Configuring VLAN

LMS collects data about devices so that you can configure and manage Virtual Local Area Network (VLAN) in your network. You must set up your LMS server properly to ensure that Data Collection is successfully performed in your network.

The configuration module in LMS helps you to manage your VLANs. You can configure and manage VLAN, Private VLAN (PVLAN), Trunk, and also assign ports to VLANs.

This chapter contains:

- Understanding Virtual LAN (VLAN)
- Using VLANs
- Configuring VLANs
- Creating Ethernet VLANs
- Configuring Token Ring 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 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 Configuration Management functionality in LMS to create, modify, and delete VLANs. You can use the Topology Services to create Ethernet VLANs.

LMS 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 **Configuration > Workflows > VLAN > Configure VLAN.**

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 11-1**

**Table 11-1 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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Click the radio button to select the Domain Selector.</td>
</tr>
<tr>
<td>All</td>
<td>Click <strong>All</strong> 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 <strong>All</strong> 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 11-2**.

<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>
</tbody>
</table>
| VLAN Index                   | Enter a number to identify the VLAN. You can enter a number within the range:  
  • 2 to 1001                
  • 1025 to 4094             
  You cannot enter 1 or a number in the range 1002 to 1024, as the VLAN Index. These are reserved numbers. |
| 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.                                                             |

Click any of the following:

- **Next** to continue.
  
  The Assign Ports to VLAN 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 behavior:

<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></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 behavior:

<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>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>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:

**Step 1** Select Configuration > Workflows > VLAN > Configure VLAN.

The VLAN Configuration page appears.

**Step 2** Select device or domain from the VLAN Configuration page.

**Step 3** Click Create.

**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 11-3 describes the entries in the Assign Ports to VLAN page.

<table>
<thead>
<tr>
<th><strong>Table 11-3 Assign Ports to VLAN Page Field Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>VLAN</td>
</tr>
<tr>
<td>Filter</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Advanced Filter</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Column</td>
</tr>
<tr>
<td>Link</td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td>Device Name</td>
</tr>
<tr>
<td>Device Address</td>
</tr>
<tr>
<td>Port Status</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 11-3** describes the fields in the Filter Ports Window, when you click Advanced Filter from the Assign Ports to VLAN Window.

**Table 11-3 Assign Ports to VLAN Page Field Description (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 11-4** describes the fields in the Filter Ports Window, when you click Advanced Filter from the Assign Ports to VLAN Window.

**Table 11-4 Filter Ports Field Description**

<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>
</tbody>
</table>
Chapter 11  Configuring VLAN

Table 11-4  Filter Ports Field Description (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Select a parameter for which you want to filter the ports. Parameter is the attribute of a port. The values displayed for Assigning ports to VLANs are:</td>
</tr>
<tr>
<td></td>
<td>• Device Name</td>
</tr>
<tr>
<td></td>
<td>• Device Address</td>
</tr>
<tr>
<td></td>
<td>• Link</td>
</tr>
<tr>
<td></td>
<td>• Port</td>
</tr>
<tr>
<td></td>
<td>• Port Status</td>
</tr>
<tr>
<td></td>
<td>• Port Description</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>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 11-5 describes the fields in the Disallow VLAN on Trunks page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Name</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 Name</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 Name</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 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 **Configuration > Workflows > VLAN > Delete VLAN.**  
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 11-6** describes the fields in the Select a VLAN to Delete dialog box.

**Table 11-6  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>
<tr>
<td>Filter Source</td>
<td>Select the Filter type of the source:</td>
</tr>
<tr>
<td></td>
<td>•  VLAN</td>
</tr>
<tr>
<td></td>
<td>•  VLAN Name</td>
</tr>
<tr>
<td></td>
<td>•  Domain Name</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>
<tr>
<td>Select</td>
<td>Select the radio button corresponding to the VLAN you want to delete.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Index of the VLAN.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>Name of the VLAN.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Name of the domain in which the VLAN belongs to.</td>
</tr>
</tbody>
</table>

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 LMS.

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:

Step 1 Select Configuration > Workflows > VLAN > Configure VLAN.
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.

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 11-7 describes the fields in the Move Affected Ports to new VLAN page.

Table 11-7 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>

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 : Gi1/6
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 that belong to the same VLAN, are assigned to the same Ethernet VLAN. For further details see Creating Ethernet VLANs.
Chapter 11  Configuring VLAN

Configuring Token Ring VLANs

A Token Ring VLAN is a set of rings interconnected through a bridging function. There are two Token Ring VLAN types defined in VTP version 2:

- Token Ring Bridge Relay Function (trBRF)—Domain of interconnected rings formed, using an internal multiport bridge function.
- Token Ring Concentrator Relay Function (trCRF)—Logical ring domains formed by defining groups of ports that have the same ring number.

You can create Token Ring Bridge Relay Function (trBRF) VLANs and Token Ring Concentrator Relay Function (trCRF) VLANs. Multiple trCRFs can be interconnected using a single trBRF.

A trBRF VLAN is a domain of interconnected rings formed using an internal multiport bridge function. A trCRF VLAN is a logical ring domain formed by defining groups of ports that have the same ring number.

This section contains:

- Understanding trBRF VLANs
- Creating trBRF VLANs
- Understanding trCRF VLANs
- Creating trCRF VLANs
- Deleting trBRF and trCRF VLANs

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 Either:
  • Select Configuration > Topology.
Or
  • Select Monitor > Monitoring Tools > Topology Services.
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.
Understanding trBRF VLANs

A Token Ring Bridge Relay Function (trBRF) is a logical grouping of trCRFs. The trBRF is used to join different trCRFs. In addition, the trBRF can be extended across a network of switches through high-speed uplinks between the switches to join trCRFs contained in different switches.

A trBRF has two global parameters: a bridge number and a bridge type. The bridge number is used to identify the logical distributed source-route bridge (SRB), which interconnects all logical rings that have the same parent trBRF.

Creating trBRF VLANs

To create Token Ring Bridge Relay Function (trBRF) VLANs in your network.

**Step 1** Select a VTP domain from the Tree View.

**Step 2** Select Tools > VLAN Management > Create > Token Ring BRF from the menu. See Table 11-8 for details.

**Table 11-8 Creating trBRF VLANs Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTP Domain</td>
<td>Name of VTP domain in which this VLAN will be created.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>Enter a name for the trBRF.</td>
</tr>
<tr>
<td>VLAN Index</td>
<td>Topology Services automatically assigns a VLAN index. This number is incremented each time you create a VLAN in this VTP domain. If you want to change the VLAN index, enter a number between 1 and 1024 to identify the VLAN.</td>
</tr>
<tr>
<td>Purpose</td>
<td>Enter a word or phrase that describes the purpose of the VLAN.</td>
</tr>
<tr>
<td>Description</td>
<td>Describe the contents of the VLAN.</td>
</tr>
<tr>
<td>Create VLAN on all Transparent Switches</td>
<td>Check this box to include this VLAN on switches configured as VTP transparent.</td>
</tr>
</tbody>
</table>

**BRF Parameters**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge Number</td>
<td>Integer in hexadecimal format. The default is 0xF.</td>
</tr>
<tr>
<td>STP Type</td>
<td>Spanning Tree protocol used in the network.</td>
</tr>
</tbody>
</table>

**Step 3** Click Apply.
Understanding trCRF VLANs

A Token Ring Concentrator Relay Function (trCRF) is a logical grouping of ports. Each trCRF is contained in only one trBRF, which is called its parent. When a port is assigned to the trCRF, only ports on that switch can belong to that trCRF.

As a rule, a trCRF cannot span different switches. This type of trCRF is called an undistributed trCRF. However, if your switches are connected through Inter-Switch Link (ISL), the Cisco Duplicate Ring Protocol (DRiP) allows two types of trCRFs in which the ports of a single trCRF can be on different switches.

These types of trCRFs are the default and the backup trCRF:

- **Default trCRF**
  The default trCRF can contain ports that are located on multiple switches. The default trCRF is associated with the default trBRF, which can span switches through ISL.
  Since the default trCRF is the only trCRF that can be associated with the default trBRF, the default trBRF does not perform any bridging functions, but uses source-route switching to forward traffic between the ports of the default trCRF.

- **Backup trCRF**
  The backup trCRF allows you to configure an alternate route for traffic between undistributed trCRFs located on separate switches that are connected by a trBRF. The backup trCRF is only used if the ISL connection between the switches becomes inactive.

Creating trCRF VLANs

You must configure a Token Ring Bridge Relay Function (trBRF) VLAN before creating the trCRFs that you want associated with the trBRF.

To create Token Ring Concentrator Relay Function (trCRF) VLANs in your network:

**Step 1** Select a trBRF from the Tree View.

**Step 2** Select Tools > VLAN Management > Create > Token Ring CRF from the menu.

For more information, see Table 11-9.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTP Domain</td>
<td>Name of VTP domain in which this VLAN will be created.</td>
</tr>
<tr>
<td>trBRF</td>
<td>Name of trBRF to which this trCRF belongs.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name for the VLAN.</td>
</tr>
<tr>
<td>VLAN Index</td>
<td>Topology Services automatically assigns a VLAN index. This number is incremented each time you create a VLAN in this VTP domain. If you want to change the VLAN index, enter a number between 1 and 1024 to identify the VLAN.</td>
</tr>
</tbody>
</table>
Chapter 11 Configuring VLAN

Configuring Token Ring VLANs

Step 3
Click Apply.

The LANE Services option is active.

To configure LANE in your network, click LANE Services.

Step 4
Click OK.

Your changes are saved and the window closes.

Deleting trBRF and trCRF VLANs

You can delete VLANs in your network. If you delete a VLAN with active ports, it disables the active ports in that VLAN.

You can use VLAN Port Assignment application to move any port to another VLAN.

You can delete a token ring Bridge Relay Function (trBRF) only if all token ring Concentrator Relay Functions (trCRFs) within it have been deleted, or if they do not contain any ports.

Deleting a VLAN with an associated ATM-VLAN does not delete the ATM-VLAN. The ATM-VLAN remains intact and appears in the Standalone ATM-VLANs folder for the ATM domain to which it belongs.

Your login determines whether you can use this option.

To delete a VLAN:

Step 1
Select Config > Topology Services.

The Topology Services Main Window appears.

Step 2
Select a VLAN that you want to delete, from the Tree View under Managed Domains.

---

### Table 11-9 Creating trCRF VLANs Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Enter a word or phrase that describes the purpose of the VLAN.</td>
</tr>
<tr>
<td>Description</td>
<td>Describe the contents of the VLAN.</td>
</tr>
<tr>
<td>Create VLAN on all Transparent Switches</td>
<td>Check this box to include this VLAN on switches configured as VTP transparent.</td>
</tr>
<tr>
<td>Ring Number</td>
<td>Enter an integer between 1 and 0FFFH, or accept the ring number Topology Services creates.</td>
</tr>
<tr>
<td>VLAN Bridge Type</td>
<td>Select a bridging mode for this trCRF.</td>
</tr>
<tr>
<td>ARE (All Routes Explorer) Hop Count</td>
<td>Enter the ARE hop count. Valid numbers are 1 to 13, and 7 is the default.</td>
</tr>
<tr>
<td>STE (Spanning Tree Explorer) Hop Count</td>
<td>Enter the STE hop count. Valid numbers are 1 to 13, and 7 is the default.</td>
</tr>
<tr>
<td>Backup CRF</td>
<td>Check this option if this trCRF is going to be the backup trCRF. A backup trCRF will replace the trBRF if the trBFR fails.</td>
</tr>
</tbody>
</table>
Step 3  Select **Tools > VLAN Management > Delete**.

The domain window appears with a message:

The selected VLAN will be deleted if no ports are associated with this VLAN. Do you want to continue?

Step 4  Check the check box **Delete** on all Transparent Switches, if required.

Step 5  Click **Yes** to delete the VLAN or click **No** to exit.

---

### Interpreting VLAN Summary Information

This section contains:

- Displaying VLAN Reports
- Interpreting VLAN Reports

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 11-10 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>
<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

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

**Step 1** Select Reports > Technology > VLAN.

The Report Generator page appears.

The left drop-down list displays LMS Reports.

**Step 2** Select VLAN from Select a Report drop-down list.

The VLAN page appears with the following information. See Table 11-11:

<table>
<thead>
<tr>
<th>Table 11-11</th>
<th><strong>VLAN Page Field Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Scheduling</td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>Select a run type from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>The following run types are available: Immediate, Once, Daily, Weekly, Monthly.</td>
</tr>
<tr>
<td></td>
<td>If you select Immediate, the Job Info fields and Scheduling Date will be dimmed.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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.</td>
</tr>
<tr>
<td>Date</td>
<td>Select the date and time at which you need to generate the report.</td>
</tr>
<tr>
<td></td>
<td>Format: 20 Apr 2005 at 01 20</td>
</tr>
</tbody>
</table>
Interpreting VLAN Summary Information

Table 11-11 VLAN Page Field Description (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Job Info</strong></td>
<td></td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter a description for this report.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter the e-mail id to which the report has to be sent.</td>
</tr>
<tr>
<td>Report Publish Path</td>
<td>Use the Default Path check box to publish the report at a specific location.</td>
</tr>
<tr>
<td></td>
<td>If you check the Default Path check box, it publishes the report in the</td>
</tr>
<tr>
<td></td>
<td>default directory path. If you uncheck the Default Path check box, it</td>
</tr>
<tr>
<td></td>
<td>allows you to specify a directory path to which the report is published.</td>
</tr>
<tr>
<td></td>
<td>If the directory path is not specified, then the report will be published to:</td>
</tr>
<tr>
<td></td>
<td>• For Windows: C:\Progra~1\CSCOpx\VLAN</td>
</tr>
<tr>
<td></td>
<td>• For Solaris and Soft Appliance: /opt/CSCOpx/VLAN</td>
</tr>
<tr>
<td></td>
<td>A PDF format of the report (along with HTML and CSV formats) is published to</td>
</tr>
<tr>
<td></td>
<td>the specified location.</td>
</tr>
<tr>
<td>Attachment Option</td>
<td>Check this check box to attach the report as a CSV file. By default a CSV</td>
</tr>
<tr>
<td></td>
<td>file is sent to the e-mail address specified in the E-Mail ID field. If you</td>
</tr>
<tr>
<td></td>
<td>check Add Full Report check box, instead of CSV a PDF format of the report</td>
</tr>
<tr>
<td></td>
<td>will be sent as an attachment to the specified e-mail id.</td>
</tr>
<tr>
<td></td>
<td>You need to enable the e-mail Attachment check box and specify the</td>
</tr>
<tr>
<td></td>
<td>Maximum Attachment size in the System Preferences dialog box (Admin &gt;</td>
</tr>
<tr>
<td></td>
<td>System &gt; System Preferences) to send the report as an e-mail.</td>
</tr>
<tr>
<td></td>
<td>If the file size exceeds the Maximum Attachment size, the URL link of</td>
</tr>
<tr>
<td></td>
<td>the report is sent as an e-mail. You can click the URL link to view the</td>
</tr>
<tr>
<td></td>
<td>report.</td>
</tr>
</tbody>
</table>

Step 3  
Click **Submit** to generate the report. The VLAN reports window appears.

Or

Click **Reset** to change the settings.

You can open VLAN reports page from Topology Services.

To open VLAN reports from Topology Services:

Step 1  
Either:

• Select **Configuration > Topology**.

Or

• Select **Monitor > Monitoring Tools > Topology Services**.

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 11-12 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, primary, 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 device operates. Device can be in ethernet, FDDI, or inactive.</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

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.

- **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.

This section explains:

- Creating PVLAN
- Configuring Promiscuous Ports
- Deleting PVLAN

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.

LMS 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:

- Creating Primary VLAN
- Creating Secondary VLAN and Associating to Primary VLAN
- Associating Ports to Secondary VLAN

Creating Primary VLAN

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

To create Primary VLANs:

Step 1  Either

- Select Configuration > Workflows > VLAN > Create Private VLAN.
  The Create PVLAN page appears.

  Or

- Select Configuration > Topology.

  Or

- Select Monitor > Monitoring Tools > Topology Services.
  The Topology Services Main Window appears.
  – Select a VTP domain from the VTP Tree View, under the Managed Domain or Network View.
  – Select Tools > PVLAN Management > Create.
  The Create PVLAN page appears.

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

Step 3  Select Primary from the Private VLAN Type drop-down list.
  The Get Primary VLANs tab and the Associated Primary VLAN field is disabled.

Step 4  Enter a name for the VLAN in the VLAN Name field.

Step 5  Enter the VLAN index number for the new Primary VLAN, in the VLAN Index field.
Step 6 Check the check boxes as required:
  • To create private VLAN on all transparent switches.
  • To copy Running to Start up 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 7 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 Either:
  • Select Configuration > Workflows > VLAN > Create Private VLAN.
    The Create PVLAN page appears.
  Or
  • Select Configuration > Topology.
  Or
  • Select Monitor > Monitoring Tools > Topology Services.
    The Topology Services Main Window appears.
      – Select a VTP domain from the VTP Tree View, under the Managed Domain or Network View.
      – Select Tools > PVLAN Management > Create.
        – The Create PVLAN page appears.

Step 2 Select one of the following options from the Private VLAN Type drop-down list:
  • Isolated
  • Community
  • Two-Way Community

Step 3 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 4 Select the Private VLAN Index.
Step 5  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 6  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 **Configuration > Workflows > VLAN > Configure Promiscuous Ports**.

The Configure Promiscuous Ports page appears.

Step 2  Select a device or entities from the list using Device Selector or Domain Selector.

Step 3  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 4  Select the ports from the ports listed in the table.

Step 5  Click **Configure**.

The Configure Promiscuous Port window appears.

The Port Details table displays:

- Device Name
- Port Name
- Device IP Address
- IfName

Step 6  Select the VLANs from the list of Available PVLANs.
Step 7  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 8  Click Apply to configure.  

Deleting PVLAN  
To delete PVLAN:  

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PVLAN List</td>
<td>You can select any of the following filter criteria:</td>
</tr>
<tr>
<td>Filter</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>
</tbody>
</table>

Enter the filter string, then click Filter.  

Step 1  Select Configuration > Workflows > VLAN > Delete Private VLAN.  
The Delete PVLAN page appears.  
Step 2  Select a device or entities from the list using Device Selector or Domain Selector.  
Step 3  Click List PVLANs to see a list of PVLANs. See Table 11-13.  

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 4  Select the check box corresponding to the PVLAN you want to delete.  
To select all, select the check-box in the table heading.  
Step 5  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

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

Prerequisite for configuring Inter-VLAN Routing

Configuration Functionality in LMS is a prerequisite for configuring Inter-VLAN Routing.

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

- LMS must manage the devices.
- The device must have the same device name when managed by LMS.

See Inventory Management with Cisco Prime LAN Management Solution 4.2 for more details on how to manage devices.

This section contains:

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

To configure Inter-VLAN Routing on a VLAN interface:

**Step 1**  
Either:  
- Select **Configuration > Topology**.  
Or  
- Select **Monitor > Monitoring Tools > Topology Services**.  
The Topology Services Main Window appears.

**Step 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 11-14.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Interface$^1$</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.
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:

### Step 1
Either:
   - Select **Configuration > Topology**.
   Or
   - Select **Monitor > Monitoring Tools > Topology Services**.
The Topology Services Main Window appears.

### Step 2
Select a device from the Topology Services Tree View, under the Network Views.

### Step 3
Right-click the device and select **Configure Inter-VLAN Routing** from the popup menu.
The Configure Inter-VLAN Routing window appears.

### 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, Encapsulation, and Subnet Mask. See **Table 11-15**

<table>
<thead>
<tr>
<th>Table 11-15 Configuring Inter-VLAN Routing Field Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>VLAN Interface$^1$</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Sub-Interface ID</td>
</tr>
<tr>
<td>Admin Status</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></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 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 2**.

**Step 7** 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**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Encapsulation  | Select the encapsulation:  
|                | - dot1Q     |
|                | - ISL       |
| Subnet Mask    | Enter the subnet mask address. |

1. You can enter the VLAN interface name to create a new interface. You cannot edit an existing VLAN interface.
Chapter 11      Configuring VLAN

This topic contains:

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

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.

For further details see Support for VTP Version 3.

Support for VTP Version 3

LMS 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 LMS, the Off mode devices are considered similar to the Transparent mode devices.

  For more details, see Figure 11-1.
• 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.
Notes on creating VLAN or PVLAN in VTP version 3 domain using LMS

- 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**

Either:
- Select **Configuration > Topology**.

Or
- Select **Monitor > Monitoring Tools > Topology Services**.

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 11-16 to interpret the fields shown in the VT Reports Summary view.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link</td>
<td>A lightning bolt indicates a port that is linked to a switch.</td>
</tr>
<tr>
<td>Port</td>
<td>Number of ports in the domain.</td>
</tr>
<tr>
<td>IfName</td>
<td>Interface Name.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of the device to which the port belongs.</td>
</tr>
<tr>
<td>Device Address</td>
<td>Address of the device to which the port belongs.</td>
</tr>
<tr>
<td>PortStatus</td>
<td>Displays the status of the port, whether the port is active or dormant.</td>
</tr>
<tr>
<td>isTrunk</td>
<td>If the box is checked, the port is configured as a VLAN Trunk.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Name of the VLAN.</td>
</tr>
<tr>
<td>Association Type</td>
<td>Type of VLAN</td>
</tr>
<tr>
<td>Port Mode</td>
<td>Displays the mode of the port. For example, PVLAN-Host, Promiscuous, or a non-PVLAN.</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 11-2

Figure 11-2  VTP Tree View

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.
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, it's 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 `nonegotiate` 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 11-17 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><strong>on</strong></td>
<td>YES, periodic</td>
<td>Trunking is active. The interfaces send 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><strong>auto</strong></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><strong>desirable</strong></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 Configuration > Workflows > VLAN > Create Trunk.

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 11-18 describes the fields in the Available Links pane.
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 11-19** describes the fields in the Create Trunk page.

**Table 11-18**  
*Available Links Field Description*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Filter      | 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 **Filter**. |
| Port 1      | Port of the first device in the link.                                      |
| Device 1    | IP Address (IPv4 or IPv6 Address) of the device to which the port1 belongs to. |
| Port 2      | Port of the second device in the link.                                     |
| Device 2    | IP Address (IPv4 or IPv6 Address) of the device to which the port2 belongs to. |

**Table 11-19**  
*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. LMS supports: Dot1Q, ISL, Negotiate.</td>
</tr>
<tr>
<td>Mode</td>
<td>Trunking mode of the port is set to <strong>Desirable</strong>. LMS 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.</td>
</tr>
<tr>
<td>1. Select the VLANs for which you do not want to configure Trunk.</td>
<td></td>
</tr>
<tr>
<td>2. Click <strong>Add</strong> to move the VLANs to Disallowed VLANs list.</td>
<td></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>2. Click <strong>Remove</strong> to move the VLANs to the list of Allowed VLANs.</td>
<td></td>
</tr>
</tbody>
</table>
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 **Configuration** > **Workflows** > **VLAN** > **Modify Trunk Attributes**.

The Modify Trunk Attributes page appears.

**Step 2**  Select devices from the device list, and click **Show Trunks**.

The trunks configured on the devices are listed in the Trunk List. See Table 11-20.
Step 3 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 4 Select the Trunk Settings

a. Select Encapsulation:
   - Dot1Q
   - ISL
   - Negotiate

b. Mode

Step 5 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 6 Click **Modify**.
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.

LMS 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. LMS supports only the Desirable mode for EtherChannel configuration.

LMS does not support EtherChannel configuration between a switch and router.

Using EtherChannel

LMS 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  Either:
- Select Configuration > Topology.

Or
- Select Monitor > Monitoring Tools > Topology Services.

The Topology Services Main Window appears.

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

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.

LMS 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, LMS must discover the network. LMS requires a properly configured network to complete network discovery.

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:

Step 1 Verify that your network is set up properly.
Step 2 Verify that the LMS server is set up properly and running.
Step 3 Select Configuration > Workflows > VLAN > Configure 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

This section provides information to assign ports to VLAN.

To assign ports to a VLAN:

**Step 1** Select Configuration > Workflows > VLAN > Configure 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 11-21 for the Port List:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>• Device Name</td>
</tr>
<tr>
<td></td>
<td>• Device Address</td>
</tr>
<tr>
<td></td>
<td>• Link</td>
</tr>
<tr>
<td></td>
<td>• Port</td>
</tr>
<tr>
<td></td>
<td>• Port Status</td>
</tr>
<tr>
<td></td>
<td>• Port Description</td>
</tr>
<tr>
<td></td>
<td>• VLAN Name</td>
</tr>
<tr>
<td></td>
<td>• VLAN Index</td>
</tr>
<tr>
<td></td>
<td>• Association Type</td>
</tr>
</tbody>
</table>

Enter the filter string, and click Filter to filter the list based on the inputs. Leave this field blank to list all ports.

**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.

**Columns**

<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>
<tr>
<td>VLAN Index</td>
<td>Index number of the VLAN to which the port belongs to.</td>
</tr>
<tr>
<td>Association Type</td>
<td>Type of Association.</td>
</tr>
</tbody>
</table>
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.

Usage Scenarios for Managing VLANs

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

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

This section contains:

- Prerequisites
- Reproducing Scenario
- Verifying Configuration
Prerequisites

In this scenario, you need the following applications and tools in LMS.

- Topology Services
- PVLAN configuration user interface
- VLAN Port Assignment
- Promiscuous port configuration user interface
- VLAN report

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** Either:
- Select **Configuration > Topology**.

Or
- Select **Monitor > Monitoring Tools > Topology Services**.

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

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