CONTENTS

Preface ix
  Audience ix
  Conventions ix
  Related Documentation xi
  Documentation Feedback xi
  Obtaining Documentation and Submitting a Service Request xi

CHAPTER 1 New and Changed Information for this Release 1
  New and Changed Information for This Release 1

CHAPTER 2 Overview 3
  Network Device Management Tasks You Can Perform in Cisco UCS Director 3
  Network Device Management Tasks You Cannot Perform in Cisco UCS Director 4
  Orchestration Tasks for Network Device Management 4
  Collecting Inventory for a Network Device 5
  Configuring the Polling Interval 5
  Viewing Connectivity and Topology for Network Devices 5
  Verifying Network Device Details in a Pod Environment 6

CHAPTER 3 Configuring Multiple Spanning Tree 7
  About MST 7
  Configuring an MST Instance 8
  Enabling MST and Configuring MST Network Parameters 8

CHAPTER 4 Configuring Per VLAN Rapid Spanning Tree Plus 11
  About PVST+ 11
  Configuring PVST+ 12
## Contents

### CHAPTER 5

**Configuring VLAN Trunking Protocol**  
About VTP  
Configuring VTP

### CHAPTER 6

**Managing MAC Addresses**  
About MAC Addresses  
Adding a MAC Address to a Switch  
Removing a MAC Address from a Switch  
Assigning MAC Address to a Port  
Unassigning MAC Address from a Port  
Configuring the Aging Time for the MAC Address Table

### CHAPTER 7

**Managing Virtual Device Contexts**  
About VDCs  
Creating a VDC  
Allocating a Port to a VDC  
Removing a Port from a VDC  
Removing a VDC

### CHAPTER 8

**Managing Ports**  
About Ports  
Configuring a Port  
Configuring an STP Port  
Configuring a Port License  
Creating a Port Profile  
Updating a Port Profile  
Configuring a Private VLAN Port Profile

### CHAPTER 9

**Configuring SVI**  
About SVI  
Configuring a SVI  
Deleting a SVI

### CHAPTER 10

**Managing TrustSec**
Contents

CHAPTER 11 Configuring SGT Exchange Protocol Connection 37
    About SXP Connection 37
    Configuring an SXP Peer Connection 37

CHAPTER 12 Configuring HSRP 41
    About HSRP 41
    Configuring HSRP 41

CHAPTER 13 Managing FC Alias 45
    About FC Alias 45
    Creating a FC Alias 45
    Updating a FC Alias 46
    Deleting a FC Alias 47

CHAPTER 14 Configuring Access Ports 49
    About Access Ports 49
    Configuring an Access Port 49

CHAPTER 15 Managing Access Control Lists 51
    About Access Control Lists 51
    Creating an ACL 52
    Configuring Context ACL 53

CHAPTER 16 Configuring Network Address Translation 55
    About NAT 55
    Configuring NAT 55
    Configuring Context NAT 56

CHAPTER 17 Configuring Quality of Services 59
    About Quality of Service Policies 59
    Configuring a QoS Policy 59
    Deleting a QoS Policy 62
Creating a SAN Zoneset 86
Adding a Member to a SAN Zoneset 86
Deleting a SAN Zoneset 87

CHAPTER 24
Managing Virtual Storage Area Networks 89
About VSANs 89
Creating a VSAN 90
Deleting a VSAN 90

CHAPTER 25
Managing Virtual Extensible LANs 93
About VXLANs 93
Creating a VXLAN 94
Encapsulating a VXLAN 95
Assigning a VXLAN to a Port Profile 96
Unassigning a VXLAN from a Port Profile 96
Removing a VXLAN 97

CHAPTER 26
Configuring ASA Context 99
About ASA Context 99
Creating an ASA Context 99

CHAPTER 27
Monitoring and Reporting 101
About General Reports 101
About Detail Reports 102
About Cisco ISE 105
About the Service Request Details Report 106
Exporting an Inventory Report 106

CHAPTER 28
Troubleshooting 107
Troubleshooting Cisco UCS Director Connectivity 107
Troubleshooting Cisco UCS Director Baremetal Agent Connectivity 108
Preface

This preface contains the following sections:

- Audience, page ix
- Conventions, page ix
- Related Documentation, page xi
- Documentation Feedback, page xi
- Obtaining Documentation and Submitting a Service Request, page xi

Audience

This guide is intended primarily for data center administrators who use Cisco UCS Director and who have responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security
- Virtualization and virtual machines

Conventions

<table>
<thead>
<tr>
<th>Text Type</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI elements</td>
<td>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.</td>
</tr>
<tr>
<td>TUI elements</td>
<td>In a Text-based User Interface, text the system displays appears in this font.</td>
</tr>
<tr>
<td>Text Type</td>
<td>Indication</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>System output</td>
<td>Terminal sessions and information that the system displays appear in this font.</td>
</tr>
<tr>
<td>CLI commands</td>
<td>CLI command keywords appear in this font. Variables in a CLI command appear in this font.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

---

**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.

**Caution**

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

**Timesaver**

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

Cisco UCS Director Documentation Roadmap

For a complete list of Cisco UCS Director documentation, see the Cisco UCS Director Documentation Roadmap available at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/ucs-director/doc-roadmap/b_UCSDirectorDocRoadmap.html.

Cisco UCS 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: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

For a complete list of all C-Series documentation, see the Cisco UCS C-Series Servers Documentation Roadmap available at the following URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc.

Note

The Cisco UCS B-Series Servers Documentation Roadmap includes links to documentation for Cisco UCS Manager and Cisco UCS Central. The Cisco UCS C-Series Servers Documentation Roadmap includes links to documentation for Cisco Integrated Management Controller.

Documentation Feedback

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation.

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
New and Changed Information for this Release

This chapter contains the following section:

- New and Changed Information for This Release, page 1

New and Changed Information for This Release

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

Table 1: New Features and Changed Behavior in Cisco UCS Director, Release 5.0

<table>
<thead>
<tr>
<th>Feature Support for Cisco Nexus 9300 and 9500 Series Switches</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature Support for Cisco Nexus 9300 and 9500 Series Switches</td>
<td>In Cisco UCS Director, the following configurations are supported on Cisco Nexus 9300 and 9500 Series switches:</td>
<td>• About VTP, on page 13</td>
</tr>
<tr>
<td></td>
<td>• VLAN Trunking Protocol (VTP) configuration</td>
<td>• About MAC Addresses, on page 15</td>
</tr>
<tr>
<td></td>
<td>• MAC address configuration</td>
<td>• About Ports, on page 25</td>
</tr>
<tr>
<td></td>
<td>• Ports and port profile configuration</td>
<td>• About Trunks, on page 65</td>
</tr>
<tr>
<td></td>
<td>• Trunk configuration</td>
<td>• About VLANs, on page 73</td>
</tr>
<tr>
<td></td>
<td>• VLAN configuration</td>
<td>• About vPCs, on page 79</td>
</tr>
<tr>
<td></td>
<td>• Virtual port channel (vPC) configuration</td>
<td></td>
</tr>
</tbody>
</table>

Feature Support for Cisco ISE

<table>
<thead>
<tr>
<th>Feature Support for Cisco ISE</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature Support for Cisco ISE</td>
<td>You can view the SGT entry of all devices that are managed in Cisco UCS Director.</td>
<td>About Cisco ISE, on page 105</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Where Documented</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Configuring Access Ports</td>
<td>You can configure access ports on the Cisco Nexus 9300 and 9500 Series switches.</td>
<td>Configuring an Access Port, on page 49</td>
</tr>
<tr>
<td>Managing Access Control Lists (ACLs)</td>
<td>You can configure ACLs on the Cisco Nexus 9300 and 9500 Series switches.</td>
<td>Creating an ACL, on page 52</td>
</tr>
<tr>
<td>Configuring Quality of Services (QoS)</td>
<td>You can configure QoS on the Cisco Nexus 9300 and 9500 Series switches.</td>
<td>Configuring a QoS Policy, on page 59</td>
</tr>
<tr>
<td>Managing Service Policy</td>
<td>You can configure service policy on the Cisco Nexus 9300 and 9500 Series switches.</td>
<td>Updating a Service Policy, on page 64</td>
</tr>
<tr>
<td>Managing MAC Addresses</td>
<td>You can assign MAC address to a port and unassign MAC address from a port.</td>
<td>Managing MAC Addresses, on page 15</td>
</tr>
<tr>
<td>Configuring Port License</td>
<td>You can configure license for a port.</td>
<td>Configuring a Port License, on page 27</td>
</tr>
<tr>
<td>Configuring Context ACL</td>
<td>You can configure context ACL.</td>
<td>Configuring Context ACL, on page 53</td>
</tr>
<tr>
<td>Configuring NAT</td>
<td>You can configure NAT.</td>
<td>Configuring Network Address Translation, on page 55</td>
</tr>
<tr>
<td>Managing TrustSec</td>
<td>You can refresh TrustSec.</td>
<td>Managing TrustSec, on page 35</td>
</tr>
<tr>
<td>Configuring SGT Exchange Protocol Connection</td>
<td>You can configure SGT Exchange Protocol (SXP) peer connection.</td>
<td>Configuring SGT Exchange Protocol Connection, on page 37</td>
</tr>
<tr>
<td>Configuring HSRP</td>
<td>You can configure HSRP.</td>
<td>Configuring HSRP, on page 41</td>
</tr>
<tr>
<td>Managing FC Alias</td>
<td>You can manage FC Alias.</td>
<td>Managing FC Alias, on page 45</td>
</tr>
<tr>
<td>Configuring ASA Context</td>
<td>You can configure ASA context.</td>
<td>Configuring ASA Context, on page 99</td>
</tr>
<tr>
<td>Reports</td>
<td>You can view reports for components of Cisco Nexus 9300 and 9500 Series switches, including the license information and summary status.</td>
<td>About Detail Reports, on page 102</td>
</tr>
</tbody>
</table>
Overview

This chapter contains the following sections:

- Network Device Management Tasks You Can Perform in Cisco UCS Director, page 3
- Network Device Management Tasks You Cannot Perform in Cisco UCS Director, page 4
- Orchestration Tasks for Network Device Management, page 4
- Collecting Inventory for a Network Device, page 5
- Configuring the Polling Interval, page 5
- Viewing Connectivity and Topology for Network Devices, page 5
- Verifying Network Device Details in a Pod Environment, page 6

Network Device Management Tasks You Can Perform in Cisco UCS Director

You can use Cisco UCS Director to perform management, monitoring, and reporting tasks for network devices within a domain.

Configuration and Administration

You can configure the following network device protocols and components in Cisco UCS Director:

- Ports and trunks
- Multiple Spanning Tree (MST), Per VLAN Spanning Tree (PVST), and VLAN Trunking Protocol (VTP)
- Storage area network (SAN) zones and zonesets
- Virtual device contexts (VDCs), virtual Fibre Channels (VFCs), and virtual port channel (vPC) domains
- VLANs and private VLANs
- Virtual storage area networks (VSANs)
- Virtual extensible local area networks (VXLANs)
Monitoring and Reporting
You can also use Cisco UCS Director to monitor and report on network devices, including:

- Service detail requests
- Configurations
- Modules
- Interfaces
- Port capabilities and profiles
- Pool policies and usage
- MAC address table configurations
- Quality of Service (QoS) policy and class maps
- Service detail requests
- SAN zones and zonesets
- vPC information
- VSAN, VLAN, and Private VLAN information

Network Device Management Tasks You Cannot Perform in Cisco UCS Director
You cannot use Cisco UCS Director to perform certain network device management tasks within a Cisco UCS domain, such as the following:

- Firmware upgrades
- User management

Orchestration Tasks for Network Device Management
Cisco UCS Director includes orchestration features that allow you to automate configuration and management of network domain tasks in one or more workflows.

A complete list of the network device orchestration tasks is available in the Workflow Designer, and in the Task Library.

For more information about orchestration in Cisco UCS Director, see the Cisco UCS Director Orchestration Guide.
Collecting Inventory for a Network Device

- **Step 1**: On the menu tab, choose **Physical > Network**.
- **Step 2**: In the **Network** pane, choose the pod.
- **Step 3**: Click the **Managed Network Elements** tab.
- **Step 4**: Select the network device for which you want to collect inventory.
- **Step 5**: Click **Collect Inventory**.

Configuring the Polling Interval

The polling interval specifies the frequency of inventory collection.

- **Step 1**: On the menu bar, choose **Administration > System**.
- **Step 2**: Click the **System Tasks** tab.
- **Step 3**: Choose an inventory task of the account and click **Manage Task**.
- **Step 4**: From the **Minutes** drop-down list, choose the polling interval.
- **Step 5**: Click **Submit**.

Viewing Connectivity and Topology for Network Devices

You can view the connectivity and topology diagram for any network device. You can choose to view a hierarchical, concentric, circular, or force-directed mode.

- **Step 1**: On the menu tab, choose **Physical > Network**.
- **Step 2**: In the **Network** pane, choose the pod.
- **Step 3**: Click the **Managed Network Elements** tab.
- **Step 4**: Select the network device that you want to view.
- **Step 5**: Click **View Connectivity**.
- **Step 6**: In the **Topology View - Network Device Connectivity** dialog box, complete the following fields:
Step 7  Click Close when you are finished verifying the connectivity of the network devices and determining their topology.

### Verifying Network Device Details in a Pod Environment

After the network device is added to the pod, all discovered components of the pod environment are displayed at the account level.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>View Mode</strong> drop-down list</td>
<td>Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Hierarchical</td>
</tr>
<tr>
<td></td>
<td>• Concentric</td>
</tr>
<tr>
<td></td>
<td>• Circular</td>
</tr>
<tr>
<td></td>
<td>• Force directed</td>
</tr>
<tr>
<td><strong>Show Link Labels</strong> check box</td>
<td>Check the check box to show link labels in the topology.</td>
</tr>
<tr>
<td><strong>Allow Item Spacing</strong> check box</td>
<td>Check the check box to allow line spacing in the view.</td>
</tr>
</tbody>
</table>
Configuring Multiple Spanning Tree

This chapter contains the following sections:

- About MST, page 7
- Configuring an MST Instance, page 8
- Enabling MST and Configuring MST Network Parameters, page 8

About MST

Multiple Spanning Tree (MST) is the IEEE 802.1s standard that allows two or more VLANs to be assigned to a spanning tree instance. Each instance has a spanning tree topology independent of other spanning tree instances. This architecture provides multiple forwarding paths for data traffic, enables load balancing, and reduces the number of Spanning Tree Protocol (STP) instances required to support a large number of VLANs. MST improves the fault tolerance of the network because a failure in one instance (forwarding path) does not affect other instances (forwarding paths). MST instances with the same name, revision number, and VLAN-to-instance mapping combine to form an MST region. The MST region appears as a single bridge to spanning tree configurations outside the region. MST fails over to IEEE 802.1D STP when it receives an 802.1D message from a neighboring switch.

Note

Spanning tree is used to refer to IEEE 802.1w and IEEE 802.1s. If the text is discussing the IEEE 802.1D Spanning Tree Protocol, 802.1D is stated specifically.

In Cisco UCS Director, MST configuration is supported on the following Cisco network devices:

- Cisco Nexus 3000 Series switches
- Cisco Nexus 5000, 5500, and 5672 Series switches
- Cisco Nexus 6000 Series switches
- Cisco Nexus 7000 Series switches
- Cisco Nexus 9000 Series switches
Configuring an MST Instance

You can configure an MST instance on a network.

Step 1 On the menu bar, click Physical > Network.
Step 2 In the Network pane, choose the pod.
Step 3 Click the Managed Network Elements tab.
Step 4 Select the network device that needs to be configured.
Step 5 Click the down-arrow icon, and choose Configure MST Instance.

You can alternatively choose Configure MST Instance command on the Summary tab that appears on selection of the network device from the left pane.

Step 6 In the Configure MST Instance dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MST Instance field</td>
<td>The MST ID number.</td>
</tr>
<tr>
<td>VLAN field</td>
<td>The VLAN to apply in this MST ID.</td>
</tr>
</tbody>
</table>

Step 7 Click Submit.

Enabling MST and Configuring MST Network Parameters

Step 1 On the menu bar, choose Physical > Network.
Step 2 In the Network pane, choose the pod.
Step 3 Click the Managed Network Elements tab.
Step 4 Select the network device that needs to be configured.
Step 5 Click the down-arrow icon, and choose Configure MST.

You can alternatively choose Configure MST command on the Summary tab that appears on selection of the network device from the left pane.

Step 6 In the Configure MST dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable MST check box</td>
<td>Check the check box to enable MST.</td>
</tr>
<tr>
<td>Note</td>
<td>To disable MST, uncheck the checkbox.</td>
</tr>
</tbody>
</table>
### Name | Description
--- | ---
**Name** field | (Required) The MST region name for the bridge. The name string has a maximum length of 32 characters and is case sensitive. The default is an empty string. **Note** For two or more bridges to be in the same MST region, they must have the identical MST name, VLAN-to-instance mapping, and MST revision number.

**Revision** field | (Required) The revision number is an unsigned 16-bit number that identifies the revision of the current MST configuration.

**Hello Time** field | The hello time between each bridge protocol data unit (BPDU) that is sent on the root bridge port used for all MST instances. These messages mean that the switch is alive. For seconds, the range is from 1 to 10, and the default is 2 seconds.

**Forward Time** field | The forward delay time for all MST instances that a port waits before changing from its spanning tree blocking and learning states to the forwarding state. For seconds, the range is from 4 to 30, and the default is 15 seconds.

**Max Hop Count** field | The Max Hop Count to be used. This is the maximum number of hops for the MST region. A region is the equivalent of Border Gateway Protocol (BGP) Autonomous Systems, which is a group of switches placed under common administration.

**Max Age in seconds** field | The maximum-aging time for all MST instances. The maximum-aging time is the number of seconds that a switch waits without receiving spanning tree configuration messages before attempting a reconfiguration. For seconds, the range is from 6 to 40, and the default is 20 seconds.

**Copy Running configuration to Startup configuration** check box | Check the check box to copy the running configuration to the startup configuration.

---

**Step 7** | In the **Select Items** dialog box, check the check boxes to choose individual ports, and click **Select**.

**Step 8** | Click **Submit**.
Configuring Per VLAN Rapid Spanning Tree Plus

This chapter contains the following sections:

• About PVST+, page 11
• Configuring PVST+, page 12

About PVST+

Per VLAN Rapid Spanning Tree Plus (PVST+) is an updated implementation of the Spanning Tree Protocol (STP) that allows you to create one spanning tree topology for each VLAN. PVST+ is the default STP mode on the switch and uses inter switch-link (ISL) trunking and allows a VLAN trunk to forward some VLANs while blocking other VLANs. Because PVST+ treats each VLAN as a separate network, it can load balance traffic (at Layer 2) by forwarding some VLANs on one trunk and other VLANs on another trunk without causing a spanning tree loop.

In Cisco UCS Director, PVST+ configuration is supported on the following Cisco network devices:

• Cisco Nexus 3000 Series switches
• Cisco Nexus 5000, 5500, and 5672 Series switches
• Cisco Nexus 6000 Series switches
• Cisco Nexus 7000 Series switches
• Cisco Nexus 9000 Series switches

Note For more detailed information about PVST+ and configuration guidelines for PVST+, see the Cisco NX-OS Software Configuration Guides.
Configuring PVST+

Per VLAN Rapid Spanning Tree Plus (PVST+) maintains a spanning tree instance for each VLAN that you configure.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>On the menu bar, choose Physical &gt; Network.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>In the Network pane, choose the pod.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Click the Managed Network Elements tab.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Select the network device that needs to be configured.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Click the down-arrow icon, and choose Configure PVST. You can alternatively choose Configure PVST command on the Summary tab that appears on selection of the network device from the left pane.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>In the Configure PVST dialog box, complete the following fields:</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Enable PVST check box</td>
<td>Check the check box to enable PVST+ on the device.</td>
</tr>
<tr>
<td>VLAN field</td>
<td>The VLAN ID within the valid range. The valid VLAN ID range value can be 2 through 4094 (except reserved VLAN values).</td>
</tr>
<tr>
<td>PVST Root Mode check box</td>
<td>Check the check box to enable PVST+ root mode which defines the tree with a root bridge and a loop-free path from the root to all switches in the network. STP forces redundant data paths into a blocked state. If a network segment in the spanning tree fails and a redundant path exists, the STP algorithm recalculates the spanning tree topology and activates the blocked path.</td>
</tr>
<tr>
<td>Priority drop-down list</td>
<td>Choose the STP port priority on the switch. This parameter is used to determine which port is put in the forwarding state and which port is put in the blocking state.</td>
</tr>
<tr>
<td>Path Cost drop-down list</td>
<td>Choose the STP path cost (long or short). This parameter is used to determine which port is put in the forwarding state and which port is put in the blocking state.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Click Submit.</td>
</tr>
</tbody>
</table>
CHAPTER 5

Configuring VLAN Trunking Protocol

This chapter contains the following sections:

• About VTP, page 13
• Configuring VTP, page 13

About VTP

VLAN Trunking Protocol (VTP) reduces the administration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain, which reduces the need to configure the same VLAN everywhere.

In Cisco UCS Director, VTP configuration is supported on the following Cisco network devices:

• Cisco Nexus 3000 Series switches
• Cisco Nexus 5000, 5500, and 5672 Series switches
• Cisco Nexus 6000 Series switches
• Cisco Nexus 7000 Series switches
• Cisco Nexus 9300 and 9500 Series switches

For more detailed information about VTP and configuration guidelines for VTP, see the Cisco NX-OS Software Configuration Guides.

Configuring VTP

You can enable or disable the VLAN Trunking Protocol (VTP) to relay VTP packets on a network.
Ensure that you are in the correct virtual device context (VDC). VLAN names and IDs can be repeated in different VDCs, so you must verify that you are working in the correct VDC.

**Step 1**
On the menu bar, choose **Physical > Network**.

**Step 2**
In the **Network** pane, choose the pod.

**Step 3**
Select the network device that needs to be configured.

**Step 4**
Click the **VTP Status** tab.

**Step 5**
Select the VTP that needs to be configured.

**Step 6**
Click **Configure VTP**.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable VTP Feature check box</td>
<td>Check the check box to enable VTP.</td>
</tr>
<tr>
<td>Domain Name field</td>
<td>The name of the VTP domain that you want this switch to join.</td>
</tr>
<tr>
<td>VTP version drop-down list</td>
<td>Choose either VTP version 1 or 2.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If you are using VTP in a Token Ring environment, you must use version 2.</td>
</tr>
<tr>
<td>File Name field</td>
<td>The filename.</td>
</tr>
<tr>
<td>Password field</td>
<td>The password.</td>
</tr>
<tr>
<td>VTP mode drop-down list</td>
<td>Choose one of the following VTP modes: <strong>Client</strong>, <strong>Server</strong>, <strong>Transparent</strong>, or <strong>Off</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: By default, the VTP mode is set as <strong>Transparent</strong> for the Cisco Nexus 9300 Series switches.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

**Step 8**
Click **Submit**.
Managing MAC Addresses

This chapter contains the following sections:

• About MAC Addresses, page 15
• Adding a MAC Address to a Switch, page 16
• Removing a MAC Address from a Switch, page 16
• Assigning MAC Address to a Port, page 17
• Unassigning MAC Address from a Port, page 18
• Configuring the Aging Time for the MAC Address Table, page 18

About MAC Addresses

The Media Access Control (MAC) address is a unique value that is associated with a network device. Layer 2 ports correlate the MAC address on a packet with the Layer 2 port information for that packet using the MAC address table. A MAC address table is built using the MAC source addresses of the frames received.

In Cisco UCS Director, MAC configuration is supported on the following Cisco network devices:

• Cisco Nexus 1000 Series switches
• Cisco Nexus 3000 Series switches
• Cisco Nexus 5000, 5500, and 5672 Series switches
• Cisco Nexus 6000 Series switches
• Cisco Nexus 7000 Series switches
• Cisco Nexus 9300 and 9500 Series switches

Note

For more detailed information about MAC addresses and configuration guidelines for MAC addresses, see the Cisco NX-OS Software Configuration Guides.
Adding a MAC Address to a Switch

Step 1 On the menu bar, choose Physical > Network.
Step 2 In the Network pane, expand the pod.
Step 3 Select the network device that needs to be configured.
Step 4 Click the MAC Address Table tab.
Step 5 Click Create MAC Address.
Step 6 In the MAC Address Parameters dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address field</td>
<td>The MAC address that is added to the switch MAC address table.</td>
</tr>
<tr>
<td>VLAN ID Select button</td>
<td>In the Select dialog box, choose the VLAN ID number associated with this MAC address.</td>
</tr>
<tr>
<td>Select Port Select button</td>
<td>In the Select dialog box, choose the LAN port (channel) for this VLAN ID number.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Step 7 Click Submit.

Removing a MAC Address from a Switch

Step 1 On the menu bar, choose Physical > Network.
Step 2 In the Network pane, expand the pod.
Step 3 Select the network device for which you need to delete MAC address.
Step 4 Click the MAC Address Table tab.
Step 5 Choose a MAC address that needs to be deleted.
Step 6 Click Delete.
Step 7 In the MAC Address Parameters dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address button</td>
<td>The MAC address on the switch that you selected for deletion.</td>
</tr>
</tbody>
</table>
### Assigning MAC Address to a Port

**Step 1** On the menu bar, choose **Physical > Network**.

**Step 2** In the **Network** pane, expand the pod.

**Step 3** Select the network device that needs to be configured.

**Step 4** Click the **MAC Address Table** tab.

**Step 5** Choose a MAC address that needs to be assigned to a port.

**Step 6** Click **Assign MAC Address Port**.

**Step 7** In the **MAC Address Parameters** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address field</td>
<td>The MAC address that needs to be assigned to a port.</td>
</tr>
<tr>
<td>Select Port button</td>
<td>Click <strong>Select</strong>. In the <strong>Select</strong> dialog box, choose the LAN port (channel).</td>
</tr>
<tr>
<td>Copy Running configuration</td>
<td>Check the check box to copy the running configuration to the startup</td>
</tr>
<tr>
<td>to Startup configuration</td>
<td>configuration.</td>
</tr>
</tbody>
</table>

**Step 8** Click **Submit**.
Unassigning MAC Address from a Port

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click the MAC Address Table tab.
Step 5  Click Unassign MAC Address Port.
Step 6  In the MAC Address Parameters dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Port button</td>
<td>Click Select. In the Select dialog box, choose the LAN port (channel).</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Step 7  Click Submit.

Configuring the Aging Time for the MAC Address Table

You can configure the amount of time that an entry (the packet source MAC address and port that packet ingresses) remains in the MAC address table.

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click the MAC Address Table Configuration tab.
Step 5  Click Configure MAC Address Table.
Step 6  In the MAC Address Parameters dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age Time field</td>
<td>The time from 120 to 918000 seconds before an entry ages out and is discarded from the MAC address table. The number 0 disables MAC aging. You can use multiples of 5. The default is 300 seconds. If a VLAN is not specified, the aging specification applies to all VLANs.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>
Step 7  Click Submit.
Managing Virtual Device Contexts

This chapter contains the following sections:

- About VDCs, page 21
- Creating a VDC, page 22
- Allocating a Port to a VDC, page 22
- Removing a Port from a VDC, page 23
- Removing a VDC, page 24

About VDCs

Virtual device contexts (VDCs) allow switches to be virtualized at the device level. Each configured VDC presents itself as a unique device to connected users within the framework of that physical switch. The VDC runs as a separate logical entity within the switch. It maintains its own unique set of running software processes, has its own configuration, and is managed by a separate administrator.

In Cisco UCS Director, you can manage VDCs on the following Cisco network devices:

- Cisco Nexus 7000 Series switches

Note

For more detailed information about VDCs and configuration guidelines for VDCs, see the Cisco NX-OS Software Configuration Guides.
Creating a VDC

You can create a VDC for a Cisco Nexus 7000 Series switch.

**Step 1** On the menu bar, choose **Physical > Network**.

**Step 2** In the **Network** pane, expand the pod and select the Cisco Nexus 7000 Series switch.

**Step 3** Click the **VDC** tab.

**Step 4** Click **Create VDC**.

**Step 5** In the **Create VDC** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDC Name field</td>
<td>The name of the VDC.</td>
</tr>
<tr>
<td>Module Type field</td>
<td>The name of the module type. For example, F2e Series.</td>
</tr>
<tr>
<td>HA Policy check box</td>
<td>Check the check box to enable the high-availability (HA) policy for the switch when an unrecoverable VDC fault occurs.</td>
</tr>
<tr>
<td>VDC Number field</td>
<td>The VDC number. VDC number 1 is reserved for the default VDC. The nondefault VDC numbers are from 2 to 9.</td>
</tr>
<tr>
<td>VDC Password field</td>
<td>The VDC admin user account password.</td>
</tr>
<tr>
<td>VDC Template Name drop-down list</td>
<td>Choose the VDC template name. VDC resource templates set the minimum and maximum limits for shared physical device resources when you create the VDC.</td>
</tr>
<tr>
<td>Select VDC Type drop-down list</td>
<td>Choose the VDC type.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running VDC configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

**Step 6** Click **Submit**.

Allocating a Port to a VDC

You can assign a port to a VDC that belongs to a Cisco Nexus 7000 Series switch.
Before You Begin
You must create a virtual device context (VDC) on a Cisco Nexus 7000 Series switch.

Step 1
On the menu bar, choose **Physical > Network**.

Step 2
In the **Network** pane, expand the pod and select the Cisco Nexus 7000 Series switch.

Step 3
Click the **VDC** tab.

Step 4
Select the VDC to which you want to assign a port.

Step 5
Click **Assign Port to VDC**.

Step 6
In the **Allocate Port VDC** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDC Name field</td>
<td>The name of the VDC.</td>
</tr>
<tr>
<td>Select Port button</td>
<td>Click <strong>Select</strong>. In the <strong>Select Items</strong> dialog box, choose the port to assign to the VDC and click <strong>Select</strong>.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running VDC configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Step 7
Click **Submit**.

Removing a Port from a VDC
You can remove a port belonging to a virtual device context (VDC) on a Cisco Nexus 7000 Series switch.

Step 1
On the menu bar, choose **Physical > Network**.

Step 2
In the **Network** pane, expand the pod and select the Cisco Nexus 7000 Series switch.

Step 3
Click the **VDC** tab.

Step 4
Select the VDC and click **Remove Port from VDC**.

Step 5
In the **Remove VDC** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDC Name field</td>
<td>The name of the VDC.</td>
</tr>
<tr>
<td>Select Port button</td>
<td>Choose the port that you want to remove from the VDC.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running VDC configuration to the startup configuration.</td>
</tr>
</tbody>
</table>
Removing a VDC

Step 1
On the menu bar, choose Physical > Network.

Step 2
In the Network pane, expand the pod and select the Cisco Nexus 7000 Series switch.

Step 3
Click the VDC tab.

Step 4
Select the VDC that you want to remove.

Step 5
Click Remove VDC.
You can alternatively choose commands by clicking the down-arrow icon.

Step 6
In the Remove VDC dialog box, complete the following field:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Step 7
Click Submit.
Managing Ports

This chapter contains the following sections:

- About Ports, page 25
- Configuring a Port, page 26
- Configuring an STP Port, page 26
- Configuring a Port License, page 27
- Creating a Port Profile, page 28
- Updating a Port Profile, page 29
- Configuring a Private VLAN Port Profile, page 30

About Ports

Switch ports are Layer 2-only interfaces that are associated with a physical port. Switch ports belong to one or more VLANs. A switch port can be an access port, a trunk port, or a tunnel port. Switch ports are used to manage the physical interface and associated Layer 2 protocols; they do not handle routing or bridging.

In Cisco UCS Director, you can configure ports and port profiles on the following Cisco network devices:

- Cisco Nexus 1000 and 1110 Series switches
- Cisco Nexus 3000 Series switches
- Cisco Nexus 5000, 5500, and 5672 Series switches
- Cisco Nexus 6000 Series switches
- Cisco Nexus 7000 Series switches
- Cisco Nexus 9300 and 9500 Series switches
- Cisco MDS 9100 Series switches
- Cisco MDS 9500 Series switches
- Cisco MDS 9700 Series switches
• Cisco ASA 5500 Series firewall
• Cisco IOS Devices
• Cisco Adaptive Security Virtual Appliance (ASAv)

For more detailed information about managing ports, see the Cisco NX-OS Software Configuration Guides.

Configuring a Port

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click the Interfaces tab.
Step 5  Click Configure Port.
Step 6  In the Configure Port dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Port field</td>
<td>The port that needs to be configured is displayed.</td>
</tr>
<tr>
<td>Enable check box</td>
<td>Check the check box to enable the port.</td>
</tr>
<tr>
<td>Copy Running configuration</td>
<td>Check the check box to copy the running configuration to the startup</td>
</tr>
<tr>
<td>Startup configuration check box</td>
<td>configuration.</td>
</tr>
</tbody>
</table>

Step 7  Click Submit.

Configuring an STP Port

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
The summary status of the device is displayed.
Step 4  Click Configure STP Port.
Step 5  In the Configure STP Port dialog box, complete the following fields:
### Configuring a Port License

**Step 1**
On the menu bar, choose **Physical > Network**.

**Step 2**
In the **Network** pane, expand the pod.

**Step 3**
Select the network device that needs to be configured. The summary status of the device is displayed.

**Step 4**
Click **Configure Port License**.

**Step 5**
In the **Configure Port License** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Port drop-down</td>
<td>Choose a port from the list.</td>
</tr>
<tr>
<td>Acquire check box</td>
<td>Check this check box to acquire the license.</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Port Select button</td>
<td>(Required) Click <strong>Select</strong>. In the <strong>Select</strong> dialog box, choose the designated STP port. Continue to Step 7 if no other parameters need to be made for this port.</td>
</tr>
<tr>
<td>VLAN field</td>
<td>The VLAN ID number from 1 to 4094 .</td>
</tr>
<tr>
<td>Cost Auto check box</td>
<td>Check this check box to enable automatic choosing of the least costly port path. Port costs break a tie for the designated port.</td>
</tr>
<tr>
<td>Hello Time field</td>
<td>The hello time to be used on this port. This is the time between each bridge protocol data unit (BPDU) that is sent on a port.</td>
</tr>
<tr>
<td>Forward Time field</td>
<td>The forward delay to be used on this port. This is the time that is spent in the listening and learning state.</td>
</tr>
<tr>
<td>Max Age field</td>
<td>The maximum length of time before a bridge port saves its configuration BPDU information.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>
Step 6  Click Submit.

Creating a Port Profile

The port profile that you create for a network device is available as a distributed port group on VMware vCenter, if there is a connection between the Virtual Supervisor Module (VSM) and vCenter.

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click the Port Profiles tab.
Step 5  Click Create Port Profile.
Step 6  In the Port Profile Configuration dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Profile Name field</td>
<td>(Required) The name for the network device port profile.</td>
</tr>
<tr>
<td>Description field</td>
<td>The description of the port profile.</td>
</tr>
<tr>
<td>Port Profile Type drop-down list</td>
<td>Choose one of the following: Vethernet or Ethernet.</td>
</tr>
<tr>
<td>Mode drop-down list</td>
<td>Choose one of the following: Access or Trunk.</td>
</tr>
<tr>
<td>Access VLAN drop-down list</td>
<td>(Required) Choose the access VLAN type.</td>
</tr>
<tr>
<td>Enable VXLAN Capability check box</td>
<td>Check the check box to enable the virtual extensible LAN (VXLAN) capability on this port profile. Uncheck the check box if you do not want to enable the VXLAN capability.</td>
</tr>
<tr>
<td>IP address field</td>
<td>The IP network address.</td>
</tr>
<tr>
<td>IP network mask field</td>
<td>The subnetwork address mask for this network.</td>
</tr>
<tr>
<td>IP next-hop address field</td>
<td>The IP next-hop address.</td>
</tr>
</tbody>
</table>
Choose the quality of service (QoS) policy map to apply to the port profile if applicable.

This field appears on selection of Vethernet as the port profile type. Click Select. In the Select dialog box, choose a SGT.

SGT support is provided for Cisco Nexus 1000 and 1110 Series switches.

Check the check box to copy the running port profile configuration to the startup configuration.

Step 7 Click Submit.

### Updating a Port Profile

**Step 1** On the menu bar, choose Physical > Network.

**Step 2** In the Network pane, expand the pod.

**Step 3** Select the network device that needs to be configured.

**Step 4** Click the Port Profiles tab.

**Step 5** Select the port profile and click Update Port Profile.

**Step 6** In the Update Port Profile Configuration dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Profile Name field</td>
<td>The name of the port profile.</td>
</tr>
<tr>
<td>Description field</td>
<td>The description of the port profile.</td>
</tr>
<tr>
<td>Port Profile Type drop-down list</td>
<td>The type of the port profile (read-only). For example, Ethernet.</td>
</tr>
<tr>
<td>Mode drop-down list</td>
<td>The mode of the port profile (read-only). For example, trunk.</td>
</tr>
<tr>
<td>Enable VXLAN Capability check box</td>
<td>Check the check box if you want to enable the VXLAN capability on this port profile. Uncheck the check box if you do not want to enable the VXLAN capability.</td>
</tr>
<tr>
<td>IP address field</td>
<td>The IP network address.</td>
</tr>
</tbody>
</table>
### Configuring a Private VLAN Port Profile

**Step 1** On the menu bar, choose Physical > Network.

**Step 2** In the Network pane, expand the pod.

**Step 3** Select the network device that needs to be configured.

**Step 4** Click the Private VLANs tab.

**Step 5** Click Configure Private VLAN Port Profile.

**Step 6** In the Configure Private VLAN Port Profile dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port Profile Name</strong> field</td>
<td>(Required) The port profile name.</td>
</tr>
<tr>
<td><strong>Port Profile Type</strong> drop-down list</td>
<td>The port profile type.</td>
</tr>
<tr>
<td><strong>Trunk</strong> check box</td>
<td>Check the check box to create the port profile in trunk mode.</td>
</tr>
<tr>
<td><strong>Type</strong> drop-down list</td>
<td>Choose either host or promiscuous.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP network mask</strong> field</td>
<td>The subnetwork address mask for this network.</td>
</tr>
<tr>
<td><strong>IP next-hop address</strong> field</td>
<td>The IP next-hop address.</td>
</tr>
<tr>
<td><strong>Access VLAN</strong> drop-down list</td>
<td>Choose the Access VLAN.</td>
</tr>
<tr>
<td><strong>Action</strong> drop-down list</td>
<td>Choose Add or Remove to add or remove the VLAN(s).</td>
</tr>
<tr>
<td><strong>Select VLANs</strong> button</td>
<td>Click Select. In the Select Items dialog box, choose one or more VLANs and</td>
</tr>
<tr>
<td></td>
<td>click Select.</td>
</tr>
<tr>
<td><strong>Select Sgt</strong> field</td>
<td>Click Select. In the Select dialog box, choose a SGT.</td>
</tr>
<tr>
<td><strong>Copy Running configuration to Startup configuration</strong> check box</td>
<td>Check the check box to copy the running port profile configuration to the startup configuration.</td>
</tr>
</tbody>
</table>
### Name | Description
--- | ---
Primary VLAN ID drop-down list | Choose the primary VLAN ID.
Secondary VLAN ID Select button | Click Select. In the Select Items dialog box, choose the valid secondary VLAN ID(s) and click Select.
Copy Running configuration to Startup configuration check box | Check the check box to copy the running configuration to the startup configuration.

**Step 7** Click Submit.
Managing Ports

Configuring a Private VLAN Port Profile
Configuring SVI

This chapter contains the following sections:

- About SVI, page 33
- Configuring a SVI, page 34
- Deleting a SVI, page 34

About SVI

A switch virtual interfaces (SVI) or VLAN interface, is a virtual routed interface that connects a VLAN on the device to the Layer 3 router engine on the same device. Only one VLAN interface can be associated with a VLAN, but you need to configure a VLAN interface for a VLAN only when you want to route between VLANs or to provide IP host connectivity to the device through a virtual routing and forwarding (VRF) instance that is not the management VRF. When you enable VLAN interface creation, Cisco NX-OS creates a VLAN interface for the default VLAN (VLAN 1) to permit remote switch administration.

You must enable the VLAN network interface feature before you can configure it.

In Cisco UCS Director, SVI configuration is supported on the following Cisco network devices:

- Cisco Nexus 5000, 5500, and 5672 Series switches
- Cisco Nexus 7000 Series switches
Configuring a SVI

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click the Interfaces tab.
Step 5  Click Add SVI.
Step 6  In the Configure SVI dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Interface Number field</td>
<td>The VLAN interface number within the valid range. The valid VLAN interface</td>
</tr>
<tr>
<td></td>
<td>range value can be 1 through 4094.</td>
</tr>
<tr>
<td>Description field</td>
<td>The description of the VLAN interface.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Step 7  Click Submit.

Deleting a SVI

Step 1  In the Interface tab, select the interface that needs to be deleted.
Step 2  Click Remove SVI.
   The Remove SVI dialog box appears to confirm deletion of SVI.
Step 3  Check the Copy Running configuration to Startup configuration check box to copy the configuration to the startup configuration.
Step 4  Click Submit.
Managing TrustSec

This chapter contains the following sections:

- About Cisco Trustsec, page 35
- Refreshing TrustSec, page 35

About Cisco Trustsec

Cisco TrustSec provides an access-control solution that builds upon an existing identity-aware infrastructure to ensure data confidentiality between network devices and integrate security access services on one platform. In the Cisco TrustSec solution, enforcement devices utilize a combination of user attributes and end-point attributes to make role-based and identity-based access control decisions. The availability and propagation of this information enables security solutions across networks at the access, distribution, and core layers of the network.

In Cisco UCS Director, you can manage Cisco Trustsec on the following Cisco network devices:

- Cisco ASA 5500 Series firewall
- Cisco Adaptive Security Virtual Appliance (ASAv)

Refreshing TrustSec

<table>
<thead>
<tr>
<th>Step 1</th>
<th>On the menu bar, choose Physical &gt; Network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Network pane, expand the pod.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select the network device that needs to be configured. The summary of the device is displayed.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click TrustSec Refresh.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the TrustSec Refresh dialog box, complete the following field:</td>
</tr>
</tbody>
</table>
### Managing TrustSec

#### Refreshing TrustSec

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy Running configuration to Startup configuration check box field</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

**Step 6**

Click **Submit**.
Configuring SGT Exchange Protocol Connection

This chapter contains the following sections:

• About SXP Connection, page 37
• Configuring an SXP Peer Connection, page 37

About SXP Connection

You can use the Security Group Tag (SGT) Exchange Protocol (SXP) to propagate the SGTs across network devices that do not have hardware support for Cisco TrustSec.

In Cisco UCS Director, SXP connection is supported on the following Cisco network devices:

• Cisco Nexus 1000 Series switches
• Cisco Nexus 5000, 5500, and 5672 Series switches
• Cisco Nexus 7000 Series switches
• Cisco ASA 5500 Series firewall
• Cisco Adaptive Security Virtual Appliance (ASAv)

Configuring an SXP Peer Connection

You must configure the SXP peer connection on both of the devices. One device is the speaker and the other is the listener. When using password protection, make sure to use the same password on both ends.
If a default SXP source IP address is not configured and you do not configure an SXP source address in the connection, the Cisco TrustSec software derives the SXP source IP address from existing local IP addresses. The SXP source address might be different for each TCP connection initiated from the switch.

**Step 1**  
On the menu bar, choose **Physical > Network**.

**Step 2**  
In the **Network** pane, expand the pod.

**Step 3**  
Select the network device that needs to be configured.  
**Note** For configuring SXP peer connection on Cisco Nexus 7000 Series switches, click the **VDC** tab, choose the Ethernet type VDC, and click **View Details**.

**Step 4**  
Click the **SXP Connection Peers** tab.

**Step 5**  
Click **Add**.

**Step 6**  
In the **Configure SXP Connection Peer** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SXP check box</td>
<td>Check the check box to enable SXP.</td>
</tr>
<tr>
<td>Default Source IP Address</td>
<td>The IP address of the default source device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If no address is specified, the connection will use the default source address, if configured, or the address of the port.</td>
</tr>
<tr>
<td>Default Password field</td>
<td>The password that SXP will use for the connection.</td>
</tr>
<tr>
<td>Peer IP Address field</td>
<td>The IP address of the peer device.</td>
</tr>
<tr>
<td>Source IP Address field</td>
<td>The IP address of the source device.</td>
</tr>
<tr>
<td>Password Option drop-down list</td>
<td>Choose one of the following as the password option:</td>
</tr>
<tr>
<td></td>
<td>• None—Do not use a password.</td>
</tr>
<tr>
<td></td>
<td>• Default—Use the default SXP password.</td>
</tr>
<tr>
<td>Mode drop-down list</td>
<td>Choose one of the following mode to specify the role of the remote peer device:</td>
</tr>
<tr>
<td></td>
<td>• Peer—The specified mode refers to the peer device.</td>
</tr>
<tr>
<td></td>
<td>• Local—The specified mode refers to the local device.</td>
</tr>
<tr>
<td>VRF field</td>
<td>The Virtual Routing and Forwarding (VRF) to the peer.</td>
</tr>
<tr>
<td>Role drop-down list</td>
<td>Choose one of the following as the role of the device:</td>
</tr>
<tr>
<td></td>
<td>• Listener—Default. Specifies that the device is the listener in the connection.</td>
</tr>
<tr>
<td></td>
<td>• Speaker—Specifies that the device is the speaker in the connection.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

**Step 7**  
Click **Submit**.
Configuring HSRP

This chapter contains the following sections:

- About HSRP, page 41
- Configuring HSRP, page 41

About HSRP

Hot Standby Router Protocol (HSRP) provides high network availability by providing redundancy for IP traffic from hosts on networks. HSRP routes IP traffic without relying on the availability of any single router. It enables a set of router interfaces to work together to present the appearance of a single virtual router or default gateway to the hosts on a LAN.

When HSRP is configured on a network or segment, it provides a virtual Media Access Control (MAC) address and an IP address that is shared among a group of configured routers. HSRP allows two or more HSRP-configured routers to use the MAC address and IP network address of a virtual router. The virtual router does not exist; it represents the common target for routers that are configured to provide backup to each other. One of the routers is selected to be the active router and another to be the standby router, which assumes control of the group MAC address and IP address should the designated active router fail.

In Cisco UCS Director, HSRP configuration is supported on the following Cisco network devices:

- Cisco Nexus 5000, 5500, and 5672 Series switches
- Cisco Nexus 7000 Series switches

Configuring HSRP

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, choose the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click View Details.
For configuring HSRP on Cisco Nexus 7000 Series switches, expand the pod and choose the network device. Click the VDC tab, choose the Ethernet type VDC, and click View Details.

**Step 5** Click the HSRP tab.

**Step 6** Click Add.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name field</td>
<td>Click Select and choose an interface on which you want to enable HSRP.</td>
</tr>
<tr>
<td>Description field</td>
<td>Description for the selected interface.</td>
</tr>
<tr>
<td>Enable Interface check box</td>
<td>Check the check box to enable the interface.</td>
</tr>
<tr>
<td>Interface IP Address field</td>
<td>The IP address of the interface.</td>
</tr>
<tr>
<td>IP Network Mask field</td>
<td>The network mask address of the interface.</td>
</tr>
<tr>
<td>HSRP Group Number field</td>
<td>The group number to which the command applies. The valid range is from 0 to 4095.</td>
</tr>
<tr>
<td>Authentication Text field</td>
<td>Enter a string to be carried in all HSRP messages.</td>
</tr>
<tr>
<td>Min Preempt Delay Time field</td>
<td>The time that is set to cause the local router to postpone taking over the active role for the number of seconds shown. The range is 0 to 3600 (1 hour); the default is 0 (no delay before taking over).</td>
</tr>
<tr>
<td>Priority field</td>
<td>Sets the group priority. The valid range is from 1 to 255; the default is 100.</td>
</tr>
<tr>
<td>Lower Threshold Time field</td>
<td>Sets the lower threshold time. The valid range is from 0 to 255 and must be lesser than priority.</td>
</tr>
<tr>
<td>Upper Threshold Time field</td>
<td>Sets the upper threshold time. The valid range is from 0 to 255 and must be greater than lower threshold time and priority.</td>
</tr>
<tr>
<td>Hello Interval field</td>
<td>The hello interval in seconds. The range is from 1 to 254; the default is 3 seconds.</td>
</tr>
<tr>
<td>Hold Time Interval field</td>
<td>The time in seconds before the active or standby router is declared to be down. The range is from 1 to 255; the default is 10 seconds.</td>
</tr>
<tr>
<td>Virtual IP Address field</td>
<td>The virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>
Step 8  Click Submit.
Managing FC Alias

This chapter contains the following sections:

- About FC Alias, page 45
- Creating a FC Alias, page 45
- Updating a FC Alias, page 46
- Deleting a FC Alias, page 47

About FC Alias

FC Alias is the alias for World Wide Port Names (WWPNs) on the fabric for a particular VSAN.

In Cisco UCS Director, you can manage FC Alias on the following Cisco network devices:

- Cisco Nexus 5000, 5500, and 5672 Series switches
- Cisco Nexus 7000 Series switches
- Cisco MDS 9100 Series switches
- Cisco MDS 9500 Series switches
- Cisco MDS 9700 Series switches

Creating a FC Alias

Step 1
On the menu bar, choose Physical > Network.

Step 2
In the Network pane, choose the pod.

Step 3
Select the network device that needs to be configured.

Step 4
Click View Details.

Note
For creating a FC Alias for Cisco Nexus 7000 Series switches, expand the pod and choose the network device. Click the VDC tab, choose the storage type VDC, and click View Details.
Updating a FC Alias

**Step 5**
Click the **FCAlias** tab.

**Step 6**
Click **Add**.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FC Alias Name</strong> field</td>
<td>Name of the alias.</td>
</tr>
<tr>
<td><strong>VSAN Id</strong> field</td>
<td>Click <strong>Select</strong>. In the <strong>Select</strong> dialog box, choose the VSAN ID.</td>
</tr>
<tr>
<td><strong>Member Type</strong> drop-down</td>
<td>Choose one of the following as the type of member:</td>
</tr>
<tr>
<td></td>
<td>• <strong>DeviceAlias</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>pWWN</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>fWWN</strong></td>
</tr>
<tr>
<td><strong>Member</strong> field</td>
<td>The value for the member.</td>
</tr>
<tr>
<td><strong>Copy Running configuration to</strong></td>
<td>Check the check box to copy the running configuration to the startup</td>
</tr>
<tr>
<td><strong>Startup configuration</strong> check box</td>
<td>configuration.</td>
</tr>
</tbody>
</table>

**Step 8**
Click **Submit**.

---

### Updating a FC Alias

**Step 1**
In the **FCAlias** tab, select the FC Alias that needs to be updated.

**Step 2**
Click **Modify**.

**Step 3**
In the Update **FCAlias** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VDC Name</strong> field</td>
<td>Click <strong>Select</strong>. In the <strong>Select</strong> dialog box, choose the VDC.</td>
</tr>
<tr>
<td><strong>Members List</strong> table</td>
<td>The list of members in the Alias.</td>
</tr>
<tr>
<td><strong>Copy Running configuration to</strong></td>
<td>Check the check box to copy the running configuration to the startup</td>
</tr>
<tr>
<td><strong>Startup configuration</strong> check box</td>
<td>configuration.</td>
</tr>
</tbody>
</table>

**Step 4**
Click **Submit**.
Deleting a FC Alias

Step 1  In the FC Alias tab, select the FC Alias that needs to be deleted.
Step 2  Click Delete. The Delete FC Alias dialog box appears to confirm deletion of FC Alias.
Step 3  Check the Copy Running configuration to Startup configuration check box to copy the configuration to the startup configuration.
Step 4  Click Submit.
Configuring Access Ports

This chapter contains the following sections:

- About Access Ports, page 49
- Configuring an Access Port, page 49

About Access Ports

Access ports in switches are used to connect end devices such as workstations and printers. When configuring an access port, you need to define which VLAN that the port belongs to.

In Cisco UCS Director, you can configure access ports on the following Cisco network devices:

- Cisco Nexus 3000 Series switches
- Cisco Nexus 5000 Series switches
- Cisco Nexus 7000 Series switches
- Cisco Nexus 6000 Series switches
- Cisco Nexus 9300 and 9500 Series switches

Configuring an Access Port

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click the Interfaces tab.
Step 5  Select the interface that you want to configure as an access port.
Step 6  Click Configure Access.
Step 7  In the Access Configuration dialog box, complete the following fields:
### Configuring Access Ports

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select Port field</strong></td>
<td>The port that you want to configure as an access port.</td>
</tr>
<tr>
<td><strong>Access VLAN field</strong></td>
<td>Click <strong>Select</strong> and choose a VLAN to which you want to associate the port to.</td>
</tr>
<tr>
<td><strong>STP Port Type drop-down list</strong></td>
<td>Choose one of the following as the port type for the Spanning Tree Protocol (STP) to use:</td>
</tr>
<tr>
<td></td>
<td>• <strong>edge</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>network</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>normal</strong></td>
</tr>
<tr>
<td><strong>Copy Running configuration to Startup configuration check box</strong></td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

**Step 8**

Click **Submit**.
Managing Access Control Lists

This chapter contains the following sections:

- About Access Control Lists, page 51
- Creating an ACL, page 52
- Configuring Context ACL, page 53

About Access Control Lists

Packet filtering can help limit network traffic and restrict network use by certain users or devices. Access control list (ACL) filters traffic as it passes through a switch and permit or deny packets cross specified interfaces. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACLs to verify that the packet has the required permissions to be forwarded.

You can use ACLs to protect networks and specific hosts from unnecessary or unwanted traffic. For example, you could use ACLs to disallow HTTP traffic from a high-security network to the Internet. You could also use ACLs to allow HTTP traffic but only to specific sites, using the IP address of the site to identify it in an IP ACL.

In Cisco UCS Director, you can configure ACLs on the following Cisco network devices:

- Cisco Nexus 9300 and 9500 Series switches firewall
- Cisco IOS Devices

In Cisco UCS Director, you can configure context ACLs on the following Cisco network devices:

- Cisco ASA 5500 Series firewall
- Cisco Adaptive Security Virtual Appliance (ASAv)
Creating an ACL

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, choose the pod.
Step 3  Select the device for which you want to create an ACL.
Step 4  Choose Create ACL Entry from the drop-arrow icon.
Step 5  In the Create ACL Entry dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL Name field</td>
<td>The name of the ACL.</td>
</tr>
<tr>
<td>Type drop-down list</td>
<td>Choose one of the following as the ACL type:</td>
</tr>
<tr>
<td></td>
<td>• IP</td>
</tr>
<tr>
<td></td>
<td>• MAC</td>
</tr>
<tr>
<td></td>
<td>• IPV6</td>
</tr>
<tr>
<td>Description field</td>
<td>The description of the ACL.</td>
</tr>
<tr>
<td>Per ACL Entry stats collection check box</td>
<td>Check the check box to collect the statistics details of the ACL entry.</td>
</tr>
<tr>
<td>Apply ACL to Interface check box</td>
<td>Check the check box to apply the ACL to an interface. The Select Interface field appears. Click Select and choose an interface to which you want to apply the ACL.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Step 6  Click Submit.
Configuring Context ACL

Step 1  On the menu bar, choose **Physical > Network**.
Step 2  In the **Network** pane, expand the pod.
Step 3  Select the device for which you want to configure context ACL.
Step 4  Click the **ACL** tab.
Step 5  Select the ACL that needs to be configured.
Step 6  Click **Configure Context ACL**.
Step 7  In the **Configure Context ACL** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL Name field</td>
<td>The name of the context ACL.</td>
</tr>
<tr>
<td>Interface Name drop-down list</td>
<td>Choose the interface name on which you want to configure the context ACL.</td>
</tr>
<tr>
<td>Permit check box</td>
<td>Check the check box to forward the packets.</td>
</tr>
<tr>
<td>InBound Traffic check box</td>
<td>Check the check box to apply the ACL to inbound packets on an interface.</td>
</tr>
<tr>
<td>Protocol drop-down list</td>
<td>Choose one of the following to filter by Application layer protocol:</td>
</tr>
<tr>
<td></td>
<td>• ip</td>
</tr>
<tr>
<td></td>
<td>• tcp</td>
</tr>
<tr>
<td></td>
<td>• udp</td>
</tr>
<tr>
<td></td>
<td>• icmp</td>
</tr>
<tr>
<td>Source IP Address/IPv6 Prefix field</td>
<td>The IP address of the source host name that you want to apply to the ACL so that the packets from host are permitted or denied as per ACL.</td>
</tr>
<tr>
<td>Source Net Mask field</td>
<td>The subnet mask of a source network that you want to apply to the ACL so that the packets from the network are permitted or denied as per ACL.</td>
</tr>
<tr>
<td>Source Port Range field</td>
<td>The range of ports that you want to apply to the ACL so that the packets from the port range are permitted or denied as per ACL.</td>
</tr>
<tr>
<td>Destination IP Address/IPv6 Prefix field</td>
<td>The IP address of the destination host name that you want to apply to the ACL so that the packets to the destination host are forwarded or denied as per ACL.</td>
</tr>
<tr>
<td>Destination Net Mask field</td>
<td>The subnet mask of a destination network that you want to apply to the ACL so that the packets to the network are permitted or denied as per ACL.</td>
</tr>
<tr>
<td>Destination Port Range field</td>
<td>The range of ports that you want to apply to the ACL so that the packets to the port range are permitted or denied as per ACL.</td>
</tr>
</tbody>
</table>
Step 8  Click Submit.
CHAPTER 16

Configuring Network Address Translation

This chapter contains the following sections:

- About NAT, page 55
- Configuring NAT, page 55
- Configuring Context NAT, page 56

About NAT

Network Address Translation (NAT) enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks, and translates the private (not globally unique) addresses in the internal network into legal addresses before packets are forwarded onto another network. NAT can be configured to advertise only one address for the entire network to the outside world. This ability provides additional security by effectively hiding the entire internal network behind that one address.

In Cisco UCS Director, you can configure NAT on the following Cisco network devices:

- Cisco ASA 5500 Series firewall
- Cisco Adaptive Security Virtual Appliance (ASAv)

Configuring NAT

Before You Begin

Ensure that the real source and destination IP addresses and mapped source and destination IP addresses are preconfigured on the device.

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
The summary of the device is displayed.

**Step 4**  
Click **Configure NAT**.

**Step 5**  
In the **Configure NAT** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Source field</td>
<td>Click <strong>Select</strong> and choose an object as real source address.</td>
</tr>
<tr>
<td>Mapped Source field</td>
<td>Click <strong>Select</strong> and choose an object as mapped source address.</td>
</tr>
<tr>
<td>Real Destination field</td>
<td>Click <strong>Select</strong> and choose an object as real destination address.</td>
</tr>
<tr>
<td>Mapped Destination field</td>
<td>Click <strong>Select</strong> and choose an object as mapped address.</td>
</tr>
</tbody>
</table>

**Step 6**  
Click **Submit**.

## Configuring Context NAT

**Step 1**  
On the menu bar, choose **Physical > Network**.

**Step 2**  
In the **Network** pane, expand the pod.

**Step 3**  
Select the network device that needs to be configured. The summary of the device is displayed.

**Step 4**  
Click **Configure Context NAT**.

**Step 5**  
In the **Configure Context NAT** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protocol</strong> drop-down</td>
<td>Choose <strong>TCP</strong> or <strong>UDP</strong> from the list.</td>
</tr>
<tr>
<td><strong>Mapped Interface Name</strong> drop-down list</td>
<td>Choose an interface name to be mapped for NAT.</td>
</tr>
<tr>
<td>Mapped IP Address Destination field</td>
<td>The IP address to be mapped for NAT.</td>
</tr>
<tr>
<td>Mapped Port field</td>
<td>The port to be mapped for NAT.</td>
</tr>
<tr>
<td>Real Interface Name drop-down</td>
<td>Choose a real interface name for NAT.</td>
</tr>
<tr>
<td>Real IP Address field</td>
<td>The real IP address for NAT.</td>
</tr>
<tr>
<td>Real Port field</td>
<td>The port for NAT.</td>
</tr>
</tbody>
</table>
Step 6  Click Submit.
Configuring Quality of Services

This chapter contains the following sections:

- About Quality of Service Policies, page 59
- Configuring a QoS Policy, page 59
- Deleting a QoS Policy, page 62

About Quality of Service Policies

You use the quality of service (QoS) feature to provide the most desirable flow of traffic through a network. QoS allows you to classify the network traffic and prioritize the traffic flow, which helps to avoid traffic congestion in a network. The control of traffic is based on the fields in the packets that flow through the system.

In Cisco UCS Director, you can configure QoS policy on the Cisco Nexus 9300 and 9500 Series switches.

Configuring a QoS Policy

Step 1 On the menu bar, choose Physical > Network.
Step 2 In the Network pane, expand the pod.
Step 3 Select the network device that needs to be configured.
Step 4 Click the down-arrow icon, and choose Configure N9K QOS.
Step 5 In the N9k QOS Configuration dialog box, complete the following fields:
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Integrate with UCS QOS Policy check box</strong></td>
<td>Check the check box to integrate the QoS policy that is defined for the Cisco UCS account with the device. When you are checking this check box, the <strong>UCS Account Name</strong> drop-down field appears. Choose the QoS policy of the UCS account that you want to integrate with the device.</td>
</tr>
<tr>
<td><strong>Configure Platinum Class check box</strong></td>
<td>Check the check box to configure the parameters for the Platinum class and apply the class to the device. To configure the parameters for the Platinum class, complete the following fields:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platinum Class ACL Name</strong> drop-down list—Choose the access control list (ACL) name to match packets against when you are configuring a traffic class.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platinum Class QOS Group</strong> drop-down list—(Optional) Choose the QoS group value to match packets against when you are configuring a traffic class. Values are from 0 to 3.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platinum Class COS</strong> drop-down list—(Optional) Choose the class of service (CoS) value to match packets against when you are classifying packets into this class. Values are from 0 to 7.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platinum Class MTU</strong> field—The maximum transmission unit (MTU) value for the class.</td>
</tr>
<tr>
<td><strong>Configure Gold Class check box</strong></td>
<td>Check the check box to configure the parameters for the Gold class and apply the class to the device. To configure the parameters for the Gold class, complete the following fields:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Gold Class ACL Name</strong> drop-down list—Choose the ACL name to match packets against when you are configuring a traffic class.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Gold Class QOS Group</strong> drop-down list—(Optional) Choose the QoS group value to match packets against when you are configuring a traffic class. Values are from 0 to 3.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Gold Class BW Percentage</strong> drop-down list—Choose the guaranteed percentage of interface bandwidth that is allocated to this class.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Gold Class COS</strong> drop-down list—(Optional) Choose the CoS value to match packets against when you are classifying packets into this class. Values are from 0 to 7.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Gold Class MTU</strong> field—The MTU value for the class.</td>
</tr>
</tbody>
</table>
### Configuring Quality of Services

#### Configuring a QoS Policy

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure Silver Class</strong></td>
<td>Check the check box to configure the parameters for the Silver class and apply the class to the device.</td>
</tr>
<tr>
<td><strong>Configure Default Class</strong></td>
<td>Check the check box to configure the parameters for the Default class and apply the class to the device.</td>
</tr>
<tr>
<td><strong>Copy Running configuration to Startup configuration</strong></td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Request Approval</strong></td>
<td>Check the check box to request for approval to deliver commands to the device.</td>
</tr>
</tbody>
</table>

To configure the parameters for the Silver class, complete the following fields:

- **Silver Class ACL Name** drop-down list—Choose the ACL name to match packets against when you are configuring a traffic class.
- **Silver Class QOS Group** drop-down list—(Optional) Choose the QoS group value to match packets against when you are configuring a traffic class. Values are from 0 to 3.
- **Silver Class BW Percentage** drop-down list—Choose the guaranteed percentage of interface bandwidth allocated to this class.
- **Silver Class COS** drop-down list—(Optional) Choose the CoS value to match packets against when you are classifying packets into this class. Values are from 0 to 7.
- **Silver Class MTU** field—The MTU value for the class.

To configure the parameters for the Default class, complete the following field:

- **Default Class BW Percentage** drop-down list—Choose the guaranteed percentage of interface bandwidth that is allocated to this class.

---

**Step 6**

Click Submit.
Deleting a QoS Policy

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>On the menu bar, choose Physical &gt; Network.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Network pane, expand the pod.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select the network device that needs to be configured.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click the down-arrow icon, and choose Delete N9K QOS.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the N9k QOS Deletion dialog box, uncheck the check box to remove the corresponding class configuration from the QoS policy.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Uncheck the Copy Running configuration to Startup configuration check box to avoid copying the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Uncheck the Request Approval check box to deliver commands to the device without approval.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Click Submit.</td>
</tr>
</tbody>
</table>
Managing Service Policies

This chapter contains the following sections:

- About Service Policies, page 63
- Updating a Service Policy, page 64

About Service Policies

A service policy is defined to apply multiple actions to an interface. The service policy provides the following two policy-map configuration modes:

- qos—Classification mode. This is the default mode. The input QoS policy is applied to incoming traffic on an Ethernet interface for classification.
- queuing—Queuing mode. The output policy is applied to all outgoing traffic that matches the specified class.

In Cisco UCS Director, you can configure service policies on the following Cisco network devices:

- Cisco Nexus 1000 Series switches
- Cisco Nexus 3000 Series switches
- Cisco Nexus 9300 and 9500 Series switches
Updating a Service Policy

**Step 1**  On the menu bar, choose Physical > Network.

**Step 2**  In the Network pane, expand the pod.

**Step 3**  Choose the network device that needs to be configured.

**Step 4**  Click the QOS Policy Maps tab.

**Step 5**  Select the service policy map that needs to be updated.

**Step 6**  Click Update Service Policy.

**Step 7**  In the Update Service Policy dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Interface field</td>
<td>Click Select and choose the interface to which you want to apply the service policy.</td>
</tr>
</tbody>
</table>
| Service Policy type drop-down list | Choose one of the following as the policy type:  
  • qos  
  • queuing |
| Service Policy direction field | The direction in which the service policy is applied based on the selected policy type:  
  • input—Appears when qos is selected as the policy type. The input keyword specifies that this policy map must be applied to traffic received on an interface.  
  • output—Appears when queuing is selected as the policy type. The output keyword specifies that this policy map should be applied to traffic transmitted from an interface. |
| Select Policy Map field     | The policy map that needs to be updated. |
| Copy Running configuration to Startup configuration check box | Check the check box to copy the running configuration to the startup configuration. |

**Step 8**  Click Submit.
Managing Trunks

This chapter contains the following sections:

- About Trunks, page 65
- Configuring a Trunk, page 66
- Updating a Trunk, page 67

About Trunks

VLAN trunks reduce networking costs by reducing the need for expensive physical connections and conserving the number of ports used on switches. The trunk connection can be passed between two switches or between a switch and a computer. Ethernet interfaces can be configured either as access ports or a trunk ports, as follows:

- An access port can have only one VLAN configured on the interface; it can carry traffic for only one VLAN.
- A trunk port can have two or more VLANs configured on the interface; it can carry traffic for several VLANs simultaneously.

In Cisco UCS Director, you can manage trunks on the following Cisco network devices:

- Cisco Nexus 1000 and 1110 Series switches
- Cisco Nexus 3000 Series switches
- Cisco Nexus 5000, 5500, and 5672 Series switches
- Cisco Nexus 6000 Series switches
- Cisco Nexus 7000 Series switches
- Cisco Nexus 9300 and 9500 Series switches
- Cisco MDS 9100 Series switches
- Cisco MDS 9500 Series switches
- Cisco MDS 9700 Series switches
Configuring a Trunk

You can configure an Ethernet port as a trunk port; a trunk port transmits untagged packets for the native VLAN plus encapsulated, tagged packets for multiple VLANs.

**Step 1**
On the menu bar, choose Physical > Network.

**Step 2**
In the Network pane, expand the pod.

**Step 3**
Select the network device that needs to be configured.

**Step 4**
Click the Interfaces tab.

**Step 5**
Click Configure Trunk. Choose the interface on which the trunk needs to be configured.

**Step 6**
In the Configure Trunk dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Name field</td>
<td>The name of port on which the trunk needs to be configured.</td>
</tr>
<tr>
<td>Native VLAN ID drop-down list</td>
<td>Choose the native VLAN ID to use. The default native VLAN ID is default [1].</td>
</tr>
<tr>
<td>Allowed VLANS field</td>
<td>Click Select. In the Select Items dialog box, check the VLAN(s) that are allowed on this trunk port.</td>
</tr>
<tr>
<td>STP Port Type drop-down list</td>
<td>Choose one of the following: Edge trunk, Network, or Normal.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running trunk configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

**Step 7**
Click Submit.
Updating a Trunk

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click the Interfaces tab.
Select the port on which the trunk needs to be updated.
Step 5  Click Update Trunk.
Step 6  In the Trunk Configuration dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Name button</td>
<td>The name of port on which the trunk needs to be updated is displayed.</td>
</tr>
<tr>
<td>Action drop-down list</td>
<td>Choose the relevant action (Add, or Remove).</td>
</tr>
<tr>
<td>Select VLANs field</td>
<td>Click Select. In the Select Items dialog box, choose the appropriate VLANs.</td>
</tr>
<tr>
<td>Copy Running configuration to</td>
<td>Check the check box to copy the running trunk configuration to the startup</td>
</tr>
<tr>
<td>Startup configuration check box</td>
<td>configuration.</td>
</tr>
</tbody>
</table>

Step 7  Click Submit.
Managing Virtual Fibre Channels

This chapter contains the following sections:

- About VFCs, page 69
- Creating a VFC, page 70
- Associating a VFC, page 71

About VFCs

Fibre Channel over Ethernet (FCoE) allows Fibre Channel and Ethernet traffic to be carried on the same physical Ethernet connection between the switch and the servers.

The Fibre Channel portion of FCoE is configured as a virtual Fibre Channel (VFC) interface. Logical Fibre Channel features (such as interface mode) can be configured on VFC interfaces.

Before you can use a VFC interface, it must be bound to a physical Ethernet interface that is directly connected to a converged network adapter (CNA). The CNA makes the connection to the Fibre Channel Forwarder (FCF) over a virtual port channel (vPC).

The following switch port modes are used to bind the VFC interface:

- Virtual fabric (VF) port—Connects to a peripheral device (host or disk) operating as an N port. A VF port can be attached to only one N port.
- Virtual expansion (VE) port—Acts as an expansion port in an FCoE network. VE ports can connect multiple FCoE switches in the network. You can bind a VE port to a physical Ethernet port or a port channel.

In Cisco UCS Director, VFC configuration is supported on the following Cisco network devices:

- Cisco Nexus 3000 Series switches
- Cisco Nexus 5000, 5500, and 5672 Series switches
- Cisco Nexus 7000 Series switches
- Cisco MDS 9100 Series switches
- Cisco MDS 9500 Series switches
Creating a VFC

Step 1
On the menu bar, choose Physical > Network.

Step 2
In the Network pane, choose the pod.

Step 3
Click the Managed Network Elements tab.

Step 4
Select the network device that needs to be configured.

Step 5
Click the down-arrow icon, and choose Create VFC. Alternately, choose the device from the expanded pod and click Create VFC on the Summary tab.

Step 6
In the Create Vfc dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VFC ID field</td>
<td>The VFC ID within the valid range from 1 to 8192. The VFC ID creates a VFC interface.</td>
</tr>
<tr>
<td>Select Port Select button</td>
<td>Click Select. In the Select dialog box, choose the port for this VFC and click Select.</td>
</tr>
<tr>
<td>Switch Port Mode drop-down list</td>
<td>Choose the switch port mode (E or F). E is for virtual expansion (VE) port. F is for virtual fabric (VF) port. The default is F mode.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Step 7
Click Submit.

Note
For more detailed information about VFCs and configuration guidelines for VFCs, see the Cisco NX-OS Software Configuration Guides.
**Associating a VFC**

**Step 1**  
On the menu bar, choose **Physical > Network**.

**Step 2**  
In the **Network** pane, choose the pod.

**Step 3**  
Click the **Managed Network Elements** tab.

**Step 4**  
Select the network device that needs to be configured.

**Step 5**  
Click the down-arrow icon, and choose **Associate VFC**. Alternatively, choose the device from the expanded pod and click **Associate VFC** on the **Summary** tab.

**Step 6**  
In the **Associate Vfc** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VFC Id Select button</td>
<td>Click <strong>Select</strong>. In the <strong>Select</strong> dialog box, choose the VFC ID and click <strong>Select</strong>.</td>
</tr>
<tr>
<td>VSAN Id Select button</td>
<td>Click <strong>Select</strong> to choose the VSAN ID that is associated with this VFC.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running VLAN configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

**Step 7**  
Click **Submit**.
Managing Virtual Fibre Channels

Associating a VFC
Managing VLANs

This chapter contains the following sections:

- About VLANs, page 73
- Creating a VLAN, page 74
- Assigning a VLAN to a User Group, page 74
- Configuring a Private VLAN Port, page 75
- Creating a Private Primary and Secondary VLAN, page 75
- Associating a Private Primary and Secondary VLAN, page 77
- Deleting a VLAN, page 77

About VLANs

A VLAN is a group of devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when they are really located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

In Cisco UCS Director, you can configure VLANs on the following Cisco network devices:

- Cisco Nexus 1000 and 1110 Series switches
- Cisco Nexus 3000 Series switches
- Cisco Nexus 5000, 5500, and 5672 Series switches
- Cisco Nexus 6000 Series switches
- Cisco Nexus 7000 Series switches
- Cisco Nexus 9300 and 9500 Series switches

Note

For more detailed information about VLANs and configuration guidelines for VLANs, see the Cisco NX-OS Software Configuration Guides.
Creating a VLAN

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click the VLANs tab.
Step 5  Click Create VLAN.
Step 6  In the Vlan Parameters dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID field</td>
<td>The VLAN ID within the valid range.</td>
</tr>
<tr>
<td>VLAN Name field</td>
<td>The VLAN name.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running VLAN configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Step 7  Click Submit.

Assigning a VLAN to a User Group

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click the VLANs tab.
Step 5  Select the VLAN that you need to assign to a user group.
Step 6  Click Assign Group.
Step 7  In the Select Group dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign To Users check box</td>
<td>Check the check box to assign the VLAN to users in a group.</td>
</tr>
<tr>
<td>Group drop-down list</td>
<td>Choose the group from the list.</td>
</tr>
<tr>
<td>Label field</td>
<td>The label for the VLAN that is assigned to a user group.</td>
</tr>
</tbody>
</table>
Configuring a Private VLAN Port

You can associate a private VLAN ID as primary and another private VLAN ID as secondary.

Step 1 On the menu bar, choose Physical > Network.
Step 2 In the Network pane, expand the pod.
Step 3 Select the network device that needs to be configured.
Step 4 Click the Private VLANs tab.
Step 5 Click Configure Private VLAN Port.
Step 6 In the Configure Private VLAN Port dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Port drop-down list</td>
<td>Choose a port on which the VLAN needs to be configured.</td>
</tr>
<tr>
<td>Type field</td>
<td>Choose one of the following as the port type for VLAN:</td>
</tr>
<tr>
<td></td>
<td>• host</td>
</tr>
<tr>
<td></td>
<td>• promiscuous</td>
</tr>
<tr>
<td>Primary VLAN ID drop-down list</td>
<td>Choose the primary VLAN ID number.</td>
</tr>
<tr>
<td>Secondary VLAN ID field</td>
<td>Choose the VLAN ID number to associate as a secondary VLAN.</td>
</tr>
<tr>
<td>Copy Running configuration to</td>
<td>Check the check box to copy the running configuration to the startup configuration. Uncheck the check box if you do not want to copy the running configuration.</td>
</tr>
<tr>
<td>Startup configuration check box</td>
<td></td>
</tr>
</tbody>
</table>

Step 7 Click Submit.

Creating a Private Primary and Secondary VLAN

A private VLAN domain has only one primary VLAN. Each port in a private VLAN domain is a member of the primary VLAN; the primary VLAN is the entire private VLAN domain. Secondary VLANs provide isolation between ports within the same private VLAN domain. The two types of secondary VLANs within a primary VLAN are as follows:
• Isolated VLANS—Ports within an isolated VLAN that cannot communicate directly with each other at the Layer 2 level.

• Community VLANS—Ports within a community VLAN that can communicate with each other but cannot communicate with ports in other community VLANS or in any isolated VLANS at the Layer 2 level.

### Step 1
On the menu bar, choose **Physical > Network**.

### Step 2
In the **Network** pane, expand the pod.

### Step 3
Select the network device that needs to be configured.

### Step 4
Click the **Private VLANs** tab.

### Step 5
Click **Create Private VLAN**.

### Step 6
In the **Create Private VLAN** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VLAN ID field</strong></td>
<td>The VLAN ID number that you choose within the valid range for the private VLAN.</td>
</tr>
<tr>
<td><strong>Private VLAN Type</strong> drop-down list</td>
<td>Choose <strong>Primary</strong> to make this VLAN the primary VLAN.</td>
</tr>
<tr>
<td><strong>Copy Running configuration to Startup configuration</strong> check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

### Step 7
Click **Submit** to create a private VLAN.

### Step 8
In the **Private VLANs** tab, click **Create Private VLAN**.

### Step 9
In the **Create Private VLAN** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VLAN ID field</strong></td>
<td>The VLAN ID number that you choose within the valid range for the private VLAN.</td>
</tr>
<tr>
<td><strong>Private VLAN Type</strong> drop-down list</td>
<td>Choose either the <strong>Community</strong> or <strong>Isolated</strong> option to make this private VLAN the secondary VLAN within the same private VLAN domain.</td>
</tr>
<tr>
<td><strong>Copy Running configuration to Startup configuration</strong> check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

### Step 10
Click **Submit**.
Associating a Private Primary and Secondary VLAN

You can associate a private VLAN ID as primary and another private VLAN ID as secondary.

**Step 1**  
On the menu bar, choose **Physical > Network**.

**Step 2**  
In the **Network** pane, expand the pod.

**Step 3**  
Select the network device that needs to be configured.

**Step 4**  
Click the **Private VLANs** tab.

**Step 5**  
Click **Associate Private VLAN**.

**Step 6**  
In the **Associate Private VLAN** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary VLAN ID</strong> field</td>
<td>The primary VLAN ID number.</td>
</tr>
<tr>
<td><strong>Action</strong> drop-down list</td>
<td>Choose <strong>add</strong> to create the association to the primary VLAN or <strong>remove</strong> to cancel an existing association to the primary VLAN.</td>
</tr>
<tr>
<td><strong>Secondary VLAN ID</strong> drop-down list</td>
<td>Choose the VLAN ID number to associate as a secondary VLAN.</td>
</tr>
<tr>
<td><strong>Copy Running configuration to Startup configuration</strong> check box</td>
<td>Check the check box to copy the running port profile configuration to the startup configuration. Uncheck the check box if you do not want to copy the running configuration.</td>
</tr>
</tbody>
</table>

**Step 7**  
Click **Submit**.

Deleting a VLAN

**Step 1**  
On the menu bar, choose **Physical > Network**.

**Step 2**  
In the **Network** pane, expand the pod.

**Step 3**  
Select the network device for which the VLAN needs to be deleted.

**Step 4**  
Click the **VLANs** tab.

**Step 5**  
Select the VLAN that needs to be deleted.

**Step 6**  
Click **Delete VLAN**.  
The **Delete VLAN** dialog box appears to confirm deletion of VLAN.
Step 7  Check the **Copy Running configuration to Startup configuration** check box to copy the VLAN configuration to the startup configuration.

Step 8  Click **Delete**.
Managing Virtual Port Channels

This chapter contains the following sections:

- About vPCs, page 79
- Configuring a vPC Domain, page 80
- Configuring a vPC Port Channel, page 81
- Removing a vPC, page 81

About vPCs

A virtual port channel (vPC) allows links that are physically connected to two different Cisco network devices to appear as a single port channel to a third device, such as a Fabric Extender, a switch, server, or any other networking device. A vPC can provide Layer 2 multipathing, which allows you to create redundancy by increasing bandwidth, enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.

In Cisco UCS Director, you can manage vPCs on the following Cisco network devices:

- Cisco Nexus 3000 Series switches
- Cisco Nexus 5000, 5500, and 5672 Series switches
- Cisco Nexus 9300 and 9500 Series switches
- Cisco MDS 9100 Series switches
- Cisco MDS 9500 Series switches
- Cisco MDS 9700 Series switches

Note: For more detailed information about vPCs and configuration guidelines for vPCs, see the Cisco NX-OS Software Configuration Guides.
Configuring a vPC Domain

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click the VPC Info tab.
Step 5  Click Configure VPC Domain.
Step 6  In the Configure vPC Domain dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain ID field</td>
<td>The virtual port channel (vPC) domain ID used to create a vPC domain.</td>
</tr>
<tr>
<td>Source Management IP Address field</td>
<td>The IP address for source management.</td>
</tr>
<tr>
<td>Destination Management IP Address field</td>
<td>The IP address for destination management.</td>
</tr>
<tr>
<td>Role Priority field</td>
<td>The role priority within the valid range for this vPC switch. The default value is 32667. The switch with a lower priority is elected as the vPC primary switch. If the peer link fails, vPC peer detects whether the peer switch is alive through the vPC peer keepalive link. If the vPC primary switch is alive, the vPC secondary switch suspends its vPC member ports to prevent potential looping while the vPC primary switch keeps all its vPC member ports active.</td>
</tr>
<tr>
<td>System Priority field</td>
<td>The system priority within the valid range for the specified vPC domain. The default value is 32667. You should manually configure the vPC system priority when you are running the Link Aggregation Control Protocol (LACP) to help ensure that the vPC peer devices are the primary devices on LACP. When you manually configure the system priority, make sure that you configure the same priority value on both vPC peer devices. If these values do not match, then the vPC is not activated.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Step 7  Click Submit.
Configuring a vPC Port Channel

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click the VPC Info tab.
Step 5  Click the down-arrow icon, and choose Configure VPC PortChannel.
Step 6  In the Configure vPC PortChannel dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Port Channel Name field</td>
<td>Click Select. In the Select dialog box choose the port channel and click Select.</td>
</tr>
<tr>
<td>VPC Peer Link check box</td>
<td>Check the check box if you want to configure the port channel as a vPC peer link for this device.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Step 7  Click Submit.

Removing a vPC

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click the VPC Info tab.
Step 5  Click Remove VPC PortChannel.
Step 6  In the Remove VPC PortChannel dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Port Channel Name field</td>
<td>Click Select. In the Select dialog box, choose the virtual Port Channel (vPC) and click Select.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>
Removing a vPC

**Step 7**  
Click Submit.
Managing SAN Zones and SAN Zonesets

This chapter contains the following sections:

• About SAN Zone and Zonesets, page 83
• Creating a SAN Zone, page 84
• Adding a Member to a SAN Zone, page 84
• Deleting a SAN Zone, page 85
• Creating a SAN Zoneset, page 86
• Adding a Member to a SAN Zoneset, page 86
• Deleting a SAN Zoneset, page 87

About SAN Zone and Zonesets

A zone is a collection of ports that can communicate between them over the SAN. It is recommended to define a zone per initiator and target, and deploy multiple small zones, rather than having larger zones defined as they consume more resources. A Zoneset is a collection of zones that define the zoning configuration applied to a VSAN. There can be only one active zoneset per VSAN, but there can be multiple zonesets configured in a switch.

Zoning configuration is based on the following characteristics:

• Enhanced Zoning is enabled for automatic full zoneset distribution and synchronization, as well as preventing multiple administrators from modifying a VSAN zoneset at the same time. It is recommended to use enhanced zoning for all configured VSANs in the SAN.

• Device-aliases is used to configure zoning, as they are independent of the zoning database and can provide name resolution to applications beyond the zone server.

In Cisco UCS Director, you can configure SAN Zone and Zonesets on the following Cisco network devices:

• Cisco Nexus 5000, 5500, and 5672 Series switches
• Cisco Nexus 7000 Series switches
• Cisco MDS 9100 Series switches
Creating a SAN Zone

Step 1 On the menu bar, choose Physical > Network.
Step 2 In the Network pane, expand the pod.
Step 3 Select the network device that needs to be configured.
Step 4 Click the SAN Zones tab.
Step 5 Click Create SAN Zone.
Step 6 In the Create SAN Zone dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone Name field</td>
<td>The name of the zone.</td>
</tr>
<tr>
<td>VSAN Id field</td>
<td>Click Select. In the Select dialog box, choose a VSAN ID.</td>
</tr>
<tr>
<td>Commit San Zone check box</td>
<td>Check this check box to enable the enhanced zoning.</td>
</tr>
<tr>
<td>Copy Running configuration to</td>
<td>Check the check box to copy the running configuration to</td>
</tr>
<tr>
<td>Startup configuration check box</td>
<td>the startup configuration.</td>
</tr>
</tbody>
</table>

Step 7 Click Submit.

Adding a Member to a SAN Zone

Step 1 On the menu bar, choose Physical > Network.
Step 2 In the Network pane, expand the pod.
Step 3 Select the network device that needs to be configured.
Step 4 Click the SAN Zones tab.
Step 5 Select the SAN zone to which you want to add a member.
Step 6 Click Add SAN Zone Member.
Step 7 In the Add Member to SAN Zone dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone Name field</td>
<td>The name of the zone.</td>
</tr>
</tbody>
</table>
Deleting a SAN Zone

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click the SAN Zones tab.
Step 5  Select the SAN zone that you want to delete.
Step 6  Click Delete SAN Zone.
Step 7  In the Delete SAN Zone dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone Name field</td>
<td>The name of the zone.</td>
</tr>
<tr>
<td>Commit San Zone check box</td>
<td>Check this check box to enable the enhanced zoning.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Step 8  Click Submit.
Creating a SAN Zoneset

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click the SAN Zonesets tab.
Step 5  Click Create SAN Zone Set.
Step 6  In the Create SAN Zone Set dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone Set Name field</td>
<td>The name of the SAN zoneset.</td>
</tr>
<tr>
<td>VSAN Id field</td>
<td>Click Select. In the Select dialog box, choose a VSAN ID.</td>
</tr>
<tr>
<td>Commit San Zone check box</td>
<td>Check this check box to enable the enhanced zoning.</td>
</tr>
<tr>
<td>Copy Running configuration to</td>
<td>Check the check box to copy the running configuration to the startup</td>
</tr>
<tr>
<td>Startup configuration check box</td>
<td>configuration.</td>
</tr>
</tbody>
</table>

Step 7  Click Submit.

Adding a Member to a SAN Zoneset

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click the SAN Zonesets tab.
Step 5  Select the SAN zoneset to which you want to add a member.
Step 6  Click Add SAN Zone Set Member.
Step 7  In the Add SAN Zone to Set dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAN Zone Set field</td>
<td>The name of the SAN zoneset.</td>
</tr>
<tr>
<td>SAN Zone field</td>
<td>Click Select and choose the zone members.</td>
</tr>
</tbody>
</table>
Deleting a SAN Zoneset

**Deleting a SAN Zoneset**

- **Step 1**: On the menu bar, choose **Physical > Network**.
- **Step 2**: In the **Network** pane, expand the pod.
- **Step 3**: Select the network device that needs to be configured.
- **Step 4**: Click the **SAN Zonesets** tab.
- **Step 5**: Select the SAN zoneset that you want to delete.
- **Step 6**: Click **Delete SAN Zone Set**.
- **Step 7**: In the **Delete SAN Zone Set** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAN Zone Set field</td>
<td>The name of the SAN zoneset.</td>
</tr>
<tr>
<td>Commit San Zone check box</td>
<td>Check this check box to enable the enhanced zoning.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

- **Step 8**: Click **Submit**.
Managing Virtual Storage Area Networks

This chapter contains the following sections:

- About VSANs, page 89
- Creating a VSAN, page 90
- Deleting a VSAN, page 90

About VSANs

A virtual storage area network (VSAN) is a dedicated virtual network that interconnects hosts and storage devices primarily to exchange SCSI traffic. Physical links in storage area networks (SANs) are used to make these interconnections. A set of protocols run over the SAN to handle routing, naming, and zoning. You can design multiple SANs with different topologies.

With VSANs, you can build a single topology that contains switches, links, and one or more VSANs. Each VSAN in this topology has the same behavior and property of a SAN.

In Cisco UCS Director, you can configure VSANs on the following Cisco network devices:

- Cisco Nexus 3000 Series switches
- Cisco Nexus 5000, 5500, and 5672 Series switches
- Cisco Nexus 7000 Series switches
- Cisco Nexus 9300 and 9500 Series switches
- Cisco MDS 9100 Series switches
- Cisco MDS 9500 Series switches
- Cisco MDS 9700 Series switches

Note

For more detailed information about VSANs and configuration guidelines for VSANs, see the Cisco NX-OS Software Configuration Guides.
Creating a VSAN

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click the VSANs tab.
Step 5  Click Create VSAN.
Step 6  In the Create VSAN dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSAN ID field</td>
<td>The virtual storage area network (VSAN) ID number within the valid range for this device.</td>
</tr>
<tr>
<td>VSAN Name field</td>
<td>The VSAN name.</td>
</tr>
<tr>
<td>Enhance check box</td>
<td>Check the check box to enable Enhanced Zoning to perform all configurations using a single configuration session. Enhanced zone enforces and exchanges the default zone setting throughout the fabric.</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running VSAN configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Step 7  Click Submit.

Deleting a VSAN

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click the VSANs tab.
Step 5  Select the VSAN that needs to be deleted.
Step 6  Click Delete VSAN.
Step 7  In the Delete VSAN dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSAN ID drop-down list</td>
<td>The virtual storage area network (VSAN) ID that you selected for deletion.</td>
</tr>
</tbody>
</table>
Check the check box to copy the running VSAN configuration to the startup configuration.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running VSAN configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Step 8  Click Submit.
Managing Virtual Extensible LANs

This chapter contains the following sections:

- About VXLANs, page 93
- Creating a VXLAN, page 94
- Encapsulating a VXLAN, page 95
- Assigning a VXLAN to a Port Profile, page 96
- Unassigning a VXLAN from a Port Profile, page 96
- Removing a VXLAN, page 97

About VXLANs

A virtual extensible LAN (VXLAN) defines a 24-bit LAN segment identifier to provide segmentation at cloud scale and an architecture that expands cloud deployments with repeatable pods in different Layer 2 (L2) domains. A VXLAN can also enable the migration of virtual machines (VMs) between servers across Layer 3 networks.

A VXLAN creates LAN segments by overlaying the original MAC (L2) frame in IP encapsulation from the VM within the Virtual Ethernet Module (VEM).

Each VEM is assigned an IP address, which is used as the source IP address when MAC frames are encapsulated and sent over the network. You can have multiple VMkernel NICs (also referred to as virtual network adapters or vmknics) per VEM that are used as sources for this encapsulated traffic. The encapsulation carries the 24-bit VXLAN identifier that scopes the MAC address of the payload frame.

Note

VMkernel NICs are used to manage physical NICs (pNICs) on a host server to connect the virtual network to the physical network.

The connected VXLAN is indicated within the port profile configuration of the virtual network interface card (vNIC) and is applied when the VM connects. Each VXLAN uses an assigned IP multicast group to carry broadcast traffic within the VXLAN segment.

In Cisco UCS Director, you can configure VXLANs on the Cisco Nexus 1000 switch.
Creating a VXLAN

Step 1
On the menu bar, choose **Physical > Network**.

Step 2
In the **Network** pane, expand the pod.

Step 3
Select the network device that needs to be configured.

Step 4
Click the **VXLAN Table** tab.

Step 5
Click **Create VXLAN**.
Alternately, you can choose the command from the drop-down icon.

Step 6
In the **Create VXLAN** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bridge Name</strong> field</td>
<td>The bridge domain name for the virtual extensible LAN (VXLAN).</td>
</tr>
<tr>
<td><strong>VXLAN Id</strong> field</td>
<td>The VXLAN ID number within the valid range.</td>
</tr>
</tbody>
</table>
| **Mode Unicast** check box | Check the check box to enable a unicast-only VXLAN.  
With a unicast-only VXLAN, the Virtual Supervisor Module (VSM) knows which VEMs have Virtual Machines (VMs) attached to a particular VXLAN segment and distributes that information to all Virtual Ethernet Modules (VEMs). Each VEM receives a per-VXLAN list of destination IP addresses to use for flooding purposes. |
| **Distribution learning MAC** check box | Check the check box to distribution learning for MAC addressing.  
MAC learning enables the distribution of the MAC addresses learned on one line card to the other line cards. |
| **Copy Running configuration to Startup configuration** check box | Check the check box to copy the running VXLAN configuration to the startup configuration. |

Step 7
Click **Submit**.
Encapsulating a VXLAN

You can configure VMkernel NICs (vmknics) for virtual extensible LAN (VXLAN) encapsulation by running the following procedure.

---

**Note**

Identify a VLAN to be used for transporting VXLAN encapsulated traffic and ensure that it is configured on the uplink port profile for all VEMs on which the VXLAN can be configured.

---

1. On the menu bar, choose **Physical > Network**.
2. In the **Network** pane, expand the pod.
3. Select the network device that needs to be configured.
4. Click the **VXLAN Table** tab.
5. Select the VXLAN domain that needs to be encapsulated.
6. Click **Encapsulate VXLAN**. Alternately, you can choose the command from the drop-down icon.
7. In the **Encapsulate VXLAN** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select Port Profile</strong> drop-down list</td>
<td>Choose the port profile that you want to use for the VXLAN.</td>
</tr>
<tr>
<td><strong>VLAN ID Select</strong> button</td>
<td>Click <strong>Select</strong>. In the <strong>Select</strong> dialog box, check the check box for the VLAN ID that you want encapsulated and click <strong>Select</strong>.</td>
</tr>
<tr>
<td><strong>Copy Running configuration to Startup configuration</strong> check box</td>
<td>Check the check box to copy the running VXLAN configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

8. Click **Submit**.
Assigning a VXLAN to a Port Profile

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click the VXLAN Table tab.
Step 5  Select the VXLAN domain that needs to be assigned to a port profile.
Step 6  Click Assign VXLAN to a Port Profile. Alternately, you can choose the command from the drop-down icon.
Step 7  In the Assign VXLAN dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Port Profile drop-down</td>
<td>Choose the port profile name for the VXLAN assignment. Note: Ensure that the</td>
</tr>
<tr>
<td>Name</td>
<td>access VLAN is enabled for a VXLAN capability in the port profile that you</td>
</tr>
<tr>
<td></td>
<td>are using for the VXLAN. For more information, see Creating a Port Profile.</td>
</tr>
<tr>
<td>Copy Running configuration</td>
<td>Check the check box to copy the running VXLAN configuration to the startup</td>
</tr>
<tr>
<td>to Startup configuration</td>
<td>configuration.</td>
</tr>
<tr>
<td>check box</td>
<td></td>
</tr>
</tbody>
</table>

Step 8  Click Submit.

Unassigning a VXLAN from a Port Profile

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the Network pane, expand the pod.
Step 3  Select the network device that needs to be configured.
Step 4  Click the VXLAN Table tab.
Step 5  Select the VXLAN domain that needs to be unassigned from a port profile.
Step 6  Click Unassign VXLAN from Port Profile. Alternately, you can choose the command from the drop-down icon.
Step 7  In the Unassign VXLAN dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Port Profile drop-down</td>
<td>Choose the port profile from which you need to unassign the VXLAN.</td>
</tr>
</tbody>
</table>
Removing a VXLAN

Note
Executing this procedure moves the ports to the default VLAN.

Step 1
On the menu bar, choose Physical > Network.

Step 2
In the Network pane, expand the pod.

Step 3
Select the network device that needs to be configured.

Step 4
Click the VXLAN Table tab.

Step 5
Select the VXLAN that needs to be removed.

Step 6
Click Remove VXLAN.

Step 7
In the Remove VXLAN dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running VLAN configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Step 8
Click Submit.
Removing a VXLAN
Configuring ASA Context

This chapter contains the following sections:

• About ASA Context, page 99
• Creating an ASA Context, page 99

About ASA Context

You can partition a single ASA into multiple virtual devices, known as security contexts. Each context acts as an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices.

In Cisco UCS Director, ASA context configuration is supported on the following Cisco network device:

• Cisco ASA 5500 Series firewall

Creating an ASA Context

Step 1
On the menu bar, choose Physical > Network.

Step 2
In the Network pane, expand the pod.

Step 3
Choose the network device that needs to be configured.

Step 4
Click the ASA Context tab.

Step 5
Click Create Asa Context.

Step 6
In the Create Asa Context dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context Name field</td>
<td>The name of the security context.</td>
</tr>
<tr>
<td>Context Description field</td>
<td>The description of the security context.</td>
</tr>
</tbody>
</table>
### Creating an ASA Context

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name field</td>
<td>The name of the security context configuration.</td>
</tr>
<tr>
<td>OutSide Interface Name drop-down list</td>
<td>Choose the outside interface name for the security context.</td>
</tr>
<tr>
<td>Inside Interfaces field</td>
<td>Click Select and choose the inside interfaces for the security context.</td>
</tr>
<tr>
<td>Mode drop-down list</td>
<td>Choose one of the following as the firewall mode for context:</td>
</tr>
<tr>
<td></td>
<td>• Routed</td>
</tr>
<tr>
<td></td>
<td>• Transparent</td>
</tr>
<tr>
<td>Copy Running configuration to Startup configuration check box</td>
<td>Check the check box to copy the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

**Step 7**

Click **Submit**.
CHAPTER 27

Monitoring and Reporting

This chapter contains the following sections:

- About General Reports, page 101
- About Detail Reports, page 102
- About Cisco ISE, page 105
- About the Service Request Details Report, page 106
- Exporting an Inventory Report, page 106

About General Reports

General reports are available for each network device. Each report has its own tab, and the tabs are visible when you choose the pod with the network device you want to view or monitor.

Information You Can View

You can view reports for components, including the following:

- Network accounts

Components You Can Monitor

You can monitor specific components, including the following:

- VTP status
- Private VLANs
- Layer 2 Neighbors
- Port Profiles
- VM network details
- Host network details
• Virtual Storage Area Networks (VSANs)
• VLANs

Note
You can also see detailed reports for Layer 2 neighbors and private VLANs, which display additional information.

About Detail Reports

In addition to the general reports available when you click a pod on the Managed Network Elements tab, Cisco UCS Director displays detail reports for network devices.

Each report has its own tab, and the tabs are visible when you select a pod with the switch, and click View Details on the Managed Network Elements tab.

Cisco Nexus 1000V Switch

You can view reports for Cisco Nexus 1000V switch components, including the license information and summary status. In addition, you can monitor components, such as the following:

• Configurations
• Modules
• Layer 2 Neighbors
• VXLAN Table
• Interfaces
• Port capabilities
• VLANs
• Private VLANs
• Port profiles
• Port profile encapsulation
• SXP Connection Peers
• Features
• MAC address table
• MAC address table configuration
• QoS class maps
• QoS policy maps
• Service request details
Cisco Nexus 5000 and 5500 Series Switches

You can view reports for Cisco Nexus 5000 and 5500 Series components, including the license information and summary status. In addition, you can monitor components, such as the following:

- Configurations
- Modules
- Layer 2 neighbors
- Interfaces
- Port capabilities
- VLANs
- Private VLANs
- Port profiles
- SXP Connection Peers
- HSRP
- VPC information
- VTP status
- Features
- MAC address tables
- MAC address table configuration
- SAN zones
- SAN zonesets
- Fabric login
- Device alias
- FCAlias
- VSANs
- QoS class maps
- QoS policy maps
- Service request details

Cisco Nexus 7000 Series Switches

You can view reports for Cisco Nexus 7000 Series components, including the license information and summary status. In addition, you can monitor components, such as the following:

- Configurations
- Modules
- Layer 2 neighbors
- Interfaces
About Detail Reports

• Port capabilities
• VLANs
• Private VLANs
• Port profiles
• VDC
  • SXP Connection Peers
  • HSRP
  • FCAlias

**Note** More reports are available for individual VDCs when they are expanded.

• VDC detail
• VDC interfaces
• VPC information
• VTP status
• Features
• MAC address table
• MAC address table configuration
• QoS policy maps
• QoS class maps
• Service request details

**Cisco Nexus 9300 and 9500 Series Switches**

You can view reports for Cisco Nexus 9300 and 9500 Series switches switch components, including the license information and summary status. In addition, you can monitor components, such as the following:

• Configurations
• Modules
• Layer 2 neighbors
• Interfaces
• Port Capabilities
• VLANs
• Private VLANs
• Port profiles
• VPC information
Cisco ISE

Cisco Identity Services Engine (Cisco ISE) is a next-generation identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. The Cisco Security Group Access (SGA) solution establishes clouds of trusted network devices to build secure networks. Each device in the Cisco SGA cloud is authenticated by its neighbors (peers). Communication between the devices in the SGA cloud is secured with a combination of encryption, message integrity checks, and data-path replay protection mechanisms.

The SGA solution uses the device and user identity information that it obtains during authentication to classify, or color, the packets as they enter the network. This packet classification is maintained by tagging packets when they enter the SGA network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The tag, also called the security group tag (SGT), allows Cisco ISE to enforce access control policies by enabling the endpoint device to act upon the SGT to filter traffic.

To view the SGT entry of all devices that are managed in Cisco UCS Director, in the network pane, expand the pod and click the Cisco ISE device. The Security Group Tag Entry tab displays the name, ID, and description of the SGT entry of devices.

About Cisco ISE

Cisco Identity Services Engine (Cisco ISE) is a next-generation identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. The Cisco Security Group Access (SGA) solution establishes clouds of trusted network devices to build secure networks. Each device in the Cisco SGA cloud is authenticated by its neighbors (peers). Communication between the devices in the SGA cloud is secured with a combination of encryption, message integrity checks, and data-path replay protection mechanisms.

The SGA solution uses the device and user identity information that it obtains during authentication to classify, or color, the packets as they enter the network. This packet classification is maintained by tagging packets when they enter the SGA network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The tag, also called the security group tag (SGT), allows Cisco ISE to enforce access control policies by enabling the endpoint device to act upon the SGT to filter traffic.

To view the SGT entry of all devices that are managed in Cisco UCS Director, in the network pane, expand the pod and click the Cisco ISE device. The Security Group Tag Entry tab displays the name, ID, and description of the SGT entry of devices.
About the Service Request Details Report

You can view the service requests that have changed the state of a selected network device or component. The Service Request ID and the change description appear under the component's Service Request Details tab. Device or component configurations, additions, modifications, and deletions are all tracked under each component on this tab.

Any network device or component that has been part of a task in an executed workflow is tracked based on the ID of the service request that modified it.

Exporting an Inventory Report

You can export an inventory report in PDF, CSV, or XLS format.

Step 1
On the menu bar, choose Physical > Network.

Step 2
In the Network pane, choose the pod.

Step 3
Click a report that you want to export.

Step 4
On the right side of the report, click the Export Report button.

Step 5
In the Export Report dialog box, choose the desired report format from the Select Report Format drop-down list and then click Generate Report.

Step 6
After the report has been generated, click Download.

Step 7
After you have downloaded the report, click Close.
Troubleshooting

This chapter contains the following sections:

- Troubleshooting Cisco UCS Director Connectivity, page 107
- Troubleshooting Cisco UCS Director Baremetal Agent Connectivity, page 108

Troubleshooting Cisco UCS Director Connectivity

Step 1

Ensure Cisco UCS Director services are active.

<table>
<thead>
<tr>
<th>Check</th>
<th>Do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS Director Virtual Machine (VM)</td>
<td>Ensure that there is sufficient resource reservation. For more information, see the System Requirements section.</td>
</tr>
<tr>
<td>Cisco UCS Director appliance</td>
<td>Access the appliance using Secure Shell (SSH) and the shelladmin user. Ensure that all the services are running (including the database). If services are not running, restart the services and wait a few minutes before accessing Cisco UCS Director through the web interface.</td>
</tr>
</tbody>
</table>

Step 2

Ensure that the IP address of Cisco UCS Director can be pinged over the network.

<table>
<thead>
<tr>
<th>Check</th>
<th>Do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS Director network configuration</td>
<td>Log into vCenter and check the network configuration of the Cisco UCS Director virtual appliance and its connectivity.</td>
</tr>
<tr>
<td>Port group and management network</td>
<td>Ping the port group and management network.</td>
</tr>
<tr>
<td>Cisco UCS Director VM</td>
<td>Ensure that the Connect check box is checked in the VM.</td>
</tr>
</tbody>
</table>
Step 3: Ensure that Cisco UCS Director can be accessed through a web browser. If you cannot access Cisco UCS Director, do the following:

**Note**: Wait for the Cisco UCS Director appliance and services to become available before connecting to Cisco UCS Director. This may take a few minutes.

<table>
<thead>
<tr>
<th>Check</th>
<th>Do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web browser cache</td>
<td>Clear the web browser cache before accessing Cisco UCS Director through the web.</td>
</tr>
<tr>
<td>Web browser version</td>
<td>Use the recommended browser version and flash version.</td>
</tr>
</tbody>
</table>

Step 4: Ensure that Cisco UCS Director is able to reach all of the hardware and software.

Step 5: Ensure that Cisco UCS Director is on the same interface as Cisco UCS Director Baremetal Agent.

---

## Troubleshooting Cisco UCS Director Baremetal Agent Connectivity

### Step 1: Ensure that the DHCP service (daemon) is active.

<table>
<thead>
<tr>
<th>Check</th>
<th>Do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP server</td>
<td>Use the following command:</td>
</tr>
<tr>
<td></td>
<td>/etc/init.d/dhcp status</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If the status is down, restart the DHCP server.</td>
</tr>
</tbody>
</table>

### Step 2: Ensure that the status of Cisco UCS Director Baremetal Agent network services is active.

<table>
<thead>
<tr>
<th>Check</th>
<th>Do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS Director Baremetal Agent</td>
<td>Use the following command:</td>
</tr>
<tr>
<td></td>
<td>ps -ef</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Entering the above command should have three Java processes display. If not, restart the services and recheck to make sure all of them are active.</td>
</tr>
<tr>
<td></td>
<td>/opt/infra/stopInfraAll.sh</td>
</tr>
<tr>
<td></td>
<td>/opt/infra/startInfraAll.sh</td>
</tr>
</tbody>
</table>
Step 3  Ensure Cisco UCS Director Baremetal Agent can ping the Cisco UCS Director Baremetal Agent IP address. If not, check the connectivity through the network configuration of the Cisco UCS Director Baremetal Agent appliance using vCenter.

Step 4  Ensure that Cisco UCS Director Baremetal Agent can ping the Cisco UCS Manager and blade server network.

<table>
<thead>
<tr>
<th>Check</th>
<th>Do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP server</td>
<td>Ensure that the DHCP server that is running on the Cisco UCS Director Baremetal Agent provides DHCP functionality for baremetal provisioning. The Cisco UCS Director Baremetal Agent should be on the same network or interface as the Cisco UCS Manager so that it can provide Preboot Execution Environment (PXE) functionality without problems. Ensure there are no DHCP servers available in the same network as the Cisco UCS Director Baremetal Agent.</td>
</tr>
</tbody>
</table>