VLAN

VLANs

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment.

Any switch port can belong to a VLAN. Unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or bridge.

VLANs are typically associated with IP subnetworks. For example, all of the end stations in a particular IP subnet belong to the same VLAN. To communicate between VLANs, you must route the traffic. By default, a newly created VLAN is operational. Additionally, you can configure VLANs to be in the active state, which is passing traffic, or in the suspended state, in which the VLANs are not passing packets. By default, the VLANs are in the active state and pass traffic.

Named VLANs

A named VLAN creates a connection to a specific external LAN. The VLAN isolates traffic to that external LAN, including broadcast traffic.

The name that you assign to a VLAN ID adds a layer of abstraction that allows you to globally update all servers associated with service profiles that use the named VLAN. You do not need to reconfigure the servers individually to maintain communication with the external LAN.

You can create more than one named VLAN with the same VLAN ID. For example, if servers that host business services for HR and Finance need to access the same external LAN, you can create VLANs named HR and Finance with the same VLAN ID. Then, if the network is reconfigured and Finance is assigned to a different LAN, you only have to change the VLAN ID for the named VLAN for Finance.

In a cluster configuration, you can configure a named VLAN to be accessible only to one fabric interconnect or to both fabric interconnects.

Guidelines for VLAN IDs

Important You cannot create VLANs with IDs from 3968 to 4047 and 4092 to 4096. These ranges of VLAN IDs are reserved.

For Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 and 6400 Series Fabric Interconnects, VLAN IDs from 1002 to 1005 are reserved for VLAN Trunking Protocol (VTP).

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

VLAN 4048 is user configurable. However, Cisco UCS Manager uses VLAN 4048 for the following default values. If you want to assign 4048 to a VLAN, you must reconfigure these values:

- After an upgrade to Cisco UCS, Release 2.0—The FCoE storage port native VLAN uses VLAN 4048 by default. If the default FCoE VSAN was set to use VLAN 1 before the upgrade, you must change it to a VLAN ID that is not used or reserved. For example, consider changing the default to 4049 if that VLAN ID is not in use.
- After a fresh install of Cisco UCS, Release 2.0—The FCoE VLAN for the default VSAN uses VLAN 4048 by default. The FCoE storage port native VLAN uses VLAN 4049.

The VLAN name is case sensitive.

Private VLANs

A private VLAN (PVLAN) partitions the Ethernet broadcast domain of a VLAN into subdomains, and allows you to isolate some ports. Each subdomain in a PVLAN includes a primary VLAN and one or more secondary VLANs. All secondary VLANs in a PVLAN must share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another.

Isolated and Community VLANs

All secondary VLANs in a Cisco UCS domain can be Isolated or Community VLANs.

Note You cannot configure an isolated VLAN to use with a regular VLAN.

Ports on Isolated VLANs

Communications on an isolated VLAN can only use the associated port in the primary VLAN. These ports are isolated ports and are not configurable in Cisco UCS Manager. A primary VLAN can have only one isolated VLAN, but multiple isolated ports on the same isolated VLAN are allowed. These isolated ports cannot communicate with each other. The isolated ports can communicate only with a regular trunk port or promiscuous port that allows the isolated VLAN.

An isolated port is a host port that belongs to an isolated secondary VLAN. This port has complete isolation from other ports within the same private VLAN domain. PVLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports. You can have more than one isolated port in a specified isolated VLAN. Each port is completely isolated from all other ports in the isolated VLAN.

Guidelines for Uplink Ports

When you create PVLANs, use the following guidelines:

- The uplink Ethernet port channel cannot be in promiscuous mode.
- Each primary VLAN can have only one isolated VLAN.
- VIFs on VNTAG adapters can have only one isolated VLAN.

Guidelines for VLAN IDs

Note You cannot create VLANs with IDs from 3915 to 4042. These ranges of VLAN IDs are reserved.

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

VLAN 4048 is user configurable. However, Cisco UCS Manager uses VLAN 4048 for the following default values. If you want to assign 4048 to a VLAN, you must reconfigure these values:

- After an upgrade to Cisco UCS, Release 2.0—The FCoE storage port native VLAN uses VLAN 4048 by default. If the default FCoE VSAN was set to use VLAN 1 before the upgrade, you must change it to a VLAN ID that is not used or reserved. For example, consider changing the default to 4049 if that VLAN ID is not in use.
- After a fresh install of Cisco UCS, Release 2.0—The FCoE VLAN for the default VSAN uses VLAN 4048 by default. The FCoE storage port native VLAN uses VLAN 4049.

The VLAN name is case sensitive.

VLAN Port Limitations

Cisco UCS Manager limits the number of VLAN port instances that you can configure under border and server domains on a fabric interconnect.

Types of Ports Included in the VLAN Port Count

The following types of ports are counted in the VLAN port calculation:

- Border uplink Ethernet ports
- Border uplink Ether-channel member ports
- FCoE ports in a SAN cloud
- Ethernet ports in a NAS cloud
- Static and dynamic vNICs created through service profiles
- VM vNICs created as part of a port profile in a hypervisor in hypervisor domain

Based on the number of VLANs configured for these ports, Cisco UCS Manager tracks the cumulative count of VLAN port instances and enforces the VLAN port limit during validation. Cisco UCS Manager reserves some pre-defined VLAN port resources for control traffic. These include management VLANs configured under HIF and NIF ports.

VLAN Port Limit Enforcement

Cisco UCS Manager validates VLAN port availability during the following operations:

- Configuring and unconfiguring border ports and border port channels
- Adding or removing VLANs from a cloud
- Configuring or unconfiguring SAN or NAS ports
- Associating or disassociating service profiles that contain configuration changes
- Configuring or unconfiguring VLANs under vNICs or vHBAs
- Receiving creation or deletion notifications from a VMWare vNIC and from an ESX hypervisor

Note This is outside the control of the Cisco UCS Manager.

- Fabric interconnect reboot
- Cisco UCS Manager upgrade or downgrade

Cisco UCS Manager strictly enforces the VLAN port limit on service profile operations. If Cisco UCS Manager detects that the VLAN port limit is exceeded, the service profile configuration fails during deployment.

Exceeding the VLAN port count in a border domain is less disruptive. When the VLAN port count is exceeded in a border domain Cisco UCS Manager changes the allocation status to Exceeded. To change the status back to **Available**, complete one of the following actions:

- Unconfigure one or more border ports
- Remove VLANs from the LAN cloud
- Unconfigure one or more vNICs or vHBAs

Configuring Named VLANs

Creating a Named VLAN Accessible to Both Fabric Interconnects (Uplink Ethernet Mode)

Important You cannot create VLANs with IDs from 3968 to 4047 and 4092 to 4096. These ranges of VLAN IDs are reserved.

For Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 and 6400 Series Fabric Interconnects, VLAN IDs from 1002 to 1005 are reserved for VLAN Trunking Protocol (VTP).

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**	Enters Ethernet uplink mode.
Step 2	UCS-A /eth-uplink # **create vlan** *vlan-name vlan-id*	Creates a named VLAN, specifies the VLAN name and VLAN ID, and enters Ethernet uplink VLAN mode. The VLAN name is case sensitive.
Step 3	UCS-A /eth-uplink/fabric/vlan # **set sharing** {**isolated** | **none** | **primary**}	Sets the sharing for the specified VLAN. This can be one of the following: • **isolated** —This is a secondary VLAN associated with a primary VLAN. This VLAN is private.

	Command or Action	Purpose
		• **none** —This VLAN does not have any secondary or private VLANs. • **primary** —This VLAN can have one or more secondary VLANs.
Step 4	UCS-A /eth-uplink/vlan # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example creates a named VLAN for both fabric interconnects, names the VLAN accounting, assigns the VLAN ID 2112, sets the sharing to none, and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create vlan accounting 2112
UCS-A /eth-uplink/vlan* # set sharing none
UCS-A /eth-uplink/vlan* # commit-buffer
UCS-A /eth-uplink/vlan #
```

Creating a Named VLAN Accessible to Both Fabric Interconnects (Ethernet Storage Mode)

Important You cannot create VLANs with IDs from 3968 to 4047 and 4092 to 4096. These ranges of VLAN IDs are reserved.

For Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 and 6400 Series Fabric Interconnects, VLAN IDs from 1002 to 1005 are reserved for VLAN Trunking Protocol (VTP).

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-storage**	Enters Ethernet storage mode.
Step 2	UCS-A /eth-storage # **create vlan** *vlan-name vlan-id*	Creates a named VLAN, specifies the VLAN name and VLAN ID, and enters Ethernet storage VLAN mode.

	Command or Action	Purpose
		The VLAN name is case sensitive.
Step 3	UCS-A /eth-storage/vlan # **create member-port** {**a** | **b**} *slot-id* *port-id*	Creates a member port for the specified VLAN on the specified fabric.
Step 4	UCS-A /eth-storage/vlan/member-port # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example creates a named VLAN for both fabric interconnects, names the VLAN accounting, assigns the VLAN ID 2112, creates a member port on slot 2, port 20, and commits the transaction:

```
UCS-A# scope eth-storage
UCS-A /eth-storage # create vlan accounting 2112
UCS-A /eth-storage/vlan* # create member-port a 2 20
UCS-A /eth-storage/vlan/member-port* # commit-buffer
UCS-A /eth-storage/vlan/member-port #
```

Creating a Named VLAN Accessible to One Fabric Interconnect (Uplink Ethernet Mode)

Important You cannot create VLANs with IDs from 3968 to 4047 and 4092 to 4096. These ranges of VLAN IDs are reserved.

For Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 and 6400 Series Fabric Interconnects, VLAN IDs from 1002 to 1005 are reserved for VLAN Trunking Protocol (VTP).

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**	Enters Ethernet uplink mode.
Step 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	Enters Ethernet uplink fabric interconnect mode for the specified fabric interconnect (A or B).

	Command or Action	Purpose
Step 3	UCS-A /eth-uplink/fabric # **create vlan** *vlan-name* *vlan-id*	Creates a named VLAN, specifies the VLAN name and VLAN ID, and enters Ethernet uplink fabric interconnect VLAN mode. The VLAN name is case sensitive.
Step 4	UCS-A /eth-uplink/fabric/vlan # **set sharing** {**isolated** | **none** | **primary**}	Sets the sharing for the specified VLAN. This can be one of the following: • **isolated** —This is a secondary VLAN associated with a primary VLAN. This VLAN is private. • **none** —This VLAN does not have any secondary or private VLANs. • **primary** —This VLAN can have one or more secondary VLANs.
Step 5	UCS-A /eth-uplink/fabric/vlan # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example creates a named VLAN for fabric interconnect A, names the VLAN finance, assigns the VLAN ID 3955, sets the sharing to none, and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # create vlan finance 3955
UCS-A /eth-uplink/fabric/vlan* # set sharing none
UCS-A /eth-uplink/fabric/vlan* # commit-buffer
UCS-A /eth-uplink/fabric/vlan #
```

Creating a Secondary VLAN for a Private VLAN (Accessible to One Fabric Interconnect)

Important You cannot create VLANs with IDs from 3968 to 4047 and 4092 to 4096. These ranges of VLAN IDs are reserved.

For Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 and 6400 Series Fabric Interconnects, VLAN IDs from 1002 to 1005 are reserved for VLAN Trunking Protocol (VTP).

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**	Enters Ethernet uplink mode.
Step 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	Enters Ethernet uplink fabric interconnect mode for the specified fabric interconnect (A or B).
Step 3	UCS-A /eth-uplink/fabric # **create vlan** *vlan-name* *vlan-id*	Creates a named VLAN, specifies the VLAN name and VLAN ID, and enters Ethernet uplink fabric interconnect VLAN mode. The VLAN name is case sensitive.
Step 4	UCS-A /eth-uplink/vlan # **set sharing isolated**	Sets the VLAN as the secondary VLAN.
Step 5	UCS-A /eth-uplink/vlan # **set pubnwname** *primary-vlan-name*	Specifies the primary VLAN to be associated with this secondary VLAN.
Step 6	UCS-A /eth-uplink/fabric/vlan/member-port # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example creates a named VLAN for fabric interconnect A, names the VLAN finance, assigns the VLAN ID 3955, makes this VLAN the secondary VLAN, associates the secondary VLAN with the primary VLAN, and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # create vlan finance 3955
UCS-A /eth-uplink/fabric/vlan* # set sharing isolated
```

```
UCS-A /eth-uplink/fabric/vlan* # set pubnwname pvlan1000
UCS-A /eth-uplink/fabric/vlan* # commit-buffer
UCS-A /eth-uplink/fabric/vlan #
```

Deleting a Named VLAN

If Cisco UCS Manager includes a named VLAN with the same VLAN ID as the one you delete, the VLAN is not removed from the fabric interconnect configuration until all named VLANs with that ID are deleted.

If you are deleting a private primary VLAN, ensure that you reassign the secondary VLANs to another working primary VLAN.

Before you begin

Before you delete a VLAN from a fabric interconnect, ensure that the VLAN was removed from all vNICs and vNIC templates.

Note If you delete a VLAN that is assigned to a vNIC or vNIC template, the vNIC might allow that VLAN to flap.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**	Enters Ethernet uplink mode.
Step 2	(Optional) UCS-A /eth-uplink # **scope fabric**{**a** | **b**}	Enters Ethernet uplink fabric mode. Use this command when you want to delete a named VLAN only from the specified fabric (a or b).
Step 3	UCS-A /eth-uplink # **delete vlan** *vlan-name*	Deletes the specified named VLAN.
Step 4	UCS-A /eth-uplink # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example deletes a named VLAN accessible to both fabric interconnects and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # delete vlan accounting
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink #
```

The following example deletes a named VLAN accessible to one fabric interconnect and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # delete vlan finance
```

```
UCS-A /eth-uplink/fabric* # commit-buffer
UCS-A /eth-uplink/fabric #
```

Configuring Private VLANs

Creating a Primary VLAN for a Private VLAN (Accessible to Both Fabric Interconnects)

Important You cannot create VLANs with IDs from 3968 to 4047 and 4092 to 4096. These ranges of VLAN IDs are reserved.

For Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 and 6400 Series Fabric Interconnects, VLAN IDs from 1002 to 1005 are reserved for VLAN Trunking Protocol (VTP).

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**	Enters Ethernet uplink mode.
Step 2	UCS-A /eth-uplink # **create vlan** *vlan-name vlan-id*	Creates a named VLAN, specifies the VLAN name and VLAN ID, and enters Ethernet uplink VLAN mode. The VLAN name is case sensitive.
Step 3	UCS-A /eth-uplink/vlan # **set sharing primary**	Sets the VLAN as the primary VLAN.
Step 4	UCS-A /eth-uplink/vlan # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example creates a named VLAN for both fabric interconnects, names the VLAN accounting, assigns the VLAN ID 2112, makes this VLAN the primary VLAN, and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create vlan accounting 2112
```

```
UCS-A /eth-uplink/vlan* # set sharing primary
UCS-A /eth-uplink/vlan* # commit-buffer
UCS-A /eth-uplink/vlan #
```

Creating a Primary VLAN for a Private VLAN (Accessible to One Fabric Interconnect)

Important You cannot create VLANs with IDs from 3968 to 4047 and 4092 to 4096. These ranges of VLAN IDs are reserved.

For Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 and 6400 Series Fabric Interconnects, VLAN IDs from 1002 to 1005 are reserved for VLAN Trunking Protocol (VTP).

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**	Enters Ethernet uplink mode.
Step 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	Enters Ethernet uplink fabric interconnect mode for the specified fabric interconnect.
Step 3	UCS-A /eth-uplink/fabric # **create vlan** *vlan-name* *vlan-id*	Creates a named VLAN, specifies the VLAN name and VLAN ID, and enters Ethernet uplink fabric interconnect VLAN mode. The VLAN name is case sensitive.
Step 4	UCS-A /eth-uplink/fabric/vlan # **set sharing primary**	Sets the VLAN as the primary VLAN.
Step 5	UCS-A /eth-uplink/fabric/vlan # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example creates a named VLAN for fabric interconnect A, names the VLAN finance, assigns the VLAN ID 3955, makes this VLAN the primary VLAN, and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # create vlan finance 3955
```

```
UCS-A /eth-uplink/fabric/vlan* # set sharing primary
UCS-A /eth-uplink/fabric/vlan* # commit-buffer
UCS-A /eth-uplink/fabric/vlan #
```

Creating a Secondary VLAN for a Private VLAN (Accessible to Both Fabric Interconnects)

Important You cannot create VLANs with IDs from 3968 to 4047 and 4092 to 4096. These ranges of VLAN IDs are reserved.

For Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 and 6400 Series Fabric Interconnects, VLAN IDs from 1002 to 1005 are reserved for VLAN Trunking Protocol (VTP).

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**	Enters Ethernet uplink mode.
Step 2	UCS-A /eth-uplink # **create vlan** *vlan-name vlan-id*	Creates a named VLAN, specifies the VLAN name and VLAN ID, and enters Ethernet uplink VLAN mode. The VLAN name is case sensitive.
Step 3	UCS-A /eth-uplink/vlan # **set sharing isolated**	Sets the VLAN as the secondary VLAN.
Step 4	UCS-A /eth-uplink/vlan # **set pubnwname** *primary-vlan-name*	Specifies the primary VLAN to be associated with this secondary VLAN.
Step 5	UCS-A /eth-uplink/vlan # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example creates a named VLAN for both fabric interconnects, names the VLAN accounting, assigns the VLAN ID 2112, makes this VLAN the secondary VLAN, associates the secondary VLAN with the primary VLAN, and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create vlan accounting 2112
```

```
UCS-A /eth-uplink/vlan* # set sharing isolated
UCS-A /eth-uplink/vlan* # set pubnwname pvlan1000
UCS-A /eth-uplink/vlan* # commit-buffer
UCS-A /eth-uplink/vlan #
```

Creating a Secondary VLAN for a Private VLAN (Accessible to One Fabric Interconnect)

Important You cannot create VLANs with IDs from 3968 to 4047 and 4092 to 4096. These ranges of VLAN IDs are reserved.

For Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 and 6400 Series Fabric Interconnects, VLAN IDs from 1002 to 1005 are reserved for VLAN Trunking Protocol (VTP).

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**	Enters Ethernet uplink mode.
Step 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	Enters Ethernet uplink fabric interconnect mode for the specified fabric interconnect (A or B).
Step 3	UCS-A /eth-uplink/fabric # **create vlan** *vlan-name* *vlan-id*	Creates a named VLAN, specifies the VLAN name and VLAN ID, and enters Ethernet uplink fabric interconnect VLAN mode. The VLAN name is case sensitive.
Step 4	UCS-A /eth-uplink/vlan # **set sharing isolated**	Sets the VLAN as the secondary VLAN.
Step 5	UCS-A /eth-uplink/vlan # **set pubnwname** *primary-vlan-name*	Specifies the primary VLAN to be associated with this secondary VLAN.
Step 6	UCS-A /eth-uplink/fabric/vlan/member-port # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example creates a named VLAN for fabric interconnect A, names the VLAN finance, assigns the VLAN ID 3955, makes this VLAN the secondary VLAN, associates the secondary VLAN with the primary VLAN, and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # create vlan finance 3955
UCS-A /eth-uplink/fabric/vlan* # set sharing isolated
UCS-A /eth-uplink/fabric/vlan* # set pubnwname pvlan1000
UCS-A /eth-uplink/fabric/vlan* # commit-buffer
UCS-A /eth-uplink/fabric/vlan #
```

Allowing PVLANs on vNICs

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org /**	Enters root organization mode.
Step 2	UCS-A /org # **scope service-profile** *profile-name*	Commits the transaction to the system configuration.
Step 3	UCS-A /org/service-profile # **scope vnic** *vnic-name*	Enters command mode for the specified vNIC.
Step 4	UCS-A /org/service-profile/vnic # **create eth-if** *community-vlan-name*	Allows the community VLAN to access the specified vNIC.
Step 5	UCS-A /org/service-profile/vnic/eth-if* # **exit**	Exits the interface configuration mode for the specified vNIC.
Step 6	UCS-A /org/service-profile/vnic* # **create eth-if** *primary-vlan-name*	Allows the primary VLAN to access the specified vNIC.
Step 7	UCS-A /org/service-profile/vnic # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to assign the community VLAN cVLAN102 and the primary VLAN primaryVLAN100 to the vNIC vnic_1 and commits the transaction.

```
UCS-A# scope org /
UCS-A /org # scope service-profile GSP1
UCS-A /org/service-profile # scope vnic vnic_1
UCS-A /org/service-profile/vnic # create eth-if cVLAN102
UCS-A /org/service-profile/vnic/eth-if* # exit
UCS-A /org/service-profile/vnic # create eth-if primaryVLAN100
UCS-A /org/service-profile/vnic* # commit-buffer
```

Creating a Primary VLAN for a Private VLAN on an Appliance Cloud

Important You cannot create VLANs with IDs from 3968 to 4047 and 4092 to 4096. These ranges of VLAN IDs are reserved.

For Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 and 6400 Series Fabric Interconnects, VLAN IDs from 1002 to 1005 are reserved for VLAN Trunking Protocol (VTP).

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-storage**	Enters Ethernet storage mode.
Step 2	UCS-A /eth-storage # **create vlan** *vlan-name vlan-id*	Creates a named VLAN, specifies the VLAN name and VLAN ID, and enters Ethernet storage VLAN mode. The VLAN name is case sensitive.
Step 3	UCS-A /eth-storage/vlan* # **set sharing primary**	Sets the VLAN as the primary VLAN.
Step 4	UCS-A /eth-storage/vlan* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example creates a named VLAN for fabric interconnect A, names the VLAN, assigns the VLAN ID, makes this VLAN the primary VLAN, and commits the transaction:

```
UCS-A# scope eth-storage
UCS-A /eth-storage # create vlan primaryvlan500 500
UCS-A /eth-storage/vlan* # set sharing primary
UCS-A /eth-storage/vlan* # commit-buffer
UCS-A /eth-storage/vlan #
```

Creating a Secondary VLAN for a Private VLAN on an Appliance Cloud

Important You cannot create VLANs with IDs from 3968 to 4047 and 4092 to 4096. These ranges of VLAN IDs are reserved.

For Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 and 6400 Series Fabric Interconnects, VLAN IDs from 1002 to 1005 are reserved for VLAN Trunking Protocol (VTP).

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-storage**	Enters Ethernet storage mode.
Step 2	UCS-A /eth-storage # **create vlan** *vlan-name vlan-id*	Creates a named VLAN, specifies the VLAN name and VLAN ID, and enters Ethernet storage VLAN mode. The VLAN name is case sensitive.
Step 3	UCS-A /eth-storage/vlan* # **set sharing isolated**	Sets the VLAN as the secondary VLAN.
Step 4	UCS-A /eth-storage/vlan* # **set pubnwname** *primary-vlan-name*	Specifies the primary VLAN to be associated with this secondary VLAN.
Step 5	UCS-A /eth-storage/vlan* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example creates a named VLAN for fabric interconnect A, names the VLAN, assigns the VLAN ID, makes this VLAN the secondary VLAN, associates the secondary VLAN with the primary VLAN, and commits the transaction:

```
UCS-A# scope eth-storage
UCS-A /eth-storage # create vlan isovlan501 501
UCS-A /eth-storage/vlan* # set sharing isolated
UCS-A /eth-storage/vlan* # set pubnwname primaryvlan500
UCS-A /eth-storage/vlan* # commit-buffer
UCS-A /eth-storage/vlan #  #
```

Community VLANs

Cisco UCS Manager supports Community VLANs in UCS Fabric Interconnects. Community ports communicate with each other and with promiscuous ports. Community ports have Layer 2 isolation from all other ports in other communities, or isolated ports within the PVLAN. Broadcasts are transmitted between the community ports associated with the PVLAN only and the other promiscuous ports. A promiscuous port can communicate with all interfaces, including the isolated and community ports within a PVLAN.

Creating a Community VLAN

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**.	Enters Ethernet uplink mode.
Step 2	UCS-A# /eth-uplink/ # **create vlan** *ID* .	Create a VLAN with the specified VLAN ID. **Note** VLAN with IDs from 1002 to 1005 are reserved for NX-OS in Creating a Community VLAN and Cisco UCS 6500 Series FI.
Step 3	UCS-A# /eth-uplink/ vlan # **set sharing** *Type* .	Specifies the vlan type.
Step 4	UCS-A# /eth-uplink/ vlan # **set pubnwname** *Name* .	Specifies the primary vlan association.
Step 5	UCS-A# /eth-uplink/ vlan # **commit-buffer**.	Commits the transaction to the system configuration.

Example

The following example shows how to create a Community VLAN:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create vlan vlan203 203
UCS-A /eth-uplink/vlan* # set sharing community
UCS-A /eth-uplink/vlan* # set pubname vlan200
UCS-A /eth-uplink/vlan* # commit-buffer
UCS-A /eth-uplink/vlan* # exit
UCS-A /vlan-group #
```

Viewing Community VLANS

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters Cisco UCS Manager organization.
Step 2	UCS-A /org # **show vlan**	Displays the available groups in the organization.

Example

The following example shows the available VLAN groups in the root org:

```
UCS-A# scope org
UCS-A# /org/# show vlan
VLAN Group:

    Name         VLAN ID         Fabric ID     Native VLAN    Sharing Type    Primary Vlan
   ---------------------------------------------------------------------------------------

    vlan100      100             Dual          No             Primary         vlan100
    vlan100      101             Dual          No             Isolated        vlan100
    vlan100      203             Dual          No             Community       vlan200
```

Allowing Community VLANs on vNICs

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters the organization mode for the specified organization. To enter the root organization mode, enter **/** as the *org-name*.
Step 2	UCS-A /org # **scope service-profile** *profile-name*	Commits the transaction to the system configuration.
Step 3	UCS-A /org/service-profile # **scope vnic** *vnic-name*	Enters command mode for the specified vNIC.
Step 4	UCS-A /org/service-profile/vnic # **create eth-if** *community-vlan-name*	Allows the community VLAN to access the specified vNIC.
Step 5	UCS-A /org/service-profile/vnic # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to assign the community VLAN cVLAN101 to the vNIC vnic_1 and commits the transaction.

```
UCS-A# scope org /
UCS-A /org # scope service-profile GSP1
UCS-A /org/service-profile # scope vnic vnic_1
UCS-A /org/service-profile/vnic # create eth-if cVLAN101
UCS-A /org/service-profile/vnic* # commit-buffer
```

Allowing PVLAN on Promiscuous Access or Trunk Port

For a promiscuous access port, the isolated and community VLANs must be associated to the same primary VLAN.

For a promiscuous trunk port, isolated and community VLANs belonging to different primary VLANs are allowed, as well as regular VLANs.

Procedure

	Command or Action	Purpose
Step 1	UCS-A # **scope eth-storage**	Enters Ethernet storage mode.
Step 2	UCS-A /eth-storage # **scope vlan** *iso-vlan-name*	Enters the specified isolated VLAN.
Step 3	UCS-A /eth-storage/vlan # **create member-port** *fabric slot- num port- num*	Creates the member port for the specified fabric, assigns the slot number and port number, and enters member port configuration scope.
Step 4	UCS-A /eth-storage/vlan/member-port # **exit**	Returns to VLAN mode.
Step 5	UCS-A /eth-storage/vlan # **exit**	Returns to Ethernet storage mode.
Step 6	UCS-A /eth-storage # **scope vlan** *comm-vlan-name*	Enters the specified community VLAN.
Step 7	UCS-A /eth-storage/vlan # **create member-port** *fabric slot- num port- num*	Creates the member port for the specified fabric, assigns the slot number and port number, and enters member port configuration scope.
Step 8	UCS-A /eth-storage/vlan/member-port # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to assign the isolated and community associated with the same primary VLAN to the same appliance port and commits the transaction.

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope vlan isovlan501
UCS-A /eth-storage/vlan # create member-port a 1 2
```

```
UCS-A /eth-storage/vlan/member-port* # exit
UCS-A /eth-storage/vlan* # exit
UCS-A /eth-storage* # scope vlan cvlan502
UCS-A /eth-storage/vlan* # create member-port a 1 2
UCS-A /eth-storage/vlan/member-port* # commit-buffer
UCS-A /eth-storage/vlan/member-port #
```

Deleting a Community VLAN

If Cisco UCS Manager includes a named VLAN with the same VLAN ID as the one you delete, the VLAN is not removed from the fabric interconnect configuration until all named VLANs with that ID are deleted.

If you are deleting a private primary VLAN, ensure that you reassign the secondary VLANs to another working primary VLAN.

Before you begin

Before you delete a VLAN from a fabric interconnect, ensure that the VLAN was removed from all vNICs and vNIC templates.

Note If you delete a VLAN that is assigned to a vNIC or vNIC template, the vNIC might allow that VLAN to flap.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**	Enters Ethernet uplink mode.
Step 2	(Optional) UCS-A /eth-uplink # **scope fabric**{**a** | **b**}	Enters Ethernet uplink fabric mode. Use this command when you want to delete a named VLAN only from the specified fabric (a or b).
Step 3	UCS-A /eth-uplink # **delete community vlan** *vlan-name*	Deletes the specified community VLAN.
Step 4	UCS-A /eth-uplink # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example deletes a Community VLAN and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # delete commnity vlan vlan203
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink #
```

Viewing the VLAN Port Count

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	Enters fabric interconnect mode for the specified fabric interconnect.
Step 2	UCS-A /fabric-interconnect # **show vlan-port-count**	Displays the VLAN port count.

Example

The following example displays the VLAN port count for fabric interconnect A:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show vlan-port-count

VLAN-Port Count:
VLAN-Port Limit     Access VLAN-Port Count     Border VLAN-Port Count     Alloc Status
----------               ---------------            ----------------          ----------
6000                           3                          0                     Available
```

VLAN Port Count Optimization

VLAN port count optimization enables mapping the state of multiple VLANs into a single internal state. When you enable the VLAN port count optimization, Cisco UCS Manager logically groups VLANs based on the port VLAN membership. This grouping increases the port VLAN count limit. VLAN port count optimization also compresses the VLAN state and reduces the CPU load on the fabric interconnect. This reduction in the CPU load enables you to deploy more VLANs over more vNICs. Optimizing VLAN port count does not change any of the existing VLAN configuration on the vNICs.

VLAN port count optimization is disabled by default. You can enable or disable the option based on your requirements.

Important

- Enabling VLAN port count optimization increases the number of available VLAN ports for use. If the port VLAN count exceeds the maximum number of VLANs in a non-optimized state, you cannot disable the VLAN port count optimization.
- On the Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 Series Fabric Interconnects and Cisco UCS 6400 Series Fabric Interconnect, the VLAN port count optimization is performed when the PV count exceeds 16000.

When the Cisco UCS 6400 Series Fabric Interconnect is in Ethernet switching mode:

- The FI does not support **VLAN Port Count Optimization Enabled**

- The FI supports 16000 PVs, similar to EHM mode, when **VLAN Port Count Optimization** is **Disabled**.

The following table illustrates the PV Count with VLAN port count optimization enabled and disabled:.

	Cisco UCS 6300 Series FI	Cisco UCS 6400 Series FI	Cisco UCS 6500 Series FI (6536 FI)	Cisco UCS Fabric Interconnects 9108 100G (UCS X-Series Direct/UCSX-S9108-100G)
PV Count with VLAN Port Count Optimization Disabled	16000	16000	16000	16000
PV Count with VLAN Port Count Optimization Enabled	64000	108000	108000	108000

Enabling Port VLAN Count Optimization

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**	Enters Ethernet uplink mode.
Step 2	UCS-A /eth-uplink# **show detail**	Displays the fabric port-channel vHBA reset configuration.
Step 3	UCS-A /eth-uplink* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows the fabric port-channel vHBA reset configuration:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # show detail
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink#

Ethernet Uplink:
Mode: End Host
MAC Table Aging Time (dd:hh:mm:ss): Mode Default
VLAN Port Count Optimization: Disabled
Fabric Port Channel vHBA reset: Disabled
service for unsupported transceivers: Disabled
```

Disabling Port VLAN Count Optimization

If you have more Port VLAN count than that is allowed in the non port VLAN port count optimization state, you cannot disable the optimization.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**	Enters Ethernet uplink mode.
Step 2	UCS-A /eth-uplink# **set vlan-port-count-optimization disable**	Disables the port VLAN count optimization.
Step 3	UCS-A /eth-uplink # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to disable VLAN port count optimization:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # set vlan-port-count-optimization disable
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink#
```

Viewing the Port VLAN Count Optimization Groups

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**	Enters Ethernet uplink mode.
Step 2	UCS-A /eth-uplink# **show vlan-port-count-optimization group**	Displays the vlan for port VLAN count optimization groups.

Example

The following example shows port VLAN count optimization group in fabric a and b:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # show vlan-port-count-optimization group
VLAN Port Count Optimization Group:
    Fabric ID  Group ID   VLAN ID
    --------   -------    -------
    A          5          6
    A          5          7
    A          5          8
    B          10         100
    B          10         101
```

VLAN Groups

VLAN groups allow you to group VLANs on Ethernet uplink ports, by function or by VLANs that belong to a specific network. You can define VLAN membership and apply the membership to multiple Ethernet uplink ports on the fabric interconnect.

Note Cisco UCS Manager supports a maximum of 200 VLAN Groups. If Cisco UCS Manager determines that you create more than 200 VLAN groups, the system disables VLAN compression.

You can configure inband and out-of-band (OOB) VLAN groups to use to access the Cisco Integrated Management Interface (CIMC) on blade and rack servers. Cisco UCS Manager supports OOB IPv4 and inband IPv4 and IPv6 VLAN groups for use with the uplink interfaces or uplink port channels.

Note Inband Management is not supported on VLAN 2 or VLAN 3.

After you assign a VLAN to a VLAN group, any changes to the VLAN group are applied to all Ethernet uplink ports that are configured with the VLAN group. The VLAN group also enables you to identify VLAN overlaps between disjoint VLANs.

You can configure uplink ports under a VLAN group. When you configure an uplink port for a VLAN group, that uplink port will support all the VLANs that are part of the associated VLAN groups and individual VLANs that are associated with the uplink using LAN Uplinks Manager, if any. Further, any uplink that is not selected for association with that VLAN group will stop supporting the VLANs that are part of that VLAN group.

You can create VLAN groups from the **LAN Cloud** or from the **LAN Uplinks Manager**.

Creating a VLAN Group

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**.	Enters Ethernet uplink mode. The VLAN Group name is case sensitive.
Step 2	UCS-A# /eth-uplink/ #**create vlan-group***Name* .	Create a VLAN group with the specified name. This name can be between 1 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Step 3	UCS-A# /eth-uplink/ vlan-group#**create member-vlan***ID* .	Adds the specified VLANs to the created VLAN group.

	Command or Action	Purpose
Step 4	UCS-A# /eth-uplink/vlan-group #**create member-port** [member-port-channel] .	Assigns the uplink Ethernet ports to the VLAN group.
Step 5	UCS-A#/vlan-group* # **commit-buffer**.	Commits the transaction to the system configuration.

Example

The following example shows how to create a VLAN group:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create vlan-group eng
UCS-A /eth-uplink/vlan-group* # create member-vlan 3
UCS-A /eth-uplink/vlan-group* # commit-buffer
UCS-A /vlan-group #
```

Creating an Inband VLAN Group

Configure inband VLAN groups to provide access to remote users via an inband service profile.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth uplink**	Enters Ethernet uplink configuration mode.
Step 2	UCS-A /eth-uplink # **create vlan-group** *inband-vlan-name*	Creates a VLAN group with the specified name and enters VLAN group configuration mode.
Step 3	UCS-A /eth-uplink/vlan-group # **create member-vlan***inband-vlan-nameinband-vlan-id*	Adds the specified VLAN to the VLAN group and enters VLAN group member configuration mode.
Step 4	UCS-A /eth-uplink/vlan-group/member-vlan # **exit**	Exits VLAN group member configuration mode.
Step 5	UCS-A /eth-uplink/vlan-group # **create member-port***fabricslot-numport-num*	Creates the member port for the specified fabric, assigns the slot number, and port number and enters member port configuration.
Step 6	UCS-A /eth-uplink/vlan-group/member-port # **commit-buffer**	Commits the transaction.

Example

The example below creates a VLAN group named inband-vlan-group, creates a member of the group named Inband_VLAN and assigns VLAN ID 888, creates member ports for Fabric A and Fabric B, and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create vlan-group inband-vlan-group
```

```
UCS-A /eth-uplink/vlan-group* # create member-vlan Inband_VLAN 888
UCS-A /eth-uplink/vlan-group/member-vlan* # exit
UCS-A /eth-uplink/vlan-group* # create member-port a 1 23
UCS-A /eth-uplink/vlan-group/member-port* # exit
UCS-A /eth-uplink/vlan-group* # create member-port b 1 23
UCS-A /eth-uplink/vlan-group/member-port* # commit-buffer
UCS-A /eth-uplink/vlan-group/member-port # exit
UCS-A /eth-uplink/vlan-group # exit
```

What to do next

Assign the inband VLAN group to an inband service profile.

Viewing VLAN Groups

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters Cisco UCS Manager organization.
Step 2	UCS-A /org # **show vlan-group**	Displays the available groups in the organization.

Example

The following example shows the available VLAN groups in the root org:

```
UCS-A# scope org
UCS-A# /org/# show vlan-group
VLAN Group:
    Name
    ----
    eng
    hr
    finance
```

Deleting a VLAN Group

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**.	Enters Ethernet uplink mode.
Step 2	UCS-A# /eth-uplink/ #**delete vlan-group***Name* .	Deletes the specified VLAN group.
Step 3	UCS-A#/eth-uplink* # **commit-buffer**.	Commits the transaction to the system configuration.

Example

The following example shows how to delete a VLAN group:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # delete vlan-group eng
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink #
```

Modifying the Reserved VLAN

This task describes how to modify the reserved VLAN ID. Modifying the reserved VLAN makes transitioning from Cisco UCS 6200 Series Fabric Interconnects to the Cisco UCS 6454 Fabric Interconnect more flexible with preexisting network configurations. The reserved VLAN block is configurable by assigning a contiguous block of 128 unused VLANs, rather than reconfiguring the currently existing VLANs that conflict with the default range. For example, if the reserved VLAN is changed to 3912, then the new VLAN block range spans 3912 to 4039. You can select any contiguous block of 128 VLAN IDs, with the start ID ranging from 2 to 3915. Changing the reserved VLAN requires a reload of the 6454 Fabric Interconnect for the new values to take effect.

For Cisco UCS 6500 FI Series, VLAN IDs from 1002 to 1005 are reserved for NX-OS.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**.	Enters Ethernet uplink mode.
Step 2	UCS-A# /eth-uplink/ #**show reserved-vlan** .	This displays the reserved VLAN IDs.
Step 3	UCS-A# /eth-uplink/ #**scope reserved-vlan**.	Enters reserved VLAN ID specification mode.
Step 4	UCS-A# /eth-uplink/reserved-vlan #**set start-vlan-id** [vlan-id] .	Assigns the new reserved VLAN starting ID. The reserved VLAN range ID can be specified from 2-3915.
Step 5	UCS-A# /eth-uplink/reserved-vlan* # **commit-buffer**.	Commits the transaction to the system configuration.

Example

The following example shows how to modify the reserved VLAN ID:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # show reserved-vlan
UCS-A /eth-uplink/ # scope reserved-vlan
UCS-A /eth-uplink/reserved-vlan # set start-vlan-id 3912
UCS-A /eth-uplink/reserved-vlan/* # commit-buffer
```

VLAN Permissions

VLAN permissions restrict access to VLANs based on specified organizations and on the service profile organizations to which the VLANs belong. VLAN permissions also restrict the set of VLANs that you can assign to service profile vNICs. VLAN permissions is an optional feature and is disabled by default. You can enable or disable the feature based on your requirements. If you disable the feature, all of the VLANs are globally accessible to all organizations.

Note If you enable the org permission in **LAN** > **LAN Cloud** > **Global Policies** > **Org Permissions**, when you create a VLAN, the **Permitted Orgs for VLAN(s)** option displays in the **Create VLANs** dialog box. If you do not enable the **Org Permissions**, the **Permitted Orgs for VLAN(s)** option does not display.

Enabling the org permission allows you to specify the organizations for the VLAN. When you specify the organizations, the VLAN becomes available to that specific organization and all of the sub organizations below the structure. Users from other organizations cannot access this VLAN. You can also modify the VLAN permission anytime based on changes to your VLAN access requirements.

Caution When you assign the VLAN org permission to an organization at the root level, all sub organizations can access the VLANs. After assigning the org permission at the root level, and you change the permission for a VLAN that belongs to a sub organization, that VLAN becomes unavailable to the root level organization.

Creating VLAN Permissions

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org**.	Enters the Cisco UCS Manager VLAN organization.
Step 2	UCS-A# /org/ #**create vlan-permit***VLAN permission name*.	Creates the specified VLAN permission and assigns VLAN access permission to the organization.
Step 3	UCS-A#/org* # **commit-buffer**.	Commits the transaction to the system configuration.

Example

The following example shows how to create a VLAN permission for an organization:

```
UCS-A# scope org
UCS-A /org # create vlan-permit dev
UCS-A /org* # commit-buffer
UCS-A /org #
```

Viewing VLAN Permissions

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters Cisco UCS Manager organization.
Step 2	UCS-A /org # **show vlan-permit**	Displays the available permissions in the organization.

Example

The following example shows the VLAN groups that have permission to access this VLAN:

```
UCS-A# scope org
UCS-A# /org/# show vlan-permit
VLAN Group:
    Name
    ----
    eng
    hr
    finance
```

Deleting a VLAN Permission

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org**.	Enters the Cisco UCS Manager VLAN organization.
Step 2	UCS-A# /org/ #**delete vlan-permit***VLAN permission name*.	Deletes the access permission to the VLAN.
Step 3	UCS-A#/org* # **commit-buffer**.	Commits the transaction to the system configuration.

Example

The following example shows how to delete a VLAN permission from an organization:

```
UCS-A# scope org
UCS-A /org # delete vlan-permit dev
UCS-A /org* # commit-buffer
UCS-A /org #
```

Fabric Port-Channel vHBA

A virtual host bus adapter (vHBA) logically connects a virtual machine to a virtual interface on the fabric interconnect and allows the virtual machine to send and receive traffic through that interface. This is currently accomplished by using the fibre channel modes (end-host mode/swtich mode).

The port-channel operations that involves addition or removal of a member link between fabric interconnect and I/O Module (IOM). Such operations may result in a long I/O pause or connection drop from virtual machines to its targets and require a vHBA reset support

With the fabric port-channel vHBA reset is set to enabled, when the Cisco UCS IOM port-channel membership changes, the fabric interconnect sends a Registered State Change Notification (RSCN) packet to each vhba configured via that Cisco UCS IOM. The RSCN enables the virtual interface card (VIC) or VIC Driver to reset the fabric port-channel vHBA and to restore the connectivity.

By default, the fabric port-channel vHBA reset is set to disabled. This configuration supports additional bandwidth and provides greater resilience.

Important The option fabric port-channel vHBA is currently supported only on Cisco UCS 6400 series Fabric Interconnects.

Enabling Fabric Port Channel vHBA reset

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**	Enters Ethernet uplink mode.
Step 2	UCS-A /eth-uplink# **set fabric-pc-vhba-reset enabled**	Sets the fabric port-channel vHBA reset state as enabled.
Step 3	UCS-A /eth-uplink* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to enable fabric port-channel vHBA reset:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # set fabric-pc-vhba-reset enabled
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink#
```

Disabling fabric port channel vHBA reset

You can disable the fabric port-channel vHBA reset.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**	Enters Ethernet uplink mode.
Step 2	UCS-A /eth-uplink# **set fabric-pc-vhba-reset disabled**	Sets the fabric port-channel vHBA reset state as disabled. This is the default state.
Step 3	UCS-A /eth-uplink # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to disable the fabric port-channel vHBA reset:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # set fabric-pc-vhba-reset disabled
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink#
```

Viewing the Fabric Port Channel vHBA Reset

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**	Enters Ethernet uplink mode.
Step 2	UCS-A /eth-uplink# **show detail**	Displays the fabric port-channel vHBA reset configuration.

Example

The following example shows the fabric port-channel vHBA reset configuration:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # show detail

Ethernet Uplink:
    Mode: End Host
    MAC Table Aging Time (dd:hh:mm:ss): Mode Default
    VLAN Port Count Optimization: Disabled
    Fabric Port Channel vHBA reset: Disabled
    service for unsupported transceivers: Disabled
```

VIC QinQ Tunneling

Starting with release 4.3(2a), Cisco UCS Manager introduces support for VIC Q-in-Q tunneling configuration. A Q-in-Q (802.1Q-in-802.1Q) tunnel allows to segregate the traffic in the infrastructure and helps to expand the VLAN space through the addition of 802.1Q tag to 802.1Q-tagged packets.

To configure VIC QinQ Tunneling, ensure **Q-in-Q Forwarding** is enabled. For more information, see Q-in-Q Forwarding.

To know more about supported combinations and limitations of VIC QinQ Tunneling: see VIC QinQ Tunneling - Supported Combinations and Limitations, on page 39.

Enabling and Managing QinQ

Enabling QinQ on a vNIC of a Service Profile

To enable QinQ on a vNIC in a service profile, do the following:

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters root organization mode.
Step 2	UCS-A /org **scope service-profile profile name**	Enters service-profile specified.
Step 3	UCS-A /org **scope vnic vnic 02**	Enters command mode for the specified vNIC.
Step 4	UCS-A /org/service-profile/vnic **Set QinQ** {**enabled** | **disabled** } **enabled**	QinQ is enabled on the specified vNIC *vnic 02*. **Note** QinQ VLAN selection on a vNIC is considered only when *Set QinQ* is enabled. For more information, see Adding a VLAN on a vNIC of a Service Profile, on page 42.
Step 5	UCS-A /org/service profile/vnic/ **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to set QinQ on the vNIC17 in the service profile SP3 and commits the transaction:

```
UCS-A# scope org
UCS-A /org # scope service-profile SP3
UCS-A /org/service-profile # scope vnic vnic17
UCS-A /org/service-profile/vnic* #Set QinQ Enabled
UCS-A /org/service-profile/vnic* #commit-buffer
UCS-A /org/service-profile/vnic #
```

Disabling QinQ on a vNIC of a Service Profile

To disable QinQ on a vNIC of a service profile, do the following:

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters root organization mode.
Step 2	UCS-A /org **scope service-profile profile name**	Enters service-profile specified.
Step 3	UCS-A /org **scope vnic vnic 01**	Enters command mode for the specified vNIC *vnic 01*.
Step 4	UCS-A /org/service-profile/vnic **Set QinQ** {**enabled** | **disabled** } **disabled**	QinQ is disabled on the specified vNIC. **Note** QinQ VLAN selection on a vNIC is considered only when QinQ is enabled. Hence, ensure to re-enable QinQ VLAN when required. For more information, see Enabling QinQ on a vNIC of a Service Profile, on page 33.
Step 5	UCS-A /org/service profile/vnic/ **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to disable *QinQ VLAN* on the *vNIC 33* in the service profile *SP1* and commits the transaction:

```
UCS-A# scope org
UCS-A /org # scope service-profile SP1
UCS-A /org/service-profile # scope vnic vnic 33
UCS-A /org/service-profile/vnic* #QinQ Offload disabled
UCS-A /org/service-profile/vnic* #commit-buffer
UCS-A /org/service-profile/vnic # show detail
------------------
Vnic:
Name: vnic 33
Type: Initial Template
Fabric ID: A
Target: Adapter
Host Interface Ethernet MTU: 1500
CDN Source: vNIC Name
Ethernet Interface Admin CDN Name:
MAC Pool:
Oper MAC Pool:
Pin Group:
QoS Policy:
Oper QoS Policy:
Network Control Policy:
Oper Network Control Policy: org-root/nwctrl-default
Stats Policy: default
Oper Stats Policy: org-root/thr-policy-default
```

```
Policy Owner: Local
Redundancy Type: No Redundancy
Redundancy Peer Template Name:
Oper Redundancy Peer Template Name:
QinQ Offload: Disabled
```

Enabling QinQ on a vNIC of LAN Connectivity Policy

To enable QinQ on a vNIC through LAN Connectivity Policy, do the following:

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters root organization mode.
Step 2	UCS-A /org **scope lann conn policy LAN Policy 12**	Enters LAN Connectivity Policy **LAN Policy 12**.
Step 3	UCS-A /org **scope vnic vnic 01**	Enters command mode of the vNIC **vnic 01**.
Step 4	UCS-A /org/lann conn pol/vnic **Set QinQ** {**enabled** | **disabled** } **enabled**	QinQ is enabled on the specified vNIC. **Note** QinQ VLAN selection on a vNIC is considered only when *Set QinQ* is enabled. For more information, see Adding a VLAN on a vNIC of LAN Connectivity Policy, on page 42.
Step 5	UCS-A /org/lann conn pol/vnic/ **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to set QinQ on the vNIC17 in the *LAN Connectivity Policy 22* and commits the transaction:

```
UCS-A# scope org
UCS-A /org # scope lann conn policy 22
UCS-A /org/lann conn pol # scope vnic vnic17
UCS-A /org/lann conn pol/vnic* #Set QinQ Enabled
UCS-A /org/lann conn pol/vnic* #commit-buffer
UCS-A /org/lann conn pol/vnic #
```

Disabling QinQ on a vNIC of LAN Connectivity Policy

To disable QinQ VLAN on a vNIC through LAN Connectivity Policy, do the following:

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters root organization mode.
Step 2	UCS-A /org **scope lann conn policy LAN Policy 12**	Enters Lan Connectivity Policy **LAN Policy 12**.
Step 3	UCS-A /org/lann conn pol **scope vnic vnic 01**	Enters command mode for the specified vNIC.
Step 4	UCS-A /org/lann conn pol/vnic **Set QinQ** {**enabled** | **disabled** } **disabled**	QinQ is disabled on the specified vNIC. **Note** QinQ VLAN selection on a vNIC is considered only when QinQ is enabled. Hence, ensure to re-enable QinQ when required. For more information, see Enabling QinQ on a vNIC of LAN Connectivity Policy, on page 35.
Step 5	UCS-A /org/lann conn pol/vnic/ **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to disable QinQ on the vNIC 33 in the Lan Connectivity Policy *LP1* and commits the transaction:

```
UCS-A# scope org
UCS-A /org # scope lann conn policy LP1
UCS-A /org/lann conn pol # scope vnic vnic 33
UCS-A /org/lann conn pol/vnic* #QinQ Offload disabled
UCS-A /org/lann conn pol/vnic* #commit-buffer
UCS-A /org/lann conn pol/vnic # show detail
------------------
Vnic:
Name: vnic 33
Type: Initial Template
Fabric ID: A
Target: Adapter
Host Interface Ethernet MTU: 1500
CDN Source: vNIC Name
Ethernet Interface Admin CDN Name:
MAC Pool:
Oper MAC Pool:
Pin Group:
QoS Policy:
Oper QoS Policy:
Network Control Policy:
Oper Network Control Policy: org-root/nwctrl-default
Stats Policy: default
Oper Stats Policy: org-root/thr-policy-default
Policy Owner: Local
Redundancy Type: No Redundancy
Redundancy Peer Template Name:
Oper Redundancy Peer Template Name:
QinQ Offload: Disabled
```

Enabling QinQ on a vNIC Template

To enable QinQ on a specified vNIC template, do the following:

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters root organization mode.
Step 2	UCS-A /org **scope vnic-templ 22**	Enters command mode for the specified vNIC template.
Step 3	UCS-A /org/vnic-templ/eth-if # **Set QinQ** {**enabled** | **disabled** } **enabled**	QinQ is enabled on the specified vNIC template. **Note** QinQ VLAN selection on a vNIC is considered only when *Set QinQ* is enabled. For more information, see Adding a VLAN on a vNIC Template, on page 41.
Step 4	UCS-A /org/vnic-templ/eth-if # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example adds a VLAN 10 on the vNIC template 01, sets the VLAN as a native VLAN, enables QinQ on the vNIC, and commits the transaction:

```
UCS-A# scope org
UCS-A /org # scope vnic-templ 01
UCS-A /org/vnic-templ/eth-if# set qinq enabled
UCS-A /org/service-profile/eth-if* #commit-buffer
UCS-A /org/vnic-templ/eth-if
```

Disabling QinQ on a vNIC Template

To disable QinQ on a specified vNIC template, do the following:

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters root organization mode.
Step 2	UCS-A /org **scope vnic-templ 22**	Enters command mode for the specified vNIC template.
Step 3	UCS-A /org/vnic-templ/eth-if # **Set QinQ** {**enabled** | **disabled** } **disabled**	QinQ is disabled on the specified vNIC template.

	Command or Action	Purpose
		Note QinQ VLAN selection on a vNIC is considered only when QinQ is enabled. Hence, ensure to re-enable QinQ when required. For more information, see Enabling QinQ on a vNIC Template, on page 37.
Step 4	UCS-A /org/vnic-templ/eth-if # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to disable QinQ on the vNIC template 01 and commits the transaction:

```
UCS-A# scope org
UCS-A /org # scope vnic-templ 01
UCS-A /org/vnic-templ/eth-if# set qinq disabled
UCS-A /org/service-profile/ethi-if* #commit-buffer
UCS-A /org/lann conn pol/vnic # show detail
------------------
Vnic:
Name: vnic 33
Type: Initial Template
Fabric ID: A
Target: Adapter
Host Interface Ethernet MTU: 1500
CDN Source: vNIC Name
Ethernet Interface Admin CDN Name:
MAC Pool:
Oper MAC Pool:
Pin Group:
QoS Policy:
Oper QoS Policy:
Network Control Policy:
Oper Network Control Policy: org-root/nwctrl-default
Stats Policy: default
Oper Stats Policy: org-root/thr-policy-default
Policy Owner: Local
Redundancy Type: No Redundancy
Redundancy Peer Template Name:
Oper Redundancy Peer Template Name:
QinQ Offload: Disabled
```

Viewing QinQ

To view QinQ VLAN on vNIC of a service profile, do the following:

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters root organization mode.

	Command or Action	Purpose
Step 2	UCS-A /org **scope service-profile profile name**	Enters service-profile specified.
Step 3	UCS-A /org **scope vnic vnic 01**	Enters command mode for the specified vNIC.
Step 4	UCS-A /org/service-profile/vnic # **show detail**	Displays the details including QinQ configuration status on the vNIC.

Example

The following example shows how to view the QinQ configuration status on vNIC through service profile. The example output displays QinQ Offload status as Enabled:

```
UCS-A# scope org
UCS-A /org # scope service-profile SP1
UCS-A /org/service-profile # scope vnic vnic 01
UCS-A /org/service-profile/vnic* #Show detail
UCS-A /org/service-profile/vnic #
-----------------------------------------
Vnic:
Name: vnic01
Type: Initial Template
Fabric ID: A
Target: Adapter
Host Interface Ethernet MTU: 1500
CDN Source: vNIC Name
Ethernet Interface Admin CDN Name:
MAC Pool:
Oper MAC Pool:
Pin Group:
QoS Policy:
Oper QoS Policy:
Network Control Policy:
Oper Network Control Policy: org-root/nwctrl-default
Stats Policy: default
Oper Stats Policy: org-root/thr-policy-default
Policy Owner: Local
Redundancy Type: No Redundancy
Redundancy Peer Template Name:
Oper Redundancy Peer Template Name:
QinQ Offload: Enabled
```

Important You can use the **show detail** command to view the QinQ status on a vNIC Template and on a vNIC in a Lan Connectivity Policy.

VIC QinQ Tunneling - Supported Combinations and Limitations

Following are the supported combinations for VIC QinQ Tunneling:

- QinQ VLAN selection is considered only when the **Enable QinQ** check box is selected on a vNIC Interface.

- QinQ Configuration supports a maximum of two VLANs on a vNIC Interface. A QinQ VLAN can be a Native or a non-Native VLAN. You can configure a Native VLAN and a Non-Native VLAN as a QinQ VLAN on the vNIC.

  When using the Native VLAN as QinQ VLAN, no additional VLAN can be configured on the vNIC.

- For Cisco UCS VIC 15000 series adapters, QinQ and Geneve Offload can be enabled on a vNIC Interface.

Following are the limitations of VIC QinQ Tunneling:

- QinQ configuration on a vNIC Interface is not supported on Cisco UCS VIC 1300 series adapters.
- The default VLAN (VLAN ID: 1) is not supported as a QinQ VLAN on a vNIC Interface.
- When a Native VLAN and a QinQ VLAN are configured on a vNIC Interface, a new VLAN configuration is not supported and results in Server Profile association failures when selected. To accommodate a new VLAN, either the Native VLAN or QinQ VLAN must be removed.
- When the QinQ VLAN is the same as the Native VLAN on a vNIC Interface, a new VLAN configuration is not supported and results in Server Profile association failures when selected. To accommodate a new VLAN, either the Native VLAN or QinQ VLAN must be modified.
- For Cisco UCS VIC 1400, 14000, and 15000 series adapters, LAN (or PXE) Boot and QinQ cannot be configured on a vNIC interface and result in configuration failures when enabled.
- For Cisco UCS VIC 1400, 14000, and 15000 series adapters, iSCSI Boot and QinQ cannot be configured on a vNIC interface and result in configuration failures when enabled.
- For Cisco UCS VIC 1400 and 14000 series adapters, QinQ and Geneve Offload cannot be configured on a vNIC interface and result in configuration failures when enabled.
- For Cisco UCS VIC 1400, 14000, and 15000 series adapters, QinQ and VMMQ cannot be configured on a vNIC interface and result in configuration failures when enabled.
- For Cisco UCS VIC 1400, 14000, and 15000 series adapters, QinQ and RDMA V2 cannot be configured on a vNIC interface and result in configuration failures when enabled.
- For Cisco UCS 6454, 64108, 6536 Fabric Interconnects, and Cisco UCS Fabric Interconnects 9108 100G, QinQ must be enabled at LAN > Global Policies to support QinQ VLAN on a VIC adapter.
- For Cisco UCS VIC 1400, 14000, and 15000 series adapters, QinQ and SR-IOV cannot be configured on a vNIC interface and result in configuration failures when enabled.
- When the Service Profile is already associated, you cannot enable or disable QinQ on a B-Series server.
- For Cisco UCS 6454, Cisco UCS 64108, Cisco UCS 6536 Fabric Interconnects, and Cisco UCS Fabric Interconnects 9108 100G, QinQ configuration for Fabric Interconnects in Global Policy > LAN Connectivity Policy must be enabled to configure QinQ on a vNIC interface.
- QinQ and usNIC cannot be enabled together on a vNIC interface.
- When VIC QinQ Tunneling is enabled, you cannot downgrade to lower release versions.

Managing VLANs

Adding a VLAN on a vNIC Template

To create a VLAN on a vNIC template, do the following:

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters root organization mode.
Step 2	UCS-A /org # **scope vnic-templ 01**	Enters command mode for the specified vNIC template.
Step 3	UCS-A /org/vnic-templ/eth if # **create eth-if** *vlan 20*	Creates a VLAN on the specified vNIC template. The VLAN name is case sensitive.
Step 4	UCS-A /org/vnic-templ/eth-if # **set default-net** {**yes** | **no** } **yes**	Sets the VLAN 10 as a Native VLAN on the vNIC template.
Step 5	UCS-A /org/vnic-templ/eth-if # **set qinq-vlan** {**yes** | **no** } **yes**	Enables VIC QinQ Tunneling on the vNIC Template. The supported QinQ VLAN ID range is 2 to 4094. A QinQ VLAN can be a Native or a Non-Native VLAN. You can configure a Native VLAN and a Non-Native VLAN as a QinQ VLAN on the vNIC. When using the Native VLAN as QinQ VLAN, no additional VLAN can be configured on the vNIC. **Note** VIC QinQ Tunneling is considered only when QinQ is enabled. For more information, see Enabling QinQ on a vNIC Template, on page 37.
Step 6	UCS-A /org/vnic-templ/vnic/eth-if # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example adds a VLAN 10 on the vNIC template 01, sets the VLAN as a native VLAN, enables QinQ on the VLAN, and commits the transaction:

```
UCS-A# scope org
UCS-A /org # scope vnic-templ 01
UCS-A /org/vnic-templ# create eth-if VLAN 10
UCS-A /org/vnic-templ/eth-if# set default-net yes
UCS-A /org/vnic-templ/eth-if# set qinq-vlan yes
```

```
UCS-A /org/vnic-templ/eth-if* #commit-buffer
UCS-A /org/vnic-templ/eth-if
```

Adding a VLAN on a vNIC of LAN Connectivity Policy

To add a VLAN on a vNIC of LAN Connectivity Policy, do the following:

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters root organization mode.
Step 2	UCS-A /org # **scope lann conn policy Lan Policy 01**	Enters LAN Connectivity Policy **Lan Policy 01**.
Step 3	UCS-A /org # **scope vnic vnic 11**	Enters command mode for the specified vNIC.
Step 4	UCS-A /org/lann conn policy/vnic **create eth-if** *vlan 10*	Creates a VLAN 10 on the specified vNIC. The VLAN name is case sensitive.
Step 5	UCS-A /org/lann conn policy/vnic/eth-if#/ **set default-net** {**yes** | **no** } **yes**	Sets the VLAN 10 as native VLAN in the service profile.
Step 6	UCS-A /org/lann conn policy/vnic/eth-if/ **set qinq-vlan** {**yes** | **no** } **yes**	Enables VIC QinQ Tunneling on the VLAN in the vNIC. The supported QinQ VLAN ID range is 2 to 4094. QinQ VLAN can be a Native or a Non-Native VLAN. You can configure a Native VLAN and a Non-Native VLAN as a QinQ VLAN on the vNIC. When using the Native VLAN as QinQ VLAN, no additional VLAN can be configured on the vNIC. **Note** VIC QinQ Tunneling is considered only when QinQ is enabled. For more information, see Enabling QinQ on a vNIC of LAN Connectivity Policy, on page 35.
Step 7	UCS-A /org/lann conn policy/vnic/eth-if/ **commit-buffer**	Commits the transaction to the system configuration.

Adding a VLAN on a vNIC of a Service Profile

To add a VLAN on a vNIC through service profile, do the following:

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters root organization mode.
Step 2	UCS-A /org # **scope service-profile profile name**	Enters service-profile named **profile name**
Step 3	UCS-A /org # **scope vnic vnic 01**	Enters command mode for the specified vNIC **vnic 01** .
Step 4	UCS-A /org/service profile/vnic **create eth-if** *vlan 10*	Creates VLAN 10 on the specified vNIC vnic 01. The VLAN name is case sensitive.
Step 5	UCS-A /org/service profile/vnic/eth-if#/ **set default-net** {**yes** | **no** } **yes**	Sets the VLAN 10 as native VLAN in the service profile.
Step 6	UCS-A /org/service profile/vnic/eth-if/ **set qinq-vlan** {**yes** | **no** } **yes**	Enables VIC QinQ Tunneling on the VLAN 10 in the vNIC 01. The supported QinQ VLAN ID range is 2 to 4094. QinQ VLAN can be a Native or a Non-Native VLAN. You can configure a Native VLAN and a Non-Native VLAN as a QinQ VLAN on the vNIC. When using the Native VLAN as QinQ VLAN, no additional VLAN can be configured on the vNIC. **Note** VIC QinQ Tunneling is considered only when QinQ is enabled. For more information, see Enabling QinQ on a vNIC of a Service Profile, on page 33.
Step 7	UCS-A /org/service profile/vnic/eth-if/ **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example creates a VLAN 20 on the vNIC 01 in a service profile, sets the VLAN as a native VLAN, enables QinQ on the VLAN, and commits the transaction:

```
UCS-A# scope org
UCS-A /org # scope service-profile SP1
UCS-A /org/service-profile # scope vnic vnic 01
UCS-A /org/service-profile/vnic # create eth-if VLAN 20
UCS-A /org/service-profile/vnic/eth-if* # set default-net no
UCS-A /org/service-profile/vnic/eth-if* # set qinq vlan yes
UCS-A /org/service-profile/vnic/eth-if* # exit
UCS-A /org/service-profile/vnic* #commit-buffer
UCS-A /org/service-profile/vnic#
```

Deleting a VLAN in a VNIC template

To delete a VLAN on the specified vNIC template, do the following:

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters root organization mode.
Step 2	UCS-A /org # **scope vnic-templ template01**	Enters vNIC template specified.
Step 3	UCS-A /org/vnic-templ/ # **delete eth-if vlan 33**	Deletes the VLAN 33 and its configuration on the specified vNIC template.
Step 4	UCS-A /org/vnic-templ/ # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to delete a VLAN 22 on the vNIC template 37, and commit the transaction:

```
UCS-A# scope org
UCS-A /org # scope vnic-templ template 37
UCS-A /org/vnic-templ/ # delete eth-if vlan 22
UCS-A /org/vnic-templ/ eth-if* # exit
UCS-A /org/vnic-templ* #commit-buffer
UCS-A /org/vnic-templ*
```

Deleting a VLAN on a vNIC of LAN Connectivity Policy

To delete a VLAN on a vNIC of LAN Connectivity Policy, do the following:

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters root organization mode.
Step 2	UCS-A /org # **scope lann conn policy lan policy 01**	Enters LAN Connectivity Policy lan policy 01 specified.
Step 3	UCS-A /org/lann conn policy # **scope vnic vnic 01**	Enters command mode for the specified vNIC *vnic 01*.
Step 4	UCS-A /org/lann conn policy/vnic # **delete eth-if vlan 23**	Deletes the VLAN 23 and its configuration on the specified vNIC.
Step 5	UCS-A /org/lann conn policy/vnic # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to delete a *VLAN 22* on the *vNIC 37* in a LAN Connectivity Policy *01* and commit the transaction:

```
UCS-A# scope org
UCS-A /org # scope lann conn policy Lan Policy 01
UCS-A /org/lann conn policy # scope vnic vnic 37
UCS-A /org/lann conn policy/vnic # delete eth-if VLAN 22
UCS-A /org/lann conn policy/vnic/eth-if* # exit
UCS-A /org/lann conn policy/vnic* #commit-buffer
UCS-A /org/lann conn policy/vnic#
```

Deleting a VLAN on a vNIC of a Service Profile

To delete a VLAN on the specified vNIC in a service profile, do the following:

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters root organization mode.
Step 2	UCS-A /org # **scope service-profile profile name**	Enters service-profile specified.
Step 3	UCS-A /org # **scope vnic vnic 01**	Enters command mode for the specified vNIC.
Step 4	UCS-A /org/service profile/vnic # **delete eth-if vlan 23**	Deletes the VLAN 23 and its configuration on the specified vNIC.
Step 5	UCS-A /org/service profile/vnic # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to delete a VLAN 22 on the vNIC 37 in a service profile SP2 and commit the transaction:

```
UCS-A# scope org
UCS-A /org # scope service-profile SP2
UCS-A /org/service-profile # scope vnic vnic 37
UCS-A /org/service-profile/vnic # delete eth-if VLAN 22
UCS-A /org/service-profile/vnic/eth-if* # exit
UCS-A /org/service-profile/vnic* #commit-buffer
UCS-A /org/service-profile/vnic#
```