VLANs

About VLANs

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

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

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

You can use the Cisco UCS Manager to manage VLANS. You can do the following:

- Configure named VLANs.
- Assign VLANS to an access or trunk port.

- Create, delete and modify VLANs.

Guidelines for Creating, Deleting, and Modifying VLANs

VLANs are numbered from 1 to 4094. All configured ports belong to the default VLAN when you first bring up a switch. The default VLAN (VLAN1) uses only default values. You cannot create, delete, or suspend activity in the default VLAN.

You configure a VLAN by assigning a number to it. You can delete VLANs or move them from the active operational state to the suspended operational state. If you attempt to create a VLAN with an existing VLAN ID, the switch goes into the VLAN submode, but does not create the same VLAN again. Newly created VLANs remain unused until you assign ports to the specific VLAN. All of the ports are assigned to VLAN1 by default. Depending on the range of the VLAN, you can configure the following parameters for VLANs (except for the default VLAN):

- VLAN name
- Shutdown or not shutdown

When you delete a specified VLAN, the ports associated to that VLAN are shut down and no traffic flows. However, the system retains all of the VLAN-to-port mappings for that VLAN. When you re-enable or recreate the specified VLAN, the system automatically re-instates all of the original ports to that VLAN.

If a vLAN group is used on a vNIC and also on a port-channel assigned to an uplink, then you cannot delete and add vLANs in the same transaction. Deleting and adding vLANs in the same transaction causes ENM pinning failure on the vNIC. vNIC configurations are done first and vLAN is deleted from the vNIC and a new vLAN is added, but this vLAN is not yet configured on the uplink. Hence, the transaction causes the pinning failure. You must add and delete a vLAN from a vLAN group in separate transactions.

About the Native VLAN

The native VLAN and the default VLAN are not the same. Native refers to VLAN traffic without an 802.1q header and can be assigned or not. The native VLAN is the only VLAN that is not tagged in a trunk, and the frames are transmitted unchanged.

You can tag everything and not use a native VLAN throughout your network, and the VLAN or devices are reachable because switches use VLAN 1 as the native by default.

The UCS Manager LAN Uplink Manager enables you to configure VLANs and to change the native VLAN setting. Changing the native VLAN setting requires a port flap for the change to take effect; otherwise, the port flap is continuous. When you change the native VLAN, there is a loss of connectivity for approximately 20-40 seconds.

Native VLAN Guidelines

- You can only configure native VLANs on trunk ports.
- You can change the native VLAN on a UCS vNIC; however, the port flaps and can lead to traffic interruptions.
- Cisco recommends using the native VLAN 1 setting to prevent traffic interruptions if using the Cisco Nexus 1000v switches. The native VLAN must be the same for the Nexus 1000v port profiles and your UCS vNIC definition.

- If the native VLAN 1 setting is configured, and traffic routes to an incorrect interface, there is an outage, or the switch interface flaps continuously, there might be incorrect settings in your disjoint layer 2 network configuration.
- Using the native VLAN 1 for management access to all of your devices can potentially cause problems if someone connects another switch on the same VLAN as your management devices.

About the Access and Trunk Ports

Access Ports on a Cisco Switch

Access ports only sends untagged frames and belongs to and carries the traffic of only one VLAN. Traffic is received and sent in native formats with no VLAN tagging. Anything arriving on an access port is assumed to belong to the VLAN assigned to the port.

You can configure a port in access mode and specify the VLAN to carry the traffic for that interface. If you do not configure the VLAN for a port in access mode, or an access port, the interface carries the traffic for the default VLAN, which is VLAN 1. You can change the access port membership in a VLAN by configuring the VLAN. You must create the VLAN before you can assign it as an access VLAN for an access port. If you change the access VLAN on an access port to a VLAN that is not yet created, the UCS Manager shuts down that access port.

If an access port receives a packet with an 802.1Q tag in the header other than the access VLAN value, that port drops the packet without learning its MAC source address.

Trunk Ports on a Cisco Switch

Trunk ports allow multiple VLANs to transport between switches over that trunk link. A trunk port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default port VLAN ID to the trunk port, all untagged traffic travels on the default port VLAN ID for the trunk port, and all untagged traffic is assumed to belong to this VLAN. This VLAN is referred to as the native VLAN ID for a trunk port. The native VLAN ID is the VLAN that carries untagged traffic on trunk ports.

The trunk port sends an egressing packet with a VLAN that is equal to the default port VLAN ID as untagged; all the other egressing packets are tagged by the trunk port. If you do not configure a native VLAN ID, the trunk port uses the default VLAN.

Note Changing the native VLAN on a trunk port, or an access VLAN of an access port flaps the switch interface.

Named VLANs

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

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

You can create more than one named VLAN with the same VLAN ID. For example, if servers that host business services for HR and Finance need to access the same external LAN, you can create VLANs named

HR and Finance with the same VLAN ID. Then, if the network is reconfigured and Finance is assigned to a different LAN, you only have to change the VLAN ID for the named VLAN for Finance.

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

Guidelines for VLAN IDs

Important VLANs with IDs from 4043 to 4047 and from 4094 to 4095 are reserved. You cannot create VLANs with IDs from this range. Until Cisco UCS Manager Release 4.0(1d), VLAN ID 4093 was in the list of reserved VLANs. VLAN 4093 has been removed from the list of reserved VLANs and is available for configuration.

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

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

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

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

The VLAN name is case sensitive.

Private VLANs

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

Isolated and Community VLANs

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

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

Ports on Isolated VLANs

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

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

Guidelines for Uplink Ports

When you create PVLANs, use the following guidelines:

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

Guidelines for VLAN IDs

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

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

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

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

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

The VLAN name is case sensitive.

VLAN Port Limitations

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

Types of Ports Included in the VLAN Port Count

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

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

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

VLAN Port Limit Enforcement

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

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

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

- Fabric interconnect reboot
- Cisco UCS Manager upgrade or downgrade

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

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

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

Configuring Named VLANs

Creating a Named VLAN

In a Cisco UCS domain that is configured for high availability, you can create a named VLAN that is accessible to both fabric interconnects or to only one fabric interconnect.

Important VLANs with IDs from 4043 to 4047 and from 4094 to 4095 are reserved. You cannot create VLANs with IDs from this range. Until Cisco UCS Manager Release 4.0(1d), VLAN ID 4093 was in the list of reserved VLANs. VLAN 4093 has been removed from the list of reserved VLANs and is available for configuration.

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

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

Procedure

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

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

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

Step 4 On the icon bar to the right of the table, click +.

If the + icon is disabled, click an entry in the table to enable it.

Step 5 In the **Create VLANs** dialog box, complete the required fields.

Step 6 If you clicked the **Check Overlap** button, do the following:

a) Click the **Overlapping VLANs** tab and review the fields to verify that the VLAN ID does not overlap with any IDs assigned to existing VLANs.

b) Click the **Overlapping VSANs** tab and review the fields to verify that the VLAN ID does not overlap with any FCoE VLAN IDs assigned to existing VSANs.

c) Click **OK**.

d) If Cisco UCS Manager identified any overlapping VLAN IDs or FCoE VLAN IDs, change the VLAN ID to one that does not overlap with an existing VLAN.

Step 7 Click **OK**.

Cisco UCS Manager adds the VLAN to one of the following **VLANs** nodes:

- The **LAN Cloud** > **VLANs** node for a VLAN accessible to both fabric interconnects.
- The ***Fabric_Interconnect_Name*** > **VLANs** node for a VLAN accessible to only one fabric interconnect.

Deleting a Named VLAN

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

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

Before you begin

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

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

Procedure

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

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

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

Step 4 Click one of the following subtabs, based on the VLAN that you want to delete:

Subtab	Description
All	Displays all VLANs in the Cisco UCS domain.
Dual Mode	Displays the VLANs that are accessible to both fabric interconnects.
Fabric A	Displays the VLANs that are accessible to only fabric interconnect A.
Fabric B	Displays the VLANs that are accessible to only fabric interconnect B.

Step 5 In the table, click the VLAN that you want to delete.

You can use the **Shift** key or **Ctrl** key to select multiple entries.

Step 6 Right-click the highlighted VLAN or VLANs and click **Delete**.

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

Configuring Private VLANs

Creating a Primary VLAN for a Private VLAN

In a Cisco UCS domain that is configured for high availability, you can create a primary VLAN that is accessible to both fabric interconnects or to only one fabric interconnect.

Important VLANs with IDs from 4043 to 4047 and from 4094 to 4095 are reserved. You cannot create VLANs with IDs from this range. Until Cisco UCS Manager Release 4.0(1d), VLAN ID 4093 was in the list of reserved VLANs. VLAN 4093 has been removed from the list of reserved VLANs and is available for configuration.

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

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

Procedure

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

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

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

Step 4 On the icon bar to the right of the table, click +.

If the + icon is disabled, click an entry in the table to enable it.

Step 5 In the **Create VLANs** dialog box, complete the required fields.

Step 6 If you clicked the **Check Overlap** button, do the following:

a) Click the **Overlapping VLANs** tab and review the fields to verify that the VLAN ID does not overlap with any IDs assigned to existing VLANs.

b) Click the **Overlapping VSANs** tab and review the fields to verify that the VLAN ID does not overlap with any FCoE VLAN IDs assigned to existing VSANs.

c) Click **OK**.

d) If Cisco UCS Manager identified any overlapping VLAN IDs or FCoE VLAN IDs, change the VLAN ID to one that does not overlap with an existing VLAN.

Step 7 Click **OK**.

Cisco UCS Manager adds the primary VLAN to one of the following **VLANs** nodes:

- The **LAN Cloud** > **VLANs** node for a primary VLAN accessible to both fabric interconnects.

- The ***Fabric_Interconnect_Name*** > **VLANs** node for a primary VLAN accessible to only one fabric interconnect.

Creating a Secondary VLAN for a Private VLAN

In a Cisco UCS domain that is configured for high availability, you can create a secondary VLAN that is accessible to both fabric interconnects or to only one fabric interconnect.

Important VLANs with IDs from 4043 to 4047 and from 4094 to 4095 are reserved. You cannot create VLANs with IDs from this range. Until Cisco UCS Manager Release 4.0(1d), VLAN ID 4093 was in the list of reserved VLANs. VLAN 4093 has been removed from the list of reserved VLANs and is available for configuration.

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

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

Before you begin

Create the primary VLAN.

Procedure

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

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

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

Step 4 On the icon bar to the right of the table, click +.

If the + icon is disabled, click an entry in the table to enable it.

Step 5 In the **Create VLANs** dialog box, specify the required fields.

Note The multicast policy is associated to the primary VLAN, not the secondary VLAN.

Step 6 If you clicked the **Check Overlap** button, do the following:

a) Click the **Overlapping VLANs** tab and review the fields to verify that the VLAN ID does not overlap with any IDs assigned to existing VLANs.

b) Click the **Overlapping VSANs** tab and review the fields to verify that the VLAN ID does not overlap with any FCoE VLAN IDs assigned to existing VSANs.

c) Click **OK**.

d) If Cisco UCS Manager identified any overlapping VLAN IDs or FCoE VLAN IDs, change the VLAN ID to one that does not overlap with an existing VLAN.

Step 7 Click **OK**.

Cisco UCS Manager adds the primary VLAN to one of the following **VLANs** nodes:

- The **LAN Cloud** > **VLANs** node for a primary VLAN accessible to both fabric interconnects.
- The ***Fabric_Interconnect_Name*** > **VLANs** node for a primary VLAN accessible to only one fabric interconnect.

Community VLANs

Cisco UCS Manager supports Community VLANs in UCS Fabric Interconnects. Community ports communicate with each other and with promiscuous ports. Community ports have Layer 2 isolation from all other ports in other communities. A promiscuous port can communicate with all interfaces.

Creating a Community VLAN

In a Cisco UCS domain configured for high availability, you can create a Community VLAN accessible to both fabric interconnects or to only one fabric interconnect.

Important VLANs with IDs from 4043 to 4047 and from 4094 to 4095 are reserved. You cannot create VLANs with IDs from this range. Until Cisco UCS Manager Release 4.0(1d), VLAN ID 4093 was in the list of reserved VLANs. VLAN 4093 has been removed from the list of reserved VLANs and is available for configuration.

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

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

Procedure

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

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

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

Step 4 On the icon bar to the right of the table, click +.

If the + icon is disabled, click an entry in the table to enable it.

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

Name	Description
VLAN Name/Prefix field	For a single VLAN, this is the VLAN name. For a range of VLANs, this is the prefix that the system uses for each VLAN name. The VLAN name is case sensitive. This name can be between 1 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Multicast Policy drop-down list	The multicast policy associated with this VLAN.
Create Multicast Policy link	Click this link to create a new multicast policy that will be available to all VLANs.
Configuration options	You can choose one of the following: • **Common/Global**—The VLANs apply to both fabrics and use the same configuration parameters in both cases. • **Fabric A**—The VLANs only apply to fabric A. • **Fabric B**—The VLAN only apply to fabric B. • **Both Fabrics Configured Differently**—The VLANs apply to both fabrics, but you can specify different VLAN IDs for each fabric. For upstream disjoint L2 networks, Cisco recommends that you choose **Common/Global** to create VLANs that apply to both fabrics.

Name	Description
VLAN IDs field	To create one VLAN, enter a single numeric ID. To create multiple VLANs, enter individual IDs or ranges of IDs separated by commas. A VLAN ID can: • Be between 1 and 3967 • Be between 4048 and 4093 • Overlap with other VLAN IDs already defined on the system For example, to create six VLANs with the IDs 4, 22, 40, 41, 42, and 43, enter **`4, 22, 40-43`**. **Important** VLANs with IDs from 4043 to 4047 and from 4094 to 4095 are reserved. You cannot create VLANs with IDs from this range. Until Cisco UCS Manager Release 4.0(1d), VLAN ID 4093 was in the list of reserved VLANs. VLAN 4093 has been removed from the list of reserved VLANs and is available for configuration. The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch. VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.
Sharing Type field	Whether this VLAN is subdivided into private or secondary VLANs. This can be one of the following: • **None**—This VLAN does not have any secondary or private VLANs. • **Primary**—This VLAN can have one or more secondary VLANs, as shown in the **Secondary VLANs** area. • **Isolated**—This is a private VLAN. The primary VLAN with which it is associated is shown in the **Primary VLAN** drop-down list.
Primary VLAN drop-down list	If the **Sharing Type** field is set to **Isolated**, this is the primary VLAN associated with the IsolatedVLAN.
Permitted Orgs for VLAN(s)	Select the organization from the list for the VLAN. This VLAN will be available for the organizations that you select.

Name	Description
Check Overlap button	Click this button to determine whether the VLAN ID overlaps with any other IDs on the system.

Step 6 If you clicked the **Check Overlap** button, do the following:

a) Click the **Overlapping VLANs** tab and review the following fields to verify that the VLAN ID does not overlap with any IDs assigned to existing VLANs.

Name	Description
Fabric ID column	This can be one of the following: • **A** • **B** • **Dual**—The component is accessible to either fabric interconnect. This setting applies to virtual LAN and SAN networks created at the system level as opposed to the fabric-interconnect level.
Name column	The name of the VLAN.
VLAN column	The numeric id for the VLAN.
DN column	The full path to the VLAN. Click the link in this column to view the properties for the VLAN.

b) Click the **Overlapping VSANs** tab and review the following fields to verify that the VLAN ID does not overlap with any FCoE VLAN IDs assigned to existing VSANs:

Name	Description
Fabric ID column	This can be one of the following: • **A** • **B** • **Dual**—The component is accessible to either fabric interconnect. This setting applies to virtual LAN and SAN networks created at the system level as opposed to the fabric-interconnect level.
Name column	The name of the VSAN.
ID column	The numeric id for the VSAN.
FCoE VLAN ID column	The unique identifier assigned to the VLAN used for Fibre Channel connections.
DN column	The full path to the VSAN. Click the link in this column to view the properties for the VSAN.

c) Click **OK**.

d) If Cisco UCS Manager identified any overlapping VLAN IDs or FCoE VLAN IDs, change the VLAN ID to one that does not overlap with an existing VLAN.

Step 7 Click **OK**.

Cisco UCS Manager adds the Community VLAN to one of the following **VLANs** nodes:

- The **LAN Cloud** > **VLANs** node for a VLAN accessible to both fabric interconnects.
- The ***Fabric_Interconnect_Name*** > **VLANs** node for a VLAN accessible to only one fabric interconnect.

Creating Promiscuous Access on Appliance Port

Cisco UCS Manager supports Promiscuous access on appliance ports. The following procedure details the configurations steps.

Before you begin

Create the PVLANs in Appliance Cloud.

Procedure

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

Step 2 Expand **LAN** > **Appliances** > ***Fabric*** > **Interfaces**.
The Interfaces pane displays.

Step 3 In the **Interfaces** pane on the icon bar to the right of the table, click **+** .
The **Appliance Links** pane displays.

Step 4 In the **Appliance Links** pane, click the **Unconfigured Ethernet Ports** to expand the **Unconfigured Ethernet Ports**.
All available Unconfigured Ethernet Ports display.

Step 5 Click the **Unconfigured Ethernet Ports** that you want to make an Appliance Port.

Step 6 Click **Make Appliance Port**.
The **Configure as Appliance Port** confirmation box displays.

Step 7 Click **Yes** to configure the appliance port.
The **Configure Appliance Port** dialog box opens.

Step 8 On the **LAN** tab, expand **LAN** > **Appliances** > ***Fabric*** > **Interfaces**.

Step 9 Expand **Appliance Ports**.

Step 10 Click the appliance port for which you want to modify the properties.

Step 11 In the **Interfaces** pane on the icon bar to the right of the table, click **Modify**.
The **Properties for Appliance Interface** dialog box displays.

Step 12 In the **VLANs** pane, click the **Access** radio button.

Step 13 Select a Primary VLAN from the **Select VLAN** drop-down list to assign to the appliance port.
A list of secondary VLANs associated with the primary VLAN displays.

Step 14 Select a set of secondary VLANs allowed on the port.

Selecting an **Isolated** or **Community** VLAN turns the **VLAN** into a **Promiscuous Port**. If you select the Primary VLAN from the **Select VLAN** drop-down list, you must select the required secondary VLAN.

Step 15 Click **Apply** to configure **Promiscuous Access on Appliance Port**.

Creating a Promiscuous Trunk on Appliance Port

Cisco UCS Manager supports Promiscuous Trunks on appliance ports. The following procedure details the configurations steps.

Before you begin

Create the Private VLANs in the Appliance Cloud.

Procedure

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

Step 2 Expand **LAN** > **Appliances** > ***Fabric*** > **Interfaces**.
The **Interfaces** pane displays.

Step 3 In the **Interfaces** pane on the icon bar to the right of the table, click **+** .
The **Appliance Links** pane displays.

Step 4 In the **Appliance Links** pane, click the **Unconfigured Ethernet Ports** to expand the **Unconfigured Ethernet Ports**.
All available Unconfigured Ethernet Ports display.

Step 5 Click the **Unconfigured Ethernet Ports** that you to want make an Appliance Port.

Step 6 Click **Make Appliance Port**.
The **Configure as Appliance Port** confirmation box displays.

Step 7 Click **Yes** to configure the appliance port.

Step 8 On the **LAN** tab, expand **LAN** > **Appliances** > ***Fabric*** > **Interfaces**.

Step 9 Expand **Appliance Ports**.

Step 10 Click the appliance port for which you want to modify the properties.

Step 11 In the **Interfaces** pane on the icon bar to the right of the table, click the **Modify** icon.
The **Properties for Appliance Interface** dialog box displays.

Step 12 In the **VLANs** pane, click the **Trunk** radio button.

Step 13 Select a **VLAN** from the available VLANs.

From the list of VLANs, you can select multiple **Isolated**,**Community**, **Primary** and **Regular** VLANs to apply on the port to make it a promiscuous trunk port.

Step 14 Click **Apply** to configure **Promiscuous on Trunk on Appliance Port**.

Viewing VLAN Optimization Sets

Cisco UCS Manager automatically creates VLAN port count optimization groups based on the VLAN IDs in the system. All of the VLANs in the group share the same IGMP policy. The following VLANs are not included in the VLAN port count optimization group:

- FCoE VLANs
- Primary PVLANs and secondary PVLANs
- VLANs that are specified as a SPAN source
- VLANs configured as a single allowed VLAN on an interface and port profiles with a single VLAN

Cisco UCS Manager GUI automatically groups the optimized VLANs.

Procedure

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

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

Step 3 In the **Navigation** pane, click **Fabric A** or **Fabric B** to expand the list.

Step 4 Click **VLAN Optimization Sets**.

The **Work** pane displays the list of VLAN optimization groups with **Name** and **Size**.

Viewing the VLAN Port Count

Procedure

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

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

Step 3 Click the fabric interconnect for which you want to view the VLAN port count.

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

Step 5 In the **General** tab, click the down arrows on the **VLAN Port Count** bar to expand that area.

Cisco UCS Manager GUI displays the following details:

Name	Description
VLAN Port Limit field	The maximum number of VLAN ports allowed on this fabric interconnect.
Access VLAN Port Count field	The number of available VLAN access ports.
Border VLAN Port Count field	The number of available VLAN border ports.

Name	Description
Allocation Status field	The VLAN port allocation status.

VLAN Port Count Optimization

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

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

Important

- Enabling VLAN port count optimization increases the number of available VLAN ports for use. If the port VLAN count exceeds the maximum number of VLANs in a non-optimized state, you cannot disable the VLAN port count optimization.
- VLAN port count optimization is not supported in Cisco UCS 6100 Series fabric interconnect.

On the Cisco UCS 6400 Series Fabric Interconnect, 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 on UCS 6200, 6300, and Cisco UCS 6400 Series Fabric Interconnects.

	6200 Series FI	6300 Series FI	6400 Series FI
PV Count with VLAN Port Count Optimization Disabled	32000	16000	16000
PV Count with VLAN Port Count Optimization Enabled	64000	64000	64000

Enabling Port VLAN Count Optimization

By default, the port VLAN count optimization is disabled. You can enable the port VLAN count optimization to optimize the CPU usage and to increase the port VLAN count.

Procedure

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

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

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

Step 4 In the **Port, VLAN Count Optimization** section, choose **Enabled**.

Step 5 Click **Save Changes**.

Step 6 If the **Port, VLAN Count Optimization** option is successfully enabled, a confirmation message displays. Click **OK** to close the dialog box.

Disabling Port VLAN Count Optimization

By default, the port VLAN count optimization is disabled. You can disable the port VLAN count optimization option if you enabled it to increase the port VLAN count and to optimize the CPU usage.

Procedure

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

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

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

Step 4 In the **Port, VLAN Count Optimization** section, choose **Disabled**.

Step 5 Click **Save Changes**.

Step 6 If the **Port, VLAN Count Optimization** option is successfully disabled, a confirmation message displays. Click **OK** to close the dialog box.

Viewing VLAN Optimization Sets

Cisco UCS Manager automatically creates VLAN port count optimization groups based on the VLAN IDs in the system. All of the VLANs in the group share the same IGMP policy. The following VLANs are not included in the VLAN port count optimization group:

- FCoE VLANs
- Primary PVLANs and secondary PVLANs
- VLANs that are specified as a SPAN source
- VLANs configured as a single allowed VLAN on an interface and port profiles with a single VLAN

Cisco UCS Manager GUI automatically groups the optimized VLANs.

Procedure

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

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

Step 3 In the **Navigation** pane, click **Fabric A** or **Fabric B** to expand the list.

Step 4 Click **VLAN Optimization Sets**.

The **Work** pane displays the list of VLAN optimization groups with **Name** and **Size**.

VLAN Groups

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

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

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

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

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

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

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

Creating a VLAN Group

You can create a **VLAN Group** from **LAN Cloud** or the **LAN Uplinks Manager**. This procedure explains creating a VLAN group from the **LAN Cloud**. You can create separate VLAN groups to use for inband and out-of-band access using service profiles.

Procedure

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

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

Step 3 Right-click **LAN Cloud** and choose **Create VLAN Group** from the drop-down list.

The **Create VLAN Group** wizard launches.

Step 4 In the **Select VLANs** dialog box, specify the name and VLANs, then click **Next**.

Step 5 (Optional) In **Add Uplink Ports** dialog box, select the **Uplink Ports** from the list and add the ports to the **Selected Uplink Ports**, then click **Next**.

Step 6 (Optional) In **Add Port Channels** dialog box, select the **Port Channels**, and add the port channels to the **Selected Port Channels**, then click **Next**.

Step 7 (Optional) In the **Org Permissions** dialog box, select the appropriate groups from the list, then click **Next**.

The VLANs that belong to the group that you are creating can only access the groups that you select.

Step 8 Click **Finish**.

This VLAN group is added to the list of **VLAN Groups** under **LAN** > **LAN Cloud** > **VLAN Groups**.

Editing the Members of a VLAN Group

Procedure

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

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

Step 3 In the **Navigation** pane, click **VLAN Groups** to expand the VLAN group list.

Step 4 From the list of VLAN groups, choose the VLAN group name to edit the group member VLANs.

You can use the **`Shift`** key or **`Ctrl`** key to select multiple entries.

Step 5 Right-click the highlighted VLAN group or VLAN groups and choose **Edit VLAN Group Members**.

The **Modify VLAN Group** *VLAN Group Name* dialog box opens.

Step 6 In the **Modify VLAN Group** *VLAN Group Name* dialog box, select the VLANs that you want to remove or add from the list and click **Next**.

Step 7 (Optional) In **Add Port Channels** pane, choose the **Port Channels**, and add them to the **Selected Port Channels**.

Step 8 (Optional) In the **Org Permissions** pane, choose the appropriate groups from the list.

The VLANs that belong to the group that you are creating can only access the groups that you select.

Step 9 Click **Finish**.

Step 10 This VLAN group is modified based on your selections.

Modifying the Organization Access Permissions for a VLAN Group

When you modify the organization access permissions for a VLAN group, the change in permissions applies to all VLANs that are in that VLAN group.

Procedure

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

Step 2 Expand **LAN** > **LAN Cloud** > **VLAN Group**, select *VLAN group name*.

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

Step 4 In **Actions**, click **Modify VLAN Groups Org Permissions**.

The **Modify VLAN Groups Org Permissions** dialog box opens.

Step 5 In **Org Permissions**, do the following:

- To add organizations, select the organizations.
- To remove access permission from an organization, click to remove the selection.

Step 6 Click **OK**.

Deleting a VLAN Group

Procedure

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

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

Step 3 In the **Navigation** pane, click **VLAN Groups** to expand the VLAN group list.

Step 4 From the displayed list of VLAN groups, choose the VLAN group name you want to delete.

You can use the **`Shift`** key or **`Ctrl`** key to select multiple entries.

Step 5 Right-click the highlighted VLAN group or VLAN groups and choose **Delete**.

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

VLAN Permissions

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

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

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

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

Enabling VLAN Permissions

By default, VLAN permissions are disabled. If you want to restrict VLAN access by creating permissions for different organizations, you must enable the org permission option.

Procedure

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

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

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

Step 4 In the **Org Permissions** section, choose **Enabled**.

Step 5 Click **Save Changes**.

Step 6 If the **Org Permissions** option is successfully enabled, a confirmation message displays. Click **OK** to close the dialog box.

Disabling VLAN Permissions

By default, VLAN permissions are disabled. You can enable VLAN permissions and assign a VLAN to a different network group or organization. You can also disable the VLAN permission globally; however, the permissions assigned to the VLANs continue to exist in the system, but are not enforced. If you want to use the org permissions later, you can enable the feature to use the assigned permissions.

Procedure

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

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

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

Step 4 In the **Org Permissions** section, choose **Disabled**.

Step 5 Click **Save Changes**.

Step 6 If the **Org Permissions** option is successfully disabled, a confirmation message displays. Click **OK** to close the dialog box.

Adding or Modifying VLAN Permissions

You can add or delete the permitted organization for a VLAN.

Note When you add an organization as a permitted organization for a VLAN, all of the descendant organizations can access the VLAN. When you remove the permission to access a VLAN from an organization, the descendant organizations no longer have access to the VLAN.

Procedure

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

Step 2 Expand **LAN** > **LAN Cloud** > **VLANs**, select *VLAN name*.

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

Step 4 In **Actions**, click **Modify VLAN Org Permissions**.

The **Modify VLAN Org Permissions** dialog box opens.

Step 5 In **Permitted Orgs for VLAN(s)**,

- To add organizations, select the organizations.
- To remove access permission from an organization, click to remove the selection.

Step 6 Click **OK**.

Modifying Reserved VLANs

This task describes how to modify the reserved VLAN ID. Modifying the reserved VLAN makes transitioning from Cisco UCS 6200 Series Fabric Interconnects to the Cisco UCS 6400 Series 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 Cisco UCS 6400 Series Fabric Interconnect for the new values to take effect.

Procedure

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

Step 2 In the **Work** pane, click the **Global Policies** tab.

Step 3 Specify a new value in the Reserved VLAN Start ID field. The reserved VLAN range ID can be specified from 2-3915.

Step 4 Click **Save Changes**.