Configuring VLANs

This chapter includes the following sections:

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 4030 to 4047. This range of VLAN IDs is reserved.

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 be used together 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 ManagerA 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. It 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, be aware of 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

Important You cannot create VLANs with IDs from 4030 to 4047. This range of VLAN IDs is reserved.

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 can be configured under border and server domains on a fabric interconnect to 6000.

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 keeps track of 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
- Upon receiving creation or deleting notifications from a VMWare vNIC, from an ESX hypervisor

Note This is outside the control of 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 you have exceeded the VLAN port limit service profile configuration will fail during deployment.

Exceeding the VLAN port count in a border domain is less disruptive. When the VLAN port count is exceeded in a border domainCisco UCS Manager changes the allocation status to Exceeded. In order to change the status back to Available, you should 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 You cannot create VLANs with IDs from 4030 to 4047. This range of VLAN IDs is reserved.

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 the **LAN** tab.

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, make sure to 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 has been removed from all vNICs and vNIC templates.

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

Procedure

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

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, depending upon what type of VLAN 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 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 select **Delete**.

Step 7 If the Cisco UCS Manager GUI displays a confirmation dialog box, 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 You cannot create VLANs with IDs from 4030 to 4047. This range of VLAN IDs is reserved.

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 the **LAN** tab.

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 You cannot create VLANs with IDs from 4030 to 4047. This range of VLAN IDs is reserved.

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 the **LAN** tab.

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 Managerprovides support for Community VLAN in UCS Fabric Interconnects. Community ports communicate with each other and 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

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

Important You cannot create VLANs with IDs from 4030 to 4047. This range of VLAN IDs is reserved.

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 the **LAN** tab.

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 has been 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, we recommend 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, you would enter 4, 22, 40-43. **Important** You cannot create VLANs with IDs from 4030 to 4047. This range of VLAN IDs is reserved. 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. • **Community—**This VLAN can communicate with other ports on the same PVLAN as well as the promiscuous port. To create a community VLAN, the sharing type should be set to **Community**.
Primary VLAN drop-down list	If the **Sharing Type** field is set to **Isolated** or **Community**, this is the primary VLAN associated with the Isolated or CommunityVLAN.
Permitted Orgs for VLAN(s)	Select the organization from the displayed list for the VLAN. This VLAN will be available for the organizations you select here.
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

The current version of **Cisco UCS Manager** now provides support for Promiscuous access on appliance ports. The following procedure details the configurations steps.

Before You Begin

PVLANs in Appliance Cloud should already be present

Procedure

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

Step 2 On the **LAN** tab, 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 one of the **Unconfigured Ethernet Ports** you 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.
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 the **Modify** icon.
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 it to the appliance port.
A list of secondary VLANs associated with the primary VLAN appears.

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 the Primary VLAN is selected from the **Select VLAN** drop down, you have to explicitly 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 provides support for Promiscuous Trunks on appliance ports. The following procedure details the configurations steps.

Before You Begin

Make sure Private VLANs in the Appliance Cloud are created.

Procedure

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

Step 2 On the **LAN** tab, 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 one of the **Unconfigured Ethernet Ports** you 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.
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 multiple**Isolated**,**Community**, **Primary** and **Regular** VLANs can be selected to be applied on the port to make it a promiscuous trunk port.

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

Allowing Private VLANs on vNICs - Community Access Mode

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 You cannot create VLANs with IDs from 4030 to 4047. This range of VLAN IDs is reserved.

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 the **LAN** tab.

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 has been 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, we recommend 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, you would enter 4, 22, 40-43. **Important** You cannot create VLANs with IDs from 4030 to 4047. This range of VLAN IDs is reserved. 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. This is a regular VLAN and not a PVLAN . • **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. • **Community**—This VLAN can communicate with other ports on the same PVLAN as well as the promiscuous port. Select this sharing type for to configure a **Community VLAN**.
Primary VLAN drop-down list	If the **Sharing Type** field is set to **Isolated** or **Community**, this is the primary VLAN associated with the Isolated or CommunityVLAN.
Permitted Orgs for VLAN(s)	Select the organization from the displayed list for the VLAN. This VLAN will be available for the organizations you select here.
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.

Configuring a Access Mode for Community Server

The Cisco UCS domain provides support for Private VLANs on vNICs. Configuring a VLAN on vNICs with access mode, allows the server to operate as an Community Access Server.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers** > **Service Profiles** > ***Service_Profile_Name***.

Step 3 On the **Servive Profile** , select a**vNIC** you want to control.
vNICs Property page displays where you can modify **VLANS**.

Step 4 Click the **Modify VLANs link**.
Displays the list of available **VLANS**.

Step 5 Click one of the Community **VLANs** you previously created.

Step 6 Click**OK**.
The Community **VLAN** is now associated with the **vNIC**. When you apply a Community VLAN on a vNIC the server operates as a *Community Access Server*.

Viewing the VLAN Port Count

Procedure

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

Step 2 On the **Equipment** tab, 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 requirement.

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.

Enabling Port VLAN Count Optimization

The port VLAN count optimization is disabled by default. If you want to optimize the CPU usage and increase the port VLAN count, you can enable this feature.

Procedure

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

Step 2 On the **LAN** tab, 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, you will see a confirmation message. Click **OK** to close the dialog box.

Disabling Port VLAN Count Optimization

The port VLAN count optimization is disabled by default. If you have enabled this feature to increase the port VLAN count and optimize CPU usage, you can disable this feature.

Procedure

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

Step 2 On the **LAN** tab, 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, you will see a confirmation message. Click **OK** to close the dialog box.

Viewing VLAN Optimization Sets

VLAN port count optimization groups are automatically created by the system based on the VLAN IDs in the system. All the VLANs in the group will 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 the **LAN** tab.

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

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.

After you assign a VLAN to a VLAN group, any changes made to the VLAN group will be 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 the uplink port for a VLAN group, that uplink port will only support all the VLANs in that 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 the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN** > **LAN Cloud**.

Step 3 Right click on **LAN Cloud** and choose **Create VLAN Group** from the drop down options.
The **Create VLAN Group** wizard launches.

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

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

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

Step 7 (Optional) In the **Org Permissions** dialog box, select appropriate groups from the displayed list, then click **Next**.
The VLANs that belong to the group you are creating here will have access only to the groups you select here.

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 the **LAN** tab.

Step 2 On the **LAN** tab, 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, in which you want 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 you want to remove or add from the displayed 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 appropriate groups from the displayed list.
The VLANs that belong to the group you are creating here will have access only to the groups you select here.

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 in that VLAN group.

Procedure

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

Step 2 On the **LAN** tab, 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:

- If you want to add organizations, select the organizations.

- If you want 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 the **LAN** tab.

Step 2 On the **LAN** tab, 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 the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

VLAN Permissions

VLAN permissions restricts access to VLANs based on specified organizations. Based on the service profile organizations the VLANs belong to, VLAN permissions also restrict the set of VLANs 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 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, you will see **Permitted Orgs for VLAN(s)** option in the **Create VLANs** dialog box. If you do not enable the **Org Permissions**, you will not see the **Permitted Orgs for VLAN(s)** option.

If you enable org permission, when creating a VLAN you will specify the organizations for the VLAN. When you specify the organizations, the VLAN will be available to that specific organization and all the sub organizations beneath the structure. Users from other organizations cannot have access to this VLAN. You can also modify the VLAN permission at any point, based on any changes in your VLAN access requirements.

Caution When you assign VLAN org permission to an organization at the root level, all sub organization can access the VLANs. After assigning org permission at root level, if 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 is 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 the **LAN** tab.

Step 2 On the **LAN** tab, 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, you will see a confirmation message. Click **OK** to close the dialog box.

Disabling VLAN Permissions

By default VLAN permissions is disabled. If you had enabled the option, assigned VLAN permission to different network groups, and no longer want to use the option, you can disable the option globally. When the VLAN org permission feature is disabled, the permissions you assigned to the VLANs will still exist in the system, but they will not be 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 the **LAN** tab.

Step 2 On the **LAN** tab, 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, you will see a confirmation message. 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 organizations for a VLAN, all the descendant organizations will have access to the VLAN. So, when you remove the permission to access a VLAN from an organization, all the descendant organizations will not be able to access the VLAN.

Procedure

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

Step 2 On the **LAN** tab, 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)**,

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

Step 6 Click **OK**.