Managing VLANs and VTP

Campus Manager collects data about devices so that you can configure and manage Virtual LANs (VLANs) in your network. You must set up your LMS/Campus Manager server properly to ensure that Data Collection is successfully performed in your network.

The Campus Manager configuration module helps you to manage your VLANs. You can configure and manage VLANs, PVLANs, Trunk, and also assign ports to VLANs.

This chapter contains:

- Understanding Virtual LAN (VLAN)
- Using VLANs
- Configuring VLANs
- Interpreting VLAN Summary Information
- Understanding Private VLAN
- Using Private VLAN
- Understanding Inter-VLAN Routing
- Using Inter-VLAN Routing
- VLAN Trunking Protocol
- Understanding Trunking
- EtherChannel
- VLAN Port Assignment
- Using VLAN Port Assignment
- Usage Scenarios for Managing VLANs

Understanding Virtual LAN (VLAN)

A Virtual Local Area Network (VLAN) allows you to create logical broadcast domains that can span across a single switch or multiple switches, regardless of physical positioning. A VLAN contains a group of devices on one or more LANs.

These devices are configured in such a way that they can communicate as if they were all on the same network segment. VLANs are based on logical connections instead of physical connections, and hence they are extremely flexible.
VLAN allows you to group ports on a switch to limit unicast, multicast, and broadcast traffic flooding. Flooded traffic originating from a particular VLAN is only flooded out to other ports belonging to that VLAN.

This helps to reduce the size of broadcast domains and it allows groups or users to be logically grouped without being physically located in the same place.

The following topics are covered in this section:

- Advantages of VLANs
- VLAN Components
- Using VLANs

Advantages of VLANs

VLANs provide the following advantages:

- Simplification of Adds, Moves, and Changes
- Controlled Broadcast Activity
- Workgroup and Network Security

Simplification of Adds, Moves, and Changes

Adds, moves, and changes are some of the greatest expenses in managing a network. Many moves require re-cabling and almost all moves require new station addressing and hub and router re-configuration.

VLANs simplify adds, moves, and changes. VLAN users can share the same network address space regardless of their location.

If a group of VLAN users move but remain in the same VLAN connected to a switch port, their network addresses do not change.

If a user moves from one location to another but stays in the same VLAN, the router configuration does not need to be modified.

Controlled Broadcast Activity

Broadcast traffic occurs in every network. Broadcasts can seriously degrade network performance or even bring down an entire network, if the network is not properly managed.

Broadcast traffic in a particular VLAN is not transmitted outside that VLAN. This substantially reduces overall broadcast traffic, frees bandwidth for real user traffic, and lowers the vulnerability of the network to broadcast storms.

You can control the size of broadcast domains by regulating the size of their associated VLANs and by restricting both the number of switch ports in a VLAN and the number of people using the ports.

You can also assign VLANs based on the application type and the amount of application broadcasts. You can place users sharing a broadcast-intensive application in the same VLAN group and distribute the application across the network.
Workgroup and Network Security

You can use VLANs to provide security Firewalls, restrict individual user access, flag any unwanted network intrusion, and control the size and composition of the broadcast domain.

You can:

- Increase security by segmenting the network into distinct broadcast groups.
- Restrict the number of users in a VLAN.
- Configure all unused ports to a default low-service VLAN.

VLAN Components

The VLAN components are:

- Switches that logically segment the end stations connected to it.
  Switches are the entry point for end-station devices into the switched domain and provide the intelligence to group users, ports, or logical addresses into common communities of interest. LAN switches also increase performance and dedicated bandwidth across the network.
  You can group ports and users into communities using a single switch or connected switches. By grouping ports and users across multiple switches, VLANs can span single-building infrastructures, interconnected buildings, or campus networks.
  Each switch can make filtering and forwarding decisions by packet and communicate this information to other switches and routers within the network.
- Routers that extend VLAN communication between workgroups.
  Routers provide policy-based control, broadcast management, and route processing and distribution. They also provide the communication between VLANs and VLAN access to shared resources such as servers and hosts.
  Routers connect to other parts of the network that are either logically segmented into subnets or require access to remote sites across wide area links.
- Transport protocols that carry VLAN traffic across shared LAN.
  The VLAN transport enables information exchange between interconnected switches and routers on the corporate backbone. This backbone acts as the aggregation point for large volume of traffic.
  It also carries end-user VLAN information and identification between switches, routers, and directly attached servers. Within the backbone, high-capacity links with high-bandwidth carry the traffic throughout the enterprise.
Using VLANs

You can use Campus Manager to create, modify, and delete VLANs. You can use the Topology Services to create Ethernet VLANs.

Campus Manager allows you to modify most of the VLAN characteristics that were entered when you created the VLAN, such as purpose, description, and LANE services.

The following sections brief on the types of VLANs supported by Topology Services:

- Ethernet VLAN (See Ethernet VLANs)
- Private VLANs (See Understanding Private VLAN)

Configuring VLANs

You can configure VLANs using VLAN Configuration wizard.

Creating VLAN

To create VLANs, the VLAN Configuration wizard directs you through:

1. Selecting Devices or Entities
2. Creating VLANs
3. Assigning Ports to VLANs
4. Disallowing VLAN on Trunks
5. Understanding VLAN Creation Summary

Deleting VLAN

To delete VLANs, the VLAN Configuration wizard directs you through:

1. Deleting VLANs
2. Moving Affected Ports to New VLAN
3. Understanding VLAN Deletion Summary

Selecting Devices or Entities

You must select the devices or entities to be included in the VLAN. Domain Selector helps you to select devices in Switch Clouds and VTP Domains.

To select devices or entities for a VLAN:

---

Step 1
Select Campus Manager > Configuration > VLAN Configuration.

The VLAN Configuration page appears.

Step 2
Select the devices using the Device Selector or the Domain Selector from the VLAN Configuration dialog box. See Table 10-1
### Configuring VLANs

**Table 10-1 VLAN Configuration Field Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Selector</td>
<td>Lists all the devices in your network. Click the radio button to select the Device Selector.</td>
</tr>
<tr>
<td>Domain Selector</td>
<td>Lists the Switch Clouds and VTP Domains in your network. Click the radio button to select the Domain Selector.</td>
</tr>
<tr>
<td>All</td>
<td>Click All to view all the devices in the network. Check the checkboxes to select the devices.</td>
</tr>
<tr>
<td>Selection</td>
<td>Displays the devices that you have selected in the All pane.</td>
</tr>
</tbody>
</table>

**Step 3**

Either:

a. Click **Create** to create VLANs.
   
   The Create VLAN page appears.

b. Go to **Creating VLANs**.

Or

a. Click **Delete** to delete the VLANs.
   
   The Select VLAN to Delete page appears.

b. Go to **Deleting VLANs**.

---

### Creating VLANs

After you select devices using the Device Selector or the Domain Selector and click Create in the VLAN Configuration page, the Create VLAN page appears. For more details, see **Selecting Devices or Entities**.

You must enter the details as described in the **Table 10-2**.

**Table 10-2 Create VLAN Field Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Name</td>
<td>Enter a name for the new VLAN.</td>
</tr>
<tr>
<td>VLAN Index</td>
<td>Enter a number between 1 and 1024 to identify the VLAN.</td>
</tr>
</tbody>
</table>
| Create on all transparent switches | Check the checkbox to include all switches that are VTP transparent.  
VTP transparent switches do not send VTP updates and do not act on VTP updates received from other switches.  
This checkbox is available only for VTP domain based VLAN creation.  
For more details on this, see Creating VLANs on Transparent Devices. |
| Copy running to start-up config | Check the checkbox to copy the running configuration to the start-up configuration. |
Configuring VLANs

Click any of the following:

- **Next** to continue.

  The Assign VLANs to Port page appears. For details, see Assigning Ports to VLANs.

Assigning ports to VLANs cannot be done for more than 100 devices at a time, since it results in memory issues. If you have selected more than 100 devices, click Finish to save VLAN creation. Do VLAN port assignment for 100 devices at a time.

- **Cancel** to exit.
- **Finish** to save changes.

VLANs are created on the specified devices and the initial VLAN Configuration page appears.

---

**Creating VLANs on Transparent Devices**

When you create VLANs without checking the Create On All Transparent Switches option in the VLAN creation page, the following is the behaviour of Campus Manager:

<table>
<thead>
<tr>
<th>Device Selected</th>
<th>Access and Trunk ports listed in the VLAN Creation flow</th>
<th>VLAN created on</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTPv2 Server</td>
<td>• VTPv2 Server</td>
<td>VTPv2Server</td>
</tr>
<tr>
<td></td>
<td>• VTPv2 Client</td>
<td></td>
</tr>
<tr>
<td>VTPv3 Primary Server</td>
<td>• VTPv3 Server</td>
<td>VTPv3 Primary Server</td>
</tr>
<tr>
<td></td>
<td>• VTPv3 Client</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• VTPv3 Primary Server</td>
<td></td>
</tr>
<tr>
<td>VTPv2 or VTPv3 Transparent device</td>
<td>Selected Transparent device</td>
<td>Selected Transparent device</td>
</tr>
<tr>
<td>Device that has VTPv3 in Off Mode</td>
<td>Selected Off Mode device</td>
<td>Selected Off Mode device</td>
</tr>
</tbody>
</table>

When you create VLANs with the Create On All Transparent Switches option in the VLAN creation page, the following is the behaviour of Campus Manager:
### Configuring VLANs

In the above tables, VTPv2 refers to VTP version 2 and VTP v3 refers to VTP version 3.

<table>
<thead>
<tr>
<th>Device Selected</th>
<th>Access and Trunk ports listed in the VLAN Creation flow</th>
<th>VLAN created on</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTPv2 Server</td>
<td>• VTPv2 Server</td>
<td>• VTPv2 Server</td>
</tr>
<tr>
<td></td>
<td>• VTPv2 Client</td>
<td>• VTPv2 Transparent</td>
</tr>
<tr>
<td></td>
<td>• VTPv2 Transparent device</td>
<td></td>
</tr>
<tr>
<td>VTPv3 Primary Server</td>
<td>• VTPv3 Server</td>
<td>• VTPv3 Primary Server</td>
</tr>
<tr>
<td></td>
<td>• VTPv3 Client</td>
<td>• VTPv3 Transparent device</td>
</tr>
<tr>
<td></td>
<td>• VTPv3 Primary Server</td>
<td>• VTPv3 Off Mode device</td>
</tr>
<tr>
<td></td>
<td>• VTPv3 Transparent device</td>
<td></td>
</tr>
<tr>
<td>VTPv2 or VTPv3 Transparent device</td>
<td>• VTPv2 or VTPv3 Transparent device</td>
<td>• VTPv2 or VTPv3 Transparent device</td>
</tr>
<tr>
<td></td>
<td>• VTPv3 Off Mode device</td>
<td>• VTPv3 Off Mode device</td>
</tr>
<tr>
<td>Device that has VTPv3 in Off Mode</td>
<td>• VTPv3 Transparent device</td>
<td>• VTPv3 Transparent device</td>
</tr>
<tr>
<td></td>
<td>• VTPv3 Off Mode device</td>
<td>• VTPv3 Off Mode device</td>
</tr>
</tbody>
</table>

In the above tables, VTPv2 refers to VTP version 2 and VTP v3 refers to VTP version 3.

## Assigning Ports to VLANs

A VLAN created in a management domain remains unused until you assign one or more switch ports to the VLAN.

The Assign VLANs to Port page appears after you create the VLAN name and index.

To assign ports to VLANs:

1. **Step 1** Select **Campus Manager > Configuration > VLAN Configuration**.
   The VLAN Configuration page appears.
2. **Step 2** Select device or domain from the VLAN Configuration page.
3. **Step 3** Click **Create**.
4. **Step 4** Enter VLAN Name and VLAN Index in the Create VLAN page and click **Next**.
   The Assign Ports to VLAN page appears.
**Step 5**  
Select the ports and click **Next**.

*Table 10-3* describes the entries in the Assign Ports to VLAN page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>Displays the name of the new VLAN.</td>
</tr>
<tr>
<td>Filter</td>
<td>Select any of the following criteria based on which you want to filter the list:</td>
</tr>
<tr>
<td></td>
<td>- Link</td>
</tr>
<tr>
<td></td>
<td>- Port</td>
</tr>
<tr>
<td></td>
<td>- Device Name</td>
</tr>
<tr>
<td></td>
<td>- Device Address</td>
</tr>
<tr>
<td></td>
<td>- Port Status</td>
</tr>
<tr>
<td></td>
<td>- VLAN Index</td>
</tr>
<tr>
<td></td>
<td>- VLAN Name</td>
</tr>
<tr>
<td></td>
<td>- Association type</td>
</tr>
<tr>
<td></td>
<td>Or enter * or leave the field blank and click <strong>Filter</strong> to get all the records.</td>
</tr>
</tbody>
</table>

**Advanced Filter**  
Click **Advanced Filter** to open Advanced Filter dialog box. Advanced filtering allows you to search ports using more search criteria. For more details on Advanced Filter, see **Advanced Filter**.

**Column**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link</td>
<td>Shows whether the port is connected to a switch or not. The value can either be True or False.</td>
</tr>
<tr>
<td>Port</td>
<td>Name of the port.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of the device to which the port belongs to.</td>
</tr>
<tr>
<td>Device Address</td>
<td>IP address of the device to which the port belongs to.</td>
</tr>
<tr>
<td>Port Status</td>
<td>Status of the port. Shows whether the port is active or down.</td>
</tr>
<tr>
<td>VLAN Index</td>
<td>Index number for the VLAN to which the port belongs to.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>Name of the VLAN to which the port belongs to.</td>
</tr>
<tr>
<td>Association Type</td>
<td>Type of VLAN association.</td>
</tr>
</tbody>
</table>

**Step 6**  
Click any of the following:

- **Next** to continue.
  
The Disallow VLAN on Trunks page appears.

- **Back** to modify the Create VLAN page.
- **Cancel** to exit.
- **Finish** to save changes.

VLANs are created on the specified devices, selected ports are assigned to new VLAN and the initial VLAN Configuration page appears.

For more details, see [Disallowing VLAN on Trunks](#).

### Advanced Filter

The Advanced Filter allows you to filter and choose the ports using various parameters and criteria, for assigning the ports to the VLAN. Table 10-4 describes the fields in the Filter Ports Window, when you click Advanced Filter from the Assign Ports to VLAN Window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match All</td>
<td>Select the radio button to filter the ports that match all the selected parameters.</td>
</tr>
<tr>
<td>Match Any</td>
<td>Select the radio button to filter the ports that match any of the selected parameter.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Select a parameter for which you want to filter the ports. Parameter is the attribute of a port.</td>
</tr>
</tbody>
</table>

The values displayed for Assigning ports to VLANs are:
- Device Name
- Device Address
- Link
- Port
- Port Status
- Port Description
- VLAN Index
- VLAN Name
- Association Type

The values displayed for Configuring Promiscuous ports are:
- Link
- Port
- Device Name
- Device Address
- VLAN Name
- Port Mode
Configuring VLANs

Table 10-4  Filter Ports Field Description (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Select the right criterion with respect to the parameter. The values are:</td>
</tr>
<tr>
<td></td>
<td>• contains</td>
</tr>
<tr>
<td></td>
<td>• begins with</td>
</tr>
<tr>
<td></td>
<td>• ends with</td>
</tr>
<tr>
<td></td>
<td>• is</td>
</tr>
<tr>
<td>Value</td>
<td>Enter a value corresponding to the parameter that you have selected.</td>
</tr>
</tbody>
</table>

Click any of the following:
- **More** to add filter.
- **Fewer** to remove filter from the existing filters.
  - You can add or remove only one filter at a time.
- **Filter** to filter the ports based on the values for the Parameters.

### Disallowing VLAN on Trunks

You can select the links on which you do not want to allow Trunking in the newly created VLAN. After you Assign the ports to the VLAN (See Assigning Ports to VLANs), the End-to-end VLAN wizard directs you to Disallow VLAN on Trunks page.

To disallow trunking on the links in your VLAN, check the checkboxes corresponding to those links, and click Next. The VLAN Creation Summary page appears.

Clicking **Back** takes you to the Assign Ports to VLAN page, where you can modify the port assignment. Clicking **Finish saves the changes and takes you to the initial VLAN Configuration page**.

For more details, see Understanding VLAN Creation Summary.

Table 10-5 describes the fields in the Disallow VLAN on Trunks page.

Table 10-5  Disallowing VLAN on Trunks Page Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>Name of the VLAN.</td>
</tr>
<tr>
<td>Port1</td>
<td>Port on the first device linked to the VLAN.</td>
</tr>
<tr>
<td>Device1</td>
<td>Name of the first device in the link.</td>
</tr>
<tr>
<td>Device1 Address</td>
<td>IP Address of the first device in the link.</td>
</tr>
<tr>
<td>Domain1</td>
<td>Domain to which the device belongs to.</td>
</tr>
<tr>
<td>Port2</td>
<td>Port on the second device linked to the VLAN.</td>
</tr>
<tr>
<td>Device2</td>
<td>Name of the second device in the link.</td>
</tr>
<tr>
<td>Device2 Address</td>
<td>IP Address of the second device in the link.</td>
</tr>
<tr>
<td>Domain 2</td>
<td>Domain to which the device belongs to.</td>
</tr>
</tbody>
</table>
Understanding VLAN Creation Summary

The VLAN Creation Summary page summarizes the operations that you performed through the VLAN Configuration wizard. The Summary provides the following information:

- **VTP Domain**—Lists the VTP domains.
- **Summary**—Lists different parameters that you have entered.
  - **VLAN Creation Parameters**—Lists the VLAN name and index, and the value of the parameters to create on all transparent switches and copy running-config to startup-config.
  - **VLAN Port Assignment Parameters**—Lists the VLAN name and index, and ports to which the VLAN is assigned.
  - **VLAN Trunk Configuration Parameters**—Lists the Trunks on which the VLAN is allowed or disallowed.

**Example:**

VLAN Creation Parameters

VLAN Name: Test  
VLAN Index: 912  
Create on all transparent switches : true  
Copy running-config to startup-config : true

-----------------------------------------

VLAN Port Assignment Parameters

VLAN Name: Test  
VLAN Index: 912  
Operation: Assign the VLAN to selected port(s)  
Port: Fa4/28  
Device: 10.77.209.43  
Device Address: 10.77.209.43

-----------------------------------------

VLAN Trunk Configuration Parameters

VLAN Name: Test  
VLAN Index: 912  
Operation: Disallow VLAN on selected Trunk(s)  
Trunk: 10.77.209.52:2/1 => 10.77.209.61:2/25  
Trunk: 10.77.210.211#2:Gi0/2 => 10.77.210.204:Gi1/0/24

Review the Summary, and click Finish to create the new VLAN, or click Back to modify the Disallow VLAN on Trunks page, or click Cancel to exit.
Deleting VLANs

You can delete the VLANs configured on the devices in your network. The VLAN Configuration wizard directs you to delete a VLAN.

**Step 1**
Select **Campus Manager > Configuration > VLAN Configuration**.

The VLAN Configuration page appears.

**Step 2**
Select devices or entities from the VLAN Configuration page.

For more details on selecting the devices, see **Selecting Devices or Entities**.

**Step 3**
Click **Delete**.

The Select VLAN to Delete page appears.

**Table 10-6 Select a VLAN to Delete Page Field Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy Running Config to Start-up Config</td>
<td>Check the checkbox to copy the running configuration to start-up configuration.</td>
</tr>
<tr>
<td>Delete on all Transparent Switches</td>
<td>Check the checkbox to delete VLANs on all transparent switches. If you have created VLANs by checking Create on all transparent switches, it is mandatory that you check Delete on all Transparent Switches option to delete the VLANs created in VTP Domains.</td>
</tr>
</tbody>
</table>
| Filter Source             | Select the Filter type of the source:  
- VLAN  
- VLAN Name  
- Domain Name  
Or enter * or leave the field blank and click **Filter** to get all the records. |
| Select                    | Select the radio button corresponding to the VLAN you want to delete. |
| VLAN                      | Index of the VLAN. |
| VLAN Name                 | Name of the VLAN. |
| Domain Name               | Name of the domain in which the VLAN belongs to. |

**Step 4**
Click any of the following:

- **Next** to continue.

The Move Affected Ports to New VLAN page appears. For more details, see **Moving Affected Ports to New VLAN**.
• **Cancel** to exit.
  The VLAN configuration appears.
• **Finish** to save changes.
  The selected VLANs are deleted from the devices. The ports in the deleted VLAN are automatically assigned to the default VLAN. The VLAN configuration page appears.

### Moving Affected Ports to New VLAN

When you delete a VLAN, any port assigned to that VLAN becomes inactive. Such ports remain associated with the VLAN (and thus inactive), until you assign them to a new VLAN. You can move affected ports to a new VLAN using Campus Manager.

You can move the ports in the VLAN you want to delete, to a new VLAN, only after you select the VLAN you want to delete. For more details on selecting a VLAN to delete, see Deleting VLANs.

To move affected ports to a new VLAN:

1. **Step 1** Select **Campus Manager > Configuration > VLAN Configuration**.
   The VLAN Configuration page appears.
2. **Step 2** Select devices or entities from the VLAN Configuration page.
   For more details on selecting the devices, see Selecting Devices or Entities.
3. **Step 3** Click **Delete**.
   The Select VLAN to Delete page appears.
4. **Step 4** Select the radio button corresponding to the VLAN you want to delete and click **Next**.
   The Move Affected Ports to New VLAN appears.
   Table 10-7 describes the fields in the Move Affected Ports to new VLAN page.

   **Table 10-7  Move Affected Ports to New VLAN Page Field Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Affected port in the VLAN.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of the device to which the port belongs to.</td>
</tr>
<tr>
<td>Device Address</td>
<td>IP address of the device.</td>
</tr>
<tr>
<td>Port Status</td>
<td>Status of the port.</td>
</tr>
<tr>
<td>Connected To</td>
<td>End Host, Network Device</td>
</tr>
</tbody>
</table>

5. **Step 5** Select the new VLAN from the Move affected ports to new VLAN drop-down menu.
   If you do not select any VLAN, the affected ports are moved to the default VLAN—VLAN 1.
Step 6  Click any of the following:

- **Next** to continue.  
  The VLAN Deletion Summary page appears. For more details, see Understanding VLAN Deletion Summary.
- **Back** to modify the Select VLAN to Delete page.
- **Cancel** to exit.  
  The VLAN configuration appears.
- **Finish** to save changes.
  The selected VLANs are deleted from the devices. The ports in the deleted VLAN are assigned to the VLANs selected by you. The VLAN configuration appears.

---

Understanding VLAN Deletion Summary

The VLAN Deletion Summary page summarizes the operations that you performed through the VLAN Configuration wizard to delete the VLAN. The Summary provides the following information:

- **VLAN Deletion**—Lists the domain name, name of the VLAN that is deleted, and the VLAN ID.
- **Operation: Move the affected Ports to another VLAN**—Lists the name and ID of the new VLAN to which the ports have been moved, and lists the details of the ports including the name and IP address of the device.

**Example:**

VLAN Deletion:

```
===================================
VLAN Domain :DMZ_10.77.209.43(T)
VLAN Deleted :VLAN0002
VLANId : 2
===================================
Operation: Move the affected Ports to another VLAN
New VLAN Name :internal VLAN 4
New VLAN Id :4
Port:G11/6
Device :172.20.118.182
Device Address :172.20.118.182
```

Review the Summary and click **Finish** to delete the VLAN, or click **Back** to modify the Select VLAN to Delete page, or click **Cancel** to exit.
Creating Ethernet VLANs

You can use Topology Services to create Ethernet VLANs (which is the typical VLAN design). For details, see Ethernet VLANs.

Ethernet VLANs

An Ethernet VLAN is the typical VLAN design. This consists of a logical group of end-stations, independent of physical location on an Ethernet network. Catalyst switches support a port-centric or static VLAN configuration.

All end stations that are connected to ports Ethernet VLANs belonging to the same VLAN, are assigned to the same Ethernet VLAN.

Creating Ethernet VLANs

Before you create Ethernet VLANs, you must create a VTP domain in your network.

Your login determines whether you can use this option.

To create Ethernet VLANs in your network:

**Step 1**
Select Campus Manager > Visualization > Topology Services from the LMS Portal.

The Topology Services Main Window appears.

**Step 2**
Select a VTP domain from the Tree View.

**Step 3**
Select Tools > VLAN Management > Create > Ethernet from the menu.

The VLAN Creation wizard appears. For more details, see Creating VLANs

Interpreting VLAN Summary Information

To display summary information about the VLANs in your network:

From Tree View in Topology Services, open a VTP domain and select a VLAN. The Summary information is displayed in the right pane of the Topology services window. See Table 10-8 to interpret this information.

Note

Information on Bridge Number and Ring Number are not applicable to Ethernet VLANs.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports</td>
<td>Number of ports in the domain.</td>
</tr>
<tr>
<td>Up Ports</td>
<td>Number of active ports in the domain.</td>
</tr>
<tr>
<td>ISL Index</td>
<td>Inter-Switch Link (ISL) index of the VLAN.</td>
</tr>
</tbody>
</table>
Chapter 10    Managing VLANs and VTP

Interpreting VLAN Summary Information

Displaying VLAN Reports

Campus Manager allows you to generate VLAN reports for devices, switch clouds, or VTP domains.

Step 1
Select Campus Manager > Reports > Report Generator.
The Report Generator page appears.
The left drop-down list displays Campus Manager Reports.

Step 2
Select VLAN from Select a Report drop-down list.
The VLAN page appears with the following information. See Table 10-9:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>Select a run type from the drop-down list. The following run types are available: Immediate, Once, Daily, Weekly, Monthly. If you select Immediate, the Job Info fields and Scheduling Date will be dimmed.</td>
</tr>
</tbody>
</table>

Note
Launching immediate VLAN reports for more than 500 devices results in an error. You can schedule reports to run for all devices or launch immediate reports for less than 500 devices.

Displaying VLAN Reports

Table 10-8     VLAN Field Description (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port List</td>
<td></td>
</tr>
<tr>
<td>Link</td>
<td>A lightning bolt indicates a port that is connected to a switch.</td>
</tr>
<tr>
<td>PortDescription</td>
<td>Description about the port.</td>
</tr>
<tr>
<td>PortName</td>
<td>Name of the port.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of device to which the port belongs.</td>
</tr>
<tr>
<td>Device Address</td>
<td>IP address of device to which the port belongs.</td>
</tr>
<tr>
<td>Port Status</td>
<td>Whether the port is active, down, dormant, or testing.</td>
</tr>
<tr>
<td>isTrunk</td>
<td>If checked, the port is configured as a VLAN trunk.</td>
</tr>
<tr>
<td>Association Type</td>
<td>Type of VLAN.</td>
</tr>
<tr>
<td>Port Mode</td>
<td>Displays mode of port. For example, PVLAN-Host, Promiscuous, or non PVLAN.</td>
</tr>
</tbody>
</table>

- Displaying VLAN Reports
- Interpreting VLAN Reports
You can open VLAN reports page from Topology Services.

To open VLAN reports from Topology Services:

Step 1  Select Campus Manager > Visualization > Topology Services from the LMS Portal.

The Topology Services Main Window appears.

Step 2  Select a view that contains the device, switch cloud, or the VTP Domain for which you want to view the report.

This view is in the Tree View in the Topology Services Main Window.

Step 3  Select Reports > VLAN Report from the menu.

or

Right-click the VTP Domain or the device, and select Display View.

The Network Topology window appears.

Step 4  Select the device or the switch cloud.

Step 5  Right-click and select VLAN Report from the popup menu.

or

Select Reports > VLAN Report.

The VLAN Report window appears.
Interpreting VLAN Reports

The following information is displayed at the top of the report:

- Device Name
- Device IP
- Device Type
- Domain

Table 10-10 describes the fields in VLAN Report.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>VLAN index.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>Name of the VLAN to which the device belongs.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of device can be operational or suspended.</td>
</tr>
<tr>
<td>VLAN Type</td>
<td>Types of VLANs to which the device is associated. The VLANs can be normal,</td>
</tr>
<tr>
<td></td>
<td>isolated, community, or two-way community VLANs.</td>
</tr>
<tr>
<td>Associated Primary</td>
<td>VLAN ID of the associated primary VLAN.</td>
</tr>
<tr>
<td>MTU Size</td>
<td>MTU size for the corresponding VLAN on that device.</td>
</tr>
<tr>
<td>Media Type</td>
<td>Explains in which media type the VLAN on that device.</td>
</tr>
</tbody>
</table>

Understanding Private VLAN

A Private VLAN (PVLAN) is a VLAN that isolates devices at Layer 2 (L2), from other ports within the same broadcast domain or subnet. PVLAN segregates traffic at L2 and converts a broadcast segment into a non-broadcast multi-access segment.

PVLANs can stop L2 connectivity between end stations on a switch without distributing them into different IP subnets, thus preventing wastage of IP addresses.

You can also assign a specific set of ports within a PVLAN, and thus control the connectivity among them. You can configure PVLANs and normal VLANs on the same switch.

This topic contains:

- Types of Private VLAN Ports
- Using Private VLAN

Types of Private VLAN Ports

The ports in a private VLAN are categorized as:

- Promiscuous Ports
- PVLAN Host Ports
- PVLAN Trunk Ports
Promiscuous Ports

Promiscuous port communicates with all other interfaces and ports within a PVLAN. Such ports are used to communicate with external routers, local directories, network management devices, backup servers, administrative workstations, etc.

Ports to the routing module in some switches are promiscuous in nature (for example, MSFC).

PVLAN Host Ports

A PVLAN host port is a port connected to a server or an end host that requires Layer 2 (L2) isolation. A host port exists in the PortFast mode and the BPDU Guard feature is enabled on these ports. These ports can be further classified into:

- **Isolated Ports**
- **Community Ports**

This depends on the secondary VLAN to which the ports belong.

**Isolated Ports**

Isolated ports are completely isolated in L2, from other ports in the same PVLAN. These ports cannot receive the broadcasts from other ports within the same PVLAN, but receive broadcasts from promiscuous ports.

Privacy for the VLAN is ensured at L2 level by blocking the traffic to all isolated ports, except the promiscuous ports. Broadcasts from an isolated port is always forwarded to all promiscuous ports.

**Community Ports**

Community ports communicate among themselves and with their promiscuous ports. These ports are isolated at L2 from all other ports in other communities, or isolated ports within their private VLAN. Broadcasts propagate only between associated community ports and the promiscuous port.

PVLAN Trunk Ports

Private VLAN Trunk ports are similar to Host ports that can carry multiple VLANs. A Trunk port carries the primary VLAN and the secondary VLANs to the neighboring switch. The Trunk port is unaware of PVLAN and will carry PVLAN traffic without any special action.

Using Private VLAN

A Private VLAN has four distinct parts:

- **Primary VLAN**
  Manages the incoming traffic from the promiscuous port to isolated, community, two-way community ports, and all other promiscuous ports, in the same primary VLAN.

- **Isolated VLAN**
  Isolated ports use this VLAN to communicate to the promiscuous ports. The traffic from an isolated port is blocked from reaching all adjacent ports within its private VLAN, except for its promiscuous ports.
Using Private VLAN

- Community VLAN
  A group of community ports use this unidirectional VLAN to communicate among themselves and to manage the outgoing traffic through the designated promiscuous ports from the private VLAN.

- Two-way community VLAN
  A group of community ports use this VLAN to communicate among themselves. This bidirectional VLAN manages the incoming and outgoing traffic for community ports and Multilayer Switch Feature Cards (MSFC).

Isolated and community VLANs are called secondary VLANs.

While creating private VLANs, you:
- Must set VTP to Transparent or Off modes, for VTP version 2.
- Can create PVLAN on primary server, Transparent and Off modes for VTP version 3.

Campus Manager enables you to:
- Create primary Private VLAN.
- Create isolated, community or two-way community VLANs.
- Associate secondary VLANs to primary VLANs.
- Assign ports to secondary VLANs.
- Configure promiscuous ports.

Creating PVLAN

To create a Private VLAN, you must designate one VLAN as primary and another as either isolated, community, or two-way community VLAN. Then, you can assign additional VLANs as secondary VLANs.

After creating primary and secondary VLANs you must associate the secondary VLANs to the respective primary VLANs.

Creating a private VLAN involves the following steps:
- Create primary VLAN
- Create secondary VLAN
- Associate secondary VLAN to primary VLAN
- Associate ports to secondary VLANs
- Configure promiscuous ports
Creating Primary VLAN

You must create primary VLAN before creating any other secondary VLAN.

To create Primary VLANs:

Step 1
Select Campus Manager > Configuration > PVLAN Configuration.
The PVLAN Configuration page appears.

Step 2
Select Create PVLAN from the TOC. Or
Select Campus Manager > Visualization > Topology Services from the LMS Portal.
The Topology Services Main Window appears.

Step 3
Select a VTP domain from the VTP Tree View, under the Managed Domain or Network View.

Step 4
Select Tools > PVLAN Management > Create.
The Create PVLAN page appears.

Step 5
Select the devices using the Device Selector or the Domain Selector. For more details, see Step 2 of Selecting Devices or Entities.

Step 6
Select Primary from the Private VLAN Type drop-down list. The Get Primary VLANs tab and the Associated Primary VLAN field is disabled.

Step 7
Enter a name for the VLAN in the VLAN Name field.

Step 8
Enter the VLAN index number for the new Primary VLAN, in the VLAN Index field.

Step 9
Check the check boxes as required:
• To create private VLAN on all transparent switches.
• To copy Running to Startup config for IOS switches.
The check box for creating private VLANs on all transparent switches, is enabled only when the VLAN contains a device in transparent mode.

Step 10
Click Create to create primary PVLAN.

Note
You must create primary VLAN before creating any other secondary VLAN.
Creating Secondary VLAN and Associating to Primary VLAN

After creating a primary VLAN, you can create secondary VLANs. Once you create a secondary VLAN, you must associate that to a primary VLAN.

To do this:

**Step 1** Select **Campus Manager > Configuration > PVLAN Configuration**.

The PVLAN Configuration page appears.

Or

Select **Campus Manager > Visualization > Topology Services** from the LMS Portal.

The Topology Services Main Window appears.

**Step 2** Select a view with a VTP domain, which has the devices listed for which you want to create PVLAN.

This view is in the Tree View in the Topology Services Main Window.

**Step 3** Select **Tools > PVLAN Management > Create**.

The Create PVLAN page appears.

**Step 4** Select one of the following options from the Private VLAN Type drop-down list:

- Isolated
- Community
- Two-Way Community

**Step 5** Select the Associated Primary VLAN.

You can associate a secondary VLAN that you have created to a primary VLAN.

VTP Domain field displays the domain you have chosen.

You may enter the Private VLAN Name that you want to assign.

**Step 6** Select the Private VLAN Index.

**Step 7** Check the check boxes as required:

- To create private VLAN on all transparent switches.
- To copy Running to Startup config for IOS switches.

The check box for creating private VLANs on all transparent switches, is enabled only when the VLAN contains a device in transparent mode.

**Step 8** Click **Apply** to create PVLAN or click **Cancel** to exit.

Associating Ports to Secondary VLAN

You must associate ports to the secondary VLAN that you have created. You can assign ports to a secondary VLAN as you assign for normal VLANs. For assigning ports to VLANs, see Using VLAN Port Assignment
Configuring Promiscuous Ports

You must associate the promiscuous ports to the PVLANs you have created, to receive traffic from outside the PVLAN.

You can configure only the ports on which Trunking is not enabled.

To configure a Promiscuous Port:

**Step 1** Select **Campus Manager > Configuration > PVLAN Configuration** from the LMS Portal.
   The PVLAN Configuration page appears.
   Or
   From Topology Services Main Window, select the device that has the ports you require and select **Tools > VLAN Port Assignment**.
   The VLAN Port Assignment window appears.

**Step 2** Click **Configure Promiscuous Ports** from the TOC.
   The Configure Promiscuous Ports page appears.

**Step 3** Select a device or entities from the list using Device Selector or Domain Selector.

**Step 4** Click **List Ports**.
   The Port List displays the list of ports on the selected devices.
   You can filter the list using the Filter or Advanced Filter.

**Step 5** Select the ports from the ports listed in the table.

**Step 6** Click **Configure**.
   The Configure Promiscuous Port window appears.
   The Port Details table displays:
   - Device Name
   - Port Name
   - Device IP Address
   - IfName

**Step 7** Select the VLANs from the list of Available PVLANs.

**Step 8** Click **Add** to add to list of **Mapped VLANs**.
   Or
   Click **Remove** to remove the VLANs from the Map VLANs table.
   You can select the Copy Running to Start-up config check-box to copy the running configuration to the start-up configuration.

**Step 9** Click **Apply** to configure.
Deleting PVLAN

To delete PVLAN:

**Step 1**
Select Campus Manager > Configuration > PVLAN Configuration from the LMS Portal.

**Step 2**
Click Delete PVLAN in the TOC.

Or

From Topology Services, select Managed Domains > VTP Domains from the Tree View in the Topology Services Main Window.

**Step 3**
Select the PVLAN which you want to delete.

**Step 4**
Select Tools > PVLAN Management > Delete.

A VTP Domain Name: Delete Private VLAN Name appears.

**Step 5**
Click List PVLANs to see a list of PVLANs. See Table 10-11.

<table>
<thead>
<tr>
<th>Table 10-11</th>
<th>Fields in PVLAN List</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>PVLAN List</td>
<td></td>
</tr>
<tr>
<td>Filter</td>
<td>You can select any of the following filter criteria:</td>
</tr>
<tr>
<td></td>
<td>• PVLAN Index</td>
</tr>
<tr>
<td></td>
<td>• PVLAN Name</td>
</tr>
<tr>
<td></td>
<td>• PVLAN Type</td>
</tr>
<tr>
<td></td>
<td>• Associated Primary</td>
</tr>
<tr>
<td></td>
<td>• Domain</td>
</tr>
<tr>
<td></td>
<td>Enter the filter string, then click Filter.</td>
</tr>
<tr>
<td>PVLAN Index</td>
<td>Index value of the PVLAN.</td>
</tr>
<tr>
<td>PVLAN Name</td>
<td>Name of the PVLAN.</td>
</tr>
<tr>
<td>PVLAN Type</td>
<td>Type of PVLAN. Values are: Primary, Secondary, Community</td>
</tr>
<tr>
<td>Associated Primary</td>
<td>Name of the Associated Primary VLAN.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain to which the VLAN belongs to.</td>
</tr>
</tbody>
</table>

**Step 6**
Select the check box corresponding to the PVLAN you want to delete.

To select all, select the check-box in the table heading.

**Step 7**
Click Delete.
Understanding Inter-VLAN Routing

Inter-VLAN Routing enables to route the traffic between different VLANs. This feature is required when an end station wants to communicate with another end station in a different VLAN. Devices within a VLAN can communicate with one another without the help of a router.

On the contrary, devices in separate VLANs require a routing device to communicate with one another. Network devices in different VLANs cannot communicate with one another without a router to route the traffic between the VLANs.

In most of the network environments, VLANs will be associated with individual networks or subnetworks. In a switched network, VLANs segregate devices into different collision domains and Layer 3 (L3) subnets.

Configuring VLANs for inter-VLAN routing helps to control the size of the broadcast domain and to keep local traffic local. You can configure one or more routers to route traffic in the network.

Layer 2 switches require a L3 routing device (either external to the switch or in another module on the same chassis).

The new L3 Switches accommodate routing capabilities. The router or the switch receives a packet, determines the VLAN to which it belongs, and sends the packet to the appropriate port on the other VLAN.

Using Inter-VLAN Routing

Configuring Inter-VLAN Routing

Campus Manager supports Inter-VLAN Routing configuration on devices like MSFC, RSM, and external routers with IPv4.

Prerequisite for configuring Inter-VLAN Routing through Campus Manager

Resource Manager Essentials is a prerequisite for configuring Inter-VLAN Routing using Campus Manager. If the server running Campus Manager does not have RME, you can use a remote server, which has the RME application.

If you want to configure Inter-VLAN Routing on a device:

- Resource Manager Essentials must manage the devices.
- The device must have the same device name when managed by Campus Manager as well as Resource Manager Essentials.

See the *User Guide for Resource Manager Essentials 4.1* for more details on how to manage devices.

Configuring Inter-VLAN Routing on RSM, MSFC, L2/L3 Devices

To configure Inter-VLAN Routing on a VLAN interface:

1. Select Campus Manager > Visualization > Topology Services from the LMS Portal.
   The Topology Services Main Window appears.
2. Select a device from the Topology Services Tree View, under the Network Views.
Step 3 Right-click the device and select **Config Inter-VLAN Routing** from the popup menu. The Configure Inter-VLAN Routing window appears. This window displays the Device Name and the Device IP of the selected device.

**Step 4** Select a device interface from Device interface configuration list.

**Step 5** Click **Edit** to edit an existing VLAN configuration.

Or

Click **New** to configure Inter-VLAN Routing for a new VLAN interface.

You can edit IP Address, Admin Status, and Subnet Mask. See **Table 10-12**.

**Table 10-12 Configuring Inter-VLAN Routing Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Interface¹</td>
<td>Enter the VLAN interface.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address for the interface</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Enter the subnet mask address.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Select the Admin status:</td>
</tr>
<tr>
<td></td>
<td>• Up</td>
</tr>
<tr>
<td></td>
<td>• Down</td>
</tr>
</tbody>
</table>

¹. You can enter the VLAN interface name to create a new interface. You cannot edit an existing VLAN interface.

You can also delete a Device Interface from the list of Interfaces for which you do not want to configure Inter-VLAN Routing.

**Step 6** Click **Move to Interface Set**.

If you want to edit the configuration details again:

a. Select the VLAN interface from the Interface Set.

b. Click **Delete from Interface Set**

c. Repeat the steps from **Step 4**.

**Step 7** Click **Apply**.

You can configure Inter-VLAN Routing for more than one VLAN interface, at a time.

The RME Server credentials window appears.

**Step 8** Enter RME Server, Server Port, User Name, and Password. See **Table 10-13**.

**Table 10-13 RME Server credentials Field Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RME Server</td>
<td>Name of the RME server or the IP address</td>
</tr>
<tr>
<td>Server Port¹</td>
<td>Enter the port number</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter the user name</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password</td>
</tr>
</tbody>
</table>

¹. In Campus Manager, 1741 is the default port for **http** mode and 443 is the default port for **SSL** (*https*) mode.
Step 9  Click OK.

Inter-VLAN Routing is configured for all the VLAN interfaces in Interface Set.

### Configuring Inter-VLAN Routing on External Routers

To configure Inter-VLAN Routing on a VLAN interface of an external router:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select Campus Manager &gt; Visualization &gt; Topology Services from the LMS Portal. The Topology Services Main Window appears.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select a device from the Topology Services Tree View, under the Network Views.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Right-click the device and select Config Inter-VLAN Routing from the popup menu. The RME Server credentials window appears.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter RME Server, Server Port, User Name, and Password. See Table 10-14</td>
</tr>
</tbody>
</table>

#### Table 10-14   RME Server Credentials Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RME Server</td>
<td>Name of the RME server or the IP address.</td>
</tr>
<tr>
<td>Server Port</td>
<td>Enter the port number.</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter the user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password.</td>
</tr>
</tbody>
</table>

1. In Campus Manager 1741 is the default port for http mode and 443 is the default port for SSL (https) mode.

| Step 5 | Click OK. The Configure Inter-VLAN Routing window appears. |
| Step 6 | Select a device interface from Device interface configuration list. |
| Step 7 | Click Edit to edit an existing VLAN configuration. Or Click New to configure Inter-VLAN Routing for a new VLAN interface. You can edit IP Address, Admin Status, Encapsulation, and Subnet Mask. See Table 10-15 |

#### Table 10-15   Configuring Inter-VLAN Routing Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Interface</td>
<td>Enter the VLAN interface.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address for the interface.</td>
</tr>
<tr>
<td>Sub-Interface ID</td>
<td>Enter the ID for the sub-interface.</td>
</tr>
</tbody>
</table>
You can also delete a device interface from the list of interfaces for which you do not want to configure Inter-VLAN Routing.

**Step 8**  
Click **Move to Interface Set**.

If you want to edit the configuration details again:  
1. Select the VLAN interface from the Interface Set.  
2. Click **Delete from Interface Set**  
3. Repeat the steps from **Step 2**.

**Step 9**  
Click **Apply**.

You can configure Inter-VLAN Routing for more than one VLAN interface, at a time. Inter-VLAN Routing is configured for all VLAN interfaces in the Interface Set.

---

**VLAN Trunking Protocol**

VLAN Trunking Protocol (VTP) is a Layer 2 multicast messaging protocol that maps VLANs across all media types and VLAN tagging methods between switches. In this way it maintains the VLAN configuration consistency throughout a network.

VTP reduces the effort in adding, deleting, or renaming a VLAN at each switch, when the VLAN extends to other switches in the network.

VTP minimizes misconfigurations and configuration inconsistencies that can result in a number of problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

With VTP, you can make configuration changes centrally on one switch and have those changes automatically communicated to all the other switches in the network.

The major function of VTP is to distribute VLAN information. You must configure VTP before you configure any VLAN.
Using VTP, each switch in server mode displays the following:

- Management domain on the Trunk ports
- Configuration revision number
- VLANs and their specific parameters.

For more details on VLAN, see Understanding Virtual LAN (VLAN), and for VTP Domains, see VTP Domains.

This topic contains:

- Understanding VLAN Trunking Protocol Version 3
- Using VLAN Trunking Protocol (VTP)
- VTP Domains

**VTP Domains**

A VTP domain is made up of one or more interconnected devices that share the same VTP domain name. A switch can be configured to be in only one VTP domain, and each VLAN has a name that is unique within a management domain.

Typically, you use a VTP domain to ease administrative control of your network or to account for physical boundaries within your network. However, you can set up as many or as few VTP domains as are appropriate for your administrative needs.

Consider that VTP is transmitted on all Trunk connections, including ISL, IEEE 802.1Q, 802.10, and LANE.

VTP Domains display and monitor the details of the VLANs in your network. Sometimes includes special cases labeled NULL or NO_VTP.

- **NULL**—Lists devices that are in transparent mode and that support VTP, but do not have configured domain names. Each of these devices is identified in the list by its IP address.
- **NO_VTP**—Lists devices that do not support VTP. Each of these devices is identified in the list by its IP address.

However, devices which do not support VTP but support VLANs (for example, Catalyst 2900XL Standard Edition switches) are placed in the NO_VTP domain.

The devices that do not support VLANs and VTP (for example, Catalyst 1900 Standard Edition switches) are placed in the domain category of the neighbor device.
Components of VTP Domains

Within a VTP domain, you can configure switches as follows:

- **Server**—VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches based on advertisements received over Trunk links. VTP server is the default mode.

- **Client**—VTP clients operate in the same way as VTP servers. However, you cannot create, change, or delete VLANs on a VTP client. VTP clients also do not broadcast VTP advertisements like the VTP servers do.

- **Transparent**—VTP transparent switches do not participate in VTP. A VTP transparent switch does not display its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements.

Your VTP domain structure influences the behavior of Topology Services.

Understanding VLAN Trunking Protocol Version 3

VTP version 3 can distribute a list of opaque databases over an administrative domain.

VTP version 3 provides these enhancements to the previous VTP versions:

- Support for extended VLANs.
- Support for creating and advertising private VLANs.
- Support for VLAN instances and MST mapping propagation instances.
- Allows improved server authentication.
- Prevents you from adding the wrong database to a VTP domain.
- Allows interaction with VTP version 1 and VTP version 2.
- Support for configuring VTP version 3 on a per-port basis.
- Enables the network to propagate the VLAN database and other databases.

VTP version 3 is a collection of protocol instances. Each instance handles one database, which is associated with a given feature. VTP version 3 runs multiple instances of the protocol by which it handles the configuration propagation of multiple databases that are independent of one another.

Support for VTP Version 3 in Campus Manager

Campus Manager supports the version 3 of VTP. Following are the major features supported in this release:

- Displays Primary server as a subfolder under the parent VTP domain:
  
  If your network contains devices running VTP version 3, the primary server is displayed as a subfolder under the parent Domain in the VTP Domains. Under Primary server folder, you can find all the server and client modes.

- Supports devices with VTP set to Off mode:
  
  The devices which are set to Off mode are supported as for the transparent mode devices. The Tree View displays the Off mode devices in subfolder under the parent domain.
- Provides VTP filters:
  Topology Filters contains a filter for devices running VTP version 3 in the Network Topology view for the VTP Domains and VTP Views.

You can enable the filters to view the primary, server, client, transparent, and **Off** mode devices. The **Off** mode devices in VTP version 2 and version 3 domains, are displayed under different subfolders of the parent domain, in the Tree View.

When you change the configuration through Campus Manager, the **Off** mode devices are considered similar to the **Transparent** mode devices.

For more details, see Figure 10-1.

**Figure 10-1  VTP Filters**

1. Menu
2. Toolbar
3. Topology map
4. Topology Update completed
5. Filter on for VTP devices
6. Check box dimmed for the filter
7. Topology filter results
8. VTP Domain Topology - PPST (admin@ANServer6.0-lms-cmdev2-ls240-so4)
9. VTP
10. VIP Devices
11. Device: 2  Links: 0

For more details, see Figure 10-1.
VLAN Trunking Protocol

Chapter 10      Managing VLANs and VTP

Using VLAN Trunking Protocol (VTP)

Using VLAN Trunking Protocol (VTP), each switch in server mode advertises its management domain on its Trunk ports, its configuration revision number, and its known VLANs and their specific parameters.

Therefore, a new VLAN must be configured on only one device in the management domain, and the information is automatically learned by all other devices (not in VTP transparent mode) in the same management domain.

After a device learns about a VLAN, it receives all frames on that VLAN from any Trunk port and, if appropriate, forwards them to each of its other Trunk ports.

This topic contains:

- Displaying VTP Reports
- Using VTP Views

Notes on creating VLAN or PVLAN in VTP version 3 domain using Campus Manager

- You must select the parent VTP domain folder under the VTP domain Tree to create VLAN or PVLAN.

- To create VLAN or PVLAN on all transparent switches in the domain, you can check the check box Create VLAN on all transparent switches in the Creating VLAN or PVLAN windows.

For more details, see Creating Ethernet VLANs and Creating PVLAN.

- You must select the primary domain subfolder under the VTP domain, while creating VLAN and PVLAN on the Primary server mode devices that has clients and secondary servers.

- You must select Transparent or Off mode subfolders under the parent VTP domain to create VLAN or PVLAN on a single Transparent or Off mode device respectively.

• Supports creating Private VLANs in VTP version 3 environment.

You can create a VLAN or PVLAN using a primary server domain or the parent domain. You can create a VLAN or PVLAN only on the Primary server, Transparent and Off mode devices, in a VTP version 3 environment.

- You must select the parent VTP domain folder under the VTP domain Tree to create VLAN or PVLAN.

- To create VLAN or PVLAN on all transparent switches in the domain, you can check the check box Create VLAN on all transparent switches in the Creating VLAN or PVLAN windows.

For more details, see Creating Ethernet VLANs and Creating PVLAN.

- You must select the primary domain subfolder under the VTP domain, while creating VLAN and PVLAN on the Primary server mode devices that has clients and secondary servers.

- You must select Transparent or Off mode subfolders under the parent VTP domain to create VLAN or PVLAN on a single Transparent or Off mode device respectively.

Using VLAN Trunking Protocol (VTP)

Using VLAN Trunking Protocol (VTP), each switch in server mode advertises its management domain on its Trunk ports, its configuration revision number, and its known VLANs and their specific parameters.

Therefore, a new VLAN must be configured on only one device in the management domain, and the information is automatically learned by all other devices (not in VTP transparent mode) in the same management domain.

After a device learns about a VLAN, it receives all frames on that VLAN from any Trunk port and, if appropriate, forwards them to each of its other Trunk ports.

This topic contains:

- Displaying VTP Reports
- Using VTP Views
Displaying VTP Reports

To display a VTP report for the VTP domains in your network.

**Step 1** Select Campus Manager > Visualization > Topology Services from the LMS Portal.

The Topology Services Main Window appears.

**Step 2** Select a VTP domain under the VTP views for which you want to view the report. This view is in the Tree View in the Topology Services Main Window.

The VTP Report, which is the Summary view, appears.

Interpreting VTP Reports

See Table 10-16 to interpret the fields shown in the VT Reports Summary view.

<table>
<thead>
<tr>
<th>Table 10-16 Field Description for VTP Report</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Link</td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td>IfName</td>
</tr>
<tr>
<td>Device Name</td>
</tr>
<tr>
<td>Device Address</td>
</tr>
<tr>
<td>PortStatus</td>
</tr>
<tr>
<td>isTrunk</td>
</tr>
<tr>
<td>VLAN</td>
</tr>
<tr>
<td>Association Type</td>
</tr>
<tr>
<td>Port Mode</td>
</tr>
</tbody>
</table>
Using VTP Views

VTP Views shows devices that participate in VTP domains. VTP Views also shows the non-VTP devices connected directly to the VTP domain. See Figure 10-2

**Figure 10-2  VTP Tree View**

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VTP domain in the Topology Tree View</td>
</tr>
<tr>
<td>2</td>
<td>Parent VTP domain</td>
</tr>
<tr>
<td>3</td>
<td>Switch in Transparent mode</td>
</tr>
<tr>
<td>4</td>
<td>VLANs under the Transparent switch mode</td>
</tr>
<tr>
<td>5</td>
<td>VTP Views under the Network View</td>
</tr>
<tr>
<td>6</td>
<td>Parent VTP domain under VTP views</td>
</tr>
</tbody>
</table>

Use the VTP views to:
- Display Device Attributes
- Display Port Attributes
- Display Link Attributes
- Display information about multi-layer switching (MLS) devices in your network. See Displaying MLS Reports
Understanding Trunking

A Trunk is a point-to-point link carrying traffic for several VLANs, and are typically used to connect switches. Instead of configuring several access links to carry multi-VLAN traffic, its economical to do it with a single trunk link.

Trunking is hence a type of configuration on an interface which allows VLANs to span the entire network, instead of just one switch. The Trunked interface that connects to another network device is allowed to pass traffic for multiple VLANs, instead of only one VLAN as in a non-Trunked interface on a switch.

This topic contains:
- Trunking Considerations
- Dynamic Trunking Protocol (DTP)
- Trunk Encapsulation
- Trunk Characteristics
- Encapsulation Types
- Creating Trunk
- Modifying Trunk Attributes

Trunking Considerations

While using a Trunk, consider the following:
- VLANs are local database of a switch. VLAN information is not passed between switches.
- Trunk links provide VLAN identification for frames traveling between switches.
- You can use either of the two Ethernet Trunking mechanisms: ISL and IEEE 802.1Q.
- Trunks carry traffic from all VLANs to and from the switch by default. However, they can be configured to carry only specified VLAN traffic too.
- Trunk links must be configured to allow Trunking on each end of the link.

Dynamic Trunking Protocol (DTP)

Dynamic Trunking Protocol (DTP) is a Cisco proprietary protocol. Trunk negotiation is managed by the DTP on a link between two devices. DTP is also used for negotiating the type of Trunking encapsulation to be used.

Dynamic Trunking is the ability to negotiate the Trunking method with the other device, and DTP is a point-to-point protocol that supports auto-negotiation of both ISL and 802.1Q Trunks. DTP sends the VTP domain name in a DTP packet.

Therefore, if you use DTP, and if the two ends of a link belong to a different VTP domain, the Trunk will not function.

The Catalyst operating system options of auto, desirable, and on, and the IOS options of dynamic auto, dynamic desirable, and trunk, configure a Trunk link using DTP. If one side of the link is configured to Trunk and sends DTP signals, the other side of the link will dynamically begin to Trunk, if the options match correctly.
To enable Trunking and not send any DTP signaling, you can use the option `nongotiate` for switches that support that function. If you want to disable Trunking completely, you can use the `off` option for a Catalyst operating system switch or the `no switchport mode trunk` command on an IOS switch.

DTP is a second generation Dynamic Inter-Switch Link Protocol (DISL) and allows the Cisco Catalyst devices to negotiate whether to use 802.1Q encapsulation. DISL and DTP do not negotiate Trunking in case of EtherChannel—they only negotiate whether to enable Trunking.

**Trunk Encapsulation**

The following Trunking encapsulations are available on all Ethernet interfaces:

- Inter-Switch Link (ISL)—A Cisco-proprietary Trunking encapsulation.
- 802.1Q—An industry-standard Trunking encapsulation.

**Trunk Characteristics**

Table 10-17 shows the DTP signaling and the characteristics of each mode.

<table>
<thead>
<tr>
<th>Trunking Mode</th>
<th>Frames Sent</th>
<th>Description</th>
<th>Final state (local port)</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>YES, periodic</td>
<td>Trunking is active. The interfaces sends DTP signals that actively attempt to convert the link to a Trunk link. The interface becomes a Trunk interface if the neighboring interface is set to <strong>on</strong>, <strong>auto</strong> or <strong>desirable</strong>, and is running DTP. A port that is in <strong>on</strong> mode always tags frames sent out from the port.</td>
<td>Trunking, unconditionally.</td>
</tr>
<tr>
<td>auto</td>
<td>YES, periodic</td>
<td>These links will only become Trunk links if they receive a DTP signal from a link that is already Trunking or desires to Trunk. This will only form a Trunk if the neighboring interface is set to <strong>on</strong> or <strong>desirable</strong>. This is the default mode for Catalyst operating system switches.</td>
<td>The port will end up in Trunking state only if the neighboring interface wants to.</td>
</tr>
<tr>
<td>desirable</td>
<td>YES, periodic</td>
<td>These links would like to become Trunk links and send DTP signals that attempt to initiate a Trunk. They will only become Trunk links if the other side responds to the DTP signal. This will form a Trunk if the neighboring interface is set to <strong>on</strong>, <strong>auto</strong>, or <strong>desirable</strong> and is running DTP. This is the default mode for all Ethernet interfaces.</td>
<td>If the port detects that the neighboring interface is able to Trunk (remote in <strong>on</strong>, <strong>desirable</strong> or <strong>auto</strong> mode), it will end up in Trunking state. Otherwise, it will stay non-Trunking.</td>
</tr>
</tbody>
</table>
Understanding Trunking

Encapsulation Types

The encapsulation type allows you to specify whether ISL or 802.1q should be used for Trunking. The parameter is only relevant if the module you are using is able to use both types of encapsulation. The parameter can have three different values as shown in table below.

<table>
<thead>
<tr>
<th>Encapsulation Type</th>
<th>Description and Trunking</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISL</td>
<td>Sets the port encapsulation to ISL.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Sets the port encapsulation to 802.1q.</td>
</tr>
</tbody>
</table>
| negotiate          | Only available in auto or desirable Trunking modes:  
|                    | • If the neighboring interface has encapsulation type set to negotiate, the Trunk will eventually be set up with ISL.  
|                    | • If the interface is configured for ISL or 802.1q or only able to use ISL or 802.1q, the Trunking encapsulation used will be the same as the neighboring interface. |

Creating Trunk

To create trunk for a port:

**Step 1** Select Campus Manager > Configuration > Trunk Configuration from the LMS Portal.  
The Create Trunk page appears.

**Step 2** Select the device or domain from the list, and click Show Links.  
The Available Links pane displays the links for each device that you have selected. Table 10-18 describes the fields in the Available Links pane.
Understanding Trunking

Step 3
Click the radio button corresponding to the link to select link for which you want to create trunk.

Step 4
Click **Create Trunk**.

Or

From Topology Map, right-click the link for which you want to create trunk, and select **Create Trunk** from the popup menu.

The Create Trunk window appears.

**Table 10-19** describes the fields in the Create Trunk page.

### Table 10-18 Available Links Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Select the filter type and then enter the string. Leave the field blank to display all.</td>
</tr>
<tr>
<td></td>
<td>You can filter the list based on the Port1, Device1, Port2, or Device2.</td>
</tr>
<tr>
<td></td>
<td>For example, if you want to see only the trunks on the selected devices which starts with IP address 10.77, select Device1 from the Filter type, then enter 10.77.* in the filter field and click <strong>Filter</strong>.</td>
</tr>
<tr>
<td>Port 1</td>
<td>Port of the first device in the link.</td>
</tr>
<tr>
<td>Device 1</td>
<td>IP address of the device to which the port1 belongs to.</td>
</tr>
<tr>
<td>Port 2</td>
<td>Port of the second device in the link.</td>
</tr>
<tr>
<td>Device 2</td>
<td>IP address of the device to which the port2 belongs to.</td>
</tr>
</tbody>
</table>

### Table 10-19 Create Trunk Page Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Information</strong></td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td>IP addresses of the devices forming the link.</td>
</tr>
<tr>
<td>Port</td>
<td>Port numbers of the devices forming the link.</td>
</tr>
<tr>
<td><strong>Trunk Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Select the Encapsulation type for the trunk. Campus Manager supports: Dot1Q, ISL, Negotiate.</td>
</tr>
<tr>
<td>Mode</td>
<td>Trunking mode of the port is set to <strong>Desirable</strong>. Campus Manager supports only the <strong>Desirable</strong> mode.</td>
</tr>
<tr>
<td><strong>Configure VLANs on Trunk</strong></td>
<td></td>
</tr>
<tr>
<td>Allow Active VLANs</td>
<td>Lists only the active VLANs. 1. Select the VLANs for which you do not want to configure Trunk.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add</strong> to move the VLANs to Disallowed VLANs list.</td>
</tr>
<tr>
<td>Disallow Active VLANs</td>
<td>1. Select the VLAN IDs of the VLANs, which must pass through the Trunk.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Remove</strong> to move the VLANs to the list of Allowed VLANs.</td>
</tr>
</tbody>
</table>
Chapter 10      Managing VLANs and VTP

Understanding Trunking

To copy the running configuration to start-up configuration, select Copy Running to Start-up Config check-box.

**Step 5**

Click **Create** to create the Trunk or click **Close** to exit.

After you click **Create**, it will be idle for 2 minutes to see if the device goes down on setting the port to trunking mode. After 2 minutes, if the creation of trunk is successful, Data Collection for these devices is triggered.

Only after the completion of Data Collection, you can see the newly configured trunk ports in the Modify Trunk Attributes page.

**Note**

If the trunk link is configured in a port that flaps between blocking and non-blocking states due to STP, then the port will be listed in both Create Trunk page and Modify Trunk Attributes page. To know whether the port is trunking or not, enable logging in the device and see the log messages.

### Modifying Trunk Attributes

To modify trunk attributes:

**Step 1**

Select **Campus Manager > Configuration > Trunk Configuration** from the LMS Portal.

**Step 2**

Click **Modify Trunk Attributes** from the TOC.

The Modify Trunk Attributes page appears.

**Step 3**

Select devices from the device list, and click **Show Trunks**.

The trunks configured on the devices are listed in the Trunk List. See Table 10-20.

---

**Table 10-19 Create Trunk Page Field Description (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure VLANs on Trunk Using Ranges</strong></td>
<td></td>
</tr>
<tr>
<td>Allow VLANs</td>
<td>Enter VLAN IDs of the VLANs, which must pass through the Trunk in the range of 1 to 1005 and 1025 to 4094. The other VLANs are not supported for Trunking.</td>
</tr>
<tr>
<td>Disallow VLANs</td>
<td>Enter VLAN IDs of the VLANs, which must not pass through the Trunk, in the range of 1 and 4096. If you enter numbers into both fields, the VLAN indexes that you are disallowing will take precedence over VLAN indexes that you are allowing. For example, if you allow 1-1024 and disallow 1-100, VLANs with ISL indexes of 101-1024 will be allowed.</td>
</tr>
</tbody>
</table>
Step 4 Select the radio-buttons corresponding the trunk you want to modify, and click **Modify Trunk**. The Modify Trunk window appears.
The Device Information pane displays the device IP address and the port number of all the devices you have selected.

Step 5 Select the Trunk Settings

a. Select Encapsulation:
   - Dot1Q
   - ISL
   - Negotiate

b. Mode

Campus Manager 3.3 supports only the **Desirable** mode.

Step 6 Configure VLANs on Trunk.

- Allow VLAN(s)—Enter VLAN IDs of the VLANs, which must pass through the Trunk, in a range between 1 to 1005 and 1025 to 4094. The other VLANs are not supported for Trunking. * indicates that the VLANs were previously disallowed.

- Disallow VLAN(s)—Enter VLAN IDs of the VLANs, which must not pass through the Trunk, in a range between 1 and 4096.

Use the Add or Remove buttons to allow or disallow VLANs.

To copy the running configuration to start-up configuration, select Copy Running to Start-up Config check-box.

Step 7 Click **Modify**.

---

**Table 10-20 Trunk List Field Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Select the filter type and then enter the string. Leave the field blank to display all. You can filter the list based on the Port1, Device1, Port2, or Device2. For example, if you want to see only the trunks on the selected devices which starts with IP address 10.77, select Device1 from the Filter type, then enter 10.77.* in the filter field and click <strong>Filter</strong>.</td>
</tr>
<tr>
<td>Port 1</td>
<td>Port number of the port of the device at one side in the link that is configured for Trunking.</td>
</tr>
<tr>
<td>Device1</td>
<td>IP address of the device to which the port1 belongs to.</td>
</tr>
<tr>
<td>Port2</td>
<td>Port number of the port of the device at the other end of the link that is configured for Trunking.</td>
</tr>
<tr>
<td>Device2</td>
<td>IP address of the device to which the port2 belongs to.</td>
</tr>
</tbody>
</table>
EtherChannel

EtherChannel is a technology that bundles individual Fast Ethernet and Gigabit Ethernet links into a single logical link that would provide higher bandwidth. EtherChannels thus enable you to aggregate up to Gigabit Ethernet connections, providing up to 16 Gbps of bandwidth (in full duplex mode).

The channel is treated as a single logical connection between two switches. If one of the connections fails in the EtherChannel, the other connections will be operating so that the connection is not down.

This topic contains:

- Understanding EtherChannel
- Using EtherChannel

Understanding EtherChannel

EtherChannel provides incremental Trunk speeds between Fast Ethernet (FE) and Gigabit Ethernet (GE) by grouping multiple equal-speed ports into a logical port channel. EtherChannel combines multiple FEs up to 800 Mbps or GES up to 8 Gbps, providing fault-tolerant, high-speed links between switches, routers, and servers.

Campus Manager supports only PAgP, the aggregation protocol. When a user selects a port or link for configuring EtherChannel, the user is prompted with all available ports that can participate in the channel (Ports that are directly connected between devices).

Admin Group ID attribute for each port is also provided under group attribute. User can change them accordingly to choose which ports need to aggregate into a channel.

All ports that have same group value will participate in channel. Campus Manager supports only the Desirable mode for EtherChannel configuration.

Campus Manager does not support EtherChannel configuration between a switch and router.

Using EtherChannel

Campus Manager allows you to:

- Aggregate multiple links between switches into one or more EtherChannels.
- Configure frame distribution parameters for EtherChannel load balancing.

Configuring EtherChannel

To configure EtherChannel:

Step 1 Select Campus Manager > Visualization > Topology Services from the LMS Portal.

The Topology Services Main Window appears.

Step 2 Select a view that contains the devices for which you want to configure EtherChannel.

This view is in the Tree View in the Topology Services Main Window.

Step 3 Right-click the view and select Display View from the popup menu.

The Network Topology View window appears.
Step 4 From the Network Topology View select the link on which you want to configure EtherChannel.

Step 5 Right-click the link and select **Configure EtherChannel**.

The EtherChannel Configuration window appears.

Protocol field displays PAgP. Port Aggregation Protocol (PAgP) is the Protocol that is supported for configuring EtherChannel.

Step 6 Select one of the Distribution Protocols from the drop-down menu:

- ip
- mac
- port
- leave default

Select **leave default** when you do not want to configure distribution protocols.

The Channel Mode field displays the mode of the port.

Campus Manager supports only the **Desirable** mode for EtherChannel configuration.

Step 7 Select one of these Distribution Address Types from the drop-down menu:

- source
- destination
- both
- leave default

Select **leave default** when you do not want to configure distribution address type.

Step 8 Select the link for which you want to configure EtherChannel.

Step 9 Click **Copy Running to StartUp config for IOS switches**, if required.

Step 10 Click **Apply** to continue or click **Close** to exit.

---

**VLAN Port Assignment**

VLAN Port Assignment is an application that displays device, port, and related VLAN information for an associated VTP domain in a tabular format and helps you manage ports on your network’s VLANs. Use VLAN Port Assignment to:

- Assign or move ports to a VLAN.
- View port, device, and Trunk attributes.
- View and find port information in a VTP domain.
- Configure VLANs on a Trunk.
- Show and highlight a selected device or VLAN on a selected VTP domain.

**Note** Assigning ports to VLANs cannot be done for more than 100 devices at a time, since it results in memory issues. Do VLAN port assignment for 100 devices at a time.
This topic contains the following sections:

- Understanding VLAN Port Assignment
- Starting VLAN Port Assignment
- Using VLAN Port Assignment

Prior to using VLAN Port Assignment, you should understand the concepts of VLANs and VTP domains. For more details on this, see:

- Understanding Virtual LAN (VLAN)
- VTP Domains

### Understanding VLAN Port Assignment

To enable end-user ports to participate in a specific VLAN, you must first assign the ports. You assign ports to specified VLANs. The VLANs allow the ports to share the same broadcasts.

Ports that are not assigned to the VLAN cannot share these broadcasts. For more information about VLANs, see Understanding Virtual LAN (VLAN).

For VLAN Port Assignment to work correctly, Campus Server must discover the network. Campus Server requires a properly configured network to complete network discovery.

For information on the various settings, see Viewing Campus Manager Home Page.

VLAN Port Assignment queries the ANI database based on criteria you enter.

After you submit the query, VLAN Port Assignment displays the device, port, and related VLAN information for an associated VTP domain. This is displayed in a tabular format.

You can use VLAN Port Assignment to:

- View and find port information in a VTP domain
- View port, device, and Trunk Attributes
- Show and highlight a selected device or VLAN in the VTP domain view

### Starting VLAN Port Assignment

To start VLAN Port Assignment:

1. **Step 1** Verify that your network is set up properly.
2. **Step 2** Verify that the Campus Manager server is set up properly and running.
   
   See Analyzing ANI Server for more details.
3. **Step 3** Select Campus Manager > Configuration > VLAN Port Assignment from the LMS Portal.
   Or
   Select Topology Services > Tools > VLAN Port Assignment.

If you are prompted to install the Java plug-in, you can download and install the plug-in using the displayed installation screens. The next time you start the application, it will automatically use the plug-in.
Using VLAN Port Assignment

To assign ports to a VLAN:

**Step 1** Select Campus Manager > Configuration > VLAN Port Assignment from the LMS Portal.
Or
Select Topology Services > Tools > VLAN Port Assignment.
The VLAN Port Assignment page appears.

**Step 2** Select device or domain from the list using Device Selector or Domain Selector.

**Step 3** Click List Ports.

A list of ports in the selected devices or entities appears under the Port List. See Table 10-21 for the Port List:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>• Device Name&lt;br&gt;• Device Address&lt;br&gt;• Link&lt;br&gt;• Port&lt;br&gt;• Port Status&lt;br&gt;• Port Description&lt;br&gt;• VLAN Name&lt;br&gt;• VLAN Index&lt;br&gt;• Association Type</td>
</tr>
<tr>
<td>Advanced Filter</td>
<td>Click Advanced Filter to open Advanced Filter dialog box. Advanced filtering allows you to search ports using more search criteria. For more details on Advanced Filter, see Advanced Filter.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link</td>
<td>Shows whether the port is connected to a switch or not. The value can either be True or False.</td>
</tr>
<tr>
<td>Port</td>
<td>Name of the port.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of the device to which the port belongs to.</td>
</tr>
<tr>
<td>Device Address</td>
<td>IP address of the device to which the port belongs to.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>Name of the VLAN to which the port belongs to.</td>
</tr>
<tr>
<td>Port Status</td>
<td>Status of the port. Shows whether the port is active or down.</td>
</tr>
<tr>
<td>Port Description</td>
<td>Description for the port. Example: Intra-area 0.2.0.0 Resilient link</td>
</tr>
</tbody>
</table>
Using VLAN Port Assignment

Step 4 Select a VLAN from the VLAN drop-down list.
To copy the running configuration to the start-up configuration, select Copy running to start-up config check-box.

Step 5 Click Assign.

Configuring Trunk Attributes

Your login determines whether you can use this option. You must have either Network Administrator or System Administrator privileges.

To configure Trunk Attributes:

Step 1 Select Campus Manager > VLAN Port Assignment from CiscoWorks desktop.
Or
From Topology Services Main Window, right-click a trunk link from a network view and select VLAN Port Assignment from the popup menu.

Step 2 In the VLAN Port Assignment window, select the VTP domain and enter appropriate search criteria, if necessary.

Step 3 Select the row that contains the Trunking port. A port is a trunking port if the isTrunk field contains a check mark.

Step 4 Select Reports > Trunk Attributes.
To interpret this information, see Table 10-24.

Step 5 Enter a range of ISL indexes between 1 and 4096 in the Allow VLAN(s) field to specify VLANs that you want to allow on this Trunk.
The range of ISL indexes from one to 4096 is applicable only if the device supports 4096 VLANs.

Step 6 Enter a range of ISL indexes between 1 and 1024 in the Disallow VLAN(s) field to specify VLANs that you want to prevent from using this Trunk.
If you enter numbers into both fields, the ISL indexes that you are disallowing will take precedence over ISL indexes that you are allowing. For example, if you allow 1-1024 and disallow 1-100, VLANs with ISL indexes of 101-1024 will be allowed.

Step 7 Click Apply to configure these attributes.
Displaying Attribute Summaries

The following topics describe how to view status information about ports, devices, and trunks in your network:

- Displaying Port Attributes
- Interpreting Port Attributes Report
- Displaying Device Attributes
- Interpreting Device Attributes Report
- Displaying Trunk Attributes
- Interpreting Trunk Attributes

Displaying Port Attributes

To display information about the status of the ports in your network:

Step 1  Select Campus Manager > Reports > Report Generator.
        The Reports Generator page appears.

Step 2  Select Campus Reports from the Select An Application drop-down list.

Step 3  Select Port Attributes from Select a Report drop-down list.
        The Port Attributes page appears.

Step 4  Select a device or domain from the list.

Step 5  Select the Scheduling Type.
        The default scheduling type is Immediate.
        You can set the time and date if you select any of the following scheduling types: Once, Daily, Weekly, Monthly.
        Enter a description for your job in the Job Description field and enter the e-mail address to which the details has to be sent.

Note  Launching immediate Port Attributes reports for more than 500 devices results in an error. You can schedule reports to run for all devices or launch immediate reports for less than 500 devices.

Step 6  Click Submit.
        For more information on Port Attributes, see Interpreting Port Attributes Report.

Interpreting Port Attributes Report

To view the Port Attributes report for a device, select the device from the Go To: list. The Go To: list contains the device name and device IP address.

Alternatively, you can scroll the page to view the report for the selected devices.

The Port Attributes report contains the following information for a device:
Table 10-22  Port Attributes Report Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Name of the port. Example: Fa4/0</td>
</tr>
<tr>
<td>Port Description</td>
<td>Description for the port. Example: Intra-area 0.2.0.0 Resilient link</td>
</tr>
<tr>
<td>Type</td>
<td>Type of port. Example: 1000Base</td>
</tr>
<tr>
<td>AdminStatus</td>
<td>Administrative status of the port.</td>
</tr>
<tr>
<td>OperStatus</td>
<td>Operational status of the port.</td>
</tr>
<tr>
<td>isLink</td>
<td>Shows whether the port is connected to another device, which is managed in Campus Manager.</td>
</tr>
<tr>
<td>isTrunk</td>
<td>Shows whether the port is part of a trunk.</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the port is working.</td>
</tr>
<tr>
<td>Duplex Mode</td>
<td>Shows whether the port is in full-duplex mode or half-duplex mode.</td>
</tr>
<tr>
<td>Protocol Enabled</td>
<td>Protocol enabled on the port.</td>
</tr>
<tr>
<td>Protocol Seen</td>
<td>Protocols seen on the port.</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN to which the port is part of.</td>
</tr>
<tr>
<td>L2L3</td>
<td>Shows whether the port is routed or switched.</td>
</tr>
<tr>
<td>Jumbo Frame</td>
<td>Displays whether Jumbo Frames are enabled or disabled on the port.</td>
</tr>
<tr>
<td>Trunk Encapsulation</td>
<td>Shows the type of trunk encapsulation.</td>
</tr>
<tr>
<td>Trunk Mode</td>
<td>Shows the trunk mode.</td>
</tr>
<tr>
<td>isChannel</td>
<td>Shows whether the port is part of a channel.</td>
</tr>
</tbody>
</table>

You can export or print the report.
To export the report to a Common Services server, click the export button at the top right of the page.
To print the page, click the printer icon on the top right of the page.

Displaying Device Attributes

To display information about a specific device.

**Step 1**  Select Campus Manager > Reports > Report Generator.
The Reports Generator page appears.

**Step 2**  Select Campus Reports from the Select An Application drop-down list.

**Step 3**  Select Device Attributes from Select a Report drop-down list.
The Device Attributes page appears.

**Step 4**  Select a device or domain from the list.
**Step 5** Select the **Scheduling Type**.

The default scheduling type is Immediate.

You can set the time and date if you select any of the following scheduling types: Once, Daily, Weekly, Monthly.

**Step 6** Enter a description for your job in the Job Description field and enter the e-mail address to which the details has to be sent.

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

For more information on Device Attributes, see Interpreting Device Attributes Report.

---

**Interpreting Device Attributes Report**

To view the device attributes report for a device, select the device from the **Go To:** list. The Go To: list contains the device name, device IP address, and the device type.

Report for each device is displayed in a table with the Device Name, Device IP Address, and Device Type as the table heading.

Alternatively, you can scroll the page to view the report for the selected devices.

The device attributes report contains the following information for a device:

**Table 10-23 Port Attributes Report Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module</td>
<td>Name of the module</td>
</tr>
<tr>
<td>Slot Number</td>
<td>Slot in which the module is connected.</td>
</tr>
<tr>
<td>Sub Module ID</td>
<td>Sub module id of the device.</td>
</tr>
<tr>
<td>#Ports</td>
<td>Number of ports in the module.</td>
</tr>
<tr>
<td>Version(s)</td>
<td>Hardware and software version of the module.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>hw:1.2 sw:12.2(25)EWfw:12.1(12r)EW</td>
</tr>
<tr>
<td>Status</td>
<td>Shows the status of the module.</td>
</tr>
<tr>
<td>Daughter Card</td>
<td>Daughter cards in the module. Empty means daughter cards are not available for the module.</td>
</tr>
</tbody>
</table>
Displaying Trunk Attributes

To display information about the status of the trunking ports in your network.

Step 1  Select Campus Manager > Configuration > Trunk Configuration from the LMS Portal.

The Trunk Configuration page appears.

Step 2  Click Modify Trunk Attributes from the TOC.

Step 3  Select device or domain from the list.

Step 4  Click Show Trunks.

A list of trunks appears.

Step 5  Select the radio-button corresponding to a trunk.

Step 6  Click Modify Trunk.

The Modify Trunk Attributes window appears with the trunk attributes.

For more information on Trunk Attributes, see Interpreting Trunk Attributes.

Interpreting Trunk Attributes

See Table 10-24 for details about the fields shown in the Trunk Attributes window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Information</strong></td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td>Device to which the port belongs.</td>
</tr>
<tr>
<td>Port</td>
<td>Name of the port.</td>
</tr>
<tr>
<td><strong>Trunk Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Type of encapsulation the trunk is using. Supported encapsulation types are: Dot1Q, ISL, Negotiate.</td>
</tr>
<tr>
<td>Mode</td>
<td>Half-duplex or full-duplex.</td>
</tr>
<tr>
<td><strong>Configure VLANs on Trunk</strong></td>
<td></td>
</tr>
<tr>
<td>Allowed VLANs</td>
<td>List of VLANs allowed. * sign indicates that the VLAN was previously disallowed.</td>
</tr>
<tr>
<td>Disallowed VLANs</td>
<td>List of disallowed VLANs. Use Add and Remove buttons to move VLANs between these lists.</td>
</tr>
</tbody>
</table>
# Troubleshooting Suggestions

Use the information in the Troubleshooting VLAN Port Assignment Table 4-3 to troubleshoot the VLAN Port Assignment application.

## Table 10-25  Troubleshooting VLAN Port Assignment

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Probable Cause</th>
<th>Possible Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Port Assignment starts, but shows an error message.</td>
<td>Server process is not running.</td>
<td>Confirm that the Campus Database engine and the Campus Server are running.</td>
</tr>
<tr>
<td>VTP Domain drop-down list box is empty and the following error message appears:</td>
<td>A seed device is not specified for the ANI Server.</td>
<td>Add a seed device. See ANI Server online help for more information about adding a seed device.</td>
</tr>
<tr>
<td>VTP Domain drop-down list box is blank and the following message appears:</td>
<td>The initial device discovery is not complete.</td>
<td>Wait for the ANI status bar to display Idle.</td>
</tr>
<tr>
<td>ANI is still in the discovery process. Please wait.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The message Operation Failure appears when you try to move a port.</td>
<td>The operation failed for one of various possible reasons.</td>
<td>Click Details to display the cause of the failure.</td>
</tr>
</tbody>
</table>
Usage Scenarios for Managing VLANs

You can use the following scenarios to manage your network using Campus Manager.

Configuring PVLANs in External Demilitarized Zone

Scenario
Web servers and Domain Name Servers (DNS) are connected to a Demilitarized Zone (DMZ) switch. The DMZ switch is configured with the VTP domain name, DMZ, where the switch is in transparent mode running VTP version 2. The servers belong to the same broadcast domain or VLAN.

Understanding the Scenario
This scenario would help you to isolate Layer 2 devices using PVLAN, and ensure that the DMZ servers do not send data across them, while internal and external hosts access these servers.

DMZ servers must be accessible from external clients as well as from the internal network. DMZ servers eventually needs access to some internal resources, and the servers must not send data across. The servers must not initiate traffic from the DMZ switch to the Internet. The DMZ servers reply only to the traffic from the internal resources.

Understanding Concepts
Campus Manager provides an end-to-end solution for configuring Private VLANs, the security feature which Campus Manager provides for managing LANs. You can configure PVLANs using Campus Manager.

You can configure PVLANs in scenarios where Demilitarized Zone (DMZ) switches are configured without adhering to the right policies, leading to potential intrusions into your network.

Demilitarized Zone
Demilitarized Zone is a small subnetwork, which lies between a secure internal network, such as a corporate private LAN, and a non-secure external network, such as the public Internet. DMZ contains devices like Web servers, FTP servers, SMTP servers and DNS that are accessible to the Internet traffic.

DMZ servers process incoming requests from the Internet, and initiate connections to certain internal servers or other DMZ segments, such as database servers.

DMZ servers must not send data or initiate any connection to the external networks. This shows that the necessary traffic flows on the basis of a trust model; but the model is not adequately enforced in many networks.

Prerequisites
In this scenario, you need the following applications and tools in Campus Manager.

- Topology Services
- PVLAN configuration user interface
- VLAN Port Assignment
- Promiscuous port configuration user interface
- VLAN report
- Path Analysis
Reproducing Scenario

To set up the scenario you must configure secondary VLAN on the servers, with isolated ports and community ports. The Firewall, the only device within the primary VLAN, must be defined in a primary VLAN with a promiscuous port.

**Step 1** Create a primary VLAN: VLAN 100.
Enter VLAN 100 in the Private VLAN Name field to name the primary VLAN. For more details on creating primary VLAN, see Creating Primary VLAN.

**Step 2** Create a community VLAN: VLAN 50.
   a. Enter VLAN 50 in the Private VLAN Name field.
   b. Associate VLAN 50 to the primary VLAN, VLAN 100.
For more details on creating secondary VLAN, see Creating Secondary VLAN and Associating to Primary VLAN.

**Step 3** Create an isolated VLAN: VLAN 60.
   a. Enter VLAN 60 in the Private VLAN Name field to name the isolated VLAN
   b. Associate VLAN 60 to the primary VLAN, VLAN 100.
For more details on creating secondary VLAN, see Creating Secondary VLAN and Associating to Primary VLAN.

**Step 4** Assign ports, which are connected to the Web servers, to the community VLAN 50.

**Step 5** Assign ports, which are connected to the DNS servers, to the isolated VLAN 60.

**Step 6** Configure the port that connects to the Firewall as a promiscuous port and map the secondary VLAN 50 and VLAN 60 to this promiscuous port. For more details, see Configuring Promiscuous Ports.
After you configure the promiscuous port, the secondary VLANs appear in the Mapped VLANs table.

You have configured promiscuous port and mapped both secondary VLANs to the primary VLAN 100. If you want to map only the community VLAN 60, you must check the configurations, and map the other isolated VLANs.

Check the Select to Unmap check box and click Apply to unmap the isolated VLAN from primary VLAN. Community VLAN 60 is unmapped from the primary VLAN.
Verifying Configuration

To verify the configuration for this scenario:

**Step 1** Select Campus Manager > Visualization > Topology Services from the CiscoWorks Homepage. The Topology Services Main Window appears.

**Step 2** From the Tree View in the Topology Services Main window, verify whether the new PVLANs are listed under DMZ VTP domain in transparent mode. Primary VLAN 100 is listed as a subfolder under the DMZ domain and the secondary VLAN under the Primary VLAN subfolder. Note that the icon for PVLANs is different from the icon for normal VLANs.

**Step 3** Generate VLAN Report for DMZ domain.

**Step 4** Verify whether the new primary VLAN and secondary VLANs are listed. The associated primary VLAN is also listed for the secondary VLANs.

**Step 5** Select Campus Manager > Diagnostics > Path Analysis from the CiscoWorks Homepage.

**Step 6** To confirm that the PVLAN configuration is functioning, you can:

- **a.** Run a trace between the Web servers. The resultant traces must be successful.
- **b.** Run a trace between any Web server and the DNS. The resultant trace must fail.
- **c.** Run a trace between the DNS servers.