



Managing VLANs and VTP

To ensure that the ANI Server successfully performs Data Collection in your network, you must set up your network properly. Campus uses ANI Server to discover devices data so that you can configure and manage virtual LANs (VLANs) in your network.

- [Understanding Virtual LAN \(VLAN\), page 9-2](#)
- [Using Virtual LANs, page 9-5](#)
- [Interpreting VLAN Summary Information, page 9-14](#)
- [Understanding Private VLAN, page 9-17](#)
- [Using Private VLAN, page 9-19](#)
- [Understanding Inter-VLAN Routing, page 9-24](#)
- [Using Inter-VLAN Routing, page 9-25](#)
- [VLAN Trunking Protocol, page 9-30](#)
- [Understanding Trunking, page 9-39](#)
- [EtherChannel, page 9-44](#)
- [VLAN Port Assignment, page 9-47](#)
- [Using VLAN Port Assignment, page 9-49](#)
- [Usage Scenarios for Managing VLANs, page 9-68](#)

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 would contain 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 is useful for reducing the size of broadcast domains, or allowing groups or users to be logically grouped without being physically located in the same place.

The following topics are covered in this chapter:

- [Advantages of VLANs, page 9-2](#)
- [VLAN Components, page 9-4](#)
- [Using Virtual LANs, page 9-5](#)

Advantages of VLANs

VLANs provide the following advantages:

- [Simplification of Adds, Moves, and Changes, page 9-2](#)
- [Controlled Broadcast Activity, page 9-3](#)
- [Workgroup and Network Security, page 9-3](#)

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 one 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 perform the following:

- 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 and ATM backbones.

The VLAN transport enables information exchange between interconnected switches and routers on the corporate backbone. The 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.

Types of VLANs Supported

Topology Services supports four types of VLANs:

- [Ethernet VLANs, page 9-6](#)
- [Understanding ATM-VLANs, page 12-1](#)
- [Token Ring VLANs, page 9-7](#)
- [Understanding Private VLAN, page 9-17](#)

Using Virtual LANs

You can use Campus to create, modify, and delete VLANs. This topic contains the following:

- [Creating VLANs](#)
- [Modifying VLANs](#)
- [Deleting VLANs](#)

Creating VLANs

You can use Topology Services to create Ethernet VLANs (which is the typical VLAN design), or you can create Token Ring VLANs. This topic contains the following:

- [Creating Ethernet VLANs](#)
- [Creating trBRF VLANs](#)
- [Creating trCRF 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 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** Start **Campus Manager > Topology Services** from the CiscoWorks Homepage.
 - Step 2** Select a VTP domain from the Tree View.
 - Step 3** Select **Tools > VLAN Management > Create > Ethernet** from the menu.
- See [Table 9-1, Creating Ethernet VLANs Field Descriptions](#) table for details.

Table 9-1 *Creating Ethernet VLANs Field Descriptions*

Field	Description
VTP Domain	Name of VTP domain in which this VLAN will be created.
VLAN Name	Name for the VLAN.
VLAN Index	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.
Purpose	Enter a word or phrase that describes the purpose of the VLAN.

Table 9-1 *Creating Ethernet VLANs Field Descriptions (continued)*

Field	Description
Description	Describe the contents of the VLAN.
Create VLAN on all transparent switches	Check this box to include this VLAN on switches configured as VTP transparent.

Step 4 Click **Apply**.

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.

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 9-2](#) for details.

Table 9-2 *Creating trBRF VLANs Field Descriptions*

Field	Description
VTP Domain	Name of VTP domain in which this VLAN will be created.
VLAN Name	Enter a name for the trBRF.
VLAN Index	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.
Purpose	Enter a word or phrase that describes the purpose of the VLAN.
Description	Describe the contents of the VLAN.
Create VLAN on all Transparent Switches	Check this box to include this VLAN on switches configured as VTP transparent.
BRF Parameters	
Bridge Number	Integer in hexadecimal format. The default is 0xF.
STP Type	Spanning Tree protocol used in the network.

- 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 referred to as 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 9-3](#).

Table 9-3 *Creating trCRF VLANs Field Descriptions*

Field	Description
VTP Domain	Name of VTP domain in which this VLAN will be created.
trBRF	Name of trBRF to which this trCRF belongs.
Name	Enter a name for the VLAN.
VLAN Index	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.
Purpose	Enter a word or phrase that describes the purpose of the VLAN.
Description	Describe the contents of the VLAN.
Create VLAN on all Transparent Switches	Check this box to include this VLAN on switches configured as VTP transparent.
Ring Number	Enter an integer between 1 and 0FFFH, or accept the ring number Topology Services creates.
VLAN Bridge Type	Select a bridging mode for this trCRF.
ARE (All Routes Explorer) Hop Count	Enter the ARE hop count. Valid numbers are 1 to 13, and 7 is the default.
STE (Spanning Tree Explorer) Hop Count	Enter the STE hop count. Valid numbers are 1 to 13, and 7 is the default.
Backup CRF	Check this option if this trCRF is going to be the backup trCRF. A backup trCRF will replace the trBRF if the trBRF fails.

Step 3 Click **Apply**.

The LANE Services option is active.

To configure LANE in your network, click **LANE Services**.

For assistance configuring LANE services, see [Managing LANE Services, page 12-6](#).

Step 4 Click **OK**.

Your changes are saved and the window closes.

Modifying VLANs

You can modify most of the VLAN characteristics that were entered when you created the VLAN, such as purpose, description, and LANE services.

You can perform these:

- [Modifying Ethernet VLANs, page 9-11](#)
- [Modifying trBRF VLANs, page 9-12](#)
- [Modifying trCRF VLANs, page 9-12](#)

Modifying Ethernet VLANs

Your login determines whether you can use this option. To modify characteristics for an Ethernet VLAN:

Step 1 Select an Ethernet VLAN from the Tree View.

Step 2 Select **Tools > VLAN Management > Modify**.

Step 3 Enter any changes that you want to perform. You can change:

- Purpose
- Description
- LANE Services

- Step 4** Click **OK**.
Your changes are saved and the window closes.
-

Modifying trBRF VLANs

Your login determines whether you can use this option. To modify characteristics for a trBRF VLAN.

- Step 1** Select a trBRF from the Tree View.
- Step 2** Select **Tools > VLAN Management > Modify**.
- Step 3** Enter any changes that you want to perform. You can change:
- Purpose
 - Description
 - Bridge Number
- Step 4** Click **OK**.
Your changes are saved and the window closes.
-

Modifying trCRF VLANs

Your login determines whether you can use this option. To modify characteristics for a trCRF VLAN.

- Step 1** Select a trCRF from the Tree View.
- Step 2** Select **Tools > VLAN Management > Modify**.

Step 3 Enter any changes that you want to perform. You can change:

- Purpose
- Description
- Ring Number
- VLAN Bridge Type
- ARE (All Routes Explorer) Hop Count
- STE (Spanning Tree Explorer) Hop Count
- Backup CRF
- LANE Services (Click **LANE Services** to modify)

Step 4 Click **OK**.

Your changes are saved and the window closes.

Deleting 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 Start **Campus Manager > Topology Services** from the CiscoWorks Homepage.

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

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

You can display summary information about the VLANs in your network.

Step 1 From Tree View in Topology Services, open a VTP domain and select a VLAN.
See [Table 9-4](#) to interpret this information.

Table 9-4 *VLAN Field Descriptions*

Field	Description
Ports	Number of ports in the domain.
Up Ports	Number of active ports in the domain.
ISL Index	Inter-Switch Link (ISL) index of the VLAN.
Bridge Number	Segment ID used to identify logical distributed source-route bridge (SRB) that interconnects all logical rings that have the same parent trBRF. This appears only if you are viewing trBRF.
Ring Number	The segment ID of the Token Ring Concentrator Relay Function (trCRF) VLAN. Only appears if you are viewing a trCRF.
Port List	
Link	A lightning bolt indicates a port that is connected to a switch.
Port	User assigned name of the specific port.
IfName	Interface name.
Device Name	Name of device to which the port belongs.
Device Address	IP address of device to which the port belongs.
Port Status	Whether the port is active, down, dormant, or testing.
isTrunk	If checked, the port is configured as a VLAN trunk.
Association Type	Type of VLAN.
Port Mode	Displays mode of port. For example, PVLAN-Host, Promiscuous, or non PVLAN.

Displaying VLAN Reports

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

-
- Step 1** Invoke Topology Services.
- 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 pop up menu.
- or
- Select **Reports > VLAN Report**.
- The VLAN Report window appears.
-

Interpreting VLAN Reports

See [Table 9-5](#) to interpret the fields in VLAN Report.

Table 9-5 *VLAN Report Field Description*

Field	Description
Device Name	Name of the devices in the VLAN.
IP Address	IP address of the device.
VLAN ID	Same as VLAN index.
VLAN Name	Name of the VLAN to which the device belongs.

Table 9-5 *VLAN Report Field Description (continued)*

Field	Description
Status	Status of device can be operational or suspended.
Media Type	Explains in which media type the device operates. Device can be in ethernet, token ring, FDDI, or inactive.
VLAN Type	Types of VLANs to which the device is associated. The VLANs can be normal, primary, isolated, community, or two-way community VLANs.
Associated Primary	VLAN ID of the associated primary VLAN.
MTU Size	MTU size for the corresponding VLAN on that device.
VTP Domain	VTP domain in which the device is placed.
Device Type	Type of the device you are referring.

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, page 9-18](#)
- [Using Private VLAN, page 9-19](#)

Types of Private VLAN Ports

The ports in a private VLAN are categorized as:

- [Promiscuous Ports, page 9-18](#)
- [PVLAN Host Ports, page 9-18](#)
- [PVLAN Trunk Ports, page 9-19](#)

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, and the like.

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, which 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.

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 4.0 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.

Hence, for creating a private VLAN you must:

- Create primary VLAN
- Create secondary VLAN
- Associate secondary VLAN to primary VLAN
- Associate ports to secondary VLANs
- Configuring promiscuous ports

Creating Primary VLAN

To create Primary VLANs:

-
- Step 1** Start **Campus Manager > Topology Services** from the CiscoWorks Homepage.

- Step 2** Select a VTP domain from the VTP Tree View, under the Managed Domain or Network View.
- Step 3** Select **Tools > PVLAN Management > Create**.
A Create Private VLAN window appears.
- Step 4** Select **Primary** Private VLAN Type from the following options you have:
- Primary
 - Isolated
 - Community
 - Two-Way Community
- VTP Domain field displays the domain you have chosen.
- Step 5** Enter the Private VLAN Name you want to assign.
You may select the Private VLAN Index, if you want to.
- Step 6** 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 7** Click **Apply** to create primary PVLAN or click **Cancel** to exit.

**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** Start **Campus Manager > Topology Services** from the CiscoWorks Homepage.

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**.

A Create Private VLAN window appears.

Step 4 Select **Secondary** Private VLAN Type from these options:

- Primary
- 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 [“Assigning Ports to VLANs” section on page 9-55](#).

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 Promiscuous Port:

Step 1 Start **Campus Manager > VLAN Port Assignment** from the CiscoWorks Homepage.

Or

From Topology Services main window, select the device, which has the ports you require and select **Tools > VLAN Port Assignment**.

The VLAN Port Assignment window appears.

Step 2 Select the VTP Domain, which has the Private VLAN port on which you want to configure the Promiscuous port.

Step 3 View the ports you want to assign. To do this, either:

- Click **Show All Ports**

Or

- Search using **Find Port** option.

The table below provides a list of ports and the details of the port.

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

Step 5 Click **Configure Promiscuous Port**

The Configure Promiscuous Port window appears. The table displaying Port details displays:

- Device Name
- Port Name
- PVLAN Mode
- Port Speed

Step 6 Select the VLANs from the Available PVLANS table and click **Add** to add to list of Map VLANs. Click **Remove** to remove the VLANs from the Map VLANs table.

Step 7 Click **Apply** to configure.

The configured port details appear in the Mapped VLANs table.

Step 8 To unmap any mapping between a primary and secondary VLANs, check the check box for that mapping in the Select to Un-map field in Mapped VLANs table.

Deleting PVLAN

To delete PVLAN:

Step 1 Invoke Topology Services.

Step 2 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 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 **Yes** to continue or click **No** to quit.

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

Prerequisite for configuring Inter-VLAN Routing through Campus Manager 4.0

Resource Manager Essentials 4.0 (RME 4.0) is a prerequisite for configuring Inter-VLAN Routing using Campus Manager 4.0. If the server running Campus Manager does not have RME 4.0, you can use a remote server, which has the RME 4.0 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 4.0* for more details on how to manage devices. To access this, go to http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/e_4_x/4_0/u_guide/device.htm

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

To configure Inter-VLAN Routing on a VLAN interface:

-
- Step 1** Invoke Topology Services.
- 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 pop up menu.

The Configure Inter-VLAN Routing window appears. The 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.

Table 9-6 *Configuring Inter-VLAN Routing Field Descriptions*

Field	Description
VLAN Interface ¹	Enter the VLAN interface.
IP Address	Enter the IP address for the interface
Subnet Mask	Enter the subnet mask address.
Admin Status	Select the Admin status: <ul style="list-style-type: none"> • Up • Down

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**.



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

RME Server credentials window appears.

Step 8 Enter RME Server, Server Port, User Name, and Password.

Table 9-7 *RME Server credentials Field Description*

Field	Description
RME Server	Name of the RME server or the IP address
Server Port ¹	Enter the port number
User Name	Enter the user name
Password	Enter the password

1. In Campus 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:

- Step 1** Start **Campus Manager > Topology Services** from the CiscoWorks Homepage.
- 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 pop up menu.

The RME Server credentials window appears.

- Step 4** Enter RME Server, Server Port, User Name, and Password.

Table 9-8 RME Server credentials Field Description

Field	Description
RME Server	Name of the RME server or the IP address.
Server Port ¹	Enter the port number.
User Name	Enter the user name.
Password	Enter the password.

1. In Campus 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.

Table 9-9 *Configuring Inter-VLAN Routing Field Descriptions*

Field	Description
VLAN Interface ¹	Enter the VLAN interface.
IP Address	Enter the IP address for the interface.
Sub-Interface ID	Enter the ID for the sub-interface.
Admin Status	Select the Admin status: <ul style="list-style-type: none"> • Up • Down
Encapsulation	Select the encapsulation: <ul style="list-style-type: none"> • 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.

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:

- a. Select the VLAN interface from the Interface Set.
- b. Click **Delete from Interface Set**
- c. Repeat the steps from [Step 2](#).

Step 9 Click **Apply**.



Note 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, thus maintaining 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 \(VLAN\)”](#) section on page 9-2, and for VTP Domains, see [“VTP Domains”](#) section on page 9-30.

This topic contains:

- [Understanding VLAN Trunking Protocol Version 3](#), page 9-32
- [Using VLAN Trunking Protocol \(VTP\)](#), page 9-35
- [VTP Domains](#), page 9-30

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 that 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) will be placed in the NO_VTP domain.

The devices that do not support VLANs and VTP (for example, Catalyst 1900 Standard Edition switches) will be 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 the same way as VTP servers, but 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 is capable of distributing a list of opaque databases over an administrative domain.

VTP version 3 provides following 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.
- Improved server authentication.
- Protects from adding the wrong database to a VTP domain.
- Interaction with VTP version 1 and VTP version 2.
- 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

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

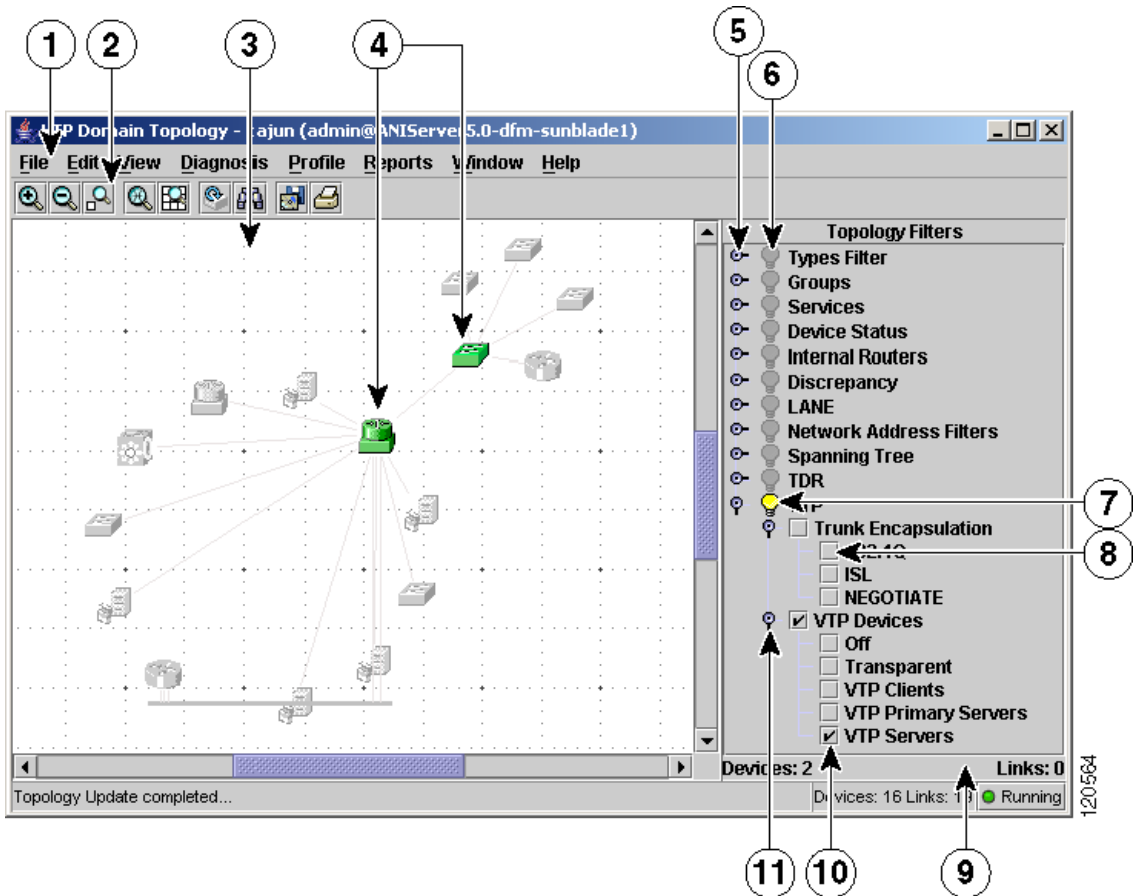
- Displays Primary server as a subfolder under the parent VTP domain:
If your network contains devices running VTP version 3, the primary server is displayed as a subfolder under the parent Domain in the VTP Domains. Under Primary server folder, you can find all the server and client modes.
- Supports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

For more details, see [Figure 9-1 on page 9-34](#).

Figure 9-1 VTP Filters



1	Menu	7	Filter on for VTP devices
2	Toolbar	8	check box disabled for the filter
3	Topology map	9	Topology filter results
4	Filtered devices	10	check box enabled for VTP Servers filter
5	Filter collapsed	11	Expand icon for the filter
6	Filter disabled		

- 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 Campus

- 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 VLANs” section on page 9-5](#) and [“Creating PVLAN” section on page 9-20](#).
- 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, page 9-36](#)
- [Using VTP Views, page 9-37](#)

Displaying VTP Reports

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

-
- Step 1** Start **Campus Manager > Topology Services** from the CiscoWorks Homepage.
- 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 9-10](#) to interpret the fields shown in the VT Reports Summary view.

Table 9-10 *Field Description for VTP Report*

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

Using VTP Views

VTP Views shows devices that participate in VTP domains. VTP Views also shows the non-VTP devices and ATM domains connected directly to the VTP domain.

Figure 9-2 VTP Tree View

The screenshot shows the Cisco Network Services Manager (NSM) interface. The left pane displays a hierarchical tree view of network services. The right pane displays the 'VLAN Summary - VLAN0100' with a 'Port List' table. Six numbered callouts (1-6) point to specific elements in the tree view:

- 1: VTP domain in the Topology Tree View
- 2: Parent VTP domain
- 3: Switch in Transparent mode
- 4: VLANs under the Transparent switch mode
- 5: VTP Views under the Network View
- 6: Parent VTP domain under VTP views

1	VTP domain in the Topology Tree View	4	VLANs under the Transparent switch mode
2	Parent VTP domain	5	VTP Views under the Network View
3	Switch in Transparent mode	6	Parent VTP domain under VTP views

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.
 - [Displaying MLS Reports, page 8-64](#)
- Display configuration information about the LANE components in your network:
 - [Diagnosing Config Server Registry, page 12-22](#)
 - [Diagnosing LE Client, page 12-23](#)
 - [Diagnosing LE Server/Broadcast Server, page 12-31](#)
 - [Diagnosing LE Configuration Server, page 12-35](#)
- View summary information about the LANE components in your network:
 - [Displaying LE Client Summary, page 12-18](#)
 - [Displaying LE/Broadcast Server Summary, page 12-19](#)
 - [Displaying LE Configuration Server Summary, page 12-21](#)

Understanding Trunking

A trunk is a point-to-point link carrying several VLANs. The purpose of a trunk is to save ports when creating a link between two devices implementing VLANs, typically two switches.

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 just one VLAN as would happen on a non-trunked interface on a switch.

This topic contains:

- [Trunking Considerations, page 9-40](#)
- [Dynamic Trunking Protocol \(DTP\), page 9-40](#)
- [Trunk Encapsulation, page 9-41](#)
- [Trunk Characteristics, page 9-41](#)
- [Encapsulation Types, page 9-42](#)

Trunking Considerations

Note 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)—ISL is a Cisco-proprietary trunking encapsulation.
- 802.1Q—802.1Q is an industry-standard trunking encapsulation.

Trunk Characteristics

Table 9-11 shows the DTP signaling and the characteristics of each mode.

Table 9-11 Trunking Mode Characteristics

Trunking Mode	Frames Sent	Description	Final state (local port)
on	YES, periodic	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 on , auto or desirable , and is running DTP. A port that is in on mode always tags frames sent out from the port.	Trunking, unconditionally.

Table 9-11 Trunking Mode Characteristics (continued)

Trunking Mode	Frames Sent	Description	Final state (local port)
auto	YES, periodic	<p>These links will only become trunk links if they receive a DTP signal from a link that is already trunking or desires to trunk.</p> <p>This will only form a trunk if the neighboring interface is set to on or desirable. This is the default mode for Catalyst operating system switches.</p>	The port will end up in trunking state only if the neighboring interface wants to.
desirable	YES, periodic	<p>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.</p> <p>This will form a trunk if the neighboring interface is set to on, auto, or desirable and is running DTP. This is the default mode for all Ethernet interfaces.</p>	<p>If the port detects that the neighboring interface is able to trunk (remote in on, desirable or auto mode), it will end up in trunking state.</p> <p>Otherwise, it will stay non-trunking.</p>
nonegotiate	NO	Sets trunking on and disables DTP. These will only become trunks with ports in on or nonegotiate mode.	Trunking, unconditionally.
off	YES	This option sets trunking and DTP capabilities off. This is usually the recommended setting for any access port since it prevents any dynamic establishments of trunk links.	Non trunking, unconditionally.

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.

Encapsulation Type	Description and Trunking
ISL	Sets the port encapsulation to ISL.
802.1Q	Sets the port encapsulation to 802.1q.
negotiate	<p>Only available in auto or desirable trunking modes:</p> <ul style="list-style-type: none"> • 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 Start **Campus Manager > VLAN Port Assignment** from the CiscoWorks Homepage.

The VLAN Port Assignment window appears.

Or

From Topology Services main window, select the device, which has the ports you require and select **Tools > VLAN Port Assignment**.

The VLAN Port Assignment window appears.

Step 2 Select the VTP Domain, which has the port on which you want to create Trunk.

Step 3 View the ports you want to assign. To do this, either:

- Click **Show All Ports**

Or

- Search using **Find Port** option.

The VTP Domain table provides a list of ports and the details of the ports.

- Step 4** Select a link port, which is a non-trunking port from the list of ports in the table. Link port icon marks the link ports in the table.
- Step 5** Click **Create Trunk**.
- The Create Trunk window appears.
- In the Create Trunk window, Device Information panel displays the device IP address and the port number of all the devices you have selected.
- Step 6** Select the Trunk Settings
- a. Select Encapsulation:
 - Dot1Q
 - ISL
 - Negotiate
 - b. Mode
- Campus Manager 4.0 supports only the **Desirable** mode.
- Step 7** Enter VLAN IDs to:
- Allow VLAN(s): Enter VLAN IDs of the VLANs, which must pass through the Trunk.
 - Disallow VLAN(s): Enter VLAN IDs of the VLANs, which must not pass through the Trunk.
- Step 8** Click **Configure**.
-

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, page 9-45](#)
- [Using EtherChannel, page 9-45](#)

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 4.0 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 supports only **desirable** mode for EtherChannel configuration.

Campus Manager 4.0 does not support EtherChannel configuration between a switch and router.

Using EtherChannel

Campus Manager 4.0 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** Start **Campus Manager > Topology Services** from the CiscoWorks Homepage.
- 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 pop up menu.
A 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 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 **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.

This topic contains the following sections:

- [Understanding VLAN Port Assignment, page 9-48](#)
- [Starting VLAN Port Assignment, page 9-49](#)
- [Navigating in VLAN Port Assignment, page 9-50](#)
- [VTP Domain Table, page 9-53](#)
- [Using VLAN Port Assignment, page 9-49](#)

Prior to using VLAN Port Assignment, you should understand the concepts of VLANs and VTP domains. See “[Understanding Virtual LAN \(VLAN\)](#)” section on page 9-2, and “[VTP Domains](#)” section on page 9-30 for more details.

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 \(VLAN\)](#)” section on page 9-2.

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

For information about setting up your network, see *Installation and Setup Guide for Campus Manager* (to access this document, go to http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/camp_mgr/camp_4x/cmgr_4_0/index.htm) or the “[Using Campus Manager Administration](#)” section on page 4-2.

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
- Configure VLANs on a trunk

Starting VLAN Port Assignment

To start VLAN Port Assignment:

-
- Step 1** Verify that your network is set up properly.
 - Step 2** Verify that the ANI Server is set up properly and running.
See [“Analyzing ANI Server” section on page 4-19](#) for more details.
 - Step 3** From the CiscoWorks desktop, select **Campus Manager > 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.

See Online help for ANI Server, for information about setting up your network and the ANI Server.

Using VLAN Port Assignment

You use VLAN Port Assignment to:

- [Navigating in VLAN Port Assignment, page 9-50](#)
- [Displaying Port Information, page 9-50](#)
- [Finding Entries in VLAN Ports Summary Table, page 9-54](#)
- [Assigning Ports to VLANs, page 9-55](#)
- [Extending VLANs Across VTP Domains, page 9-56](#)
- [Configuring Trunk Attributes, page 9-57](#)
- [Starting CiscoView, page 8-61](#)
- [Starting Telnet, page 8-62](#)

Navigating in VLAN Port Assignment

The VLAN Port Assignment main window provides command menu options, a drop-down list box of discovered VTP domains, searching criteria fields, and a table displaying matching port information.

The following topics contain descriptions of the VLAN Port Assignment commands and the table where discovered port information appears:

- [VLAN Port Assignment Commands, page 9-58](#)
- [VTP Domain Table, page 9-53](#)
- [VLAN Port Assignment Command Shortcuts, page 9-65](#)

Displaying Port Information

VLAN Port Assignment displays port information for a VTP domain. You can do the following:

- [Displaying All Ports in Specified VTP Domains, page 9-50](#)
- [Querying Ports in Specified VTP Domains, page 9-51](#)
- [Displaying Ports in Unspecified VTP Domains, page 9-53](#)

Displaying All Ports in Specified VTP Domains

You can use VLAN Port Assignment to list all ports in every VLAN that participates in a selected VTP domain. To do this:

Step 1 Select a VTP domain from the VTP Domain drop-down list box.

Sometimes, NULL and NO_VTP appear in the list of domains:

- NULL contains devices that do not have a configured domain name. A device in transparent mode is displayed as *NULL_ip address*.
- NO_VTP contains devices that do not support VTP. These devices are displayed as *NO_VTP_ip address*.

If you want to display all ports that are assigned to auxiliary VLANs, verify that the multi-access port check box is selected.

Step 2 Click **Show All Ports**.

All port information in all VLANs associated with the selected VTP domain are displayed in the VTP Domain table.

Querying Ports in Specified VTP Domains

You can use VLAN Port Assignment to find specific ports in a known VTP domain by entering search criteria. To do this:

Step 1 Select a VTP domain from the VTP Domain drop-down list box.

Sometimes, NULL and NO_VTP appear in the list of domains:

- NULL contains devices that do not have a configured domain name. A device in transparent mode is displayed as *NULL_ip address*.
- NO_VTP contains devices that do not support VTP. These devices are displayed as *NO_VTP_ip address*.

Step 2 Select your search criteria from the drop-down list boxes and enter a phrase to search for.

The [Table 9-12](#) describes these search criteria.

Table 9-12 *VLAN Port Assignment Search Criteria Descriptions*

Search Criterion	Description
Radio Buttons	
Match all of the following	Filters results that match both the first and second rows of search criteria.
Match any of the following	Filters results that match either the first or second row of search criteria.
Left Column	
Port Name	Name of the port.
Device Name	Name of device the port belongs to.

Table 9-12 VLAN Port Assignment Search Criteria Descriptions (continued)

Search Criterion	Description
Interface Name	Name of the interface.
Device Address	IP address of device the port belongs to.
VLAN Name	Assigned name of the associated VLAN.
VLAN Index	Assigned index number for that VLAN.
Ring Number	Segment ID of the Token Ring Concentrator Relay Function (trCRF) VLAN.
Bridge Number	Segment ID used to identify the logical distributed source-route bridge (SRB), which interconnects all logical rings that have the same parent Token Ring Bridge Relay Function (trBRF). The bridge number is an integer in hexadecimal format.
Right Column	
contains	Searches for the string that contains the specified pattern.
begins with	Searches for the string that begins with the specified pattern.
ends with	Searches for the string that ends with the specified pattern.
is	Searches for the string that matches the specified pattern.

If you want to display all ports that are assigned to auxiliary VLANs, verify that the multi-access ports check box is selected.

Step 3 Click **Get Ports**.

Ports that match the search criteria are displayed in the VTP Domain table.

Displaying Ports in Unspecified VTP Domains

When you do not know what VTP domain a device resides on, you can search all VTP domains by providing a device address or name. To do this:

-
- Step 1** Select All from the VTP Domain drop-down list box.
 - Step 2** Select Device Address or Device Name from the Where drop-down list box.
 - Step 3** Enter the appropriate information in the field.
If you want to display all ports that are assigned to auxiliary VLANs, verify that the multi-access ports check box is selected.
 - Step 4** Click **Get Ports**.
-

Ports that match the device address or name you entered appear in the VTP Domain table. The VTP domain name appears above the [VTP Domain Table](#) in the VTP Domain field.

VTP Domain Table

The VTP Domain table displays port information for an associated VTP domain:

-
- Step 1** Start **Campus Manager > VLAN Port Assignment** from CiscoWorks Homepage.
The VLAN Port Assignment window appears.
 - Step 2** Select a VTP Domain and click **Show All Ports** or **Get Ports**.
The VTP Domain table lists the ports, which are in that VTP domain.
-

Ports configured for multiple VLAN access will have two VLANs assigned: native and auxiliary. A native VLAN carries data traffic and an auxiliary VLAN carries voice and data traffic.

If you check the multi-access ports check box, each VLAN type is displayed as a separate entry in the table. If the multi-access ports check box is not selected, only native VLANs are displayed.



Note To sort this information according to fields, click on the column name.

See [Table 9-13](#) to interpret this information.

Table 9-13 *VLAN Ports Summary Table Fields*

Field	Description
Link	Lightning bolt indicates a port that is connected to a switch.
Port	User assigned port name.
IfName	Interface name.
Device Name	Name of device the port belongs to.
Device Address	IP address of device the port belongs to.
Port Status	State of the port (whether it is active, down, dormant, or testing).
isTrunk	If selected, the port is configured as a VLAN trunk.
VLAN Name	Assigned name of the associated VLAN.
VLAN Index	Assigned index number for that VLAN.
Association Type	Associated VLAN type (native or auxiliary).
Port Mode	Displays the mode of the port. For example, PVLAN-Host, Promiscuous, or a non-PVLAN.

Finding Entries in VLAN Ports Summary Table

You can perform a string search to find a specific entry or range of entries in the VTP Domain table. To do this:

-
- Step 1** Select **Edit > Find** in Table.
The Find dialog box appears.
- Step 2** In the Find dialog box, enter the appropriate settings, as described in [Table 9-14](#).

Table 9-14 *VLAN Port Assignment Find Field Descriptions*

Field	Description
Find	Enter a search string.
From	Select either one of these: <ul style="list-style-type: none"> • Start — Search for the entry from the beginning of the screen display. • Selection — Search for the entry in the selected field.
Ignore Case	Ignore use of upper and lower case.
Exact Match	Search for the exact text entered in the Find field.

Step 3 Click **Next** or **Previous** to start the search process.

Step 4 Click **Cancel** to close the Find dialog box.

Assigning Ports to VLANs

After you create VLANs, you can assign ports to the VLANs that you have created. You can use VLAN Port Assignment to assign access ports on network switches to different VLANs.

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

To assign ports:

Step 1 Select the VTP Domain and enter appropriate search criteria, if necessary. See [“Displaying Port Information” section on page 9-50](#) for more information.

Step 2 Select the row in the VLAN Ports Summary Table that contains the port you want to move.

To select multiple ports, press and hold the Ctrl key while highlighting each row; to select contiguous ports, press and hold the Shift key as you click on the ports.

Considerations:

- If you are selecting a port on a transparent switch, the VLAN that you are moving the port to must exist on that switch.
- You cannot move a trunking port. (A port is a trunking port if the isTrunk field contains a check mark in the VTP Domain table.)
- The destination VLAN should match the VLAN association type (native or auxiliary) of the originating VLAN.

Step 3 From the drop-down list box in the Move Selected Ports to field, select the VLAN that you want the port to be moved to.

Step 4 Click **Move**.

The port is moved to the selected VLAN.

Extending VLANs Across VTP Domains

A trunk is a point-to-point link that transmits and receives traffic between switches or between switches and routers. Trunks carry the traffic of multiple VLANs and can extend VLANs across an entire network.

100BaseT and Gigabit Ethernet trunks use Inter-Switch Link (ISL) or industry-standard IEEE 802.1Q to carry traffic for multiple VLANs over a single link.

To use ISL, you must configure the ports on both sides of the link as trunk ports.

When two VTP domains are interconnected using an ISL trunk between two LAN switches by default, no VLAN traffic is forwarded. However, you can configure the ports on each switch to receive and forward specific VLANs.

To enable port configuration, the VLANs on either side of the ISL trunk must be identical and share VLAN characteristics such as VLAN names, VLAN indexes, and so on.

Configuring Trunk Attributes

You can use VLAN Port Assignment to specify the VLAN indexes that you want to allow on a trunk.

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** Start **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. For more information, see [Querying Ports in Specified VTP Domains, page 9-51](#).
- Step 3** Select the row that contains the trunking port in the [VTP Domain Table, page 9-53](#). 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 9-16](#).
- 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.
-

VLAN Port Assignment Commands

You can run VLAN Port Assignment commands from the menu. See [Table 9-15](#) for details.

Table 9-15 VLAN Port Assignment Command Description




Menu	Command	Toolbar Button	Description
File	Print		Prints the information from the “VTP Domain Table” section on page 9-53 .
	Export	None	Exports the information from the “VTP Domain Table” section on page 9-53 to a text file.
	Exit	None	Exits VLAN Port Assignment.
Edit	Find		Opens Find window and helps in “ Finding Entries in VLAN Ports Summary Table ” section on page 9-54 .
View	Show Toolbar	None	Shows or hides the toolbar.
	Refresh Summary		Rediscovers port information in the “VTP Domain Table” section on page 9-53 .
	Show VTP Domain	None	Displays the VTP domain view.
	Show VLAN	None	Highlights a specified VLAN in the VTP domain view.
	Show Device	None	Highlights a specified device in the VTP domain view.
Reports	Trunk Attributes	None	Displays descriptive information about the links that are configured as trunks.
	Port Attributes	None	Displays descriptive information about the ports belonging to the selected device.
	Device Attributes	None	Displays descriptive information about the selected device.

Table 9-15 VLAN Port Assignment Command Description (continued)

Menu	Command	Toolbar Button	Description
Tools	CiscoView	None	CiscoView starts if it has been configured with information about the selected device.
	Telnet	None	Initiates a remote terminal connection with the Cisco Systems Console on a device that supports Telnet
Help	Using VLAN Port Assignment	None	Opens the online help for VLAN Port Assignment, page 9-47 .
	About	None	Shows version and copyright information for VLAN Port Assignment.

Displaying Topology Views and Attribute Summaries

The following topics describe how to use VLAN Port Assignment to display topology views of a VTP domain and attribute summaries for devices:

- [Displaying Topology Views, page 9-60](#)
- [Displaying Attribute Summaries, page 9-62](#)
- [VLAN Port Assignment Command Shortcuts, page 9-65](#)

Displaying Topology Views

You can use VLAN Port Assignment for:

- [Displaying VTP Domain, page 9-60](#)
- [Highlighting VLANs, page 9-61](#)
- [Highlighting Devices, page 9-61](#) (includes display of Layer 2 view)

Topology Services must be running to enable you to display these views.

Displaying VTP Domain

To use VLAN Port Assignment to display the VTP domain view:

-
- Step 1** Start **Campus Manager > VLAN Port Assignment** from CiscoWorks desktop.
 - Step 2** In the VLAN Port Assignment window, select the VTP domain and enter appropriate search criteria, if necessary.
For more information, see [Querying Ports in Specified VTP Domains, page 9-51](#).
 - Step 3** Select any row from the [VTP Domain Table, page 9-53](#).
 - Step 4** Right-click the row and select **Show VTP Domain**.

The network topology view for the VTP domain appears. If you select a port, which is in transparent mode, the network topology view highlights the device.

Highlighting VLANs

You can use VLAN Port Assignment to highlight all devices and links belonging to a specific VLAN in the VTP domain view. To do this:

-
- Step 1** Start **Campus Manager > VLAN Port Assignment** from CiscoWorks Homepage.
- Step 2** In the VLAN Port Assignment window, select the VTP domain and enter appropriate search criteria, if necessary.
- For more information, see [Querying Ports in Specified VTP Domains, page 9-51](#).
- Step 3** From the VTP Domain table, select the row that contains the VLAN.
- For more information, see [VTP Domain Table, page 9-53](#).
- Step 4** Right-click the row and select **Show VLAN**.
- The network topology view for the VLAN appears. If you select a port, which is in transparent mode, the network topology view highlights the device.
-

Highlighting Devices

You can use VLAN Port Assignment to highlight a specific device in the VTP domain view, as well as display the Layer 2 view.

-
- Step 1** Start **Campus Manager > Topology Services** from the CiscoWorks Homepage, if it is not already running.
- Step 2** Click **Tools > VLAN Port Assignment**.
- The VLAN Port Assignment window appears.
- Step 3** Select the VTP domain and enter appropriate search criteria, if necessary.
- For more information, see [Querying Ports in Specified VTP Domains, page 9-51](#).
- Step 4** From the VTP Domain table, select the row that contains the device.
- For more information, see [VTP Domain Table, page 9-53](#).
- Step 5** Right-click the row and select **Show Device**.

The network topology view for the VTP domain which has the device, appears. If you select a port, which is in transparent mode, the network topology view highlights the device.

Displaying Attribute Summaries

The following topics describe how to use VLAN Port Assignment to display status information about ports, devices, and trunks in your network:

- [Displaying Port Attributes, page 9-62](#)
- [Displaying Device Attributes, page 9-63](#)
- [Displaying Trunk Attributes, page 9-63](#)

Displaying Port Attributes

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

-
- Step 1** Start **Campus Manager > VLAN Port Assignment** from the CiscoWorks Homepage.
- The VLAN Port Assignment window appears.
- Step 2** Select the VTP domain and enter appropriate search criteria, if necessary. For more information, see [Querying Ports in Specified VTP Domains, page 9-51](#).
- Step 3** Select the row that contains the port from the VTP Domain table. For more information, see [VTP Domain Table, page 9-53](#).
- Step 4** Select **Reports > Port Attributes**.
- The Port Attributes window appears.
- For more information on Port Attributes, see [Interpreting Port Attributes, page 8-59](#).
-

Displaying Device Attributes

To display information about a specific device.

-
- Step 1** Start **Campus Manager > VLAN Port Assignment** from the CiscoWorks Homepage.
- The VLAN Port Assignment window appears.
- Step 2** Select the VTP domain and enter appropriate search criteria, if necessary. For more information, see [Querying Ports in Specified VTP Domains, page 9-51](#).
- Step 3** Select the row that contains the device from the VTP Domain table. For more information, see [VTP Domain Table, page 9-53](#).
- Step 4** Select **Reports > Device Attributes**.
- The Device Attributes window appears.
- For more information on Device Attributes, see [Interpreting Device Attributes, page 8-58](#).
-

Displaying Trunk Attributes

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

-
- Step 1** Start **Campus Manager > VLAN Port Assignment** from the CiscoWorks Homepage.
- The VLAN Port Assignment window appears.
- Step 2** Select VTP domain and enter appropriate search criteria, if necessary. For more information, see [Querying Ports in Specified VTP Domains, page 9-51](#).
- Step 3** Select the row that contains the trunking port from VTP Domain table. For more information, see [VTP Domain Table, page 9-53](#).

Step 4 Select **Reports > Trunk Attributes**.

The Trunk Attributes window appears.

For more information on Trunk Attributes, see [Interpreting Trunk Attributes](#), page 9-64.

Interpreting Trunk Attributes

See [Table 9-16](#) for details about the fields shown in the Trunk Attributes window.

Table 9-16 *Trunk Attributes Field Descriptions*

Field	Description
Trunk Ports	
—	Serial number of the trunking ports.
Device Name	Device to which the port belongs.
Port Name	Name of the port.
Port Mode	Half-duplex or full-duplex.
Port Speed	Speed of the link, such as 10Mbps.
Trunk Encapsulation	
—	Trunking encapsulation for the interface.
VLANs	
VLAN(s) allowed on Trunk	ISL indexes of all VLANs allowed to participate on the trunk.
VLAN(s) active on Trunk	
VLAN Index	VLAN indexes of all VLANs active on trunk.
VLAN Name	VLAN names of all VLANs active on trunk.
The status bar for the VLANs table displays the number of rows in the table.	

Table 9-16 Trunk Attributes Field Descriptions (continued)

Field	Description
Configure VLAN(s) on Trunk	
Allow VLAN(s)	Enter valid ISL indexes or a range of valid ISL indexes, separated by commas, like 1,3,5-1000.
Disallow VLAN(s)	Enter valid ISL indexes or a range of valid ISL indexes, such as 1,3,5-1000.

VLAN Port Assignment Command Shortcuts

After the you click **Show All Ports** or **Get Ports**, and the VTP Domain table has entries, you can select a row and issue several commands that are normally accessed through the command menu. To do this:

-
- Step 1** Select the VTP domain and enter appropriate search criteria if necessary. For more information, see [Querying Ports in Specified VTP Domains, page 9-51](#).
 - Step 2** Select a row in the VTP Domain table.
 - Step 3** Right-click the selected row.
A popup menu appears.
 - Step 4** Select the command you want to perform.

[Table 9-17](#) displays the commands displayed in the popup menu.

Table 9-17 VPA Menu Descriptions

Field	Description
Show VTP Domain	Displays the VTP domain view.
Show VLAN	Highlights a specified VLAN in the VTP domain view.
Show Device	Highlights a specified device in the VTP domain view.
Telnet	Starts a Telnet session, which initiates a remote terminal connection with the Cisco Systems Console on a device.
Device Center	Starts Device Center application, which provides a device summary, and various tools, reports, and tasks that you can perform on selected devices.
CiscoView	Starts CiscoView, which displays specific device configuration and diagnostic information.

Troubleshooting Suggestions

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

Table 9-18 Troubleshooting VLAN Port Assignment

Symptom	Probable Cause	Possible Solution
VLAN Port Assignment starts, but shows an error message.	Server process is not running.	Confirm that the ANI Database engine and the ANI Server are running.
VTP Domain drop-down list box is empty and the following error message appears: Discovery seed not defined for ANI Server	A seed device is not specified for the ANI Server.	Add a seed device. See ANI Server online help for more information about adding a seed device. See the <i>User Guide for CiscoWorks Common Services</i> or the <i>Online help for Campus Manager 4.0</i> for more information about adding a seed device.
VTP Domain drop-down list box is empty and the following message appears: ANI is still in the discovery process. Please wait.	The initial ANI discovery is not complete.	Wait for the ANI status bar to display <code>Idle</code> .
The message <code>Operation Failure</code> appears when you try to move a port.	The operation failed for one of various possible reasons.	Click Details to display the cause of the failure.

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 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, page 9-20](#).

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, page 9-21](#).

- 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, page 9-21](#).

- Step 4** Assign ports, which are connected to the Web servers, to the community VLAN 50. For more details, see [Assigning Ports to VLANs, page 9-55](#).
- Step 5** Assign ports, which are connected to the DNS servers, to the isolated VLAN 60. For more details, see [Assigning Ports to VLANs, page 9-55](#).
- 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, page 9-23](#).

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** Start **Campus Manager > Topology Services** from the CiscoWorks Homepage.
- 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** Start **Campus Manager > 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.
-

