Global VLANs

Cisco UCS Central enables you to define global VLANs in a LAN cloud at the domain group root, or at the domain group level. You can create a single VLAN or multiple VLANs in one operation.

Global VLAN resolution takes place in Cisco UCS Central prior to global service profiles deployment. If a global service profile references a global VLAN, and that VLAN does not exist, the global service profile deployment fails in the Cisco UCS domain due to insufficient resources. All global VLANs created in Cisco UCS Central must be resolved before deploying that global service profile.

Global VLANs are pushed to Cisco UCS domain along with the global service profiles that reference them. Global VLAN information is visible to Cisco UCS Manager only if a global service profile with reference to a global VLAN is deployed in that Cisco UCS domain. When a global VLAN is deployed and becomes available in the Cisco UCS domain, locally-defined service profiles and policies can reference the global VLAN. A global VLAN is not deleted when a global service profile that references it is deleted.

If a global VLAN is part of a global service profile, or a global port configuration, automatic VLAN resolution takes place when the service profile is pushed down, and the VLANs are available for local consumption in the Cisco UCS domain. If the global VLANs are not associated to a global service profile, or a global port configuration, you must manually publish them to deploy them to Cisco UCS Manager. Cisco UCS Central provides a command to manually publish the global VLAN to sync with Cisco UCS Manager. For more information on Publishing VLANs see Cisco UCS Central CLI Reference Manual.

You must have created the VLAN in Cisco UCS Central prior to publishing it to push it down to Cisco UCS Manager.
If a VLAN group is used to allow VLANs on a Fabric Interconnect’s uplink, the global VLAN must be manually published to Cisco UCS Manager and added to the VLAN group, prior to adding to the service profile assigned to the Cisco UCS domain. If the global VLAN is not published and added to the VLAN group, the vNIC will shut down as the uplink will not allow the global VLAN to pass through.

Note

A global VLAN is not deleted when a global service profile that references it is deleted.

You cannot delete a global VLAN from Cisco UCS Manager. If you want to delete a global VLAN from Cisco UCS Manager, you have to localize the VLAN and then delete it.

**VLAN Org Permission**

All VLANs configured in Cisco UCS Central are common to the orgs in which they are created. You must assign organization permissions before the Cisco UCS Manager instances that are part of the organizations can consume the resources. When you assign org permission to a VLAN, the VLAN is visible to those organizations, and available to be referenced in service profiles maintained by the Cisco UCS Manager instances that are part of the organization.

VLAN name resolution takes place within the hierarchy of each domain group. If a VLAN with the same name exists in multiple domain groups, the organization permissions are applied to all VLANs with the same name across the domain groups.

You can create, modify or delete VLAN org permission.

Note

Make sure to delete the VLAN org permission from the same org you created it in. On Cisco UCS Central GUI you can view the org structure where this VLAN is associated. But at the sub org level on the Cisco UCS Central CLI, you cannot view the VLAN org permission association hierarchy, so if you try to delete the VLAN at the sub org level on the Cisco UCS Central CLI the delete operation will fail.

### Creating or Editing a VLAN

You can create a VLAN at the domain group root or at a specific domain group level, and specify the orgs that can access the VLAN.

You can edit the **VLAN ID**, **Multicast Policy** and access for control for any selected VLANs. After creating a VLAN in a domain group, you can not change the **Domain Group Location** or the **VLAN Name**.

To watch a video on creating a VLAN, see Video: Creating a VLAN and Assigning Org Permission.

#### Procedure

**Step 1**
In the **Actions** bar, type Create VLAN and press Enter.

**Step 2**
In the **VLAN** dialog box, choose the type of VLAN that you want to create.

This can be one of the following:
• **LAN**—The VLAN is used for communication with an external LAN.

• **Appliance**—The VLAN is used for appliance ports and port channels only.

**Step 3**  
In **Basic**, click **Domain Group Location** and select the location in which you want to create this VLAN.

**Step 4**  
Enter a **Name** for this VLAN.  
The VLAN name is case sensitive.

**Important**  
Do not use the name **default** when you create a VLAN in Cisco UCS Central. If you want to create a global default VLAN, you may use **globalDefault** for the name.

**Step 5**  
Enter the **VLAN ID**.  
A VLAN ID can:

- Be between 1 and 3967
  
  **Note**  
  If the registered Cisco UCS Domain has Cisco UCS Manager version 2.2(4) or above the ID range can be between 1 and 4027.

- Be between 4048 and 4093

- Overlap with other VLAN IDs already defined in other domain groups

**Step 6**  
(Optional) Choose whether to enable **Check VLAN Name Overlap** and **Check VLAN ID Overlap** to identify any overlaps.

**Step 7**  
(Optional) if you want to associate a **Multicast Policy** with this VLAN, enter the multicast policy name. Cisco UCS Central identifies the multicast policy and attaches it to the VLAN in the back end.

**Step 8**  
In **Private VLAN**, click the **Sharing Type** to determine whether the 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 be associated with one or more secondary VLANs.

- **Isolated**—This is a private VLAN. Select the primary VLAN with which it is associated 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 the primary VLAN with which it is associated in the Primary VLAN drop-down list.

**Step 9**  
In **Access Control**, click the plus sign to display available orgs.

**Step 10**  
Select the organizations and click the checkmark to apply the selected orgs as **Permitted Orgs** for this VLAN.

**Step 11**  
In **Aliased VLANs**, you can view the existing VLANs to see if a VLAN of the same name already exists.

**Step 12**  
Click **Create**.
Creating or Editing a VLAN Range

Procedure

Step 1  In the Actions bar, type Create VLAN Range and press Enter.

Step 2  In the VLAN Range dialog box, click Basic and choose the Domain Group Location in which you want to create this VLAN.

Step 3  Enter a Name Prefix for this VLAN range.

Step 4  Enter VLAN ID.

A VLAN ID can:

- Be between 1 and 3967
- Be between 4048 and 4093
- Overlap with other VLAN IDs already defined in other domain groups

Example:

For example, to create six VLANs with IDs 4, 22, 40, 41, 42, and 43, you would enter 4, 22, 40-43.

Step 5  (Optional) Choose whether to enable Check VLAN Name Overlap and Check VLAN ID Overlap to identify any overlaps.

Step 6  (Optional) If you want to associate a Multicast Policy with this VLAN range, enter the multicast policy name.

Cisco UCS Central identifies the multicast policy and attaches it to the VLAN range in the back end.

Step 7  In Private VLAN, click the Sharing Type to determine whether the 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 be associated with one or more secondary VLANs.
- Isolated—This is a private VLAN. Select the primary VLAN with which it is associated 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 the primary VLAN with which it is associated in the Primary VLAN drop-down list.

Step 8  In Access Control, click the plus sign display available orgs.

Step 9  Select the orgs and click the checkmark to apply the selected orgs as Permitted Orgs for this VLAN.

Step 10  In Aliased VLANs, you can view the existing VLANs to see if a VLAN of the same name already exists.

Step 11  Click Create.
Managing VLAN Access

From the Manage VLAN Access dialog box, you can add or remove permissions to one or more VLANs at the same time.

Note

You can only add or remove access each time you open the dialog box. If you want to do both actions, you will need to relaunch the dialog box.

Procedure

Step 1

In the Actions bar, type Manage VLAN Access and press Enter.

Step 2

To add access permissions to VLANs, do the following in the VLAN Access dialog box:

a) Click Add Org Permissions.

b) Select the VLAN name or range that you want to use to filter the VLANs and click Search.

c) Click the check boxes for the VLANs that you want to change the permissions for, or select the top check box to select all VLANs on the page.

d) Click the Plus icon, and select the organizations for which you want to grant permissions.

Step 3

To remove access permissions to VLANs, do the following:

a) Click Remove Org Permissions.

b) Select the organization for which you want to remove access permissions.

c) Select the VLAN name or range that you want to use to filter the VLANs and click Search.

d) Click the check boxes for the VLANs that you want to remove the permissions for, or select the top check box to select all VLANs on the page.

Step 4

Click Apply to save and apply your changes.