow control, (PFC) also referred to as Class-based Flow Control (CBFC) or Per Priority Pause (PPP), is a mechanism that prevents frame loss that is due to congestion. PFC functions on a per class-of-service (CoS) basis. A PFC storm could occur in the network due to a malfunctioning NIC or switch, causing the PFC frames to be propagated to all senders. This could cause a complete stall in network traffic. To mitigate a PFC storm, you can use a PFC watchdog timer. Configure a PFC watchdog interval to detect whether packets in a no-drop queue are being drained within a specified time period. If packets are present in buffer longer than the configured time period, once the time period is exceeded, all outgoing packets are dropped on the interfaces that match the PFC queue that is not being drained.

Use of watchdog timer and slow drain on are mutually exclusive options. You can enable either the slow drain or watchdog timer, but not both. Starting with Cisco UCS Manager Release 4.2(1), the slow drain timeout timer is disabled and the watchdog timer is enabled by default. The default watchdog interval is 500 with a shutdown multiplier of 1.

Configuring the Watchdog Timer

The watchdog timer cannot be used in connection with slow drain.

Before you begin

If slow drain was used previously, disable slow drain.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud**.

Step 3 Select a fabric interconnect and click on **QoS System Class**.

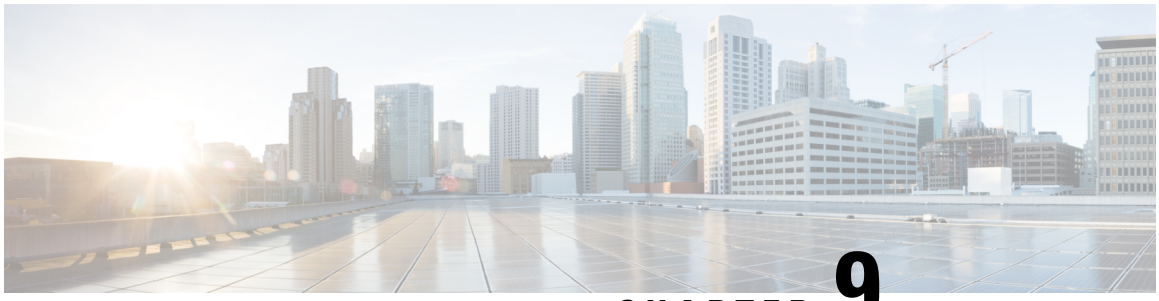
Step 4 In the **General** tab, click on **Configure Watchdog Timers**.

Step 5 In the **Configure WD Timers** window, click **On** for the **WD admin state** to globally enable the PFC watchdog interval for all interfaces, then select a watchdog interval betweem 100 and 1000 milliseconds and a shutdown multiplier between 1 and 10.

The default watchdog interval is 500 and the default shutdown multiplier is 1.

Step 6 Click **OK**.

Step 7 Click **Save Changes**.



CHAPTER 9

Upstream Disjointed Layer-2 Networks

Upstream Disjoint Layer-2 Networks

Upstream disjoint layer-2 networks (disjoint L2 networks) are required if you have two or more Ethernet clouds that never connect, but must be accessed by servers or virtual machines located in the same Cisco UCS domain. For example, you could configure disjoint L2 networks if you require one of the following:

- Servers or virtual machines to access a public network and a backup network
- Servers or virtual machines for more than one customer are located in the same Cisco UCS domain, and that need to access the L2 networks for both customers in a multi-tenant system

Note By default, data traffic in Cisco UCS works on a principle of mutual inclusion. All traffic for all VLANs and upstream networks travels along all uplink ports and port channels. If you have upgraded from a release that does not support upstream disjoint layer-2 networks, you must assign the appropriate uplink interfaces to your VLANs, or traffic for those VLANs continues to flow along all uplink ports and port channels.

The configuration for disjoint L2 networks works on a principle of selective exclusion. Traffic for a VLAN that is designated as part of a disjoint network can only travel along an uplink Ethernet port or port channel that is specifically assigned to that VLAN, and is selectively excluded from all other uplink ports and port channels. However, traffic for VLANs that are not specifically assigned to an uplink Ethernet port or port channel can still travel on all uplink ports or port channels, including those that carry traffic for the disjoint L2 networks.

In Cisco UCS, the VLAN represents the upstream disjoint L2 network. When you design your network topology for disjoint L2 networks, you must assign uplink interfaces to VLANs not the reverse.

For information about the maximum number of supported upstream disjoint L2 networks, see the appropriate *Cisco UCS Configuration Limits for Cisco UCS Manager Guide*.

Guidelines for Configuring Upstream Disjoint L2 Networks

When you plan your configuration for upstream disjoint L2 networks, consider the following:

Ethernet Switching Mode Must Be End-Host Mode

Cisco UCS only supports disjoint L2 networks when the Ethernet switching mode of the fabric interconnects is configured for end-host mode. You cannot connect to disjoint L2 networks if the Ethernet switching mode of the fabric interconnects is switch mode.

Symmetrical Configuration Is Recommended for High Availability

If a Cisco UCS domain is configured for high availability with two fabric interconnects, we recommend that both fabric interconnects are configured with the same set of VLANs.

VLAN Validity Criteria Are the Same for Uplink Ethernet Ports and Port Channels

The VLAN used for the disjoint L2 networks must be configured and assigned to an uplink Ethernet port or uplink Ethernet port channel. If the port or port channel does not include the VLAN, Cisco UCS Manager considers the VLAN invalid and does the following:

- Displays a configuration warning in the **Status Details** area for the server.
- Ignores the configuration for the port or port channel and drops all traffic for that VLAN.

Note The validity criteria are the same for uplink Ethernet ports and uplink Ethernet port channels. Cisco UCS Manager does not differentiate between the two.

Overlapping VLANs Are Not Supported

Cisco UCS does not support overlapping VLANs in disjoint L2 networks. You must ensure that each VLAN only connects to one upstream disjoint L2 domain.

Each vNIC Can Only Communicate with One Disjoint L2 Network

A vNIC can only communicate with one disjoint L2 network. If a server needs to communicate with multiple disjoint L2 networks, you must configure a vNIC for each of those networks.

To communicate with more than two disjoint L2 networks, a server must have a Cisco VIC adapter that supports more than two vNICs.

Appliance Port Must Be Configured with the Same VLAN as Uplink Ethernet Port or Port Channel

For an appliance port to communicate with a disjoint L2 network, you must ensure that at least one uplink Ethernet port or port channel is in the same network and is therefore assigned to the same VLANs that are used by the appliance port. If Cisco UCS Manager cannot identify an uplink Ethernet port or port channel

that includes all VLANs that carry traffic for an appliance port, the appliance port experiences a pinning failure and goes down.

For example, a Cisco UCS domain includes a global VLAN named vlan500 with an ID of 500. vlan500 is created as a global VLAN on the uplink Ethernet port. However, Cisco UCS Manager does not propagate this VLAN to appliance ports. To configure an appliance port with vlan500, you must create another VLAN named vlan500 with an ID of 500 for the appliance port. You can create this duplicate VLAN in the **Appliances** node on the **LAN** tab of the Cisco UCS Manager GUI or the **eth-storage** scope in the Cisco UCS Manager CLI. If you are prompted to check for VLAN Overlap, accept the overlap and Cisco UCS Manager creates the duplicate VLAN for the appliance port.

Default VLAN 1 Cannot Be Configured Explicitly on an Uplink Ethernet Port or Port Channel

Cisco UCS Manager implicitly assigns default VLAN 1 to all uplink ports and port channels. Even if you do not configure any other VLANs, Cisco UCS uses default VLAN 1 to handle data traffic for all uplink ports and port channels.

Note After you configure VLANs in a Cisco UCS domain, default VLAN 1 remains implicitly on all uplink ports and port channels. You cannot explicitly assign default VLAN 1 to an uplink port or port channel, nor can you remove it from an uplink port or port channel.

If you attempt to assign default VLAN 1 to a specific port or port channel, Cisco UCS Manager raises an Update Failed fault.

Therefore, if you configure a Cisco UCS domain for disjoint L2 networks, do not configure any vNICs with default VLAN 1 unless you want all data traffic for that server to be carried on all uplink Ethernet ports and port channels and sent to all upstream networks.

VLANs for Both FIs Must be Concurrently Assigned

When you assign a port to a global VLAN, the VLAN is removed from all of the ports that are not explicitly assigned to the VLAN on both fabric interconnects. The ports on both FIs must be configured at the same time. If the ports are only configured on the first FI, traffic on the second FI will be disrupted.

Upstream Disjoint L2 Networks Pinning Considerations

Communication with an upstream disjoint L2 network requires that you ensure that the pinning is properly configured. Whether you implement soft-pinning or hard-pinning, a VLAN membership mismatch causes traffic for one or more VLANs to be dropped.

Soft-Pinning

Soft-pinning is the default behavior in Cisco UCS. If you plan to implement soft-pinning, you do not need to create LAN pin groups to specify a pin target for a vNIC. Instead, Cisco UCS Manager pins the vNIC to an uplink Ethernet port or port channel according to VLAN membership criteria.

With soft-pinning, Cisco UCS Manager validates data traffic from a vNIC against the VLAN membership of all uplink Ethernet ports and port channels. If you have configured disjoint L2 networks, Cisco UCS Manager must be able to find an uplink Ethernet port or port channel that is assigned to all VLANS on the vNIC. If no

uplink Ethernet port or port channel is configured with all VLANs on the vNIC, Cisco UCS Manager does the following:

- Brings the link down.
- Drops the traffic for all of the VLANs on the vNIC.
- Raises the following faults:
  - Link Down
  - VIF Down

Cisco UCS Manager does not raise a fault or warning about the VLAN configuration.

For example, a vNIC on a server is configured with VLANs 101, 102, and 103. Interface 1/3 is assigned only to VLAN 102. Interfaces 1/1 and 1/2 are not explicitly assigned to a VLAN, which makes them available for traffic on VLANs 101 and 103. As a result of this configuration, the Cisco UCS domain does not include a border port interface that can carry traffic for all three VLANS for which the vNIC is configured. As a result, Cisco UCS Manager brings down the vNIC, drops traffic for all three VLANs on the vNIC, and raises the Link Down and VIF Down faults.

hard-pinning

hard-pinning occurs when you use LAN pin groups to specify the pinning target for the traffic intended for the disjoint L2 networks. In turn, the uplink Ethernet port or port channel that is the pinning target must be configured to communicate with the appropriate disjoint L2 network.

With hard-pinning, Cisco UCS Manager validates data traffic from a vNIC against the VLAN membership of all uplink Ethernet ports and port channels, and validates the LAN pin group configuration to ensure it includes the VLAN and the uplink Ethernet port or port channel. If the validation fails at any point, Cisco UCS Manager does the following:

- Raises a Pinning VLAN Mismatch fault with a severity of Warning.
- Drops traffic for the VLAN.
- Does not bring the link down, so that traffic for other VLANs can continue to flow along it.

For example, if you want to configure hard-pinning for an upstream disjoint L2 network that uses VLAN 177, do the following:

- Create a LAN pin group with the uplink Ethernet port or port channel that carries the traffic for the disjoint L2 network.
- Configure at least one vNIC in the service profile with VLAN 177 and the LAN pin group.
- Assign VLAN 177 to an uplink Ethernet port or port channel included in the LAN pin group

If the configuration fails at any of these three points, then Cisco UCS Manager warns of a VLAN mismatch for VLAN 177 and drops the traffic for that VLAN only.

Note If changes are made to soft-pinning configurations resulting in vNIC VLANs not resolving with disjoint L2 uplink, a warning dialog box is displayed. The warning dialog box allows you to proceed with your configuration or cancel it. If you decide to proceed with the mis- configuration, you will experience a reduction is server traffic performance.

Configuring Cisco UCS for Upstream Disjoint L2 Networks

When you configure a Cisco UCS domain to connect with upstream disjoint L2 networks, you need to ensure that you complete all of the following steps.

Before you begin

Before you begin this configuration, ensure that the ports on the fabric interconnects are properly cabled to support your disjoint L2 networks configuration.

Procedure

	Command or Action	Purpose
Step 1	Configure Ethernet switching mode for both fabric interconnects in Ethernet End-Host Mode.	The Ethernet switching mode must be in End-Host Mode for Cisco UCS to be able to communicate with upstream disjoint L2 networks. For more information, see the *LAN Ports and Port Channel* chapter in this guide..
Step 2	Configure the ports and port channels that you require to carry traffic for the disjoint L2 networks.	
Step 3	(Optional) Configure the LAN pin groups required to pin the traffic for the appropriate uplink Ethernet ports or port channels.	
Step 4	Create one or more VLANs.	These can be named VLANs or private VLANs. For a cluster configuration, we recommend that you create the VLANs accessible to both fabric interconnects.
Step 5	Assign the desired ports or port channels to the VLANs for the disjoint L2 networks.	When this step is complete, traffic for these VLANs is be sent through the trunks for the assigned ports and/or port channels.
Step 6	Ensure that the service profiles for all servers that need to communicate with the disjoint L2 networks include the correct LAN connectivity configuration. This configuration ensures that the vNICs direct the traffic to the appropriate VLAN.	You can complete this configuration through one or more vNIC templates, or when you configure the networking options for the service profile. For more information about vNIC templates and service profiles, see the *Cisco UCS Manager Storage Management Guide*.

Creating a VLAN for an Upstream Disjoint L2 Network

For upstream disjoint L2 networks, we recommend that you create VLANs in the VLAN Manager.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 On the **LAN** tab, click the **LAN** node.

Step 3 In the **Work** pane, click the **LAN Uplinks Manager** link on the **LAN Uplinks** tab.

The LAN Uplinks Manager opens in a separate window.

Step 4 In the LAN Uplinks Manager, click **VLANs** > **VLAN Manager**.

You can create the VLAN on any of the sub tabs. However, if you use the **All** sub tab, you can view all of the configured VLANs in the table.

Step 5 On the icon bar to the right of the table, click +.

If the + icon is disabled, click an entry in the table to enable it.

Step 6 In the **Create VLANs** dialog box, specify the required fields and then click **OK**.

You cannot create VLANs with IDs from 3968 to 4047. This range of VLAN IDs is reserved.

Step 7 Repeat Steps 6 and 7 to create additional VLANs.

What to do next

Assign ports and port channels to the VLANs.

Assigning Ports and Port Channels to VLANs

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 On the **LAN** tab, click the **LAN** node.

Step 3 In the **Work** pane, click the **LAN Uplinks Manager** link on the **LAN Uplinks** tab.

The LAN Uplinks Manager opens in a separate window.

Step 4 In the LAN Uplinks Manager, click **VLANs** > **VLAN Manager**.

You can create the VLAN on any of the sub tabs. However, if you use the **All** sub tab, you can view all of the configured VLANs in the table.

Step 5 Click one of the following sub tabs to configure ports and port channels on that fabric interconnect:

Subtab	Description
Fabric A	Displays the ports, port channels, and VLANs that are accessible to fabric interconnect A.
Fabric B	Displays the ports, port channels, and VLANs that are accessible to fabric interconnect B.

Step 6 In the **Ports and Port Channels** table, do the following:

- To assign an Uplink Ethernet port channel to a VLAN, expand the **Port Channels** node and click the port channel you want to assign to the VLAN.
- To assign an Uplink Ethernet port to the VLAN, expand the **Uplink Interfaces** node and click the port you want to assign to the VLAN

You can hold down the **Ctrl** key and click multiple ports or port channels to assign to them to the same VLAN or set of VLANs .

Step 7 In the **VLANs** table, expand the appropriate node if necessary and click the VLAN to which you want to assign the port or port channel.

You can hold down the **Ctrl** key and click multiple VLANs if you want to assign the same set of ports and/or port channels to them.

Step 8 Click the **Add to VLAN/VLAN Group** button.

Step 9 If a confirmation dialog box displays, click **Yes**.

Step 10 To assign additional ports or port channels to VLANs on the same fabric, repeat Steps 6, 7, and 8.

Step 11 To assign additional ports or port channels to VLANs on a different fabric, repeat Steps 5 through 8.

If the Cisco UCS domain is configured for high availability with two fabric interconnects, we recommend that you create the same set of VLANs on both fabric interconnects.

Step 12 If a confirmation dialog box displays, click **Yes**.

Step 13 Click **Apply** if you want to continue to work in the VLAN Manager, or click **OK** to close the window.

After a port or port channel is assigned to one or more VLANs, it is removed from all other VLANs.

Viewing Ports and Port Channels Assigned to VLANs

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 On the **LAN** tab, click the **LAN** node.

Step 3 In the **Work** pane, click the **LAN Uplinks Manager** link on the **LAN Uplinks** tab.

The LAN Uplinks Manager opens in a separate window.

Step 4 In the LAN Uplinks Manager, click **VLANs** > **VLAN Manager**.

You can create the VLAN on any of the sub tabs. However, if you use the **All** sub tab, you can view all of the configured VLANs in the table.

Step 5 Click one of the following sub tabs to configure ports and port channels on that fabric interconnect:

Subtab	Description
Fabric A	Displays the ports, port channels, and VLANs that are accessible to fabric interconnect A.
Fabric B	Displays the ports, port channels, and VLANs that are accessible to fabric interconnect B.

Step 6 In the **VLANs** table, expand the appropriate node and the VLAN for which you want to view the assigned ports or port channels.

Removing Ports and Port Channels from VLANs

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 On the **LAN** tab, click the **LAN** node.

Step 3 In the **Work** pane, click the **LAN Uplinks Manager** link on the **LAN Uplinks** tab.

The LAN Uplinks Manager opens in a separate window.

Step 4 In the LAN Uplinks Manager, click **VLANs** > **VLAN Manager**.

You can create the VLAN on any of the sub tabs. However, if you use the **All** sub tab, you can view all of the configured VLANs in the table.

Step 5 Click one of the following sub tabs to configure ports and port channels on that fabric interconnect:

Subtab	Description
Fabric A	Displays the ports, port channels, and VLANs that are accessible to fabric interconnect A.
Fabric B	Displays the ports, port channels, and VLANs that are accessible to fabric interconnect B.

Step 6 In the **VLANs** table, expand the appropriate node and the VLAN from which you want to remove a port or port channel.

Step 7 Click the port or port channel that you want to remove from the VLAN.

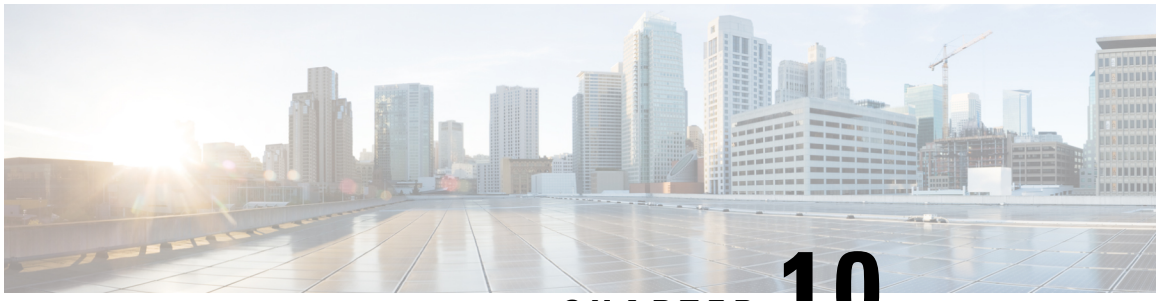
Hold down the **Ctrl** key to click multiple ports or port channels.

Step 8 Click the **Remove from VLAN/VLAN Group** button.

Step 9 If a confirmation dialog box displays, click **Yes**.

Step 10 Click **Apply** if you want to continue to work in the VLAN Manager, or click **OK** to close the window.

Important
If you remove all port or port channel interfaces from a VLAN, the VLAN returns to the default behavior and data traffic on that VLAN flows on all uplink ports and port channels. Based on the configuration in the Cisco UCS domain, this default behavior can cause Cisco UCS Manager to drop traffic for that VLAN. To avoid this occurrence, Cisco recommends that you assign at least one interface to the VLAN or delete the VLAN.



CHAPTER 10

Network-Related Policies

Configuring vNIC Templates

vNIC Template

The vNIC LAN connectivity policy defines how a vNIC on a server connects to the LAN.

Cisco UCS Manager does not automatically create a VM-FEX port profile with the correct settings when you create a vNIC template. If you want to create a VM-FEX port profile, you must configure the target of the vNIC template as a VM. You must include this policy in a service profile for it to take effect.

You can select VLAN groups in addition to any individual VLAN while creating a vNIC template.

Note If your server has two Emulex or QLogic NICs (Cisco UCS CNA M71KR-E or Cisco UCS CNA M71KR-Q), you must configure vNIC policies for both adapters in your service profile to get a user-defined MAC address for both NICs. If you do not configure policies for both NICs, Windows still detects both of them in the PCI bus. Then because the second eth is not part of your service profile, Windows assigns it a hardware MAC address. If you then move the service profile to a different server, Windows sees additional NICs because one NIC did not have a user-defined MAC address.

Creating a vNIC Template

Before you begin

This policy requires that one or more of the following resources already exist in the system:

- Named VLAN
- MAC pool
- QoS policy
- LAN pin group
- Statistics threshold policy
- Network Control policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multi tenancy, expand the **root** node.

Step 4 Right-click the **vNIC Templates** node and choose **Create vNIC Template**.

Step 5 In the **Create vNIC Template** dialog box:

a) In the **General** area, complete the following fields:

Name	Description
Name field	The name of the vNIC template. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Description field	A user-defined description of the template. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).

Name	Description
Fabric ID field	The fabric interconnect associated with the component. If you want vNICs created from this template to be able to access the second fabric interconnect if the default one is unavailable, check the **Enable Failover** check box. **Note** Do not enable vNIC fabric failover under the following circumstances: • If the Cisco UCS domain is running in Ethernet switch mode. vNIC fabric failover is not supported in that mode. If all Ethernet uplinks on one fabric interconnect fail, the vNICs do not fail over to the other. • If you plan to associate one or more vNICs created from this template to a server with an adapter that does not support fabric failover, such as the Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter. If so, Cisco UCS Manager generates a configuration fault when you associate the service profile with the server.
Redundancy Type	The Redundancy type that you choose initiates a fabric failover using vNIC/HBA redundancy pairs. • **Primary Template**— Creates configurations that can be shared with the Secondary template. Any other shared changes on the Primary template are automatically synchronized to the Secondary template. • **Secondary Template**—All shared configurations are inherited from the Primary template. • **No Redundancy**—Legacy vNIC/vHBA template behavior. Select this option if you do not want to use redundancy.
Target list box	A list of the possible targets for vNICs created from this template. The target you choose determines whether or not Cisco UCS Manager automatically creates a VM-FEX port profile with the appropriate settings for the vNIC template. This can be one of the following: • **Adapter**—The vNICs apply to all adapters. No VM-FEX port profile is created if you choose this option. • **VM**—The vNICs apply to all virtual machines. A VM-FEX port profile is created if you choose this option.
Template Type field	• **Initial Template**: vNICs created from this template are not updated if the template changes. • **Updating Template**: vNICs created from this template are updated if the template changes.

Name	Description
Enable QinQ check box	Check this check box to allow VIC QinQ Tunneling.
Enable EtherChannel Pinning check box	Check this check box to allow the vNIC adapters that support EtherChannel to utilize multiple uplink ports for traffic distribution. This setting is applicable only to adapters with EtherChannel capabilities. **Note** Ensure that the number of transmit queues (Tx) configured in a vNIC is greater than 1 (minimum of 2). It is recommended to use an even number of transmit queues.

b) In the **VLANs** area, use the table to select the VLAN to assign to vNICs created from this template. The table contains the following columns:

Name	Description
Select column	Check the check box in this column for each VLAN that you want to use. **Note** VLANs can not be assigned to the same vNIC.
Name column	Displays the name of the VLAN.
Native VLAN column	Click the radio button in this column to designate one of the VLANs as the native VLAN. **Note** When modifying the Native VLAN settings, a warning message will inform you about the required port flap and its brief connectivity impact (20-40 seconds). You can choose to proceed with the changes by selecting Yes, No, or Cancel.
VLAN ID column	The unique identifier of the VLAN.
QinQ VLAN column	Click the radio button in this column to allow VIC QinQ Tunneling on the VLAN. The supported QinQ VLAN ID range is 2 to 4094. QinQ VLAN can be a Native or a Non-Native VLAN. You can configure a Native VLAN and a Non-Native VLAN as a QinQ VLAN on the vNIC. When using the Native VLAN as QinQ VLAN, no additional VLAN can be configured on the vNIC. **Note** This *QinQ VLAN* selection is considered only when the *Enable QinQ* check box is selected.

c) In the **VLAN Groups** area, use the table to select the VLAN group to assign to vNICs created from this template. The table contains the following columns:

Name	Description
Select column	Check the check box in this column for each VLAN Group that you want to use.
Name column	The name of the VLAN Group.

d) In the **Policies** area, complete the following fields:

Name	Description
CDN Source field	This can be one of the following options: • **vNIC Name**—Uses the vNIC template name of the vNIC instance as the CDN name. This is the default option. • **User Defined**—Displays the CDN Name field for you to enter a user-defined CDN name for the vNIC template. Refer to the *Cisco UCS Manager Server Management Guide* for more information on Consistent Device Naming.
CDN Name field	Enter the CDN Name. This field is displayed only when the **CDN Source - User Defined** option is selected.
MTU field	The maximum transmission unit, or packet size, that vNICs created from this vNIC template should use. Enter an integer between 1500 and 9000. **Note** If the vNIC template has an associated QoS policy, the MTU specified here must be equal to or less than the MTU specified in the associated QoS system class. If this MTU value exceeds the MTU value in the QoS system class, packets may be dropped during data transmission. For VIC 1400 Series, VIC 14000 Series, and VIC 15000 Series adapters, you can change the MTU size of the vNIC from the host interface settings. When the Overlay network is configured, make sure that the new value is equal to or less than the MTU specified in the associated QoS system class or packets could be dropped during data transmission.
MAC Pool drop-down list	The MAC address pool that vNICs created from this vNIC template should use.
QoS Policy drop-down list	The quality of service policy that vNICs created from this vNIC template should use.
Network Control Policy drop-down list	The network control policy that vNICs created from this vNIC template should use.
Pin Group drop-down list	The LAN pin group that vNICs created from this vNIC template should use.

Name	Description
Stats Threshold Policy drop-down list	The statistics collection policy that vNICs created from this vNIC template should use.

e) In the **Connections Policies** area, complete the following fields:

Name	Description
Connection Policy radio button	Choose the type of connection policy to associate with the vNIC. This can be one of the following: • **Dynamic vNIC** • **usNIC** • **VMQ** • **SRIOV HPN**
Connection Policy drop-down list	Choose the connection policy that the vNIC should use. The values displayed depend on the type of connection policy chosen. You can also create a new connection policy in this area.

Step 6 Click **OK**.

What to do next

Include the vNIC template in a service profile.

Creating vNIC Template Pairs

Procedure

Step 1 In the Navigation pane, click the **LAN** tab. On the **LAN** tab, expand **LAN > Policies.**

Step 2 Expand the node for the organization where you want to create the policy. If the system does not include multi-tenancy, expand the root node.

Step 3 Right-click the **vNIC Templates** node and choose **Create vNIC Template**. In the **Create vNIC Template** dialog box, assign a **Name**, **Description**, and select the **Fabric ID** for the template.

Step 4 Select the **Redundancy Type** as **Primary** or **Secondary** or **No Redundancy**. See the redundancy type descriptions below.

Step 5 Select the **Peer Redundancy Template**—to choose the name of the corresponding **Primary** or **Secondary** redundancy template to perform the template pairing from the **Primary** or **Secondary** redundancy template.

- **Primary**—Creates configurations that can be shared with the Secondary template. Any other shared changes on the Primary template are automatically synchronized to the Secondary template.
  - **VLANS**

- **Template Type**
- **MTU**
- **Network Control Policies**
- **Connection Policies**
- **QoS Policy**
- **Stats Threshold Policy**

Following is a list of non-shared configurations:

- **Fabric ID**

  Note
  The Fabric ID must be mutually exclusive. If you assign the Primary template to Fabric A, then Fabric B is automatically assigned to the Secondary template as part of the synchronization from the Primary template.

- **CDN Source**
- **MAC Pool**
- **Description**
- **Pin Group Policy**

- **Secondary**—

  All shared configurations are inherited from the Primary template.
- **No Redundancy**—

  Legacy vNIC template behavior.

Step 6 Click **OK**.

What to do next

After you create the vNIC redundancy template pair, you can use the redundancy template pair to create redundancy vNIC pairs for any service profile in the same organization or sub-organization.

Undo vNIC Template Pairs

You can undo the vNIC template pair by changing the Peer Redundancy Template so that there is no peer template for the Primary or the Secondary template. When you undo a vNIC template pair, the corresponding vNIC pairs also becomes undone.

Procedure

Select **not set** from the **Peer Redundancy Template** drop-down list to undo the paring between the peer Primary or Secondary redundancy template used to perform the template pairing. You can also select **None** as the **Redundancy Type** to undo the pairing.

Note
If you delete one template in a pair, you are prompt to delete the other template in the pair. If you do not delete the other template in the pair, that template resets its peer reference and retains its redundancy type.

Binding a vNIC to a vNIC Template

You can bind a vNIC associated with a service profile to a vNIC template. When you bind the vNIC to a vNIC template, Cisco UCS Manager configures the vNIC with the values defined in the vNIC template. If the existing vNIC configuration does not match the vNIC template, Cisco UCS Manager reconfigures the vNIC. You can only change the configuration of a bound vNIC through the associated vNIC template. You cannot bind a vNIC to a vNIC template if the service profile that includes the vNIC is already bound to a service profile template.

Important If the vNIC is reconfigured when you bind it to a template, Cisco UCS Manager reboots the server associated with the service profile.

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Service Profiles**.

Step 3 Expand the node for the organization that includes the service profile with the vNIC you want to bind.

If the system does not include multi-tenancy, expand the **root** node.

Step 4 Expand ***Service_Profile_Name*** > **vNICs**.

Step 5 Click the vNIC you want to bind to a template.

Step 6 In the **Work** pane, click the **General** tab.

Step 7 In the **Actions** area, click **Bind to a Template**.

Step 8 In the **Bind to a vNIC Template** dialog box, do the following:

a) From the **vNIC Template** drop-down list, choose the template to which you want to bind the vNIC.
b) Click **OK**.

Step 9 In the warning dialog box, click **Yes** to acknowledge that Cisco UCS Manager may need to reboot the server if the binding causes the vNIC to be reconfigured.

Unbinding a vNIC from a vNIC Template

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Service Profiles**.

Step 3 Expand the node for the organization that includes the service profile with the vNIC you want to unbind.

If the system does not include multi-tenancy, expand the **root** node.

Step 4 Expand ***Service_Profile_Name*** > **vNICs**.

Step 5 Click the vNIC you want to unbind from a template.

Step 6 In the **Work** pane, click the **General** tab.

Step 7 In the **Actions** area, click **Unbind from a Template**.

Step 8 If a confirmation dialog box displays, click **Yes**.

Deleting a vNIC Template

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies** > ***Organization_Name***.

Step 3 Expand the **vNIC Templates** node.

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

Step 5 If a confirmation dialog box displays, click **Yes**.

Configuring Adapter Policies

Ethernet and Fibre Channel Adapter Policies

These 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 a cluster configuration with two fabric interconnects

Note For Fibre Channel adapter policies, the values displayed by Cisco UCS Manager may not match those displayed by applications such as QLogic SANsurfer. For example, the following values may result in an apparent mismatch between SANsurfer and Cisco UCS Manager:

- Max LUNs Per Target—SANsurfer has a maximum of 256 LUNs and does not display more than that number. Cisco UCS Manager supports a higher maximum number of LUNs. This parameter is applicable only for FC-Initiator.
- Link Down Timeout—In SANsurfer, you configure the timeout threshold for link down in seconds. In Cisco UCS Manager, you configure this value in milliseconds. Therefore, a value of 5500 ms in Cisco UCS Manager displays as 5s in SANsurfer.
- Max Data Field Size—SANsurfer has allowed values of 512, 1024, and 2048. Cisco UCS Manager allows you to set values of any size. Therefore, a value of 900 in Cisco UCS Manager displays as 512 in SANsurfer.
- LUN Queue Depth—The LUN queue depth setting is available for Windows system FC adapter policies. Queue depth is the number of commands that the HBA can send and receive in a single transmission per LUN. Windows Storport driver sets this to a default value of 20 for physical miniports and to 250 for virtual miniports. This setting adjusts the initial queue depth for all LUNs on the adapter. Valid range for this value is 1 - 254. The default LUN queue depth is 20. This feature only works with Cisco UCS Manager version 3.1(2) and higher. This parameter is applicable only for FC-Initiator.
- IO TimeOut Retry—When the target device does not respond to an IO request within the specified timeout, the FC adapter cancels the pending command then resends the same IO after the timer expires. The FC adapter valid range for this value is 1 - 59 seconds. The default IO retry timeout is 5 seconds. This feature only works with Cisco UCS Manager version 3.1(2) and higher.

From Cisco UCS Manager 4.3(4a), the adapter settings are optimized for Windows, Linux, and VMware for Cisco UCS VIC 1400 Series adapters, Cisco UCS VIC 14000 Series adapters, and Cisco UCS VIC 15000 Series adapters.

Operating System Specific Adapter Policies

By default, Cisco UCS provides a set of Ethernet adapter policies and Fibre Channel 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.

Important 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.

However, if you are creating an Ethernet adapter policy for an OS (instead of using the default adapter policy), you must use the following formulas to calculate values that work for that OS.

Depending on the UCS firmware, your driver interrupt calculations may be different. Newer UCS firmware uses a calculation that differs from previous versions. Later driver release versions on Linux operating systems now use a different formula to calculate the Interrupt Count. In this formula, the Interrupt Count is the maximum of either the Transmit Queue or the Receive Queue plus 2.

Interrupt Count in Linux Adapter Policies

Drivers on Linux operating systems use differing formulas to calculate the Interrupt Count, depending on the eNIC driver version. The UCS 3.2 release increased the number of Tx and Rx queues for the eNIC driver from 8 to 256 each.

Use one of the following strategies, according to your driver version.

For Linux drivers before the UCS 3.2 firmware release, use the following formula to calculate the Interrupt Count.

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

On drivers for UCS firmware release 3.2 and higher, the Linux eNIC drivers use the following formula to calculate the Interrupt Count.

Interrupt Count = Max(Tx, Rx) + 2

For example:

Interrupt Count wq = 32, rq = 32, cq = 64 - then Interrupt Count = Max(32, 32) + 2 = 34
Interrupt Count wq = 64, rq = 8, cq = 72 – then Interrupt Count = Max(64, 8) + 2 = 66
Interrupt Count wq = 1, rq = 16, cq = 17 - then Interrupt count = Max(1, 16) + 2 = 18

Interrupt Count in Windows Adapter Policies

For Windows OS, the recommended adapter policy in UCS Manager for VIC 1400 series and above adapters is Win-HPN and if RDMA is used, the recommended policy is Win-HPN-SMB. For VIC 1400 series and above adapters, the recommended interrupt value setting is 512 and the Windows VIC driver takes care of allocating the required number of Interrupts.

For VIC 1300 and VIC 1200 series adapters, the recommended UCS Manager adapter policy is Windows and the Interrupt would be TX + RX + 2, rounded to closest power of 2. The maximum supported Windows queues is 8 for Rx Queues and 1 for Tx Queues.

Example for VIC 1200 and VIC 1300 series adapters:

Tx = 1, Rx = 4, CQ = 5, Interrupt = 8 (1 + 4 rounded to nearest power of 2), Enable RSS

Example for VIC 1400 series , 14000 series and 15000 series adapters and above adapters:

Tx = 1, Rx = 4, CQ = 5, Interrupt = 512 , Enable RSS

NVMe over Fabrics using Fibre Channel

The NVM Express (NVMe) interface allows host software to communicate with a non-volatile memory subsystem. This interface is optimized for Enterprise non-volatile storage, which is typically attached as a register level interface to the PCI Express (PCIe) interface.

NVMe over Fabrics using Fibre Channel (FC-NVMe) defines a mapping protocol for applying the NVMe interface to Fibre Channel. This protocol defines how Fibre Channel services and specified Information Units (IUs) are used to perform the services defined by NVMe over a Fibre Channel fabric. NVMe initiators can access and transfer information to NVMe targets over Fibre Channel.

FC-NVMe combines the advantages of Fibre Channel and NVMe. You get the improved performance of NVMe along with the flexibility and the scalability of the shared storage architecture. Cisco UCS Manager Release 4.0(2) supports NVMe over Fabrics using Fibre Channel on UCS VIC 1400 Series adapters.

Starting with UCS Manager release 4.3(2b), NVMeoF using RDMA is supported on Cisco UCS VIC 14000 series adapters.

Starting with UCS Manager release 4.2(2), NVMeoF using Fibre Channel is supported on Cisco UCS VIC 15000 series adapters.

Cisco UCS Manager provides the recommended FC NVME Initiator adapter policies in the list of pre-configured adapter policies. To create a new FC-NVMe adapter policy, follow the steps in the *Creating a Fibre Channel Adapter Policy* section.

NVMe over Fabrics Using RDMA

NVMe over Fabrics (NVMeoF) is a communication protocol that allows one computer to access NVMe namespaces available on another computer. NVMeoF is similar to NVMe, but differs in the network-related steps involved in using the NVMeoF storage devices. The commands for discovering, connecting, and disconnecting a NVMeoF storage device are integrated into the **nvme** utility provided in Linux..

The NVMeoF fabric that Cisco supports is RDMA over Converged Ethernet version 2 (RoCEv2). RoCEv2 is a fabric protocol that runs over UDP. It requires a no-drop policy.

The eNIC RDMA driver works in conjunction with the eNIC driver, which must be loaded first when configuring NVMeoF.

Cisco UCS Manager provides the default Linux-NVMe-RoCE adapter policy for creating NVMe RoCEv2 interfaces. Do not use the default Linux adapter policy. For complete information on configuring RoCEv2 over NVMeoF, refer to the *Cisco UCS Manager Configuration Guide for RDMA over Converged Ethernet (RoCE) v2*.

NVMeoF using RDMA is supported on M5 B-Series or C-Series Servers with Cisco UCS VIC 1400 Series adapters.

Starting with UCS Manager release 4.3(2b), NVMeOF using RDMA is supported on Cisco UCS VIC 14000 series adapters.

Starting with UCS Manager release 4.2(2), NVMeOF using RDMA is supported on Cisco UCS VIC 15000 series adapters.

Accelerated Receive Flow Steering

Accelerated Receive Flow Steering (ARFS) is hardware-assisted receive flow steering that can increase CPU data cache hit rate by steering kernel level processing of packets to the CPU where the application thread consuming the packet is running.

Using ARFS can improve usage CPU efficiency and reduce network traffic latency. Each receive queue of a CPU has an interrupt associated with it. You can configure the Interrupt Service Routine (ISR) to run on a CPU. The ISR moves the packet from the receive queue to the backlog of one of the current CPUs, which processes the packet later. If the application is not running on this CPU, the CPU must copy the packet to non-local memory, which adds to latency. ARFS can reduce this latency by moving that particular stream to the receive queue of the CPU on which the application is running.

ARFS is disabled by default and can be enabled through Cisco UCS Manager. To configure ARFS, do the following:

1. Create an adapter policy with ARFS enabled.
2. Associate the adapter policy with a service profile.
3. Enable ARFS on a host:
   a. Turn off Interrupt Request Queue (IRQ) balance.
   b. Associate IRQ with different CPUs.
   c. Enable ntuple by using ethtool.

Guidelines and Limitations for Accelerated Receive Flow Steering

- ARFS supports 64 filters per vNIC
- ARFS is supported on the following adapters:
  - Cisco UCS VIC 1300 Series
  - Cisco UCS VIC 1400 Series
  - Cisco UCS VIC 14000 Series
  - Cisco UCS VIC 15000 Series
- ARFS is supported on the following Operating Systems:
  - Red Hat Enterprise Linux 8.4 and higher versions
  - Red Hat Enterprise Linux 9.0 and higher versions
  - SUSE Linux Enterprise Server 15 SP4 and higher versions
  - Ubuntu 20.04 and higher versions

Interrupt Coalescing

Adapters typically generate a large number of interrupts that a host CPU must service. Interrupt coalescing reduces the number of interrupts serviced by the host CPU. This is done by interrupting the host CPU only once for multiple occurrences of the same event over a configurable coalescing interval.

When interrupt coalescing is enabled for receive operations, the adapter continues to receive packets, but the host CPU does not immediately receive an interrupt for each packet. A coalescing timer starts when the first packet is received by the adapter. When the configured coalescing interval times out, the adapter generates one interrupt with the packets received during that interval. The NIC driver on the host then services the multiple packets that are received. Reduction in the number of interrupts generated reduces the time spent by the host CPU on context switches. This means that the CPU has more time to process packets, which results in better throughput and latency.

Adaptive Interrupt Coalescing

Due to the coalescing interval, the handling of received packets adds to latency. For small packets with a low packet rate, this latency increases. To avoid this increase in latency, the driver can adapt to the pattern of traffic flowing through it and adjust the interrupt coalescing interval for a better response from the server.

Adaptive interrupt coalescing (AIC) is most effective in connection-oriented low link utilization scenarios including email server, databases server, and LDAP server. It is not suited for line-rate traffic.

Guidelines and Limitations for Adaptive Interrupt Coalescing

- Adaptive Interrupt Coalescing (AIC) does not provide any reduction in latency when the link utilization is more than 80 percent.
- Enabling AIC disables static coalescing.
- AIC is supported on the following Operating Systems:
  - Red Hat Enterprise Linux 6.4 and higher versions
  - SUSE Linux Enterprise Server 11 SP2 and higher versions
  - XenServer 6.5 and higher versions
  - Ubuntu 14.04.2 and higher versions

PTP Adapter Policy

Precision Time Protocol (PTP) precisely synchronizes the server clock with other devices and peripherals on Linux operating systems. PTP must be set for each adapter, and is only supported on Cisco UCS VIC 15000 Series and later adapters.

Clocks managed by PTP follow a client-worker hierarchy, with workers synchronized to a master client The hierarchy is updated by the best master clock (BMC) algorithm, which runs on every clock. One PTP interface per adapter must be enabled to synchronize it to the grand master clock. After enabling PTP, the host must be rebooted.

The time stamping parameters displayed by **`ethtool -T int_name`** will show a field for PTP Hardware Clock. The value of `PTP Hardware Clock: 0` shows that PTP is enabled for the interface. Otherwise, it will show `PTP Hardware Clock: none`.

Note PTP Adapter Policy is not supported on Cisco UCS VIC 1400 and 14000 series adapters.

RDMA Over Converged Ethernet Overview

Remote Direct Memory Access (RDMA) improves performance by enabling direct data exchange in and out of a server. NVMe over Ethernet (NVMeoF) support for RDMA provides faster access to NVMe namespaces on another computer. RDMA over Converged Ethernet (RoCE) allows direct memory access over an Ethernet network. RoCE is a link layer protocol, and hence, it allows communication between any two hosts in the same Ethernet broadcast domain. RoCE delivers superior performance compared to traditional network socket implementations because of lower latency, lower CPU utilization and higher utilization of network bandwidth. Windows 2012 R2 and later versions use RDMA for accelerating and improving the performance of SMB file sharing and Live Migration.

Cisco UCS Manager supports RoCE for Microsoft SMB Direct. It sends additional configuration information to the adapter while creating or modifying an Ethernet adapter policy. Basic RoCE is also referred to as RoCE version 1 (RoCEv1), and is supported on UCS Manager releases from UCS Manager 2.2(4b) to 4.1(1a).

With Cisco UCS Manager 4.1(1a) and later releases, the RoCEv2 protocol is used.

RDMA Over Converged Ethernet (RoCE) v2

RDMA over Converged Ethernet version 2 (RoCEv2) is an *internet layer* protocol, which means that RoCEv2 packets can be routed. RoCEv2 allows direct memory access over the network by encapsulating an Infiniband (IB) transport packet over Ethernet.

The RoCEv2 protocol exists on top of either the UDP/IPv4 or the UDP/IPv6 protocol. The UDP destination port number 4791 has been reserved for RoCEv2. Since RoCEv2 packets are routable, the RoCEv2 protocol is sometimes called Routable RoCE.

RoCEv2 is supported on the Windows, Linux, and ESXi Operating Systems.

Guidelines for Using SMB Direct support on Windows using RDMA over converged Ethernet (RoCE) v2

General Guidelines and Limitations:

- Cisco UCS Manager release 4.1.x and later releases support Microsoft SMB Direct with RoCEv2 on Microsoft Windows Server 2019 and later. Cisco recommends that you have all KB updates from Microsoft for your Windows Server release.

Note RoCEv2 is not supported on Microsoft Windows Server 2016.

- Cisco recommends you check UCS Hardware and Software Compatibility specific to your UCS Manager release to determine support for Microsoft SMB Direct with RoCEv2 on Microsoft Windows.
- Microsoft SMB Direct with RoCEv2 is supported only with Cisco UCS VIC 1400 Series, 14000 Series, and 15000 Series adapters. It is not supported with UCS VIC 1200 Series and 1300 Series adapters. SMB Direct with RoCEv2 is supported on all UCS Fabric Interconnects.

Note RoCEv1 is not supported with Cisco UCS VIC 1400 Series, Cisco UCS VIC 14000 Series, and Cisco UCS VIC 15000 Series.

- RoCEv2 configuration is supported only between Cisco adapters. Interoperability between Cisco adapters and third party adapters is not supported.
- RoCEv2 supports two RoCEv2 enabled vNIC per adapter and four virtual ports per adapter interface, independent of SET switch configuration.
- RoCEv2 cannot be used on the same vNIC interface as NVGRE, NetFlow, and VMQ features.
- RoCEv2 cannot be used with usNIC.
- RoCEv2-enabled vNIC interfaces must have the no-drop QoS system class enabled in UCS Manager.
- The RoCE Properties queue pairs setting must for be a minimum of 4 queue pairs.
- Maximum number of queue pairs per adapter is 2048.
- The QoS No Drop class configuration must be properly configured on upstream switches such as Cisco Nexus 9000 series switches. QoS configurations will vary between different upstream switches.
- The maximum number of memory regions per rNIC interface is 131072.
- UCS Manager does not support fabric failover for vNICs with RoCEv2 enabled.
- SMB Direct with RoCEv2 is supported on both IPv4 and IPv6.
- RoCEv2 cannot be used with GENEVE offload.

MTU Properties:

- In older versions of the VIC driver, the MTU was derived from either a UCS Manager service profile or from the Cisco IMC vNIC MTU setting in non-cluster setup. This behavior changes on Cisco UCS VIC 1400 Series and later adapters, where MTU is controlled from the Windows OS Jumbo Packet advanced property. A value configured from UCS Manager or Cisco IMC has no effect.
- The RoCEv2 MTU value is always power-of-two and its maximum limit is 4096.
- RoCEv2 MTU is derived from the Ethernet MTU.
- RoCEv2 MTU is the highest power-of-two that is less than the Ethernet MTU. For example:
  - if the Ethernet value is 1500, then the RoCEv2 MTU value is 1024
  - if the Ethernet value is 4096, then the RoCEv2 MTU value is 4096
  - if the Ethernet value is 9000, then the RoCEv2 MTU value is 4096

Windows NDPKI Modes of Operation:

- Cisco's implementation of Network Direct Kernel Provider Interface (NDPKI) supports two modes of operation: Mode 1 and Mode 2. Mode 1 and Mode 2 relate to the implementation of Network Direct Kernel Provider Interface (NDKPI): Mode 1 is native RDMA, and Mode 2 involves configuration for the virtual port with RDMA. Cisco does not support NDPKI Mode 3 operation.
- The recommended default adapter policy for RoCEv2 Mode 1 is Win-HPN-SMBd .
- The recommended default adapter policy for RoCEv2 Mode 2 is MQ-SMBd.
- RoCEv2 enabled vNICs for Mode2 operation require the QoS host control policy set to full.
- Mode 2 is inclusive of Mode 1: Mode 1 must be enabled to operate Mode 2.

- On Windows, the RoCEv2 interface supports MSI & MSIx interrupt modes. By default, it is in MSIx interrupt mode. Cisco recommends you avoid changing interrupt mode when the interface is configured with RoCEv2 properties.

Downgrade Limitations: Cisco recommends you remove the RoCEv2 configuration before downgrading to any non-supported RoCEv2 release. If the configuration is not removed or disabled, downgrade will fail.

Guidelines for using NVMe over Fabrics (NVMeoF) with RoCEv2 on Linux

General Guidelines and Limitations:

- Cisco recommends you check UCS Hardware and Software Compatibility specific to your UCS Manager release to determine support for NVMeoF. NVMeoF is supported on UCS M5 and later B-Series and C-Series servers.
- NVMe over RDMA with RoCEv2 is supported with the fourth generation Cisco UCS VIC 1400 Series UCS VIC 14000, and UCS VIC 15000 Series and UCS VIC 15000 Series adapters. NVMe over RDMA is not supported on UCS 6324 Fabric Interconnects or on UCS VIC 1200 Series and 1300 Series adapters.
- When creating RoCEv2 interfaces, use Cisco UCS Manager provided Linux-NVMe-RoCE adapter policy.

Note Do not use the default Linux Adapter policy with RoCEv2; RoCEv2 interfaces will not be created in the OS.

- When configuring RoCEv2 interfaces, use both the enic and enic_rdma binary drivers downloaded from Cisco.com and install the matched set of enic and enic_rdma drivers. Attempting to use the binary enic_rdma driver downloaded from Cisco.com with an inbox enic driver will not work.
- RoCEv2 supports maximum two RoCEv2 enabled interfaces per adapter.
- Booting from an NVMeoF namespace is not supported.
- Layer 3 routing is not supported.
- RoCEv2 does not support bonding.
- Saving a crashdump to an NVMeoF namespace during a system crash is not supported.
- NVMeoF cannot be used with usNIC, VMFEX, VxLAN, VMQ, VMMQ, NVGRE, GENEVE Offload, and DPDK features.
- Netflow monitoring is not supported on RoCEv2 interfaces.
- In the Linux-NVMe-RoCE policy, do not change values of Queue Pairs, Memory Regions, Resource Groups, and Priority settings other than to Cisco provided default values. NVMeoF functionality may not be guaranteed with different settings for Queue Pairs, Memory Regions, Resource Groups, and Priority.
- The QoS no drop class configuration must be properly configured on upstream switches such as Cisco Nexus 9000 series switches. QoS configurations will vary between different upstream switches.
- Set MTU size correctly on the VLANs and QoS policy on upstream switches.
- Spanning Tree Protocol (STP) may cause temporary loss of network connectivity when a failover or failback event occurs. To prevent this issue from occurring, disable STP on uplink switches.

- UCS Manager does not support fabric failover for vNICs with RoCEv2 enabled.

Interrupts

- Linux RoCEv2 interface supports only MSIx interrupt mode. Cisco recommends avoiding changing interrupt mode when the interface is configured with RoCEv2 properties.
- The minimum interrupt count for using RoCEv2 with Linux is 8.

Downgrade Limitations:

- Cisco recommends you remove the RoCEv2 configuration before downgrading to any non-supported RoCEv2 release.

Guidelines for using RoCEv2 Protocol in the Native ENIC driver on ESXi

General Guidelines and Limitations:

- Cisco UCS Manager release 4.2(3b) supports RoCEv2 only on ESXi 7.0 U3.
- Cisco recommends you check UCS Hardware and Software Compatibility specific to your UCS Manager release to determine support for ESXi. RoCEv2 on ESXi is supported on UCS B-Series and C-Series servers with Cisco UCS VIC 15000 Series and later adapters.
- RoCEv2 on ESXi is not supported on UCS VIC 1200, 1300 and 1400 Series adapters.
- RDMA on ESXi nENIC currently supports only ESXi NVME that is part of the ESXi kernel. The current implementation does not support the ESXi user space RDMA application.
- Multiple mac addresses and multiple VLANs are supported only on VIC 15000 Series adapters.
- RoCEv2 supports maximum two RoCEv2 enabled interfaces per adapter.
- Pvrdma, VSAN over RDMA, and iSER are not supported.
- The COS setting is not supported on UCS Manager.

Downgrade Limitations:

- Cisco recommends you remove the RoCEv2 configuration before downgrading to any non-supported RoCEv2 release.

GENEVE Offload

Cisco UCS Manager now supports Generic Network Virtualization Encapsulation (GENEVE) Offload on the ESXi platform, which allows essentially any information to be encoded in a packet and passed between tunnel endpoints. GENEVE provides the overlay capability to create isolated, multi-tenant broadcast domains across data center fabrics on UCS VIC 1400 Series, VIC 14000 Series, and VIC 15000 Series adapters. Using the GENEVE protocol allows you to create logical networks that span physical network boundaries.

GENEVE offload is present in all Ethernet adapter policies and is disabled by default.

Cisco recommends configuring the following values in the Ethernet adapter policy when GENEVE offload is enabled:

- Transmit Queues: 1

- TX Ring Size: 4096
- Receive Queues: 8
- RX Ring Size: 4096
- Completion Queues: 16
- Interrupts: 32

The following features are not supported when GENEVE offload is enabled on any interface:

- Azure Stack QoS
- RoCEv2

Beginning with Cisco UCS Manager 4.3(4a), GENEVE offload-enabled interfaces support Advanced Filters and NetQueue on Cisco UCS 15000 Series VIC adapters. GENEVE offload also supports ENS, VMQ, and aRFS.

Limitations with GENEVE offload:

- GENEVE offload is supported only with Cisco UCS VIC1400, VIC 14000, and VIC 15000 series adapters. It is not supported on Cisco UCS VIC 1300 Series and 1200 Series adapters.
- External outer IPV6 is not supported with GENEVE offload.
- Cisco UCS Manager 4.3(5a) supports IPv6 overlay offload functionality and is compatible with ESXi 8.0 U1 and its later versions.
- Cisco recommends that you remove the GENEVE offload configuration before downgrading to any non-supported release versions.

Enhanced Network Stack support with Geneve Offload

Enhanced Network Stack (ENS) also known as Enhanced Data Path Mode on ESXi, uses DPDK-like techniques for higher throughput and employs polling to achieve high packet rates. It utilizes the VMware ENS stack and the VIC ENS driver (`nenic-ens`) for uplink ports. The ESXi operating system selects the appropriate driver (`nenic` for standard mode or `nenic-ens` for ENS mode) based on the mode set on the NSX-T vSwitch.

Capabilities of nenic-ens Driver:

- Supports TSO for both IPv4 & IPv6.
- Supports Geneve offload with IPv4/v6 outer header.
- Supports Tx/Rx checksum offload for IPv4/v6 inner/outer packets.
- Supports NetQueue (also known as Geneve filter in ESXi environments).
- Does not support RSS.

Recommended Ethernet Adapter Policy Settings:

For ENS for releases prior to 4.3(4a):

- Single Tx/Rx queue
- Tx/Rx ring size of 4096
- Enable GENEVE offload

For releases 4.3(4a) or later:

- Enable **Multi Tx/Rx queues** (NetQueue allows the use of multiple transmit (Tx) and receive (Rx) queues for network traffic and helps in distributing the load more evenly across multiple CPU cores.)
- Enable **Advanced Filter**.
- Enable **GENEVE offload**.
- Enable **VMQ Connection Policy** with 2 or more VMQ queues, applied to vNICs for VM data path.

Note For detailed information on implementing GENEVE offload configuration, see the VMware NSX-T.

Creating an Ethernet Adapter Policy

Tip If the fields in an area do not display, click the **Expand** icon to the right of the heading.

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multi tenancy, expand the **root** node.

Step 4 Right-click **Adapter Policies** and choose **Create Ethernet Adapter Policy**.

Step 5 Enter a **Name** and optional **Description** for the policy.

This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

Step 6 (Optional) In the **Resources** area, adjust the following values:

Name	Description
Pooled radio button	Whether the queue resources are pooled or not. • **Disabled**—Pooling is disabled. • **Enabled**—Pooling is enabled. When pooling is enabled, the counts of queue resources specified in the Adapter Policy will be the total number of queues allocated across all vPorts.

Name	Description
Transmit Queues field	The number of transmit queue resources to allocate. Enter an integer between 1 and 1000.
Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 16384. Cisco UCS VIC 1400 series and 14000 series adapters support maximum 4K (4096) Ring Size. Cisco UCS VIC 15000 Series and above adapters support up to 16K (16384) Ring Size.
Receive Queues field	The number of receive queue resources to allocate. Enter an integer between 1 and 1000.
Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 16384. Cisco UCS VIC 1400 series and 14000 series adapters support maximum 4K (4096) Ring Size. Cisco UCS VIC 15000 Series and above adapters support up to 16K (16384) Ring Size.
Completion Queues field	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Enter an integer between 1 and 2000.
Interrupts field	The number of interrupt resources to allocate. In general, this value should be equal to (Completion Queues + 2) rounded up to nearest power of 2. Enter an integer between 1 and 1024. 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

Step 7 (Optional) In the **Options** area, adjust the following values:

Note
The RoCE Version 2 Option should be used with UCS Manager 4.2.1 and later releases.

Name	Description
Transmit Checksum Offload radio button	This can be one of the following: • **Disabled**—The CPU calculates all packet checksums. • **Enabled**—The CPU sends all packets to the hardware so that the checksum can be calculated. This option may reduce CPU overhead. **Note** This option affects only packets sent from the interface.
Receive Checksum Offload radio button	This can be one of the following: • **Disabled**—The CPU validates all packet checksums. • **Enabled**—The CPU sends all packet checksums to the hardware for validation. This option may reduce CPU overhead. **Note** This option affects only packets received by the interface.
TCP Segmentation Offload radio button	This can be one of the following: • **Disabled**—The CPU segments large TCP packets. • **Enabled**—The CPU sends large TCP packets to the hardware to be segmented. This option may reduce CPU overhead and increase throughput rate. **Note** This option is also known as Large Send Offload (LSO) and affects only packets sent from the interface.
TCP Large Receive Offload radio button	This can be one of the following: • **Disabled**—The CPU processes all large packets. • **Enabled**—The hardware reassembles all segmented packets before sending them to the CPU. This option may reduce CPU utilization and increase inbound throughput. **Note** This option affects only packets received by the interface.
Receive Side Scaling radio button	RSS distributes network receive processing across multiple CPUs in multiprocessor systems. This can be one of the following: • **Disabled**—Network receive processing is always handled by a single processor even if additional processors are available. • **Enabled**—Network receive processing is shared across processors whenever possible.

Name	Description
Accelerated Receive Flow Steering radio button	Packet processing for a flow must be performed on the local CPU. This is supported for Linux operating systems only. This can be one of the following: • **Disabled**—The CPU is not specified. • **Enabled**—Packet processing is performed on the local CPU.
Network Virtualization using Generic Routing Encapsulation radio button	Whether NVGRE overlay hardware offloads for TSO and checksum are enabled. This can be one of the following: • **Disabled**—NVGRE overlay hardware offloads are not enabled. • **Enabled**—NVGRE overlay hardware offloads are enabled. NVGRE overlay hardware offloads can be enabled when using UCS VIC 1400 and 14000 Series adapters.
Virtual Extensible LANradio button	Whether VXLAN overlay hardware offloads for TSO and checksum are enabled. This can be one of the following: • **Disabled**—VXLAN overlay hardware offloads are not enabled. • **Enabled**—VXLAN overlay hardware offloads are enabled. VXLAN overlay hardware offloads can be enabled with RoCE and VMQ when using UCS VIC 1400 Series adapters. VXLAN overlay hardware offloads can be enabled with RoCEv2 and VMQ when using Cisco UCS VIC 1400 ,VIC 14000, or 15000 Series adapters
GENEVE radio button	Whether Generic Network Virtualization Encapsulation (GENEVE) overlay hardware offloads are enabled. GENEVE offload provides the overlay capability to create isolated, multi-tenant broadcast domains across data center fabrics on VIC 1400, VIC 14000, and VIC 15000 series adapters. GENEVE Offload supports both IPv4 and IPv6 protocols for ESXi on Cisco UCS 15000 series adapters. This can be one of the following: • **Disabled**—GENEVE overlay offloads are not enabled. • **Enabled**—GENEVE overlay offloads are enabled.

Name	Description
AzureStack-Host QoS radio button	Enable this feature to successfully deploy Azure Stack based solutions with RDMA enabled. • **Enabled**—Enabling AzureStack-Host QoS on an adapter allows the user to carve out traffic classes for RDMA traffic and ensure a desired portion of the bandwidth is allocated to it. • **Disabled**—Disables the AzureStack-Host QoS feature on the adapter.
Failback Timeout field	After a vNIC has started using its secondary interface, this setting controls how long the primary interface must be available before the system resumes using the primary interface for the vNIC. Enter a number of seconds between 0 and 600.
Interrupt Mode radio button	The preferred driver interrupt mode. This can be one of the following: • **MSI X**—Message Signaled Interrupts (MSI) with the optional extension. This is the recommended option. **Note** If you set **Interrupt Mode** as **Msi-X**, and if **pci=nomsi** parameter is enabled in `/boot/grub/grub.conf` on RHEL system, then **pci=nomsi** would block the eNIC/fNIC driver to run in the Msi-X mode, impacting system performance. • **MSI**—MSI only. • **IN Tx**—PCI IN Tx interrupts. **Note** INTx interrupt mode is not supported with the ESX nenic driver and Windows nenic driver. MSI interrupt mode on Fibre Channel interfaces is not supported. If the MSI interrupt mode is configured for Fibre Channel interface, Fibre Channel interfaces will come up in MSIx mode.
Interrupt Coalescing Type radio button	This can be one of the following: • **Min**—The system waits for the time specified in the **Interrupt Timer** field before sending another interrupt event. • **Idle**—The system does not send an interrupt until there is a period of no activity lasting as least as long as the time specified in the **Interrupt Timer** field.
Interrupt Timer field	The time to wait between interrupts or the idle period that must be encountered before an interrupt is sent. Enter a value between 1 and 65535. To turn off interrupt coalescing, enter 0 (zero) in this field.

Name	Description
RoCE radio button	Whether Remote Direct Memory Access over an Ethernet network is enabled. This can be one of the following: • **Disabled**—RoCE is disabled on the Ethernet adapter. • **Enabled**—RoCE is enabled on the Ethernet adapter.
RoCE Properties area	Lists the RoCE properties. This area is enabled only if you enable RoCE.
Version 1 radio button	RoCE Version 1 is a link layer protocol. It allows communication between any two hosts in the same Ethernet broadcast domain. Whether RoCE Version 1 is enabled. This can be one of the following: • **Disabled**—RoCE version 1 is disabled on the Ethernet adapter. • **Enabled**—RoCE version 1 is enabled on the Ethernet adapter.
Version 2 radio button	RoCEv2 is an internet layer protocol. RoCEv2 packets can be routed. This is possible because RoCEv2 packets now include an IP and UDP header. Whether RoCE Version 2 is enabled. This can be one of the following: • **Disabled**—RoCE version 2 is disabled on the Ethernet adapter. • **Enabled**—RoCE version 2 is enabled on the Ethernet adapter.
Queue Pairs field	The number of queue pairs per adapter. Enter an integer between 1 and 8192. It is recommended that this number be an integer power of 2.
Memory Regions field	The number of memory regions per adapter. Enter an integer between 1 and 524288. It is recommended that this number be an integer power of 2.
Resource Groups field	The number of resource groups per adapter. Enter an integer between 1 and 128. It is recommended that this number be an integer power of 2 greater than or equal to the number of CPU cores on the system for optimum performance.

Name	Description
Priority field	Priority is set as **Platinum** by default. The supported values include: • Fibre Channel • Best Effort • Bronze • Silver • Gold • Platinum For RoCE version 2, set **Priority** as **Platinum**.
Advance Filter radio button	Whether Advance Filter over an Ethernet network is enabled. This can be one of the following: • **Disabled**—Advance filter is disabled on the Ethernet adapter. • **Enabled**—Advance filter is enabled on the Ethernet adapter.
Interrupt Scaling radio button	Whether Interrupt Scaling over an Ethernet network is enabled. This can be one of the following: • **Disabled**—Interrupt Scaling is disabled on the Ethernet adapter. • **Enabled**—Interrupt Scaling is enabled on the Ethernet adapter.
Adapter PTP radio button	Whether Precision Time Protocol is implemented for adapters on an Ethernet network. PTP is only available on Linux operating systems and can only be enabled for UCS VIC 15000 series and later adapters. • **Disabled**—PTP is disabled on the Ethernet adapter. • **Enabled**—PTP is enabled on the Ethernet adapter.

Step 8 Click **OK**.

Step 9 If a confirmation dialog box displays, click **Yes**.

Receive Side Scaling (RSS)

Receive Side Scaling Version 2 (RSSv2)

Beginning with Cisco UCS Manager release 4.3(2a), UCS Manager supports Receive Side Scaling Version 2 (RSSv2). RSSv2 is supported on Windows 2019 and Windows 2022 Operating System (OS) and it requires Windows NENIC driver.

Receive Side Scaling (RSS) supports multiple cores to process the incoming data traffic. With RSS enabled Windows NENIC driver and Cisco UCS VIC adapter, you can configure multiple hardware receive queues

on the Physical Function (PF). With VMMQ enabled on the VIC, you can configure multiple hardware receive queues per Virtual Machine (VM). RSSv2 is compatible with RSS. Before using the RSSv2 functionality, ensure the NENIC driver supports RSSv2. In general, a NENIC driver supports 4 queues. With RSSv2, the NENIC driver has no upper limit on the number of hardware queues for PF or VM.

RSSv2 is supported on the following adapters and servers:

- Cisco UCS VIC 15000 Series adapters
- Cisco UCS B-Series, C-Series, and X-Series M6 and later versions of servers.

RSSv2 is compatible with the following features:

- Remote Direct Memory Access (RDMA)
- Virtual Machine Multi Queues (VMMQ)
- Virtual Extensible LAN (VXLAN)
- Network Virtualization using Generic Routing Encapsulation (NVGRE)
- Azure Stack QoS

Note For more information on RSSv2 with Windows Driver, see Microsoft > Windows Driver > Network documentation.

Configuring an Ethernet Adapter Policy to Enable RSS on Windows Operating Systems

To enable Receive Side Scaling (RSS) or Receive Side Scaling Version 2 (RSSv2) and configure an Ethernet Adapter Policy, do the following:

Procedure

Step 1 In the Navigation pane, click **Servers**.

Step 2 Expand **Servers > Policies**.

Step 3 Expand the node for the organization where you want to create the policy. If the system does not include multi tenancy, expand the root node.

Step 4 Right-click **Adapter Policies** and choose **Create Ethernet Adapter Policy**.

Step 5 Enter a **Name** and optional **Description** for the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

Step 6 Create an Ethernet adapter policy.

In the **Resources** area, use the following values when creating the Ethernet adapter policy:

Name	Description
Pooled radio button	Whether the queue resources are pooled or not. • **Disabled**—Pooling is disabled. • **Enabled**—Pooling is enabled. When pooling is enabled, the counts of queue resources specified in the Adapter Policy will be the total number of queues allocated across all vPorts.
Transmit Queues field	The number of transmit queue resources to allocate. Enter an integer between 1 and 1000.
Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 16384. Cisco UCS VIC 1400 Series and older adapters support maximum 4K (4096) Ring Size. Cisco UCS VIC 14000 Series and older adapters support maximum 16K (4096) Ring Size. Cisco UCS VIC 15000 Series and above adapters support up to 16K (16384) Ring Size.
Receive Queues field	The number of receive queue resources to allocate. Enter an integer between 1 and 1000.
Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 16384. Cisco UCS VIC 1400 Series and older adapters support maximum 4K (4096) Ring Size. Cisco UCS VIC 14000 Series and above adapters support up to 16K (16384) Ring Size. Cisco UCS VIC 15000 Series and above adapters support up to 16K (16384) Ring Size.
Completion Queues field	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources.
Interrupts field	The number of interrupt resources to allocate. In general, this value should be equal to (Completion Queues + 2) rounded up to nearest power of 2.

In the **Options** area, use the following values:

Name	Description
Transmit Checksum Offload radio button	This can be one of the following: • **Disabled**—The CPU calculates all packet checksums. • **Enabled**—The CPU sends all packets to the hardware so that the checksum can be calculated. This option may reduce CPU overhead.
Receive Checksum Offload radio button	This can be one of the following: • **Disabled**—The CPU validates all packet checksums. • **Enabled**—The CPU sends all packet checksums to the hardware for validation. This option may reduce CPU overhead.
TCP Segmentation Offload radio button	This can be one of the following: • **Disabled**—The CPU segments large TCP packets. • **Enabled**—The CPU sends large TCP packets to the hardware to be segmented. This option may reduce CPU overhead and increase throughput rate.
TCP Large Receive Offload radio button	This can be one of the following: • **Disabled**—The CPU processes all large packets. • **Enabled**—The hardware reassembles all segmented packets before sending them to the CPU. This option may reduce CPU utilization and increase inbound throughput.
Receive Side Scaling radio button	RSS distributes network receive processing across multiple CPUs in multiprocessor systems. This can be one of the following: • **Disabled**—Network receive processing is always handled by a single processor even if additional processors are available. • **Enabled**—Network receive processing is shared across processors whenever possible. Click **Enabled** to support RSS or RSSv2.
Accelerated Receive Flow Steering radio button	Packet processing for a flow must be performed on the local CPU. This is supported for Linux operating systems only. This can be one of the following: • **Disabled**—The CPU is not specified. • **Enabled**—Packet processing is performed on the local CPU.

Name	Description
Network Virtualization using Generic Routing Encapsulation radio button	Whether NVGRE overlay hardware offloads for TSO and checksum are enabled. This can be one of the following: • **Disabled**—NVGRE overlay hardware offloads are not enabled. • **Enabled**—NVGRE overlay hardware offloads are enabled. NVGRE overlay hardware offloads can be enabled when using UCS VIC 1400 and 14000 Series adapters.
Virtual Extensible LAN radio button	Whether VXLAN overlay hardware offloads for TSO and checksum are enabled. This can be one of the following: • **Disabled**—VXLAN overlay hardware offloads are not enabled. • **Enabled**—VXLAN overlay hardware offloads are enabled. VXLAN overlay hardware offloads can be enabled with RoCE and VMQ when using UCS VIC 1400 Series adapters. VXLAN overlay hardware offloads can be enabled with RoCEv2 and VMQ when using Cisco UCS VIC 1400 or VIC 15000, VIC 14000, or 15000 Series Series adapters
GENEVE	Whether Generic Network Virtualization Encapsulation (GENEVE) overlay hardware offloads are enabled. GENEVE offload provides the overlay capability to create isolated, multi-tenant broadcast domains across data center fabrics on Cisco UCS VIC 1400, VIC 14000, or 15000 Series series adapters. This can be one of the following: • **Disabled**—GENEVE overlay offloads are not enabled. • **Enabled**—GENEVE overlay offloads are enabled.
AzureStack-Host QoS	Enable this feature to successfully deploy Azure Stack based solutions with RDMA enabled. • **Enabled**—Enabling AzureStack-Host QoS on an adapter allows the user to carve out traffic classes for RDMA traffic and ensure a desired portion of the bandwidth is allocated to it. • **Disabled**—Disables the AzureStack-Host QoS feature on the adapter.
Failback Timeout field	After a vNIC has started using its secondary interface, this setting controls how long the primary interface must be available before the system resumes using the primary interface for the vNIC. Enter a number of seconds between 0 and 600.

Name	Description
Interrupt Mode radio button	The preferred driver interrupt mode. • **MSI X**—Message Signaled Interrupts (MSI) with the optional extension. RSS or RSSv2 is supported only on *MSI X*. • **MSI**—MSI only. • **IN Tx**—PCI IN Tx interrupts.
Interrupt Coalescing Type radio button	This can be one of the following: • **Min**—The system waits for the time specified in the **Interrupt Timer** field before sending another interrupt event. • **Idle**—The system does not send an interrupt until there is a period of no activity lasting as least as long as the time specified in the **Interrupt Timer** field.
Interrupt Timer field	The time to wait between interrupts or the idle period that must be encountered before an interrupt is sent. Enter a value between 1 and 65535. To turn off interrupt coalescing, enter 0 (zero) in this field.
RoCE radio button	Whether Remote Direct Memory Access over an Ethernet network is enabled. This can be one of the following: • **Disabled**—RoCE is disabled on the Ethernet adapter. • **Enabled**—RoCE is enabled on the Ethernet adapter.
RoCE Properties area	Lists the RoCE properties. This area is enabled only if you enable RoCE.
Version 1 radio button	RoCE Version 1 is a link layer protocol. It allows communication between any two hosts in the same Ethernet broadcast domain. Whether RoCE Version 1 is enabled. This can be one of the following: • **Disabled**—RoCE version 1 is disabled on the Ethernet adapter. • **Enabled**—RoCE version 1 is enabled on the Ethernet adapter.
Version 2 radio button	RoCEv2 is an internet layer protocol. RoCEv2 packets can be routed. This is possible because RoCEv2 packets now include an IP and UDP header. Whether RoCE Version 2 is enabled. This can be one of the following: • **Disabled**—RoCE version 2 is disabled on the Ethernet adapter. • **Enabled**—RoCE version 2 is enabled on the Ethernet adapter. If you enable RoCE version 2, you can also set the **Priority** field.

Name	Description
Queue Pairs field	The number of queue pairs per adapter. Enter an integer between 1 and 8192. It is recommended that this number be an integer power of 2.
Priority drop-down list	Pre-defined set of Global (system wide) QoS classes. These are: • Fibre Channel • Best Effort • Bronze • Silver • Gold • Platinum For RoCE version 2, set **Priority** as **Platinum**.
Memory Regions field	The number of memory regions per adapter. Enter an integer between 1 and 524288. It is recommended that this number be an integer power of 2.
Resource Groups field	The number of resource groups per adapter. Enter an integer between 1 and 128. It is recommended that this number be an integer power of 2 greater than or equal to the number of CPU cores on the system for optimum performance.
Advance Filter radio button	Whether Advance Filter over an Ethernet network is enabled. This can be one of the following: • **Disabled**—Advance filter is disabled on the Ethernet adapter. • **Enabled**—Advance filter is enabled on the Ethernet adapter.
Interrupt Scaling radio button	Whether Interrupt Scaling over an Ethernet network is enabled. This can be one of the following: • **Disabled**—Interrupt Scaling is disabled on the Ethernet adapter. • **Enabled**—Interrupt Scaling is enabled on the Ethernet adapter.
Adapter PTP radio button	Whether Precision Time Protocol is implemented for adapters on an Ethernet network. PTP is only available on Linux operating systems and can only be enabled for Cisco UCS VIC 14000 and Cisco UCS VIC 15000 series and later adapters. • **Disabled**—PTP is disabled on the Ethernet adapter. • **Enabled**—PTP is enabled on the Ethernet adapter.

Click **OK**. Click **Yes** to confirm the Ethernet Adapter Policy creation.

Step 7 Install RSS or RSSv2 capable latest NENIC driver version.

Note
For more information, see Cisco UCS Virtual Interface Card Drivers Installation Guide.

Step 8 Reboot the server.

Configuring an Ethernet Adapter Policy to Enable eNIC Support for RSS on VMware ESXi

Cisco UCS Manager includes eNIC support for the Receive Side Scaling (RSS) feature on ESXi 5.5 and later releases.

Procedure

Step 1 Create an Ethernet adapter policy.

Use the following parameters when creating the Ethernet adapter policy.

In the **Resources** area, set the following options:

- Transmit Queues = 1
- Receive Queues = n (up to 16)
- Completion Queues = # of Transmit Queues + # of Receive Queues
- Interrupts = (# Completion Queues +2) rounded up to the nearest power of 2

In the **Options** area, set the following option:

- Receive Side Scaling (RSS) = Enabled

Step 2 Install the appropriate drivers according to the UCS Hardware and Software Compatibility.

For more information, see the *Cisco UCS Virtual Interface Card Drivers Installation Guide*.

Step 3 Reboot the server.

Configuring an Ethernet Adapter Policy to Support RSS and Multiple Transmit Queues on VMware ESXi

This configuration enables Receive Side Scaling (RSS) and multiple transmit (Tx) queues for improved network performance in VMware ESXi 8.0 U3 and later, using Ethernet Adapter Policy in Cisco UCS Manager.

Prerequisites:

- **Cisco UCS Manager:** Supported from Cisco UCS Manager Release 4.3(6a) onwards.
- **VMware ESXi:** Version 8.0 U3 or later
- **nenic driver on ESXi:** Minimum required nenic driver version is 2.0.17.0-1OEM.800.1.0.20613240 (for ESXi 8.0U3).
- **Hardware:** Supported on Cisco UCS 1400, 14000, and 15000 series adapters.

Procedure

Step 1 Create an Ethernet adapter policy. Use the following parameters when creating the Ethernet adapter policy.

In the **Resources** area, set the following options:

- Transmit Queues = n (up to 16)
- Receive Queues = n (up to 16)
- Completion Queues = # of Transmit Queues + # of Receive Queues
- Interrupts = (# Completion Queues +2) rounded up to the nearest power of 2

In the **Options** area, set the following option:

- Receive Side Scaling (RSS) = Enabled
- VMQ Connection Policy = Disabled

Note
When VMQ is disabled, RSS engines handle the queue distribution, which may result in the Rx netqueue count appearing as 1 in ESXi command outputs. If VMQ is enabled, the Rx queue count will reflect the VMQ queues, and RSS engines may not be reported as active. Hence, to support RSS with multiple transmit queues, VMQ must be disabled and RSS must be enabled.

For more information, see Creating an Ethernet Adapter Policy, on page 168.

Step 2 Install the appropriate drivers according to the UCS Hardware and Software Compatibility.

For more information, see the *Cisco UCS Virtual Interface Card Drivers Installation Guide*.

Step 3 Reboot the server.

Configuring an Ethernet Adapter Policy to Enable eNIC Support for MRQS on Linux Operating Systems

Cisco UCS Manager includes eNIC support for the Multiple Receive Queue Support (MRQS) feature on Red Hat Enterprise Linux Version 6.x and SUSE Linux Enterprise Server Version 11.x.

Procedure

Step 1 Create an Ethernet adapter policy.

Use the following parameters when creating the Ethernet adapter policy:

- Transmit Queues = 1
- Receive Queues = n (up to 8)
- Completion Queues = # of Transmit Queues + # of Receive Queues
- Interrupts = # Completion Queues + 2
- Receive Side Scaling (RSS) = Enabled
- Interrupt Mode = Msi-X

Note
If you set **Interrupt Mode** as **Msi-X**, and if **pci=nomsi** parameter is enabled in `/boot/grub/grub.conf` on RHEL system, then **pci=nomsi** would block the eNIC/fNIC driver to run in the **Msi-X** mode, impacting system performance.

Step 2 Install an eNIC driver Version 2.1.1.35 or later.

For more information, see the *Cisco UCS Virtual Interface Card Drivers Installation Guide*.

Step 3 Reboot the server.

Configuring an Ethernet Adapter Policy to Enable Stateless Offloads with NVGRE

Cisco UCS Manager supports stateless offloads with NVGRE on Cisco UCS VIC 1300 Series adapters that are installed on servers running on Windows Server 2012 R2 operating systems and higher versions. NVGRE feature is also supported on servers with Cisco UCS VIC 1400 Series, Cisco UCS VIC 14000 Series , and Cisco UCS VIC 15000 Series adapters running on Windows Server 2016. Stateless offloads with NVGRE cannot be used with Netflow, usNIC, or VM-FEX.

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multi tenancy, expand the **root** node.

Step 4 Right-click **Adapter Policies** and choose **Create Ethernet Adapter Policy**.

a) In the **Resources** area, set the following options:

- Transmit Queues = 1
- Receive Queues = n (up to 8)
- Completion Queues = # of Transmit Queues + # of Receive Queues
- Interrupts = # Completion Queues + 2

b) In the **Options** area, set the following options:

- Network Virtualization using Generic Routing Encapsulation = Enabled
- Interrupt Mode = Msi-X

Note
If you set **Interrupt Mode** as **Msi-X**, and if **pci=nomsi** parameter is enabled in `/boot/grub/grub.conf` on RHEL system, then **pci=nomsi** would block the eNIC/fNIC driver to run in the **Msi-X** mode, impacting system performance.

For more information on creating an Ethernet adapter policy, see Creating an Ethernet Adapter Policy, on page 168.

Step 5 Click **OK** to create the Ethernet adapter policy.

Step 6 Install an eNIC driver Version 3.0.0.8 or later.

For more information, see the *Cisco UCS Virtual Interface Card Drivers Installation Guide*.

Step 7 Reboot the server.

Configuring an Ethernet Adapter Policy to Enable Stateless Offloads with VXLAN

VXLAN with Receive Side-Scaling (RSS) support starts with the Cisco UCS Manager 3.1(2) release. RSS is supported with VXLAN stateless offload on VIC adapters 1300 Series and SIOC on Cisco UCS S3260 system for ESXi 5.5 and later releases.

Cisco UCS Manager 4.0(1a) Release introduces VXLAN support on servers with Cisco UCS VIC 1400 Series running ESXi 6.5 and later releases. Stateless offloads with VXLAN cannot be used with NetFlow, usNIC, VM-FEX, or Netqueue.

VXLAN support for Linux and Windows 2016 starts with Cisco UCS Manager 4.0(1a) for VIC 1400 Series adapters.

VXLAN is now supported on Cisco UCS VIC 1300, 1400, 14000, and 15000 Series adapters.

The maximum amount of receive queues may be up to 16 for Cisco UCS VIC 1300 Series and Cisco UCS 1400 and 14000 Series adapters on ESXi.

Cisco UCS VIC 15000 Series adapters also support up to 16 receive queues on ESXi.

Note VXLAN stateless hardware offloads are not supported with Guest OS TCP traffic over IPv6 on UCS VIC 1300 Series adapters. However, Cisco UCS VIC 1400, 14000, and 15000 series adapters do not have this VxLAN offload limitation.

- To run VXLAN encapsulated TCP traffic over IPV6, disable the VXLAN stateless offloads feature.
- To disable the VXLAN stateless offload feature in UCS Manager, disable the Virtual Extensible LAN field in the Ethernet Adapter Policy.

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multi tenancy, expand the **root** node.

Step 4 Right-click **Adapter Policies** and choose **Create Ethernet Adapter Policy**.

a) In the **Resources** area, set the following options:

- Transmit Queues = 1
- Receive Queues = n (up to 16)
- Completion Queues = # of Transmit Queues + # of Receive Queues
- Interrupts = # Completion Queues + 2

b) In the **Options** area, set the following options:

- Receive Side Scaling = Enabled
- Virtual Extensible LAN = Enabled
- Interrupt Mode = Msi-X

Note
If you set **Interrupt Mode** as **Msi-X**, and if **pci=nomsi** parameter is enabled in `/boot/grub/grub.conf` on RHEL system, then **pci=nomsi** would block the eNIC/fNIC driver to run in the **Msi-X** mode, impacting system performance.

For more information on creating an ethernet adapter policy, see Creating an Ethernet Adapter Policy, on page 168.

Step 5 Click **OK** to create the Ethernet adapter policy.

Step 6 Install an eNIC driver Version 2.1.2.59 or later.

For more information, see the *Cisco UCS Virtual Interface Card Drivers Installation Guide*.

Step 7 Reboot the server.

Deleting an Ethernet Adapter Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **LAN** > **Policies** > ***Organization_Name***.
Step 3 Expand the **Adapter Policies** node.
Step 4 Right-click the Ethernet adapter policy that you want to delete and choose **Delete**.
Step 5 If a confirmation dialog box displays, click **Yes**.

Configuring the Default vNIC Behavior Policy

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**—Cisco UCS Manager 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, Cisco UCS Manager 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 a Default vNIC Behavior Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **LAN** > **Policies**.

Step 3 Expand the **root** node.

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

Step 4 Click **Default vNIC Behavior**.

Step 5 On the **General Tab**, in the **Properties** area, click one of the following radio buttons in the **Action** field:

- **None**—Cisco UCS Manager 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, Cisco UCS Manager creates the required vNICs based on the adapter installed in the server associated with the service profile.

Step 6 Click **Save Changes**.

Configuring LAN Connectivity Policies

About the LAN and SAN Connectivity Policies

Connectivity policies determine the connections and the network communication resources between the server and the LAN or SAN on the network. These policies use pools to assign MAC addresses, WWNs, and WWPNs to servers and to identify the vNICs and vHBAs that the servers use to communicate with the network.

Note We do not recommend that you use static IDs in connectivity policies, because these policies are included in service profiles and service profile templates and can be used to configure multiple servers.

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.

Interactions between Service Profiles and Connectivity Policies

You can configure the LAN and SAN connectivity for a service profile through either of the following methods:

- LAN and SAN connectivity policies that are referenced in the service profile
- Local vNICs and vHBAs that are created in the service profile
- Local vNICs and a SAN connectivity policy
- Local vHBAs and a LAN connectivity policy

Cisco UCS maintains mutual exclusivity between connectivity policies and local vNIC and vHBA configuration in the service profile. You cannot have a combination of connectivity policies and locally created vNICs or vHBAs. When you include a LAN connectivity policy in a service profile, all existing vNIC configuration is erased, and when you include a SAN connectivity policy, all existing vHBA configuration in that service profile is erased.

Creating a LAN Connectivity Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multi tenancy, expand the **root** node.

Step 4 Right-click **LAN Connectivity Policies** and choose **Create LAN Connectivity Policy**.

Step 5 In the **Create LAN Connectivity Policy** dialog box, enter a name and optional description.

Step 6 Do one of the following:

- To add vNICs to the LAN connectivity policy, continue with Step 7.
- To add iSCSI vNICs to the LAN connectivity policy and use iSCSI boot with the server, continue with Step 8.

Step 7 To add vNICs, click **Add** next to the plus sign and complete the following fields in the **Create vNIC** dialog box:

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

You can also create a MAC pool from this area.

b) Choose the **Fabric ID**, select the **VLANs** that you want to use, enter the **MTU**, and choose a **Pin Group**.

You can also add a VLAN and enable QinQ on a vNIC. For more information, see Enabling QinQ on a vNIC of a Service Profile, on page 120.

Note
Cisco recommends using the native VLAN 1 setting to prevent traffic interruptions if using the Cisco Nexus 1000V Series Switches because changing the native VLAN 1 setting on a vNIC causes the port to turn on and off. You can only change the native VLAN setting on a Virtual Private Cloud (VPC) secondary port, and then change the primary port on the VPC.

c) In the **Operational Parameters** area, choose a **Stats Threshold Policy**.
d) 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, QoS policy, and network control policy from this area.

e) In the Connection Policies area, choose the **Dynamic vNIC**, **usNIC** or **VMQ** radio button, then choose the corresponding policy.

You can also create a dynamic vNIC, usNIC, or VMQ connection policy from this area.

Note
Cisco UCS 6400 Series Fabric Interconnect, Cisco UCS 6536 Fabric Interconnect, and Cisco UCS 6664 Fabric Interconnect do not support dynamic vNICs.

f) Click **OK**.

Step 8 If you want to use iSCSI boot with the server, click the down arrows to expand the **Add iSCSI vNICs** bar and do the following:

a) Click **Add** on the table icon bar.
b) In the **Create iSCSI vNIC** dialog box, enter the **Name** and choose the **Overlay vNIC**, **iSCSI Adapter Policy**, and **VLAN**.

You can also create an iSCSI adapter policy from this area.

Note
For the Cisco UCS M81KR Virtual Interface Card and the Cisco UCS VIC-1240 Virtual Interface Card, the VLAN that you specify must be the same as the native VLAN on the overlay vNIC.

For the Cisco UCS M51KR-B Broadcom BCM57711 Adapter, the VLAN that you specify can be any VLAN assigned to the overlay vNIC.

c) In the **MAC Address Assignment** drop-down list in the **iSCSI MAC Address** area, choose one of the following:

- Leave the MAC address unassigned, select **Select (None used by default)**. Select this option if the server that will be associated with this service profile contains a Cisco UCS M81KR Virtual Interface Card adapter or a Cisco UCS VIC-1240 Virtual Interface Card.

  Important
  If the server that will be associated with this service profile contains a Cisco UCS NIC M51KR-B adapter, you must specify a MAC address.

- A specific MAC address, select **00:25:B5:XX:XX:XX** and enter the address in the **MAC Address** field. To verify that this address is available, click the corresponding link.

- A MAC address from a pool, select the pool name from the list. Each pool name is followed by a pair of numbers in parentheses. The first number is the number of available MAC addresses in the pool and the second is the total number of MAC addresses in the pool.

  If this Cisco UCS domain is registered with Cisco UCS Central, there might be two pool categories. **Domain Pools** are defined locally in the Cisco UCS domain and **Global Pools** are defined in Cisco UCS Central.

d) (Optional) If you want to create a MAC pool that will be available to all service profiles, click **Create MAC Pool** and complete the fields in the **Create MAC Pool** wizard.

For more information, see the *UCS Manager Storage Management Guide*, Pools chapter, Creating a MAC Pool topic.

e) Click **OK**.

Step 9 After you have created all the vNICs or iSCSI vNICs you need for the policy, click **OK**.

What to do next

Include the policy in a service profile or service profile template.

Deleting a LAN Connectivity Policy

If you delete a LAN connectivity policy that is included in a service profile, it also deletes all vNICs and iSCSI vNICs from that service profile, and disrupt LAN data traffic for the server associated with the service profile.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies** > ***Organization_Name***.

Step 3 Expand the **LAN Connectivity Policies** node.

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

Step 5 If a confirmation dialog box displays, click **Yes**.

Creating a vNIC for a LAN Connectivity Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies** > ***Organization_Name***.

Step 3 Expand the **LAN Connectivity Policies** node.

Step 4 Choose the policy to which you want to add a vNIC.

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

Step 6 On the icon bar of the **vNICs** table, click **Add**.

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 Choose the **Fabric ID**, select the **VLANs** that you want to use, enter the **MTU**, and choose a **Pin Group**.

You can also create a VLAN and a LAN pin group from this area.

Step 9 In the **Operational Parameters** area, choose a **Stats Threshold Policy**.

Step 10 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, QoS policy, and network control policy from this area.

Step 11 In the Connection Policies area, choose the **Dynamic vNIC**, **usNIC** or **VMQ** radio button, then choose the corresponding policy.

You can also create a dynamic vNIC, usNIC, or VMQ connection policy from this area.

Note
Cisco UCS 6400 Series Fabric Interconnects and Cisco UCS 6536 Fabric Interconnect do not support dynamic vNICs.

Step 12 Click **OK**.

Step 13 Click **Save Changes**.

Deleting a vNIC from a LAN Connectivity Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies** > ***Organization_Name***.

Step 3 Expand the **LAN Connectivity Policies** node.

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

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

Step 6 In the **vNICs** table, do the following:

a) Click the vNIC you want to delete.
b) On the icon bar, click **Delete**.

Step 7 If a confirmation dialog box displays, click **Yes**.

Step 8 Click **Save Changes**.

Creating an iSCSI vNIC for a LAN Connectivity Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies** > ***Organization_Name***.

Step 3 Expand the **LAN Connectivity Policies** node.

Step 4 Choose the policy to which you want to add an iSCSI vNIC.

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

Step 6 On the icon bar of the **Add iSCSI vNICs** table, click **Add**.

Step 7 In the **Create iSCSI vNIC** dialog box, complete the following fields:

Name	Description
Name field	The name of the iSCSI vNIC. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Overlay vNIC drop-down list	The LAN vNIC associated with this iSCSI vNIC, if any. The selection of an Overlay vNIC may influence the available VLAN options, especially for specific Virtual Interface Cards.
iSCSI Adapter Policy drop-down list	The iSCSI adapter policy associated with this iSCSI vNIC, if any. This drop-down list displays available policies, including default policies such as 'default' (supports IPv4 address) and 'default-new' (supports both IPv4 and IPv6 addresses). These policies define the iSCSI adapter's behavior and settings.
Create iSCSI Adapter Policy link	Click this link to create a new iSCSI adapter policy that will be available to all iSCSI vNICs.
VLAN drop-down list	The virtual LAN associated with this iSCSI vNIC. The default VLAN is **default**. **Note** For the Cisco UCS M81KR Virtual Interface Card and the Cisco UCS VIC-1240 Virtual Interface Card, the VLAN that you specify must be the same as the native VLAN on the overlay vNIC. For the Cisco UCS M51KR-B Broadcom BCM57711 Adapter, the VLAN that you specify can be any VLAN assigned to the overlay vNIC.

Step 8 In the **MAC Address Assignment** drop-down list in the **iSCSI MAC Address** area, choose one of the following:

- Leave the MAC address unassigned, select **Select (None used by default)**. Select this option if the server that will be associated with this service profile contains a Cisco UCS M81KR Virtual Interface Card adapter or a Cisco UCS VIC-1240 Virtual Interface Card.

  Important
  If the server that will be associated with this service profile contains a Cisco UCS NIC M51KR-B adapter, you must specify a MAC address.

- A specific MAC address, select **00:25:B5:XX:XX:XX** and enter the address in the **MAC Address** field. To verify that this address is available, click the corresponding link.
- A MAC address from a pool, select the pool name from the list. Each pool name is followed by a pair of numbers in parentheses. The first number is the number of available MAC addresses in the pool and the second is the total number of MAC addresses in the pool.

  If this Cisco UCS domain is registered with Cisco UCS Central, there might be two pool categories. **Domain Pools** are defined locally in the Cisco UCS domain and **Global Pools** are defined in Cisco UCS Central.

Step 9 (Optional) If you want to create a MAC pool that will be available to all service profiles, click **Create MAC Pool** and complete the fields in the **Create MAC Pool** wizard.

For more information, see the *UCS Manager Storage Management Guide*, Pools chapter, Creating a MAC Pool topic.

Step 10 Click **OK**.

Step 11 Click **Save Changes**.

Deleting a vNIC from a LAN Connectivity Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies** > ***Organization_Name***.

Step 3 Expand the **LAN Connectivity Policies** node.

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

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

Step 6 In the **vNICs** table, do the following:

a) Click the vNIC you want to delete.
b) On the icon bar, click **Delete**.

Step 7 If a confirmation dialog box displays, click **Yes**.

Step 8 Click **Save Changes**.

Configuring SRIOV HPN Connection Policies

Single Root I/O Virtualization HPN Connection Policy

Beginning with the release 4.3(4b), Cisco UCS Manager provides Single Root I/O Virtualization High Performance Networking (SRIOV-HPN) Connection Policy support on Cisco UCS C-Series M8 servers with UCS VIC 15000 series adapters.

Beginning with the release 4.3(2b), Cisco UCS Manager provides Single Root I/O Virtualization High Performance Networking (SRIOV-HPN) Connection Policy support on Cisco UCS C-Series M5, M6, and M7 servers with UCS VIC 1400, 14000, and 15000 series adapters.

Single Root I/O Virtualization allows multiple VMs running a variety of guest operating systems to share a single PCIe network adapter within a host server. SR-IOV allows a VM to move data directly to and from the network adapter, bypassing the hypervisor for increased network throughput and lower server CPU burden.

To configure the SRIOV-HPN policy in a service profile, select **SRIOV-HPN** from **vNIC Adapter Policy** drop-down list.

You cannot enable the following when SRIOV-HPN is enabled:

- QinQ on the same vNIC
- VXLAN on the same vNIC
- Geneve offload on the same vNIC
- ENS on the same vNIC
- RoCE V2 on the same vNIC
- Netqueue on the same vNIC

Note

- CDN is supported on the host interface only and is not supported on the VM interface.
- Microsoft stand-alone NIC Teaming on SRIOV-HPN enabled vNICs is not supported.
- DPDK is supported on Linux VM.
- RSS is supported on the same vNIC

Creating or Viewing SRIOV HPN Connection Policy Properties

Procedure

	Command or Action	Purpose
Step 1	In the **Navigation** pane, click **LAN**.	
Step 2	Expand **Servers** > **Policies**.	

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td>Step 3</td><td>Expand the node for the organization where you want to create and view the SRIOV-HPN Connection Policies.</td><td>If the system does not include multi-tenancy, expand the root node.</td></tr>
<tr><td>Step 4</td><td>To create SRIOV HPN Connection Policy, right click on SRIOV HPN Connection Policies.</td><td></td></tr>
<tr><td>Step 5</td><td>In the General tab, you can view and and modify the created SRIOV HPN Connection Policy properties.</td><td>
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Name field</td><td>The name of the policy.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</td></tr>
<tr><td>Description field</td><td>Brief description of the policy.</td></tr>
<tr><td>Number of SRIOV HPN vnics field</td><td>Enter an integer between 1 and 64.</td></tr>
<tr><td>Transmit Queues field</td><td>The number of descriptors in each transmit queue.
Enter an integer between 1 and 8.</td></tr>
<tr><td>Receive Queues field</td><td>The number of receive queue resources to allocate.
Enter an integer between 1 and 8.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Completion Queues field</td><td>The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources.
Enter an integer between 1 and 16.</td></tr>
<tr><td>Interrupt Count field</td><td>The number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources.
Enter an integer between 1 and 16.</td></tr>
</table>
</td></tr>
<tr><td>Step 6</td><td>Click OK to save the changes, if any.</td><td></td></tr>
</table>

Assigning SRIOV HPN Connection Policy to a vNIC

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 On the **Servers** tab, expand **Servers** > **Service Profile** > **root**.

Step 3 Expand the service profile that you want to configure for SRIOV-HPN policy and then click **vNICs**.

Step 4 Choose the desired vNIC.

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

Step 6 In the **Policies** area, select **SRIOV-HPN** from the drop-down list.

Step 7 In the **Connection Policies** area, click the **SRIOV-HPN** radio button.

The **SRIOV HPN Connection Policy** drop-down list is displayed.

Step 8 Select the desired policy from the **SRIOV HPN Connection Policy** drop-down list.

Step 9 Click **OK**.

Step 10 Click **Save Changes**.

Deleting a SRIOV HPN Connection Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **Servers** > **Policies** > *Organization_Name*.
Step 3 Expand **SRIOV HPN Connection Policies**.
Step 4 Right-click the policy you want to delete and select **Delete**.
Step 5 If a confirmation dialog box displays, click **Yes**.

Configuring Network Control 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 Manager 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 Manager 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 Manager 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.

NIC Teaming and Port Security

NIC teaming is a grouping together of network adapters to build in redundancy, and is enabled on the host. This teaming or bonding facilitates various functionalities, including load balancing across links and failover. When NIC teaming is enabled and events such as failover or reconfiguration take place, MAC address conflicts and movement may happen.

Port security, which is enabled on the fabric interconnect side, prevents MAC address movement and deletion. Therefore, you must not enable port security and NIC teaming together.

Configuring Link Layer Discovery Protocol for Fabric Interconnect vEthernet Interfaces

Cisco UCS Manager allows you to enable and disable LLDP on a vEthernet interface. You can also retrieve information about these LAN uplink neighbors. This information is useful while learning the topology of the LAN connected to the UCS system and while diagnosing any network connectivity issues from the fabric interconnect (FI). The fabric interconnect of a UCS system is connected to LAN uplink switches for LAN connectivity and to SAN uplink switches for storage connectivity. When using Cisco UCS with Cisco Application Centric Infrastructure (ACI), LAN uplinks of the fabric interconnect are connected to ACI leaf nodes. Enabling LLDP on a vEthernet interface will help the Application Policy Infrastructure Controller (APIC) to identify the servers connected to the fabric interconnect by using vCenter.

To permit the discovery of devices in a network, support for Link Layer Discovery Protocol (LLDP), a vendor-neutral device discovery protocol that is defined in the IEEE 802.1ab standard, is introduced. LLDP is a one-way protocol that allows network devices to advertise information about themselves to other devices on the network. LLDP transmits information about the capabilities and current status of a device and its interfaces. LLDP devices use the protocol to solicit information only from other LLDP devices.

You can enable or disable LLDP on a vEthernet interface based on the Network Control Policy (NCP) that is applied on the vNIC in the service profile.

Creating a Network Control Policy

MAC address-based port security for Emulex converged Network Adapters (N20-AE0102) is not supported. When MAC address-based port security is enabled, the fabric interconnect restricts traffic to packets that contain the MAC address that it first learns. This is either the source MAC address used in the FCoE

Initialization Protocol packet, or the MAC address in an ethernet packet, whichever is sent first by the adaptor. This configuration can result in either FCoE or Ethernet packets being dropped.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multi tenancy, expand the **root** node.

Step 4 Right-click the **Network Control Policies** node and select **Create Network Control Policy**.

Step 5 In the **Create Network Control Policy** dialog box, complete the required fields.

Step 6 In the LLDP area, do the following:

a) To enable the transmission of LLDP packets on an interface, click **Enabled** in the **Transmit** field.

b) To enable the reception of LLDP packets on an interface, click **Enabled** in the **Receive** field.

Step 7 In the **MAC Security** area, do the following to determine whether the server can use different MAC addresses when sending packets to the fabric interconnect:

a) Click the **Expand** icon to expand the area and display the radio buttons.

b) Click one of the following radio buttons to determine whether forged MAC addresses are allowed or denied when packets are sent from the server to the fabric interconnect:

- **Allow**— All server packets are accepted by the fabric interconnect, regardless of the MAC address associated with the packets.
- **Deny**— After the first packet has been sent to the fabric interconnect, all other packets must use the same MAC address or they will be silently rejected by the fabric interconnect. In effect, this option enables port security for the associated vNIC.

If you plan to install VMware ESX on the associated server, you must configure the **MAC Security** to **allow** for the network control policy applied to the default vNIC. If you do not configure **MAC Security** for **allow**, the ESX installation may fail because the MAC security permits only one MAC address while the installation process requires more than one MAC address.

Step 8 Click **OK**.

Deleting a Network Control Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies** > ***Organization_Name***.

Step 3 Expand the **Network Control Policies** node.

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

Step 5 If a confirmation dialog box displays, click **Yes**.

Configuring Multicast Policies

Multicast Policy

This policy is used to configure Internet Group Management Protocol (IGMP) snooping, IGMP querier, and IGMP source IP proxy. 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 to one or more VLANs. When a multicast policy is modified, all VLANs associated with that multicast policy are re-processed to apply the changes.

By default, IGMP snooping is enabled and IGMP querier is disabled. When IGMP snooping is enabled, the fabric interconnects send the IGMP queries only to the hosts. They do not send IGMP queries to the upstream network. To send IGMP queries to the upstream, do one of the following:

- Configure IGMP querier on the upstream fabric interconnect with IGMP snooping enabled
- Disable IGMP snooping on the upstream fabric interconnect
- Change the fabric interconnects to switch mode

By default, IGMP Source IP Proxy state is enabled. When IGMP Source IP Proxy is enabled, the fabric interconnect acts as a proxy for its hosts and manages the membership of hosts and routing devices in multicast groups. IP hosts use IGMP to report their multicast group memberships to any immediately neighboring multicast routing devices. When IGMP source IP proxy is disabled, the fabric interconnect will forward the IGMP messages from the hosts towards the upstream router or switch without any change.

The following limitations and guidelines apply to multicast policies:

- Only the default multicast policy is allowed for a global VLAN.
- We highly recommend you use the same IGMP snooping state on the fabric interconnects and the associated LAN switches. For example, if IGMP snooping is disabled on the fabric interconnects, it should be disabled on any associated LAN switches as well.
- The option to enable or disable IGMP source IP proxy is supported on the following fabric interocnnects:
  - Cisco UCS 6600 Series Fabric Interconnect
  - Cisco UCS Fabric Interconnects 9108 100G
  - Cisco UCS 6500 Series Fabric Interconnects
  - Cisco UCS 6400 Series Fabric Interconnects

Creating a Multicast Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies**.

Step 3 Expand the **root** node.

Step 4 Right-click the **Multicast Policies** node and select **Create Multicast Policy**.

Step 5 In the **Create Multicast Policy** dialog box, specify the name, IGMP snooping, and IGMP source IP proxy information.

Note
Follow these guidelines if you choose to set IGMP Snooping querier IP addresses for a multicast policy:

a. In the Ethernet Switch-Mode configuration, you must set the querier IP addresses for each FI in the domain.

b. In the Ethernet End-Host mode, you can set the querier IP address just for FI A, and optionally for FI B as well. If an IP address is not set explicitly for FI-B, it uses the same address set for FI A.

Querier IP address can be any valid IP address. However, IP address from same subnet is required if there is a strict subnet check in the host.

Step 6 Click **OK**.

Modifying a Multicast Policy

This procedure describes how to change the IGMP snooping state, IGMP snooping querier state, and IGMP Source IP Proxy state of an existing multicast policy.

Note You cannot change the name of the multicast policy once it has been created.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies**.

Step 3 Expand the **root** node.

Step 4 Click the policy that you want to modify.

Step 5 In the work pane, edit the fields as needed.

Step 6 Click **Save Changes**.

Deleting a Multicast Policy

Note If you assigned a non-default (user-defined) multicast policy to a VLAN and then delete that multicast policy, the associated VLAN inherits the multicast policy settings from the default multicast policy until the deleted policy is re-created.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies**.

Step 3 Expand the **root** node.

Step 4 Right-click the **Multicast Policies** node and select **Delete Multicast Policy**.

Step 5 If a confirmation dialog box displays, click **Yes**.

Configuring LACP Policies

LACP Policy

Link Aggregation combines multiple network connections in parallel to increase throughput and to provide redundancy. Link aggregation control protocol (LACP) provides additional benefits for these link aggregation groups. Cisco UCS Manager enables you to configure LACP properties using LACP policy.

You can configure the following for a lacp policy:

- **Suspended-individual**: If you do not configure the ports on an upstream switch for lacp, the fabric interconnects treat all ports as uplink Ethernet ports to forward packets. You can place the lacp port in suspended state to avoid loops. When you set suspend-individual on a port-channel with LACP, if a port that is part of the port-channel does not receive PDUs from the peer port, it will go into suspended state.
- **Timer values**: You can configure rate-fast or rate-normal. In rate-fast configuration, the port is expected to receive 1 PDU every 1 second from the peer port. The time out for this is 3 seconds. In rate-normal configuration, the port is expected to receive 1 PDU every 30 seconds. The timeout for this is 90 seconds.

System creates a default LACP policy at system start up. You can modify this policy or create a new policy. You can also apply one LACP policy to multiple port-channels.

Creating a LACP Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multi tenancy, expand the **root** node.

Step 4 In the **Work Pane**, click **LACP Policies** tab, and click the **+** sign.

Step 5 In the **Create LACP Policy** dialog box, fill in the required fields.

Step 6 Click **OK**.

Modifying a LACP Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multi tenancy, expand the **root** node.

Step 4 In the **Work Pane**, **LACP Policies** tab, and click on the policy you want to edit.

Step 5 Click the **Properties** icon on the right.

Step 6 In the **Properties** dialog box, make the required changes and click **Apply**.

Step 7 Click **OK**.

Configuring UDLD Link Policies

Understanding 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 a Link Profile

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies** > **LAN Cloud**.

Step 3 Right-click the **Link Profile** node and choose **Create Link Profile**.

Step 4 In the **Create Link Profile** dialog box, specify the name and the UDLD link policy.

Step 5 Click **OK**.

Creating a UDLD Link Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **LAN** > **Policies** > **LAN Cloud**.
Step 3 Right-click the **UDLD Link Policy** node and choose **Create UDLD Link Policy**.
Step 4 In the **Create UDLD Link Policy** dialog box, specify the name, admin state, and mode.
Step 5 Click **OK**.

Modifying the UDLD System Settings

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **LAN** > **Policies** > **LAN Cloud**.
Step 3 On the LAN tab, expand **LAN** > **Policies** > **root**.
Step 4 Expand the **Link Protocol Policy** node and click **UDLD System Settings**.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 In the **Properties** area, modify the fields as needed.
Step 7 Click **Save Changes**.

Assigning a Link Profile to a Port Channel Ethernet Interface

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **LAN** > **LAN Cloud** > *Fabric* > **Port Channels**.
Step 3 Expand the port channel node and click the Eth Interface where you want to assign a link profile.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Properties** area, choose the link profile that you want to assign.
Step 6 Click **Save Changes**.

Assigning a Link Profile to an Uplink Ethernet Interface

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 On the **LAN** tab, expand **LAN** > **LAN Cloud** > ***Fabric*** > **Uplink Eth Interface**.
Step 3 Click the Eth Interface where you want to assign a link profile.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Properties** area, choose the link profile that you want to assign.
Step 6 Click **Save Changes**.

Assigning a Link Profile to a Port Channel FCoE Interface

Procedure

Step 1 In the **Navigation** pane, click **SAN**.
Step 2 On the **SAN** tab, expand **SAN** > **SAN Cloud** > ***Fabric*** > **FCoE Port Channels**.
Step 3 Expand the FCoE port channel node and click the FCoE Interface where you want to assign a link profile.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Properties** area, choose the link profile that you want to assign.
Step 6 Click **Save Changes**.

Assigning a Link Profile to an Uplink FCoE Interface

Procedure

Step 1 In the **Navigation** pane, click **SAN**.
Step 2 On the **SAN** tab, expand **SAN** > **SAN Cloud** > ***Fabric*** > **Uplink FC Interfaces**.
Step 3 Click the FCoE interface where you want to assign a link profile.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Properties** area, choose the link profile that you want to assign.
Step 6 Click **Save Changes**.

Configuring VMQ and VMMQ Connection Policies

VMQ Connection Policy

Cisco UCS Manager enables you to configure VMQ connection policy for a vNIC. VMQ provides improved network performance to the entire management operating system. Configuring a VMQ vNIC connection policy involves the following:

- Create a VMQ connection policy
- Create a static vNIC in a service profile
- Apply the VMQ connection policy to the vNIC

If you want 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 1300 Series
- UCS VIC 1400 Series
- UCS VIC 14000 Series
- UCS-VIC-15000 Series

The following are the supported Operating Systems for VMQ:

- Windows 2012
- Windows 2012R2
- Windows 2016
- Windows 2019
- Windows 2022

Note The Cisco UCS VIC 1400, UCS VIC 14000, and UCS VIC 15000 Series adapters are not supported on Windows 2012 VMQ and Windows 2012 R2 VMQ

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

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

Creating a VMQ Connection Policy

Before you create a VMQ connection policy, consider the following:

- VMQ Tuning on the Windows Server—When an adapter is placed on a virtual switch, running the **Get-NetAdapterVmq** cmdlet displays `True` for VMQ.
- Virtual machine level—By default, VMQ is enabled on all newly deployed VMs. VMQ can be enabled or disabled on existing VMs.
- Microsoft SCVMM—VMQ must be enabled on the port profile. If not, you will not be able to successfully create the virtual switch in SCVMM.
- Microsoft Azure Stack extends the existing VMQ support for host-side virtual switch ports called vPorts to Virtual Machine Multi Queues (VMMQ). You can configure VMMQ by enabling multi queues in the VMQ Connection Policy.

For Cisco UCS VIC 1400 Series or above adapters to support VMQ functionality, the vNIC should be configured in the VMQ connection policy with the multi-queue option enabled.

Note Microsoft stand-alone NIC Teaming and Virtual Machine Queue (VMQ) support for adapters:

Microsoft stand-alone NIC teaming works only with VMQ. For Cisco UCS VIC 1400 , VIC 14000 , and VIC 15000 Series adapters, the supported VMQ is VMMQ with single queue. To support VMMQ with single queue, you must create a new VMMQ adapter policy containing a 1 TQ, 1 RQ and 2 CQ combination, then assign it to the VMQ Connection Policy.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 In the **LAN** tab, expand **Policies**.

Step 3 Expand the nodes for the organization where you want to create the policy. If the system does not include multitenancy, expand the root node.

Step 4 Right-click the **VMQ Connection Policies** node and select **Create VMQ Connection Policy**.

Step 5 In the **Create VMQ Connection Policy** dialog box, complete the following fields:

Name	Description
Name field	The VMQ connection policy name.
Description field	The description of the VMQ connection policy.

Name	Description
Multi Queue radio button	Whether Virtual Machine Multi-Queue (VMMQ) is enabled in the policy. With VMMQ, multiple queues are allocated to a single VM. • **Disabled**—Multi Queue is disabled and you can configure a VMQ policy. When Multi Queue is disabled, the following fields appear: • **Number of VMQs** • **Number of Interrupts** • **Enabled**—Multi Queue is enabled and the vNIC is placed into VMMQ mode. You can specify a VMMQ Adapter Policy. When Multi Queue is enabled, the following fields appear: • **Number of Sub vNICs** • **VMMQ Adapter Policy** **Note** For Cisco UCS VIC 1400 Series and above adapters, enable the Multi-Queue option to support both VMQ and VMMQ functionality. For more information on creating a VMQ Connection Policy with Multi-Queue enabled, see Creating a VMMQ Connection Policy, on page 213.
Number of VMQs field	The number of VMQs per adapter must be one more than the maximum number of VM NICs. The default value is 64.
Number of Interrupts field	The number of CPU threads or logical processors available in the server. The default value is 64. **Note** The minimum interrupt to be used is “2 x number of CPU core + 4”.

Step 6 Click **OK**.

Assigning VMQ Setting to a vNIC

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 On the **Servers** tab, expand **Servers** > **Service Profile** > **root** .

Step 3 Expand the service profile that you want to configure for VMQ and then click **vNICs**.

Step 4 In the **Work Pane**, click the **Network** tab.

Step 5 In the **vNICs** area, choose a vNIC and double-click the **Actual Order** column.

Modify vNIC window is displayed.

Step 6 In the **Adapter Performance Profile** area of the Modify vNIC dialog box, choose **Windows** from the Adapter Policy drop-down list.

Step 7 In the **Connection Policies** area, click the **VMQ** radio button.

Step 8 Select the **VMQ Connection Policy** from the VMQ Connection Policy drop-down list.

Step 9 Click **OK**.

Step 10 Click **Save Changes**.

Enabling VMQ and NVGRE Offloading on the same vNIC

Perform the tasks in the table below to enable VMQ and NVGRE offloading on the same vNIC.

Note VMQ is not supported along with VXLAN on the same vNIC except for Cisco UCS VIC 1400 Series adapters and above. Cisco UCS VIC 1400, VIC 14000, and VIC 15000 Series adapters support VMQ and VMMQ along with VXLAN or NVGRE on the same vNIC.

Task	Description	See
Enable normal NVGRE offloading	Perform this task by setting the corresponding flags in the adapter profile which is associated with the given vNIC. **Note** The Transmit checksum offload and TSO must be enabled for the NVGRE offloading to be effective.	Configuring an Ethernet Adapter Policy to Enable Stateless Offloads with NVGRE, on page 183
Enable VMQ	Perform this task by setting the appropriate connection policy when you add a vNIC to the service profile.	Creating a VMQ Connection Policy, on page 208 Assigning VMQ Setting to a vNIC, on page 211

VMMQ Connection Policy

Cisco UCS Manager introduces support for Virtual Machine Multi Queues (VMMQ). VMMQ allows you to configure multiple I/O queues to a single VM and, thus, distribute traffic across multiple CPU cores in a VM. VMMQ is supported on UCS VIC 1400 Series and above adapters with Windows 2016 and later versions. VMMQ with RDMA/RDMA Over Converged Ethernet (RoCEv2) mode 2 is supported from Windows 2019 and later.

The VMQ Connection Policy has an option called **Multi Queue**. When **Multi Queue** is enabled, the vNIC is placed into VMMQ mode. In this mode, you can configure sub vNICs and specify a VMMQ Adapter policy. The policy includes the aggregate queue counts for VMMQ and determines how the connectivity between VMs and Azure Stack vPorts is configured.

Enabling VMMQ on a vNIC involves the following two configurations:

- Attach an adapter-policy for the vNIC. The recommended adapter policy for VMMQ is **Win-HPN**, available in UCS Manager.
- Include a VMQ connection policy on the vNIC. The VMQ connection policy defines Tx/Rx queues for the vPorts. For the VMQ connection policy, Cisco recommends using a pre-defined multi-queue (MQ) policy, which is available in UCS Manager. Pre-defined policies are available in UCSM: **MQ** for regular VMMQ. The pre-defined policies are good for 64 sub vNICs or vPorts in pooled mode.

Note To use RDMA, you must enable RDMA in the options under the vNIC adapter policy . For RDMA, refer to the *Cisco UCS Manager Configuration Guide for RDMA over Converged Ethernet (RoCE) v2*.

There are two different ways to define the total number of queues available for vPorts. In the pooled mode, the resource counts in the VMMQ adapter policy are the totals available across vPorts. In non-pooled mode, the total available is the selected resource count from the VMMQ adapter policy * subvnic count. In VMMQ mode, these are the default queue counts:

Queue Resource	Pooled Mode	Non Pooled Mode
Transmit Queue	64	1
Receive Queue	512	8
Completion Queue	576	9

Creating a VMMQ Connection Policy, on page 213 provides detailed information about creating a VMMQ connection policy.

VMMQ Guidelines

- Each VMMQ vPort may use one Transmit Queue and multiple Receive Queues. When VMMQ is enabled, a pool of queues is created, and the host driver assigns queues to vPorts. Different vPorts may be assigned different numbers of queues based on the number of cores that the vPort will be servicing.
- VXLAN and NVGRE offloads are supported with VMMQ functionality. The option is enabled in the vNIC adapter policy and not in the sub vNIC adapter policy.

- RSS is supported on VMMQ Receive Queues, including inner packet of overlay packets.
- VMMQ vNICs support a rate limit set by the host, not from Cisco UCS Manager. COS will not be adjustable per vPort from Cisco UCS Manager.
- vNICs with the VMQ feature, specified through the VMQ Connection Policy with **Multi Queue** disabled, are not allowed on the same adapter as Multi Queue-enabled vNICs.
- FCoE and VMMQ vNICs can coexist on the same server.
- usNIC and Multi-Queue VMQ can not be enabled on the same VIC.
- Modifying the VMMQ adapter policy through the VMQ connection policy results in exceeding the maximum Completion Queue (CQ) value. Each VIC 1400 Series or above adapter supports a maximum of 2000 hardware CQ resources. If this number is exceeded, the `Out of CQ Resources` error appears in the Cisco UCS Manager GUI, and vNIC creation fails with a configuration failure at service profile association.
- Use the following PS command to enable VMMQ on the vport.

```
Set-VMNetworkAdapter -Name (vmNIC Name) -VMName (VM_NAME) -VmmqEnabled $true
-VmmqQueuePairs (Queue_Pair_Count) -VrssEnabled $true
```

Creating a VMMQ Connection Policy

A VMMQ connection policy can be created using VMQ policy with Multi Queue enabled.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 In the **LAN** tab, expand **Policies**.

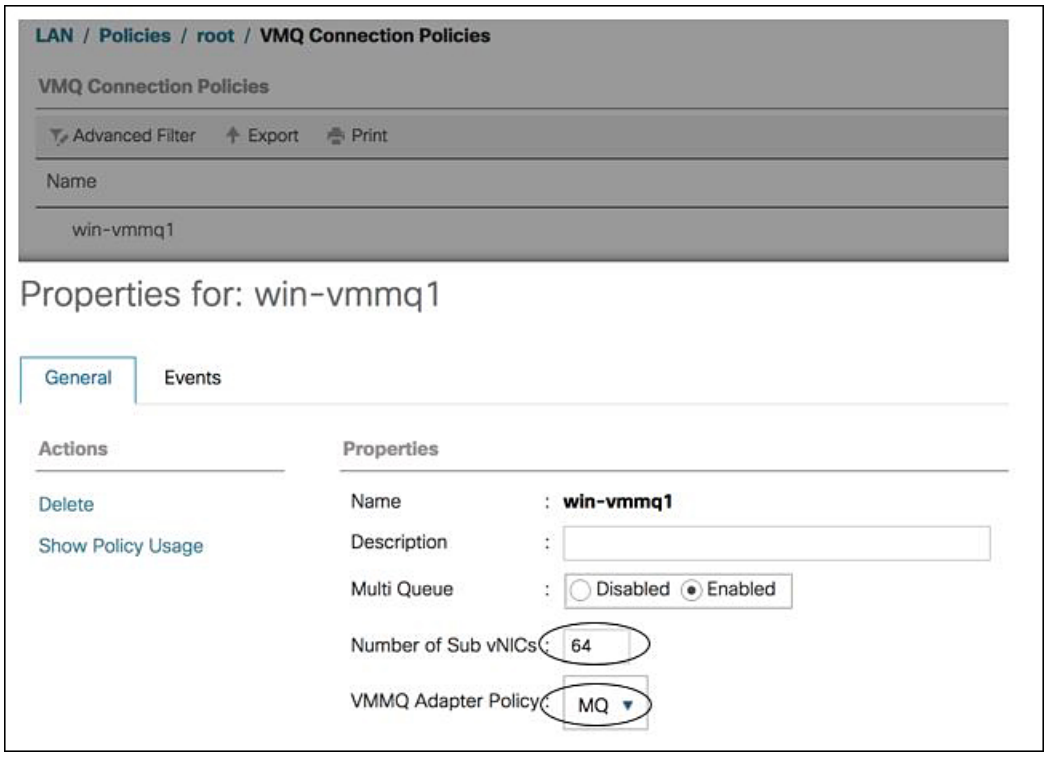
Step 3 Expand the nodes for the organization where you want to create the policy. If the system does not include multitenancy, expand the root node.

Step 4 Right-click the **VMQ Connection Policies** node and select **Create VMQ Connection Policy**.

Step 5 In the **Create VMQ Connection Policy** dialog box, complete the following fields:

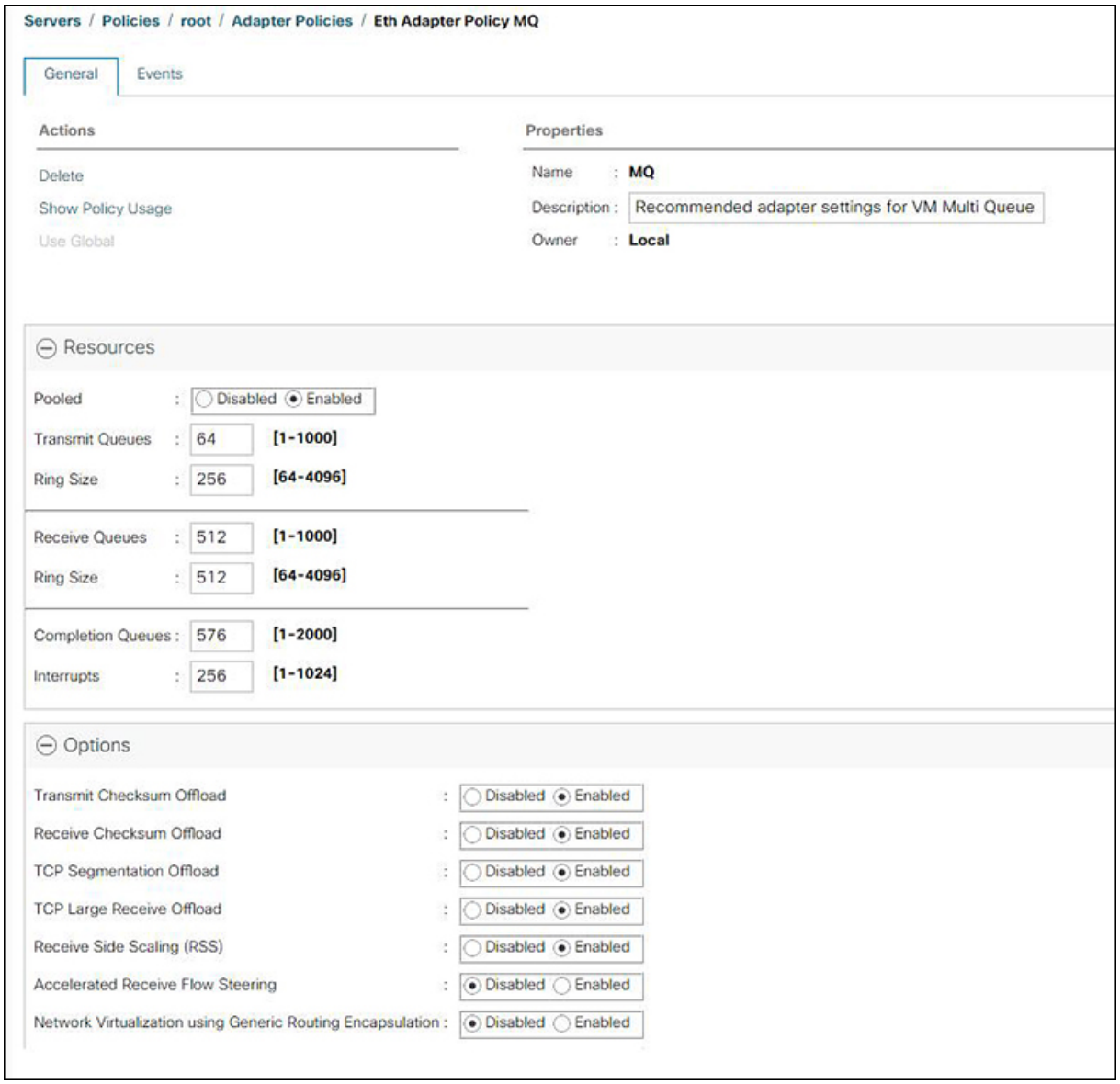
Name	Description
Name field	The VMQ connection policy name.
Description field	The description of the VMQ connection policy.

Name	Description
Multi Queue radio button	When Virtual Machine Multi-Queue (VMMQ) is enabled in the policy, multiple queues are allocated to a single vport. • **Enabled**—Multi Queue is enabled and the vNIC is placed into VMMQ mode. You can specify a VMMQ Adapter Policy. When Multi Queue is enabled, the following fields appear: • **Number of Sub vNICs** • **VMMQ Adapter Policy** **Note** For Cisco UCS VIC 1400, VIC 14000, and VIC 15000 series adapters, enable the Multi-Queue option to support both VMQ and VMMQ functionality.
Number of Sub vNICs field	Number of sub vNICs that are available for Multi Queue. The default value is 64. **Note** The TQ and RQ resource value of VMMQ adapter policy should be greater than or equal to the configured number of sub vNICs.
VMMQ Adapter Policy drop-down list	Name of the VMMQ adapter policy. Cisco recommends using the default MQ Adapter Policy. The default MQ policy includes the aggregate queue counts for VMMQ. **Note** You can also specify a custom policy designed for a specific configuration,



Step 6 Click **OK**.

Step 7 Go to the new policy under **VMQ Connection Policies**



Step 8 Set the number of **Transmit Queues** to 64 and **Receive Queues** to 8 times the transmit queues (512). The **Completion Queues** is the total of these two numbers (576).

Step 9 Set the **Interrupt** count to 256.

Step 10 Enable **Pooled** resources.

Step 11 Enable **Receive Side Scaling (RSS)**.

Step 12 Click **OK**.

What to do next

Assign a QoS policy.

Creating a QoS Policy for VMMQ

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

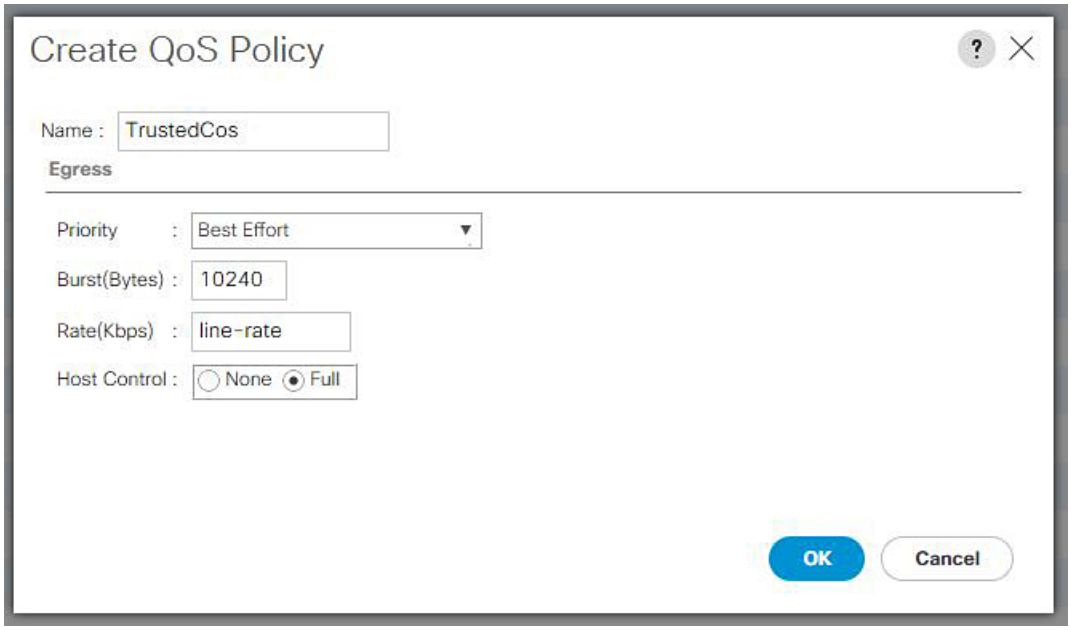
Step 2 In the **LAN** tab, expand **Policies**.

Step 3 Expand the nodes for the organization where you want to create the pool. If the system does not include multitenancy, expand the **root** node.

Step 4 Right-click the **QoS Policy** dialog box and enter the name of the policy in the **Name** field. VMMQ uses **TrustedCos** as the policy. Assign this policy to the vNIC QoS.

Step 5 Select the desired priority in the **Priority** drop-down list.

Step 6 In the **Host Control** field, click the **Full** radio button.



Step 7 Click **OK**.

What to do next

Assign the VMMQ Setting to a vNIC.

Assigning a VMMQ Setting to a vNIC

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 In the **Servers** tab, expand **Servers > Service Profiles > root**.

Step 3 Expand the service profile that you want to configure VMMQ and click **vNICs**.

Step 4 In the **Work Pane**, click the **Network** tab.

Step 5 In the **vNICs** area, choose the desired vNIC and double-click the **Actual Order** column.

Modify vNIC window is displayed.

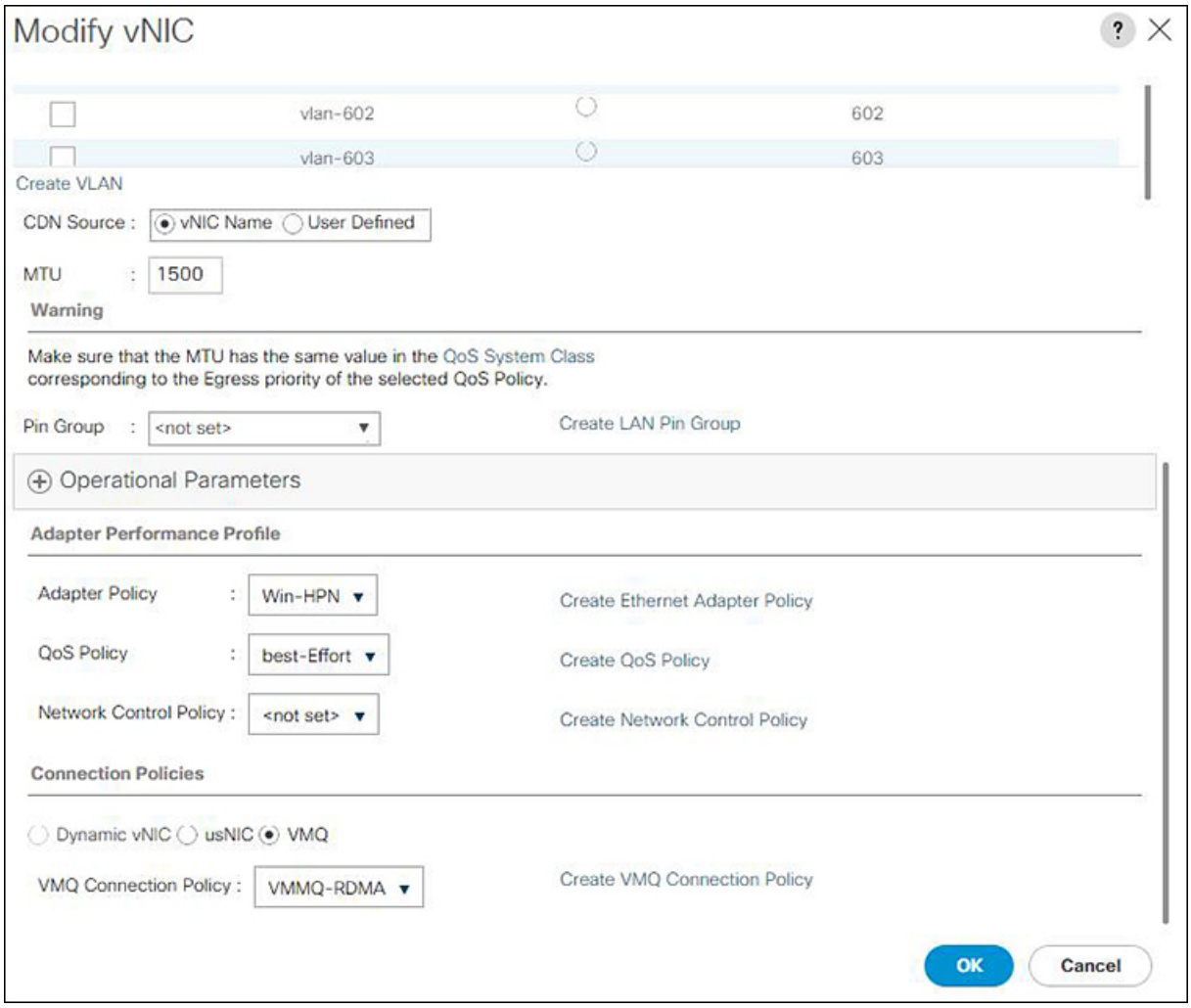
Step 6 In the **Adapter Performance Profile** area of the **Modify vNIC** dialog box, choose **WIN-HPN** from the **Adapter Policy** drop-down list.

Step 7 From the **QoS Policy** drop-down list, select the created QoS policy for VMMQ.

Step 8 In the **Connection Policies** area, click the **VMQ** radio button.

Step 9 Choose the created VMQ connection policy with Multi-Queue enabled from the **VMQ Connection Policy** drop-down list.

Step 10 Click **OK**.



Step 11 Click **Save Changes**.

NetQueue

Information About NetQueue

NetQueue improves traffic performance by providing a network adapter with multiple receive queues. These queues allow the data interrupt processing that is associated with individual virtual machines to be grouped.

Note NetQueue is supported on servers running VMware ESXi operating systems.

Configuring NetQueue

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 In the **LAN** tab, expand **Policies**.

Step 3 Expand the nodes for the organization where you want to create the policy. If the system does not include multitenancy, expand the root node.

Step 4 Right-click the **VMQ Connection Policies** node and select **Create VMQ Connection Policy**.

Step 5 In the **Create VMQ Connection Policy** dialog box, complete the following fields:

Name	Description
Name field	The NetQueue policy name.
Description field	The description of the NetQueue.
Multi Queue radio button	Select disabled for NetQueue.
Number of VMQs field	Enter a number between 1 to 64 to specify the number of NetQueues for this connection policy. The driver supports up to 16 NetQueues per port for standard frame configurations. **Note** VMware recommends that you use up to eight NetQueues per port for standard frame configurations.
Number of Interrupts field	The number of interrupts count of each VNIC. The value should be set to 2 x number of VMQs + 2.

Step 6

Step 7 Click **OK**.

Step 8 In the **Navigation** pane, click **Servers**.

Step 9 On the **Servers** tab, expand **Servers > Service Profiles > root**.

Step 10 Expand the service profile that you want to configure NetQueue and click vNICs.

Step 11 In the **Work** pane, click the **Network** tab.

Step 12 In the **vNICs** area, choose a vNIC and double-click the **Actual Order** column.

Modify vNIC window is displayed.

Step 13 In the **Adapter Performance Profile** area of the Modify vNIC dialog box, choose **VMWare** from the Adapter Policy drop-down list.

Step 14 In the **Connection Policies** area, click the **VMQ** radio button.

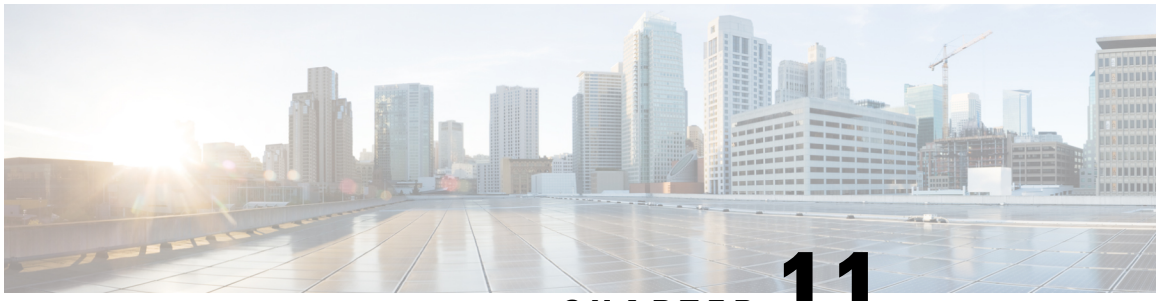
Step 15 Choose the created VMQ connection policy for NetQueue from the VMQ Connection Policy drop-down list.

Step 16 Click **OK**.

Step 17 Click **Save Changes**.

Note

NetQueue should be enabled only on MSIX systems and disabled on 1GB NICs.



CHAPTER 11

Configuring MACsec

About MACsec

MACsec is an IEEE 802.1AE standards-based Layer 2 hop-by-hop encryption that provides data confidentiality and integrity for media access independent protocols.

MACsec provides MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys.

MACsec encrypts the entire data except for the Source and Destination MAC addresses of an Ethernet packet. It offers the following capabilities:

- Provides line rate encryption.
- Ensures data confidentiality by providing strong encryption at Layer 2.
- Provides integrity checking to help ensure that data cannot be modified in transit.
- Key Lifetime and Hitless Key Rollover, on page 224
- Fallback Key, on page 224

Key Lifetime and Hitless Key Rollover

A MACsec keychain can have multiple pre-shared keys (PSKs), each configured with a key ID and an optional lifetime. A key lifetime specifies at which time the key activates and expires. In the absence of a lifetime configuration, the default lifetime is unlimited. When a lifetime is configured, MKA rolls over to the next configured pre-shared key in the keychain after the lifetime is expired. The time zone of the key can be local or UTC. The default time zone is UTC.

To configure a MACsec keychain, see Creating a MACsec Keychain, on page 230

A key can roll over to a second key within the same keychain by configuring the second key (in the keychain) and configuring a lifetime for the first key. When the lifetime of the first key expires, it automatically rolls over to the next key in the list. If the same key is configured on both sides of the link at the same time, then the key rollover is hitless (that is, the key rolls over without traffic interruption).

Note The lifetime of the keys are overlapped to achieve hitless key rollover.

Fallback Key

A MACsec session can fail due to a key/key ID (CKN) mismatch or a finite key duration between the Fabric Interconnect and the peer. If a MACsec session fails, a fallback session can take over if a fallback key is configured. A fallback session prevents downtime due to primary session failure and allows a user time to fix the key issue causing the failure. A fallback key also provides a backup session if the primary session fails to start. This feature is optional.

For more information, see Creating a MACsec Keychain .

Guidelines and Limitations for MACsec

MACsec functionality supports the following:

- Ethernet Uplink interfaces
- Ethernet Port-channel member link interfaces

- MKA is the only supported key exchange protocol for MACsec.

Note The Security Association Protocol (SAP) is not supported.

MACsec functionality does not support the following:

- Unified uplink
- FCoE uplinks
- Server, Storage, and Appliance ports
- QSA
- Link-level flow control (LLFC) and priority flow control (PFC)
- Multiple MACsec peers (different SCI values) for the same interface
- 1G port or any port on a MAC block that has 1G ports on it.

Note MACsec configuration is supported only on end host mode.

Cisco UCS Fabric Interconnect Support

Cisco UCS Manager 4.3(4a) release introduces MACsec functionality for Cisco UCS 6536, Cisco UCS 6454, and Cisco UCS 64108 fabric interconnects.

Cisco UCS Manager 6.0(1b) release extends MACsec functionality support for Cisco UCS 6664 Fabric Interconnect and Cisco UCS Fabric Interconnect 9108 100G (Cisco UCS X-Series Direct) Fabric Interconnect.

Keychain Limitations

- You cannot overwrite the Key Hex String when the MACsec Keychain is applied on the interface. Instead, you must delete the old key and create the new key or a new keychain.
- For a given keychain, key activation time must overlap to avoid any period of time when no key is activated. If a time period occurs during which no key is activated, session negotiation fails and traffic drops can occur. The key with the latest start time among the currently active keys takes precedence for a MACsec key rollover.
- A MACSec session cannot be established if the CKN (Key ID) or CAK (Key Hex String) is set to all zeros.

Fallback Limitations

- If a MACsec session is secured on an old primary key, it does not go to a fallback session in case of mismatched latest active primary key. So the session remains secured on the old primary key and shows as rekeying on the old CA (Connectivity Association) under status. And the MACsec session on the new key on primary PSK will be in the Init state.
- Use only one key with infinite lifetime in the fallback key chain. Multiple keys are not supported.

- The key ID (CKN) used in the fallback key chain must not match with any of the key IDs (CKNs) used in the primary key chain of the same switch interface and peer upstream switch interface.
- Once configured, fallback configuration on an interface cannot be removed, unless the complete MACsec configuration on the interface is removed.

MACsec Policy Limitations

- BPDU packets can be transmitted before a MACsec session becomes secure.
- We recommend you to apply the same security policy **Should Secure-Should Secure** or **Must Secure-Must Secure** on the fabric interconnect and the peer switch interface.
- While making changes to the MACSec policy parameters, do not change the **Key Server Priority** along with other parameters if the policy is already applied to any of the uplinks.

Note Configuring MACsec with security-policy as **must-secure** on an Uplink Interface brings down the port, and the traffic drops until the MACsec session is secured.

Layer 2 Tunneling Protocol (L2TP) Restrictions

MACsec is not supported on ports that are configured for dot1q tunneling or L2TP.

MACsec EAPOL Limitations

- For enabling EAPOL (Extensible Authentication Protocol over LAN) configuration, the range of Ethernet type between 0 to 0x599 is invalid.
- While configuring EAPOL packets, the following combinations must not be used:
  - MAC Address 0100.0ccd.cdd0 with any ethertype
  - Any MAC Address with Ether types: 0xfff0, 0x800, 0x86dd
  - The default destination MAC address, 0180.c200.0003 with the default Ethernet type, 0x888e
  - Different EAPOL DMAC addresses and Ethertype on both MACsec peers. The MACsec session works only if the MACsec peer is sending MKAPDUs with the DMAC and Ethertype configured locally.
  - Within the same slice of the forwarding engine, EAPOL ethertype and dot1q ethertype cannot have the same value.
  - More than one custom EAPOL is not supported.
  - You cannot modify a custom EAPOL configuration if applied on any interface.

Statistics Limitations

- Statistics are cumulative.
- Few CRC errors may occur during the transition between MACsec and non-MACsec mode (regular port shut/no shut).

- The IEEE8021-SECY-MIB OIDs secyRxSAStatsOKPkts, secyTxSAStatsProtectedPkts, and secyTxSAStatsEncryptedPkts can carry only up to 32 bits of counter values, but the traffic may exceed 32 bits.

Enabling or Disabling MACsec Configuration

Note Disabling MACsec only deactivates this feature and does not remove the associated MACsec configurations.

Before you begin

Ensure that MACsec is enabled.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec**.

Step 3 Click the **General** tab.

Step 4 In the **Admin State** field, click the **Enabled** radio button to enable MACsec or the **Disabled** radio button to disable MACsec.

Table 11: Properties Area

Name	Description
Admin State radio button	Allows you to enable the MACsec feature. Disabling the MACsec feature removes the operational MACsec configuration from the interface, which causes the interface to go down.

Step 5 Click **Save Changes** to save the configuration change.

Creating a MACsec Policy

You can create multiple MACsec policies with different parameters. However, only one policy can be active on an interface.

Before you begin

Ensure that MACsec is enabled.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Policy**.

Step 3 Click **Add**.

Step 4 In the **Create MACsec Policy** dialog box, complete the following fields:

Name	Description
Name field	Name of the MACsec policy.
Description field	Enter a brief description for the policy.
Cipher Suite radio button	Allows you to select the cipher suite used for the encryption along with associated attributes of related to the encryption. This can be one of the following: • GCM AES XPN 256 • GCM AES XPN 128 • GCM AES 256 • GCM AES 128
Key Server Priority field	Allows you to enter the key server priority. You can enter a value between 0-255. Lower the value, higher the preference to be selected as the key server.
Security Policy radio button	Allows you to configure the security policy parameters. This can be one of the following: • **Must Secure**—Must-Secure imposes only MACsec encrypted traffic to flow. Hence, until the MKA session is not secured, traffic is dropped. • **Should Secure**— Allows unencrypted traffic to flow until the MKA session is secured. After the MKA session is secured, the **Should-Secure** policy imposes only encrypted traffic to flow. This is the default value.
Replay Window Size field	Allows you to configure the window size.
Sak Expiry Time field	Configures the time in seconds to force an SAK rekey.

Name	Description
Conf Offset radio button	Configures one of the following confidentiality offsets in the Layer 2 frame, where encryption begins: CONF-OFFSET-0, CONF-OFFSET-30, or CONF-OFFSET-50.
Include Icv Param radio button	Configure the ICV for the frame arriving on the port.

Step 5 Click **OK**.

Viewing or Modifying a MACsec Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Policy**.

Step 3 Select the MACsec policy, which you want to view or modify.

Step 4 In the **General** tab, under the **Properties** window, you can view or modify the following:

Name	Description
Name field	Name of the MACsec policy.
Description field	Enter a brief description for the policy.
Cipher Suite radio button	Allows you to select the cipher suite used for the encryption along with associated attributes of related to the encryption. This can be one of the following: • GCM AES XPN 256 • GCM AES XPN 128 • GCM AES 256 • GCM AES 128
Key Server Priority field	Allows you to enter the key server priority. You can enter a value between 0-255. Lower the value, higher the preference to be selected as the key server.

Name	Description
Security Policy radio button	Allows you to configure the security policy parameters. This can be one of the following: • **Must Secure**—Must-Secure imposes only MACsec encrypted traffic to flow. Hence, until the MKA session is not secured, traffic is dropped. • **Should Secure**— Allows unencrypted traffic to flow until the MKA session is secured. After the MKA session is secured, the **Should-Secure** policy imposes only encrypted traffic to flow. This is the default value.
Replay Window Size field	Allows you to configure the window size.
Sak Expiry Time field	Configures the time in seconds to force an SAK rekey.
Conf Offset radio button	Configures one of the following confidentiality offsets in the Layer 2 frame, where encryption begins: CONF-OFFSET-0, CONF-OFFSET-30, or CONF-OFFSET-50.
Include Icv Param radio button	Configure the ICV for the frame arriving on the port.

Step 5 Click **Save Changes** to save the configuration change.

Deleting a MACsec Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Navigate to **LAN** > **MACsec** > **Policy**.
Step 3 In the **Actions** area, click **Delete** to delete a MACsec policy configuration.
Step 4 Click **Yes** in the confirmation dialog box.

Creating a MACsec Keychain

Only MACsec keychains result in converged MKA sessions.

You can create a MACsec keychain and keys on the device.

Before you begin

Ensure that MACsec is enabled.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Keychain**.

Step 3 Click **Add** to create a MACsec Keychain.

Step 4 In the **Create MACsec Keychain** dialog box, complete the following fields:

Name	Description
Name field	Enter a suitable name for the keychain and click **OK** to save.

Step 5 Click **OK**.

Viewing or Modifying a MACsec Keychain

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Keychain**.

Step 3 Select the MACsec keychain, which you want to view or modify.

Step 4 In the **General** tab, under the **Properties** window, you can view and modify of the following:

Name	Description
Name field	Enter a suitable name for the keychain and click **OK** to save.

Step 5 Click **Save Changes** to save the configuration change.

Deleting a MACsec Key

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Keychain**.

Step 3 Choose a MACsec key.

Step 4 In the **Actions** area, click **Delete** to delete a MACsec key.

Step 5 Click **Yes** in the confirmation dialog box.

Creating a MACsec Key

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Keychain**.

Step 3 Choose a MACsec keychain.

Step 4 In the **Actions** area, click **Create MACsec Key**.

Step 5 In the **Create MACsec Key** dialog box, complete the following fields:

Name	Description
Key ID field	Allows you to enter the key ID (CKN) used in the primary key chain. **Note** Key IDs must be unique under a keychain configuration.

Name	Description
Key Hex String field	Enter the key between 32 and 144 hexadecimal characters. The key length is based on the encryption type and cryptographic algorithm. **Type 0** (Unencrypted Key) • AES_128_CMAC: 32 hexadecimal characters • AES_256_CMAC: 64 hexadecimal characters **Type 7** • AES_128_CMAC: 66 hexadecimal characters • AES_256_CMAC: 130 hexadecimal characters **Type 6** • AES_128_CMAC: 100 hexadecimal characters • AES_256_CMAC: 144 hexadecimal characters
Encrypt Type radio button	Allows you to select the encrypt type. The encrypt type includes the following: • **Type 0**—Select this option to configure the key-hex-string as an unencrypted key. • **Type 7**—Select this option to configure the key-hex-string as a Type-7 encrypted key. • **Type 6**—Select this option to configure the key as an AES encrypted key. Type 6 encryption utilizes the Advanced Encryption Standard (AES) for an enhanced security. For more information, see *Security Management > Creating AES Encryption* in Administration Management Guide.
Cryptographic Algorithm radio button	Set cryptographic authentication algorithm with 128-bit or 256-bit encryption.

Step 6 Click **OK**.

Viewing or Modifying a MACsec Key

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Keychain**.

Step 3 Select the MACsec Key, which you want to view or modify.

Step 4 In the **General** tab, under the **Properties** window, you can view and modify of the following:

Name	Description
Key ID field	Allows you to enter the key ID (CKN) used in the primary key chain. **Note** Key IDs must be unique under a keychain configuration.
Key Hex String field	Enter the key between 32 and 144 hexadecimal characters. The key length is based on the encryption type and cryptographic algorithm. **Type 0** (Unencrypted Key) • AES_128_CMAC: 32 hexadecimal characters • AES_256_CMAC: 64 hexadecimal characters **Type 7** • AES_128_CMAC: 66 hexadecimal characters • AES_256_CMAC: 130 hexadecimal characters **Type 6** • AES_128_CMAC: 100 hexadecimal characters • AES_256_CMAC: 144 hexadecimal characters

Name	Description
Encrypt Type radio button	Allows you to select the encrypt type. The encrypt type includes the following: • **Type 0**—Select this option to configure the key-hex-string as an unencrypted key. • **Type 7**—Select this option to configure the key-hex-string as a Type-7 encrypted key. • **Type 6**—Select this option to configure the key as an AES encrypted key. Type 6 encryption utilizes the Advanced Encryption Standard (AES) for an enhanced security. For more information, see *Security Management > Creating AES Encryption* in Administration Management Guide.
Cryptographic Algorithm radio button	Set cryptographic authentication algorithm with 128-bit or 256-bit encryption.

Step 5 Click **Save Changes** to save the configuration change.

Deleting a MACsec Key

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Navigate to **LAN** > **MACsec** > **Keychain**.
Step 3 Choose a MACsec key.
Step 4 In the **Actions** area, click **Delete** to delete a MACsec key.
Step 5 Click **Yes** in the confirmation dialog box.

Creating a LifeTime

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Navigate to **LAN** > **MACsec** > **Keychain**.

Step 3 Choose a MACsec key.

Step 4 In the **Actions** area, click **Create LifeTime**.

Step 5 In the **Create LifeTime** dialog box, complete the following fields:

Name	Description
Start Date Time field	The start date time is the time of day and date that the key becomes active. Allows you to enter a start date in YYYY-MM-DD HH:MM:SS format.
End Date Time field	Allows you to enter an end date in YYYY-MM-DD HH:MM:SS format.
Duration field	Allows you to enter length of the LifeTime in seconds. The duration is the length of the lifetime in seconds. The maximum length is 2147483646 seconds (approximately 68 years).
Time Zone radio button	Allows you to select a timezone.

Step 6 Click **OK**.

Viewing or Modifying a MACsec Key Lifetime

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Keychain**.

Step 3 Select the MACsec Key Lifetime, which you want to view or modify.

Step 4 In the **General** tab, under the **Properties** window, you can view and modify the following:

Name	Description
Start Date Time field	The start date time is the time of day and date that the key becomes active. Allows you to enter a start date in YYYY-MM-DD HH:MM:SS format.
End Date Time field	Allows you to enter an end date in YYYY-MM-DD HH:MM:SS format.
Duration field	Allows you to enter length of the LifeTime in seconds. The duration is the length of the lifetime in seconds. The maximum length is 2147483646 seconds (approximately 68 years).
Time Zone radio button	Allows you to select a timezone.

Step 5 Click **Save Changes** to save the configuration change.

Deleting a MACsec Key Lifetime

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Navigate to **LAN** > **MACsec** > **Keychain**.
Step 3 Select the MACsec key, which you want to delete.
Step 4 In the **Actions** area, click **Delete LifeTime** to delete a MACsec Lifetime configuration.
Step 5 Click **Yes** in the confirmation dialog box.

Creating a MACsec Interface Configuration

Configure different keychain for primary and fallback PSKs.

We recommend that you first change the primary PSK and save the changes. Then, change the fallback PSK.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Navigate to **LAN** > **MACsec** > **Interface Configuration**.
Step 3 In the **Properties** area, click **Add**.
Step 4 In the **Create MACsec Interface Configuration** dialog box, complete the following fields:

Name	Description
Name field	Enter a name for the MACsec interface configuration.
MACsec Keychain Name drop-down list	Allows you to select MACsec keychain from the drop-down list.
MACsec Fallback KeyChain Name drop-down list	Allows you to select MACsec backup keychain from the drop-down list.
MACsec Policy Name drop-down list	Allows you to select MACsec policy from the drop-down list.
MACsec EAPOL Name drop-down list	Allows you to select MACsec EAPOL from the drop-down list.

For more information on MACsec EAPOL, see Configurable EAPOL Destination and Ethernet Type.

Step 5 Click **OK**.

Viewing or Modifying a MACsec Interface Configuration

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Interface Configuration**.

Step 3 Select the MACsec interface configuration, which you want to view or modify.

Step 4 In the **General** tab, under the **Properties** window, you can view and modify the following:

Name	Description
Name field	Enter a name for the MACsec interface configuration.
MACsec Keychain Name drop-down list	Allows you to select MACsec keychain from the drop-down list.
MACsec Fallback KeyChain Name drop-down list	Allows you to select MACsec backup keychain from the drop-down list.
MACsec Policy Name drop-down list	Allows you to select MACsec policy from the drop-down list.
MACsec EAPOL Name drop-down list	Allows you to select MACsec EAPOL from the drop-down list.

For more information on MACsec EAPOL, see Configurable EAPOL Destination and Ethernet Type.

Step 5 Click **Save Changes** to save the configuration change.

Deleting a MACsec Key Lifetime

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Keychain**.

Step 3 Select the MACsec key, which you want to delete.

Step 4 In the **Actions** area, click **Delete LifeTime** to delete a MACsec Lifetime configuration.

Step 5 Click **Yes** in the confirmation dialog box.

Creating a MACsec Interface Configuration

Configure different keychain for primary and fallback PSKs.

We recommend that you first change the primary PSK and save the changes. Then, change the fallback PSK.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Interface Configuration**.

Step 3 In the **Properties** area, click **Add**.

Step 4 In the **Create MACsec Interface Configuration** dialog box, complete the following fields:

Name	Description
Name field	Enter a name for the MACsec interface configuration.
MACsec Keychain Name drop-down list	Allows you to select MACsec keychain from the drop-down list.
MACsec Fallback KeyChain Name drop-down list	Allows you to select MACsec backup keychain from the drop-down list.
MACsec Policy Name drop-down list	Allows you to select MACsec policy from the drop-down list.
MACsec EAPOL Name drop-down list	Allows you to select MACsec EAPOL from the drop-down list.

For more information on MACsec EAPOL, see Configurable EAPOL Destination and Ethernet Type.

Step 5 Click **OK**.

Viewing or Modifying a MACsec Interface Configuration

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Interface Configuration**.

Step 3 Select the MACsec interface configuration, which you want to view or modify.

Step 4 In the **General** tab, under the **Properties** window, you can view and modify the following:

Name	Description
Name field	Enter a name for the MACsec interface configuration.
MACsec Keychain Name drop-down list	Allows you to select MACsec keychain from the drop-down list.
MACsec Fallback KeyChain Name drop-down list	Allows you to select MACsec backup keychain from the drop-down list.
MACsec Policy Name drop-down list	Allows you to select MACsec policy from the drop-down list.
MACsec EAPOL Name drop-down list	Allows you to select MACsec EAPOL from the drop-down list.

For more information on MACsec EAPOL, see Configurable EAPOL Destination and Ethernet Type.

Step 5 Click **Save Changes** to save the configuration change.

Deleting MACsec on an Uplink Interface

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud** > *Fabric* > **Uplink Eth Interfaces**.

Step 3 Select an Ethernet Uplink interface.

Step 4 In the **Properties** area, in the **MACsec Interface Configuration** field, choose **<not-set>** to delete an interface.

Step 5 Click **Save Changes** to save the configuration change.

Configuring MACsec on an Uplink Port Channel Member Interface

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud** > *Fabric* > **Port Channels**.

Step 3 Select a Ethernet Port Channel Member interface.

Step 4 In the **Properties** area, in the **MACsec Interface Configuration** field, choose the MACsec interface configuration that was created, and apply it on the interface.

Step 5 Click **Save Changes** to save the configuration change.

Viewing or Modifying MACsec on an Uplink Port Channel Member Interface

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud** > *Fabric* > **Port Channels**.

Step 3 Select a Ethernet Port Channel Member interface.

Step 4 In the **Properties** area, view or modify the properties as required.

Step 5 Click **Save Changes** to save the configuration change.

Deleting MACsec on an Uplink Port Channel Member Interface

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud** > *Fabric* > **Port Channels**.

Step 3 Select a Ethernet Port Channel Member interface.

Step 4 In the **Properties** area, in the **MACsec Interface Configuration** field, choose **<not-set>** to delete an interface.

Step 5 Click **Save Changes** to save the configuration change.

Configurable EAPOL Destination and Ethernet Type

Configurable EAPOL MAC and Ethernet type provides you the ability to change the MAC address and the Ethernet type of the MKA packet, to allow CE device to form MKA sessions over the ethernet networks that consume the standard MKA packets.

The EAPOL destination Ethernet type can be changed from the default Ethernet type of 0x888E to an alternate value or, the EAPOL destination MAC address can be changed from the default DMAC of 01:80:C2:00:00:03 to an alternate value, to avoid being consumed by a provider bridge.

This feature is available at the interface level and the alternate EAPOL configuration can be changed on any interface at any given time as follows:

- If the MACsec is already configured on an interface, the sessions comes up with a new alternate EAPOL configuration.
- When MACsec is not configured on an interface, the EAPOL configuration is applied to the interface and is effective when MACsec is configured on that interface.

Creating a MACsec EAPOL

You can enable the EAPOL configuration on any available interface.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **EAPOL**.

Step 3 In the **Properties** area, click **Add** to create a MACsec EAPOL configuration.

Step 4 In the **Create MACsec EAPOL** dialog box, complete the following fields:

Name	Description
Name field	Enter a name for the MACsec EAPOL.
Description field	Enter a brief description for the MACsec EAPOL.
MAC Address field	Enter the MAC address where you wish to enable the EAPOL configuration.
Ether Type field	Enter the Ethernet type.

Step 5 Click **OK**.

Viewing or Modifying a MACsec EAPOL

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **EAPOL**.

Step 3 Select the MACsec EAPOL, which you want to view or modify.

Step 4 In the **General** tab, under the **Properties** window, you can view and modify the following:

Name	Description
Name field	Enter a name for the MACsec EAPOL.
Description field	Enter a brief description for the MACsec EAPOL.
MAC Address field	Enter the MAC address where you wish to enable the EAPOL configuration.
Ether Type field	Enter the Ethernet type.

Step 5 Click **Save Changes** to save the configuration change.

Deleting a MACsec EAPOL

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **EAPOL**.

Step 3 In the **Actions** area, click **Delete** to delete a MACsec EAPOL configuration.

Step 4 Click **Yes** in the confirmation dialog box .

Displaying MACsec Sessions

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > **Fabric_Interconnect_Name** > **Fixed Module** > **Ethernet Ports** .

Step 3 Click a port under the Ethernet Ports node.

Step 4 Click the **General** tab.

The Operational states of the MACsec session on an interface are displayed.

The possible values for operational states are as follows:

- MACsec Status—Init, Pending, Secured, Rekeyed
- MACsec Key-server—yes, no

- MACsec Auth-mode—Primary-PSK, Fallback-PSK

Displaying MACsec Statistics

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > **Fabric_Interconnect_Name** > **Fixed Module** > **Ethernet Ports** .

Step 3 Click a port under the Ethernet Ports node.

Step 4 In the Work pane, click the **Statistics** tab.

The MACsec RX Stats and MACsec TX Stats counters are displayed.

The following example shows the MACsec security statistics for a specific Ethernet interface.

Note
The following differences exist for uncontrolled and controlled packets in Rx and Tx statistics:

Rx statistics:

- Uncontrolled = Encrypted and unencrypted
- Controlled = Decrypted

Tx statistics:

- Uncontrolled = Unencrypted
- Controlled = Encrypted