

Virtual LANs

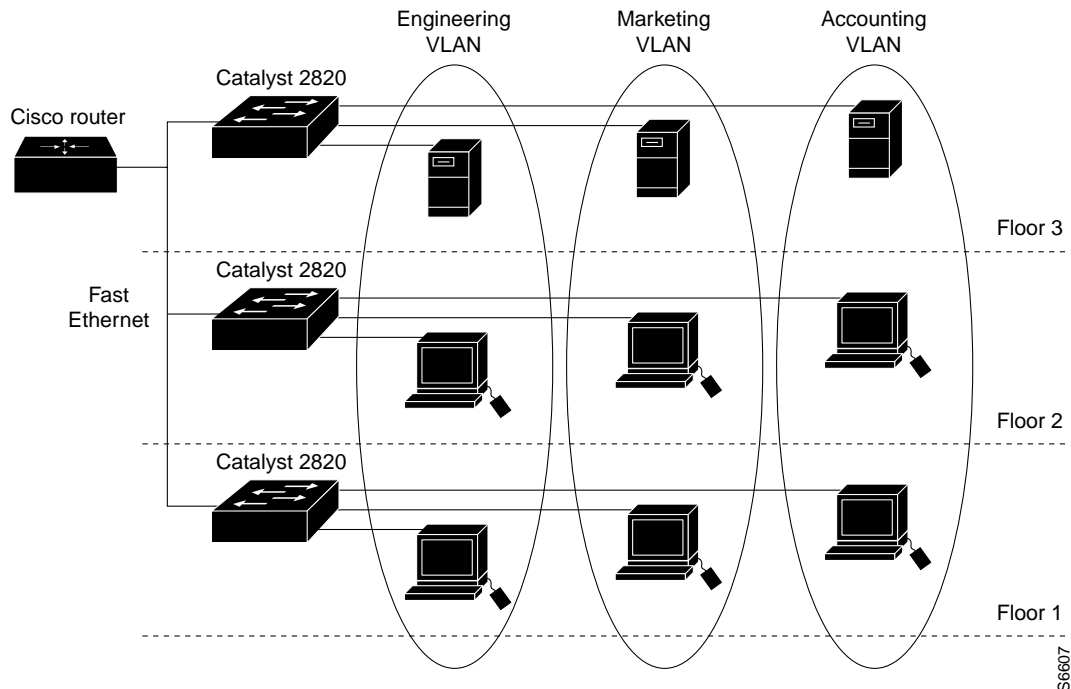
This chapter describes virtual LAN (VLAN) features and functionality, the Virtual LAN Menu of the Catalyst 1900 and Catalyst 2820 switches, and procedures for creating VLANs and assigning ports to VLANs.

VLAN Description

A VLAN is a switched network that is logically segmented by functions, project teams, or applications without regard to the physical location of users. For example, several end stations might be grouped as a department, such as engineering or accounting. When the end stations are physically located close to one another, you can group them into a LAN segment. If any of the end stations are in different buildings (not the same physical LAN segment), you can then group them into a VLAN.

You can assign each switch port to a VLAN. Ports in a VLAN share broadcast traffic. Ports that do not belong to that VLAN do not share the broadcast traffic. Ports from multiple Catalyst 1900 and Catalyst 2820 switches can be members of the same VLAN. Figure 2-1 shows an example of VLANs that span multiple switches and multiple floors or a building.

Figure 2-1 VLANs Spanning Multiple Switches and Multiple Floors



Note All VLAN features are disabled if you have configured bridge groups on the switch. For more information on bridge groups, see the “Bridge Groups” section in Chapter 3, “Additional Features.”

Features

VLANs provide the following features:

- Simplification of end-station moves, adds, and changes

When an end station is physically moved to a new location, its attributes can be reassigned from a network management station through Simple Network Management Protocol (SNMP) or through the user interface menus. When an end station is moved within the same VLAN, it retains its previously assigned attributes in its new location. When an end station is moved to a different VLAN, the attributes of the new VLAN are applied to the end station.

You can assign the Internet Protocol (IP) address of a switch to any VLAN. A network management station and workstations on any Catalyst series switch VLAN then have direct access to other Catalyst 1900 and Catalyst 2820 switches on the same VLAN, without needing a router. Only one IP address can be assigned to a switch; if the IP address is reassigned to a different VLAN, the previous IP address assignment to a VLAN is invalid.

- Controlled traffic activity

VLANs allow ports on the same or different switches to be grouped so that traffic is confined to members of only that group. This feature restricts broadcast, unicast, and multicast traffic (flooding) only to ports included in a certain VLAN. The management domain is a group of VLANs that are managed by a single administrative authority. From a single switch, you can create VLANs for an entire management domain.

- Workgroup and network security

You can increase security by segmenting the network into distinct broadcast domains. To this end, VLANs can restrict the number of users in a broadcast domain. You can also control the size and composition of the broadcast domain by controlling the size and composition of a VLAN.

VLAN Description

Table 2-1 shows the capabilities and defaults for the Catalyst 1900 and Catalyst 2820 series VLAN features.

Table 2-1 Catalyst 2820 and Catalyst 1900 VLAN Features

Feature	Capability	Default
Trunk ports	Supports a maximum of two trunks. The Catalyst 1900 switch supports a maximum of two Inter-Switch Link (ISL) trunks. The Catalyst 2820 switch supports both ISL and Asynchronous Transfer Mode (ATM) LAN emulation (LANE) trunk connections and ATM permanent virtual connections (PVCs). Fast Ethernet trunk ports can be grouped using the Fast EtherChannel feature to form a single trunk.	No trunk ports are enabled.
Load sharing	Supports Spanning-Tree Protocol (STP) on VLAN trunks to load share.	No load sharing is set up.
VLAN Trunk Protocol (VTP)	Supports server, client, and transparent modes. Server and transparent modes support a maximum of 128 VLANs. From server mode, the switch automatically transitions to client mode if it learns more than 128 VLANs from advertisements. Client mode supports 1005 VLANs.	Configured to server mode. Set to no-management domain state.
VTP pruning	Supports pruning.	Pruning is disabled.
VLAN membership	Supports dynamic and static ports.	The default VLAN membership of all ports is static, and all ports reside in VLAN 1.
VLAN Membership Policy Server (VMPS)	Does not function as a VMPS on the network. (The Catalyst 5000 series switches support this feature.)	No default.
STP	Runs on a maximum of 64 VLANs at one time.	VLANs 1 to 64 are enabled with STP.

Components

Networks that have VLANs contain one or more of the following components:

- Switches that logically segment connected end stations

Switches are the entry points into the switched fabric for end-station devices and can group users, ports, or logical addresses into common communities of interest.

You can use both a single switch or multiple connected switches to group ports and users into communities. By grouping ports and users together across multiple switches, VLANs can span single-building infrastructures, interconnected buildings, or campus networks.

Switches use frame identification, or tagging, to logically group users into administratively defined VLANs. Based on rules you define, tagging determines where the frame is to be sent by placing a unique identifier in the header of each frame before it is forwarded throughout the switch fabric. The identifier is examined and understood by each switch prior to any broadcasts or transmissions to other switches, routers, or end-station devices. When the frame exits the switch fabric, the switch removes the identifier before the frame is transmitted to the target end station.

You can logically group users on Ethernet and ATM networks by mapping VLANs on the Ethernet network to emulated LANs (ELANs) on the ATM network.

- Routers that provide VLAN communications between workgroups

Routers provide policy-based control, broadcast management, and route processing and distribution. They also provide the communication between VLANs and the 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 that require access to remote sites across wide area links. Routers are integrated into the switching fabric by using high-speed backbone connections over Fast Ethernet links, FDDI, or ATM for higher throughput between switches and routers.

- Transport protocols that carry VLAN traffic across shared LAN and ATM backbones

The VLAN transport protocol enables information to be exchanged between interconnected switches residing on the corporate backbone.

The backbone acts as the aggregation point for high-volume traffic. It also carries end-user VLAN information and identification between switches, routers, and directly attached servers. Within the backbone, high-bandwidth, high-capacity links carry the traffic throughout the enterprise.

- Interoperability with previously installed LAN systems

VLANs provide compatibility with previously installed systems, such as shared hubs and stackable devices. You can add shared hubs without changing existing network equipment. You also can share traffic and network resources that attach directly to switching ports with VLAN designations.

VLAN Configuration Tasks

Use the Virtual LAN Menu to perform the following tasks, which are described in this chapter:

- Access the Virtual LAN menu
- Assign a management domain
- Define a VLAN
- Group switch ports to VLANs
- Configure trunks
- Configure VTP
- Configure VTP pruning
- Configure dynamic port membership

Accessing the Virtual LAN Menu

To access the Virtual LAN Menu, enter [V] **Virtual LAN** at the selection prompt on the Main Menu. The following display appears:

```
Catalyst 1900 - Virtual LAN Configuration
-----Information-----
VTP version: 1
Configuration revision: 1
Maximum VLANs supported locally: 1005
Number of existing VLANs: 6
Configuration last modified by: 0.0.0.0 at 01-03-2000 18:35:56

-----Settings-----
[N] Domain name
[V] VTP mode control           Server
[F] VTP pruning mode         Disabled
[O] VTP traps                 Enabled

-----Actions-----
[L] List VLANs                [A] Add VLAN
[M] Modify VLAN              [D] Delete VLAN
[E] VLAN Membership          [S] VLAN Membership Servers
[T] Trunk Configuration     [W] VTP password
[P] VTP Statistics           [X] Exit to Main Menu

Enter Selection:
```

When configuring the functions displayed on the menu, you might not use the options in the order in which they appear in the menu. Many of the menu entries prompt you for an additional selection and then return you to the Virtual LAN Menu for the next step.

Management Domains

When creating a VLAN, you must first determine and configure the management domain on the switch. Management domains group VLANs into zones of different administrative responsibilities. Catalyst 1900 and Catalyst 2820 switches support only one management domain for each switch.

Catalyst 1900 and Catalyst 2820 switches operate in one of three modes: server, client, or transparent mode. By default, a switch in the no-management domain state is a VTP server; that is, it learns from received advertisements on a configured trunk port. If trunks are

configured on the switch, VTP receives and transmits VLAN advertisements. From the server mode, you can add or delete VLANs by using the VTP Management Information Base (MIB) SNMP management station, the command-line interface (CLI), or the console menus.

A switch configured in VTP server mode advertises VLAN configuration to neighboring switches through its trunks and learns new VLAN configurations from those neighbors. Use the server mode to add or delete VLANs and to modify VLAN information by using the VTP MIB, the CLI, or the console menus. For example, when you add a VLAN, VTP advertises the new VLAN to other switches, and both servers and clients prepare to receive traffic on their trunk ports.

The Catalyst 1900 and Catalyst 2820 switches automatically change from VTP server mode to VTP client mode when they receive an advertisement with more than 128 VLANs. You cannot configure a Catalyst 1900 or Catalyst 2820 switch for VTP client mode. As in VTP server mode, a switch in VTP client mode also transmits advertisements and learns new information from advertisements. However, you cannot add, delete, or modify a VLAN through the MIB or the console. The VTP client does not maintain VLAN information in nonvolatile storage; when it starts, it learns the configuration by receiving advertisements from the trunk ports.

In VTP transparent mode, the switch does not advertise or learn VLAN configurations from the network. When a switch is in VTP transparent mode, you can modify, add, or delete VLANs through the console menus, the CLI, or the MIB.

When a switch is in the no-management domain state and running in either server or client mode, it inherits a management domain name and configuration revision number upon receiving an advertisement from a configured trunk port. The configuration revision number reflects the latest revision of the VTP configuration. If a management domain for the switch is defined, the switch ignores advertisements with a different management domain or a lower configuration revision number and checks all received advertisements with the same management domain for consistency. If the information contained in the received advertisement is consistent, the switch propagates the advertisements to other trunk ports and adds the newly learned information locally. Because all devices in the same management domain learn about any new VLANs configured in the transmitting device, you need to configure a new VLAN on only one device in the management domain.

Assigning a Management Domain

A management domain is a group of VLANs that is under the same administrative responsibility. By default, a Catalyst 1900 or Catalyst 2820 switch resides in the no-management domain state until it is configured with a management domain or receives an advertisement for a management domain. To assign a management domain, do the following:

Step	Action
1 Access the VLAN Configuration Menu.	Select [V] Virtual LAN Menu from the Main Menu.
2 Define the VLAN management domain of the switch.	<p>a. Select [N] Domain Name Menu from the Virtual LAN Menu.</p> <p>b. Enter the management domain name at the selection prompt.</p> <p>c. Press Return. The Virtual LAN Menu reappears.</p>

Verifying the Management Domain Assignment

To verify that you have assigned the management domain, view the domain name on the Virtual LAN Configuration Menu.

VLAN Characteristics

To create a new VLAN, you need to define the VLAN characteristics. The Enterprise Edition software prompts you to define these characteristics:

- VLAN number—the VLAN identifier.

Note When configuring an ATM module as a trunk port, each VLAN must be either mapped to a LANE client or bound to one or multiple PVCs. In each case, you specify the VLAN number when you create a LANE client or a PVC on the ATM module. For more information on configuring LANE clients, refer to the *Catalyst 2820 ATM Modules Installation and Configuration Guide*.

- VLAN name—the VLAN name. The VLAN name must be a unique name in the management domain.
- VLAN type—Ethernet, FDDI, Token-Ring, FDDI-Net, or Token-Ring-Net.
- Maximum transmission unit (MTU)—the maximum packet size, in bytes, that the VLAN can use.
- 802.10 SAID—the IEEE 802.10 security association identifier (SAID) of a VLAN.
- VLAN state—enabled or suspended. When a VLAN is suspended, all traffic on the switch for that VLAN is blocked.
- Translational bridge—the VLAN identifier of the translationally bridged VLAN. The VLANs that are translationally bridged must be of different types.
- Ring number—the ring number of an FDDI or Token-Ring VLAN. The ring number is used for source routing in a Token-Ring architecture.
- Parent VLAN—the parent VLAN of an FDDI or Token-Ring VLAN. The parent VLAN must be an FDDI-Net or Token-Ring-Net VLAN. The parent VLAN specifies the VLAN ID to which an FDDI or Token-Ring VLAN is attached for bridging functions.
- STP type—IBM or IEEE (for FDDI-Net or Token-Ring-Net VLANs).
- Bridge number—the bridge number of an FDDI-Net or Token-Ring-Net VLAN.

Defining a VLAN

To define a VLAN, you need to specify its attributes. Complete the following steps to set the VLAN number, name, IEEE 802.10 SAID value, and MTU size.

Step	Action
1 Access the VLAN Configuration Menu.	Select [V] Virtual LAN Menu from the Main Menu.
2 Add the specified VLAN to the VLAN list.	Select [A] Add VLAN from the Virtual LAN Menu.
3 Define the type of VLAN to be added.	Enter the type of VLAN at the selection prompt. For Ethernet, enter [1] Ethernet. Press Return .

Step	Action
4 Define the VLAN number.	At the next menu, select [N] VLAN Number , and enter the number of the VLAN to be added. Press Return .
5 Define the VLAN name.	At the next menu, select [V] VLAN Name , and enter the name of the VLAN to be added. Press Return .
6 Set the IEEE 802.10 SAID value.	At the next menu, select [I] 802.10 SAID , and enter the appropriate value. The value must be within the range shown on the screen, and the value cannot be the same as the value of another IEEE 802.10 value. After you enter the value, press Return .
7 Set the MTU size.	At the next menu, select [M] MTU Size , and enter the appropriate value. Press Return .
8 Enable the VLAN.	At the next menu, select [T] VLAN State , and select Enabled. Press Return .
9 Save the configuration.	Select [S] Save .

Verifying the VLAN Definition

To verify that you have configured the VLAN, view the VLAN settings on the Virtual LAN Configuration Menu. To do this, select **[L] List VLANs** from the Virtual LAN Menu to access the list of defined VLANs. Verify that the defined VLAN was added to the list. To get a complete list of parameters for a particular VLAN, select **[M] Modify VLANs**.

Grouping Switch Ports to VLANs

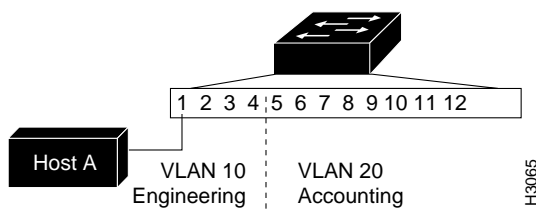
Before configuring a VLAN, you need to determine its structure and consider how to group users into VLANs. Based on access, security, and bandwidth requirements, decide which users need to be part of the same VLAN according to these considerations:

- Media type—All ports in the VLAN must support the same media type as defined in the VLAN.
- Access—As an example, consider assigning VLAN membership based on product-team membership or department groupings.

- Traffic—If a particular server interface is a bottleneck because of heavy traffic, you might want to add a second interface to the server and divide the users into two VLANs.
- Number of VLANs—You can configure from 1 to 1005 VLANs.

Figure 2-2 shows a local VLAN configuration that groups switch ports into VLAN 10 and VLAN 20.

Figure 2-2 Local VLAN Configuration



A VLAN created in a management domain remains unused until it is mapped to switch ports. The VLAN Membership menu maps the VLANs to ports. The default configuration has all switched Ethernet ports statically assigned to VLAN 1. If a port is assigned to a VLAN that is not created or to a VLAN in a suspended state, that port acquires the disabled-no-VLAN status. The port cannot forward or receive traffic until the VLAN assigned to that port is enabled.

To group the switch ports to VLANs, do the following:

Step	Action
1 Access the Virtual LAN Menu.	Select [V] Virtual LAN from the Main Menu.
2 Access the VLAN Membership screen.	Select [E] VLAN Membership .
3 Access the VLAN Assignment screen.	Select [V] VLAN Assignment .
4 Select the appropriate VLAN for each port.	Enter the appropriate port numbers at the selection prompt, and select the VLAN to group the ports at the next selection prompt. Press Return .

Note When selecting VLANs, you can only assign VLAN 0 to dynamic ports. You cannot assign VLAN 0 to static ports. Dynamic ports are listed as VLAN 0 on the VLAN Assignment screen if no VLAN has been obtained. If a VLAN has been obtained, the VLAN number is shown on the screen. You can assign VLAN 1 to VLAN 1005 to static ports.

A Fast Ethernet port can function as an ISL trunk, a static VLAN member port, or a dynamic VLAN member port. An ATM module can function as a LANE trunk or a static VLAN member port. You can configure a Fast Ethernet port as a static VLAN member port by following the steps listed. To configure an ATM port as a static VLAN member port, you must also configure a LANE client. For more information on configuring LANE clients, refer to the *Catalyst 2820 ATM Modules Installation and Configuration Guide*.

Verifying the Grouping of Switch Ports

To verify that you have grouped switch ports to VLANs, do the following:

Step	Action
1	Access the Virtual LAN Menu. Select [V] Virtual LAN from the Main Menu.
2	Access the VLAN Membership screen. Select [E] VLAN Membership .

VLAN Trunking

A VLAN trunk can connect two Catalyst 1900 or Catalyst 2820 switches; it can also connect these switches to a Catalyst 5000 series switch or to a router. For concepts about VLAN with load sharing, refer to “VLAN Trunking and Load Sharing” later in this section.

The Catalyst 1900 and Catalyst 2820 switches support two Fast Ethernet ISL trunks. A trunk can be a one-port Fast Ethernet TX, a one-port Fast Ethernet FX, or an ATM module. Refer to the *Catalyst 2820 ATM Modules Installation and Configuration Guide* to determine the firmware version that supports trunking.

For each enabled VLAN that is known to the VTP and included in the allowed list for the trunk port, a Fast Ethernet ISL trunk automatically carries traffic for the VLAN and extends VLANs from one Catalyst switch to another.

VLAN Trunking With ATM

For an ATM trunk to carry traffic for a VLAN, all of the following conditions must be met:

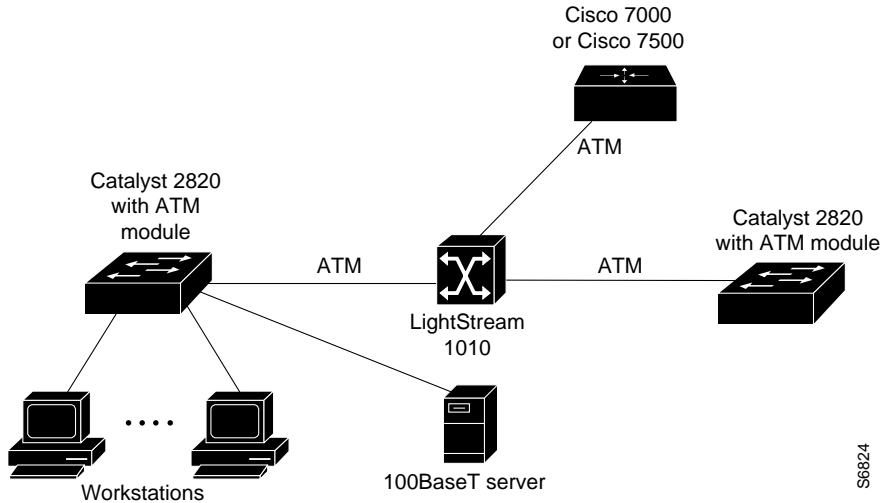
- The VLAN must be enabled.
- The VLAN must be known to the VTP.
- The VLAN must be included in the allowed list.
- A corresponding ELAN name mapped to the specified VLAN ID must be defined on the ATM module, and the VLAN ID must match the VLAN used on the switch. For a PVC, the VLAN ID must be bound to a PVC.

The ATM trunk module does not forward frames from the switch for a VLAN until you define a LANE client. Each VLAN must be associated with either a LANE client or a PVC before the ATM trunk module forwards traffic to and from a VLAN. When creating a LANE client or PVC on the module, a VLAN number is needed to map the ATM connection to a VLAN. For more information on configuring LANE clients, refer to the *Catalyst 2820 ATM Modules Installation and Configuration Guide*.

To configure support for RFC 1483, you must bind PVCs to the VLAN, and the VLAN ID must match the VLAN ID used on the switch. Each ATM trunk module supports a maximum of 64 active VLANs at one time.

Figure 2-3 shows the Catalyst 2820 switch using ATM trunking.

Figure 2-3 Catalyst 2820 ATM ELAN Configuration with a Router



VLAN Trunking and Load Sharing

There are three ways to configure load sharing using trunk ports. One way uses STP port priorities; the second way uses STP path costs. (For a third method, refer to the “Fast EtherChannel Feature” section in Chapter 3, “Additional Features.”) If you configure load sharing using STP port priorities, both load-sharing links must be connected to the same switch. If you configure load sharing using STP path costs, each load-sharing link can be connected to the same switch or to two different switches.

Load Sharing Using Port Priorities

To use load sharing with port priorities, you must use STP parameters on a VLAN basis. These parameters define which VLANs have priority access to a trunk and which VLANs use the trunk as a backup.

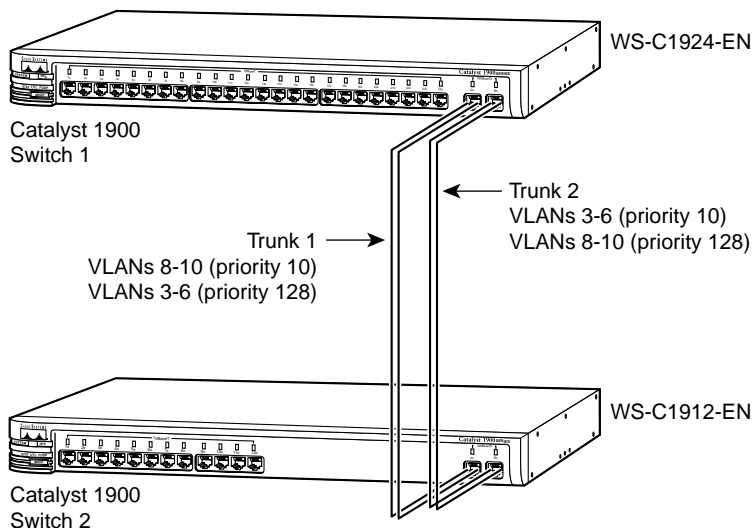
Each trunk port supports two STP port priorities. You can assign one of the two priorities to each VLAN. As a result, the trunk port with the higher priority (lower integer values) for a VLAN remains in the forwarding state. The trunk port with the lower priority (higher integer values) for the same VLAN remains in the blocking state. One trunk port transmits or receives all traffic for the VLAN.

Figure 2-4 shows two trunks that are connected to the switched 100BaseTX ports on two Catalyst 1900 switches. The port cost of carrying VLAN traffic across these trunks is equal.

- VLANs 8 through 10 are assigned a port priority of 10 on Trunk 1.
- VLANs 3 through 6 retain the default port priority of 128 on Trunk 1.
- VLANs 3 through 6 are assigned a port priority of 10 on Trunk 2.
- VLANs 8 through 10 retain the default port priority of 128 on Trunk 2.

Trunk 1 carries traffic for VLANs 8 through 10, and Trunk 2 carries traffic for VLANs 3 through 6. If the active trunk fails, the trunk with lower priority takes over and carries the traffic for all of the VLANs.

Figure 2-4 Load Sharing Using Port Priorities



H10750

Assigning STP Port Priority for Load Sharing

Catalyst 1900 and Catalyst 2820 switches use load sharing on parallel trunks. By setting STP parameters on a VLAN basis, you can define which VLANs have priority access to a trunk and which VLANs use the trunk as a backup when another trunk fails.

Note This feature cannot be used with the Fast EtherChannel feature.

When two ports on the same bridge form a loop, port priority determines which port is enabled and which port is in standby mode. A trunk port supports two port priorities. These priorities are assigned from the Trunk Port STP Configuration Menu. You can enter a port priority value from 0 to 255, with the lowest value having the highest priority.

To assign a priority to a port, do the following:

Step	Action
1 Access the Port Configuration Menu.	Enter [P] Port Configuration at the selection prompt in the Main Menu.
2 Specify the port (or trunk port) to be prioritized.	Enter the port number at the selection prompt, and press Return .
3 Access the Trunk STP Configuration Menu.	Enter [T] Trunk STP Configuration at the selection prompt.
4 Select the port priority value for option 1 and option 2.	<ul style="list-style-type: none"> a. Select [I] Port Priority (spanning tree) - option 1. b. Enter the port priority at the selection prompt. Press Return. c. Select [J] Port Priority (spanning tree) - option 2. d. Enter the port priority at the selection prompt. Press Return.
5 Assign the VLANs to port priority option 1 or port priority option 2.	<ul style="list-style-type: none"> a. Select [M] Assign VLANs to option 1 port priority. b. Enter the VLAN numbers that are to use port priority option 1 at the selection prompt. Press Return. c. Select [O] Assign VLANs to option 2 port priority. d. Enter the VLAN numbers that are to use port priority option 2 at the selection prompt. Press Return.

Verifying the STP Port Priority for Load Sharing

To verify the port priority option values and the assignment of VLANs to port priority options 1 and 2, access the Trunk Port STP Configuration Menu, and select **[E] Show VLAN port priorities** to show the assignment of VLANs to port priority options.

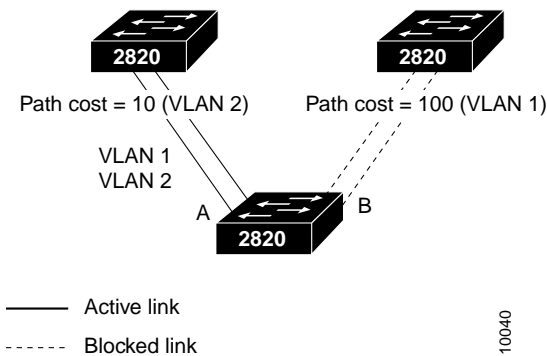
Load Sharing Using STP Path Costs

You can configure load sharing between trunk ports by assigning two STP path costs (path-cost option 1 and path-cost option 2) to each trunk and then assigning different VLANs to the different path costs.

Note STP path costs cannot be used with the Fast EtherChannel feature.

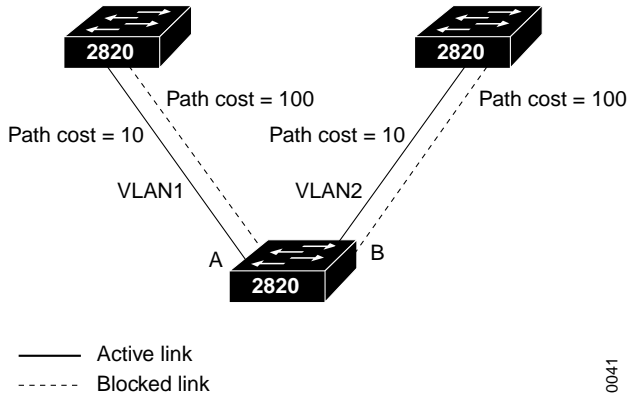
By default, trunk ports are assigned the same STP path costs for option 1 and option 2. Consequently, STP selects the path for VLAN traffic by using the Bridge ID. All VLANs then use the same path to forward traffic, as shown in Figure 2-5.

Figure 2-5 Traffic Path Without Load Sharing



You can configure VLAN 1 to use a different path than VLAN 2 by assigning two path costs per trunk and assigning each VLAN to use a different path cost on each trunk, as shown in Figure 2-6.

Figure 2-6 Traffic Path With Load Sharing



Note In Figure 2-5 and Figure 2-6, path costs are applied to the bottom switch.

Configuring Load Sharing Using Path Costs

To configure load sharing using path costs, do the following:

- Set the trunk state for trunk A and trunk B to one of these options:
 - On
 - Desirable
 - Auto
 - No-negotiate

The trunk state on the remote end of the trunk connection (that is, on the other switch) must be in a state that allows trunking. Refer to the “DISL Port States” section for more information on this subject.

Note Load sharing cannot be configured on a trunk that is in the off state.

- Set the two path-cost options on trunk A to different values.
- Assign one VLAN to use the higher path cost for trunk A, and assign another VLAN to use the lower path cost for trunk A.
- Set the two path-cost options on trunk B to the same values as those you assigned to trunk A.
- Assign the VLAN that used the higher trunk A path cost to use the lower trunk B path cost.
- Assign the VLAN that used the lower trunk A path cost to use the higher trunk B path cost.

Load Sharing Example

The following example configures load sharing by configuring the following parameters:

- Trunk A path-cost option 1 is 10 (default).
- Trunk A path-cost option 2 is a value less than or equal to 10.

Note The value of path cost option 2 on *any* trunk must be less than or equal to the value for path cost option 1 on the same trunk.

- Trunk B path-cost option 1 is 10 (default).
- Trunk B path-cost option 2 is a value less than or equal to 10.
- VLAN 1 is assigned to use trunk A path-cost option 1 and trunk B path-cost option 2.
- VLAN 2 is assigned to use trunk A path-cost option 2 and trunk B path-cost option 1.

Step	Action
1	Access the Virtual LAN Menu. Select [V] Virtual LAN from the Main Menu.
2	Access the Trunk Configuration Menu. Enter [T] Trunk Configuration .

Step	Action
3 Select trunk A.	At the next menu, enter [A] , and press Return .
4 Access the trunking setting.	Enter [T] Trunking .
5 Configure the trunking state for the selected port.	At the next menu, select a state: <ul style="list-style-type: none"> • [1] On • [3] Desirable • [4] Auto • [5] Nonnegotiate Press Return .
6 Select trunk B.	At the next menu, enter [N] Next Trunk .
7 Access the trunking setting.	Enter [T] Trunking .
8 Configure the trunking state for the selected port.	At the next menu, select a state: <ul style="list-style-type: none"> • [1] On • [3] Desirable • [4] Auto • [5] Nonnegotiate Press Return .
9 Return to the Main Menu.	Enter [X] Exit , twice.
10 Access the Port Configuration Menu.	Enter [P] Port Configuration .
11 Select trunk A.	At the next menu, enter [A] , and press Return .
12 Access the trunk port A STP Configuration Menu.	Enter [T] Trunk STP configuration .
13 Select the path-cost for option 2.	At the next menu, select [B] Path cost (spanning tree) - option 2 .
14 Enter the new path-cost for option 2.	At the prompt, enter 100 , and press Return .
15 Assign VLAN1 to path-cost option 1.	a. Select [T] Assign VLANs to option 1 Path cost . b. Enter 1 and press Return .

Step	Action
16 Assign VLAN2 to path-cost option 2.	<p>a. Select [Y] Assign VLANs to option 2 Path cost.</p> <p>b. Enter 2 and press Return.</p>
17 Access the trunk port B STP configuration menu.	a. Enter [N] Next Trunk.
18 Select the path-cost for option 2.	At the next menu, select [B] Path cost (spanning tree) - option 2.
19 Enter the new path-cost for option 2.	At the prompt, enter 100 , and press Return.
20 Assign VLAN1 to path-cost option 2.	<p>a. Select [Y] Assign VLANs to option 2 Path cost.</p> <p>b. Enter 1, and press Return.</p>
21 Assign VLAN2 to path-cost option 1.	<p>a. Select [T] Assign VLANs to option 1 Path cost.</p> <p>b. Enter 2, and press Return.</p>

Table 2-2 summarizes the VLAN and path-costs assigned in this example.

Table 2-2 VLAN Path-Cost Assignments

	Path Cost = 10	Path Cost = 100
Trunk A	VLAN 1	VLAN 2
Trunk B	VLAN 2	VLAN 1

Load sharing is achieved as follows:

- For VLAN 1, STP puts trunk A in forwarding state and trunk B in blocking state.
- For VLAN 2, STP puts trunk B in forwarding state and trunk A in blocking state.

Configuring VLAN Trunks

A VLAN trunk physically links two VLAN-capable switches or a VLAN-capable switch and a VLAN-capable router. VLAN trunks carry the traffic of multiple VLANs so you can extend VLANs from one Catalyst series switch to another.

Note VLANs cannot be connected by bridge groups.

The Cisco Catalyst 1900 and 2820 Enterprise Edition Software supports a maximum of 27 switched ports. On the Catalyst 2820 switch, the only ports you can configure as trunks are the single-port 100BaseTX, 100BaseFX, and ATM modules. On the Catalyst 1900 switch, you can configure the 100BaseTX or 100Base FX ports as trunks. (Refer to the *Catalyst 2820 ATM Modules Installation and Configuration Guide* to determine the firmware version that supports trunking.)

The Dynamic Inter-Switch Link Protocol (DISL) protocol synchronizes the configuration of two interconnected Fast Ethernet interfaces into an ISL trunk. The DISL protocol ensures that both of the Fast Ethernet interfaces are either in trunking or nontrunking mode.

Note DISL cannot be used if you have configured bridge groups on the switch. For more information on bridge groups, see the “Bridge Groups” section in Chapter 3, “Additional Features.”

If you are using VTP to propagate VLAN information, you must enable a trunk to receive and propagate VLAN information through network advertisements. The switch then learns the management domain and the VLANs within it that are defined on all other switches. Refer to “Configuring VTP” on page 34 for instruction for setting this option. ISL-capable switch ports process DISL packets from switches that have the same VTP domain name or a null domain name. If a switch port receives a DISL packet with a different VTP domain name than the domain name configured on the switch, the packet is discarded.

Figure 2-7 shows an example of a Fast Ethernet ISL configuration.

Table 2-3 DISL Port States

Port State	Description
On	Configures the port in permanent ISL trunk mode and negotiates with the connected device to convert the link to trunk mode. The port converts to a trunk, even if the other end of the link does not. This state is used when an ISL port is connected to another ISL port that does not support the DISL protocol.
Off	Disables port trunking and negotiates with the connected device to convert the link to nontrunk. The port converts to a nontrunk mode, even if the other end of the link does not. This state is used when an ISL port is connected to another ISL port that does not support the DISL protocol. (Default)
Desirable	Triggers the port to negotiate the link from nontrunking to trunking mode. The port negotiates to a trunk port if the connected device is either in the On, Desirable, or Auto state. Otherwise, the port becomes a nontrunk port.
Auto	Enables a port to become a trunk only if the connected device has the state set to On or Desirable.
No-negotiate	Configures the port in permanent ISL trunk mode, but the port does not generate or process DISL frames. Use this state when an ISL port is connected to another ISL port (such as a router ISL port) that does not support the DISL protocol.

The *status* of a VLAN port is shown in the grayed out field in the Status column of the web console Port Management Page. These non-configurable VLAN states indicate the DISL status of a port and whether or not the port has been disabled or suspended because no VLAN has been configured for the port. (See Table 2-4.)

Table 2-4 VLAN Port Status

VLAN Port Status	Description
Suspended-DISL	The port is suspended due to DISL negotiation.
Suspended No-VLAN	The port is suspended because there is no VLAN assigned to the port.
Disabled No-VLAN	The port is disabled because the VLAN assigned to the port does not exist.

Precautions for Trunking State

The on (or off) trunking state might cause configuration problems. Use the on or off state when an ISL port is connected to a device that you know does not support the DISL protocol. Because configurations can change, we advise you to set the trunking state to auto or desirable. If the other port does not support DISL, the port then functions as normal in static mode.

Using the on trunking state when the DISL protocol is in use might lead to ISL-mode mismatches where one end of the link is trunking while the other end is not. The situation can arise if the switch on the other end of the trunk is in no-negotiate state. Therefore, if a trunk is desired, use the desirable trunking state.

Using the off trunking state is not recommended when using DISL protocol. The risk of creating an ISL-mode mismatch is lower with the off mode, but if a trunk is not desired, use auto mode.

Table 2-5 shows the possible combinations of DISL port states for two switches, Switch 1 and Switch 2. For each port state combination, it also lists the trunking mode of the switch. An asterisk (*) indicates a misconfigured state that, if configured, results in a loss of connectivity.

Table 2-5 DISL Port State Combinations

Switch 1 Port State	Switch 2 Port State	Switch 1 Mode	Switch 2 Mode
Off	Off	Nontrunking	Nontrunking
Off	On	Nontrunking	Trunking*
Off	Desirable	Nontrunking	Nontrunking
Off	Auto	Nontrunking	Nontrunking
Off	No-negotiate	Nontrunking	Trunking*
On	Off	Trunking	Nontrunking*
On	On	Trunking	Trunking
On	Desirable	Trunking	Trunking
On	Auto	Trunking	Trunking
On	No-negotiate	Trunking	Trunking
Desirable	Off	Nontrunking	Nontrunking

Table 2-5 DISL Port State Combinations (continued)

Switch 1 Port State	Switch 2 Port State	Switch 1 Mode	Switch 2 Mode
Desirable	On	Trunking	Trunking
Desirable	Desirable	Trunking	Trunking
Desirable	Auto	Trunking	Trunking
Desirable	No-negotiate	Nontrunking	Trunking*
Auto	Off	Nontrunking	Nontrunking
Auto	On	Trunking	Trunking
Auto	Desirable	Trunking	Trunking
Auto	Auto	Nontrunking	Nontrunking
Auto	No-negotiate	Nontrunking	Trunking*
No-negotiate	Off	Trunking*	Nontrunking*
No-negotiate	On	Trunking	Trunking
No-negotiate	Desirable	Trunking*	Nontrunking*
No-negotiate	Auto	Trunking	Nontrunking*
No-negotiate	No-negotiate	Trunking	Trunking

You cannot change the trunking state of an ATM module. The trunking state of trunk-capable ATM modules defaults to on. The trunking state of ATM modules not capable of trunking defaults to off.

Configuring Trunks

To configure a trunk, do the following:

Step	Action
1 Access the Virtual LAN Menu.	Select [V] Virtual LAN from the Main Menu.
2 Access the Trunk Configuration Menu.	Enter [T] Trunk Configuration .
3 Select the appropriate trunk port.	At the next menu, enter [A] or [B] at the selection prompt, and press Return .

Step	Action
4 Access the trunking setting.	Enter [T] Trunking .
5 Configure the trunking state for the selected port.	At the next menu, select a setting: <ul style="list-style-type: none">• [1] On• [2] Off• [3] Desirable• [4] Auto• [5] Nonegotiate Press Return .

Verifying Trunk Configuration

To verify that you have configured the selected port as a trunk port, check the trunking status and encapsulation type at the top of the Trunk Configuration screen. (When a link is present, a Fast Ethernet trunk shows ISL encapsulation. An ATM module shows LANE encapsulation.) From the Main Menu, access the Virtual LAN Menu to see the status of each active VLAN.

Adding a VLAN to an Allowed List

Each trunk has a list of VLANs called *allowed VLANs* that are enabled to receive and transmit all types of traffic on that trunk. You must configure the VLAN and add it to the allowed list for the trunk so that it can receive trunk traffic. By default, all configured VLANs are allowed on a trunk. To add a VLAN to the allowed list, do the following:

Step	Action
1 Access the Virtual LAN Menu.	Select [V] Virtual LAN from the Main Menu.
2 Access the Trunk Configuration Menu.	Enter [T] Trunk Configuration .
3 Select the appropriate trunk port.	At the next menu, enter [A] or [B] at the selection prompt, and press Return .

Step	Action
4 Add the VLAN to the allowed list for the trunk.	<p>a. Enter [A] Add Allowed VLANs at the selection prompt.</p> <p>b. Enter the appropriate VLAN number at the selection prompt in the next menu. The Trunk Configuration Menu reappears.</p>

Traffic will not be forwarded to or from a VLAN that is not included in the VLAN allowed list.

Verifying a VLAN Allowed List Addition

To verify that you have added a VLAN to the allowed list, select **[V] List Allowed VLANs** from the Trunk Configuration Menu, and examine the contents of the display.

Deleting a VLAN from the Allowed List

To delete a VLAN from the allowed list, do the following:

Step	Action
1 Access the Virtual LAN Menu.	Select [V] Virtual LAN from the Main Menu.
2 Access the Trunk Configuration Menu.	Enter [T] Trunk Configuration .
3 Select the appropriate trunk port.	At the next menu, enter [A] or [B] at the selection prompt, and press Return .
4 Delete the VLAN number.	<p>a. Select [D] Delete Allowed VLAN(s).</p> <p>b. Enter the appropriate VLAN number at the selection prompt in the next menu, and press Return.</p>

Viewing the List of Allowed VLANs

To view the list of allowed VLANs, select **[V] List Allowed VLANs** from the Trunk Configuration Menu.

Adding a Pruning-Eligible VLAN

The flood traffic of a VLAN is typically sent to all switches in the same management domain that are connected by trunks. Pruning VLANs restricts the flood traffic of a VLAN to just those switches that have member ports. When you prune eligible VLANs, you restrict the flood traffic of those VLANs. To add a pruning-eligible VLAN, do the following:

Step	Action
1 Access the Virtual LAN Menu.	Select [V] Virtual LAN from the Main Menu.
2 Access the Trunk Configuration Menu.	Enter [T] Trunk Configuration .
3 Select the appropriate trunk port.	At the next menu, enter [A] or [B] at the selection prompt, and press Return .
4 Add the pruning eligible VLAN.	<p>a. Enter [E] Add Pruning Eligible VLAN(s) at the selection prompt.</p> <p>b. Enter the appropriate VLAN number at the selection prompt in the next menu. The Trunk Configuration Menu reappears.</p>

Verifying Pruning-Eligible VLAN Additions

To verify that you have added a pruning-eligible VLAN, select **[T] Trunk Configuration**, and view the contents of the display. To view additional VLAN information, select **[F] List Pruning Eligible VLANs**.

Deleting a Pruning-Eligible VLAN

To delete a pruning-eligible VLAN, do the following:

Step	Action
1 Access the Virtual LAN Menu.	Select [V] Virtual LAN from the Main Menu.

Step	Action
2 Access the Trunk Configuration Menu.	Enter [T] Trunk Configuration .
3 Select the appropriate trunk port.	At the next menu, enter [A] or [B] at the selection prompt, and press Return .
4 Delete the VLAN number.	<p>a. Select [C] Delete Pruning Eligible VLAN(s).</p> <p>b. Enter the appropriate VLAN number at the selection prompt in the next menu, and press Return.</p>

Viewing a List of Pruning-Eligible VLANs

To view the list of pruning-eligible VLANs, select **[F] List Pruning Eligible VLANs** from the Trunk Configuration Menu.

For more information about pruning, refer to the “Configuring VTP Pruning” section in this chapter.

Displaying VLANs Transmitting and Receiving Flooded Traffic

You can use the Trunk Configuration Menu to display the following lists:

- A list of VLANs on which flooded traffic is transmitted over a specified trunk

If a remote switch on a specified trunk requests the local switch to transmit flooded traffic on a specific list of VLANs, you can display that VLAN list on the local switch. At the selection prompt of the Trunk Configuration Menu, select **[S] List VLANs that Transmit Flooded Traffic**.
- A list of VLANs on which flooded traffic is received over a specified trunk

If a local switch on a specified trunk requests the remote switch to transmit flooded traffic on a specific list of VLANs, you can display that VLAN list on the local switch. At the selection prompt of the Trunk Configuration Menu, select **[R] List VLANs that Receive Flooded Traffic**.

VLAN Trunk Protocol

The VTP maintains VLAN configuration consistency throughout the network. VTP manages the addition, deletion, and modification of VLANs at the system level, automatically communicating this information to all the other switches in the network. In addition, VTP minimizes these possible configuration inconsistencies that can result in security violations:

- VLANs can become cross-connected when duplicate names are used.
- VLANs can become internally disconnected when they are incorrectly mapped between one LAN type and the other.

VTP Modes

You can configure VLANs on Catalyst 1900 and Catalyst 2820 switches when the switch is in VTP server or transparent mode. You can use the CLI, console menus, or the MIB (when using a SNMP management station) to modify a VLAN configuration when the switch is in either server or transparent modes.

A switch configured in VTP server mode advertises VLAN configuration to neighboring switches through its trunks and learns new VLAN configurations from those neighbors. Use the server mode to add or delete VLANs and to modify VLAN information by using either the VTP MIB, the CLI, or the console. For example, when you add a VLAN, VTP advertises the new VLAN, and both servers and clients prepare to receive traffic on their trunk ports.

After the switch automatically transitions to VTP client mode, it transmits advertisements and learns new information from advertisements. However, you cannot add, delete, or modify a VLAN through the MIB, the CLI, or the console. The VTP client does not maintain VLAN information in nonvolatile storage; when it starts, it learns the configuration by receiving advertisements from the trunk ports.

In VTP transparent mode, the switch does not advertise or learn VLAN configurations from the network. When a switch is in VTP transparent mode, you can modify, add, or delete VLANs through the console, the CLI, or the MIB.

Table 2-6 shows the maximum number of VLANs stored in nonvolatile RAM (NVRAM), the console or MIB configuration options, the advertisement options, and the maximum number of active VLANs for Catalyst 1900 and Catalyst 2820 switches.

Table 2-6 Catalyst 1900 and Catalyst 2820 VTP Modes

Mode	Maximum Number of VLANs in NVRAM	MIB, CLI, or Console Configuration	Switch Receives Advertisements	Maximum Number of VLANs
VTP server	128	MIB, CLI, or console configuration for up to 128 VLANs	Yes	128
VTP transparent	128	MIB, CLI, or console configuration for up to 128 VLANs	No	128
VTP client	0	MIB, CLI, or console configuration	Yes	1005

Note If a switch in VTP server mode receives advertisements containing more than 128 VLANs, the switch automatically transitions to VTP client mode.

Note If you change the switch from VTP client mode to VTP transparent mode, the switch retains only the first 128 VLANs and deletes the remaining VLANs.

Transmitting VTP Information

Using VTP, each Catalyst 1900 and 2820 switch advertises on its trunk ports its management domain, which defines the boundary of a specified VLAN, its configuration revision number, and its known VLANs and their specific parameters. A switch can reside in only one VTP management domain.

Through trunks, VTP servers transmit information to other switches and receive updates. VTP servers also maintain information, such as the list of VLANs in the VTP management domain in NVRAM.

VTP also dynamically maps VLANs across multiple LAN types, using unique names and internal index associations. VTP information is transmitted on all trunk connections, including ISL, IEEE 802.10, and LANE. The VTP MIB provides the SNMP instrumentation for the VTP, allowing the reading and setting of specific VTP parameters.

VTP establishes global configuration values and distributes the following global configuration information:

- VLAN IDs (ISL)
- Emulated LAN names (ATM LANE)
- IEEE 802.10 SAID values (FDDI)
- Maximum transmission unit (MTU) size for a VLAN

Configuring VTP

VTP maintains VLAN consistency throughout the network and manages VLAN modifications at the system level. With VTP, VLAN changes are automatically communicated to all other switches in the network.

To configure VTP, do the following:

Step	Action
1 Access the Virtual LAN Menu.	Select [V] Virtual LAN from the Main Menu.
2 Verify the setting of a management domain name.	Access [N] Domain Name on the Virtual LAN Menu. Verify that the server has a VTP management domain so that VTP information can be sent to other VTP switches in the management domain. Press Return to view the Virtual Lan Menu.
3 Access the VTP Mode Control Menu.	Select [V] VTP Mode Control from the VLAN Configuration Menu.
4 Select the server mode.	Enter [S] Server at the selection prompt. The VLAN Configuration Menu reappears.

Note The switch learns advertisements only if other VTP devices reside on the network, and at least one trunk port must be configured on the switch. VTP learns from advertisements within 5 minutes.

Verifying VTP Configuration

To verify that VTP is enabled and the switch is transmitting and receiving advertisements, do the following:

Step	Action
1 Access the Virtual LAN Menu.	Select [V] Virtual LAN from the Main Menu.
2 Access the list of defined VLANs.	Select [L] List VLANs from the Virtual LAN Menu.
3 View the VTP statistics.	Select [P] VTP Statistics at the selection prompt of the Virtual LAN Menu, and view the contents on the display.

Configuring a VTP Password

By default, the management domain is set to nonsecure mode and has no assigned password. Adding a password sets the management domain to secure mode. The same password must be set on all VTP devices in a management domain. To configure a password, do the following:

Step	Action
1 Access the Virtual LAN Menu.	Select [V] Virtual LAN from the Main Menu.
2 Enter a password.	<p>a. Select [W] VTP Password from the Virtual LAN Menu.</p> <p>b. Enter a password at the selection prompt.</p>

VTP Pruning

Catalyst 1900 and Catalyst 2820 switches

Catalyst 1900 and Catalyst 2820 switches

Monitoring VTP

Enabling VTP Pruning

To enable VTP pruning, do the following:

Step	Action
1 Access the Virtual LAN Menu.	Select [V] Virtual LAN from the Main Menu.
2 Access the VTP Pruning Mode screen.	Select [F] VTP Pruning Mode .
3 Enable VTP pruning.	Enter Enable at the selection prompt. The VLAN Configuration Menu reappears.

Verifying VTP Pruning

To verify that you have enabled VTP pruning, select **[F] VTP Pruning Mode**, and view the VTP pruning state.

Monitoring VTP

You can monitor VTP by displaying its configuration information: the domain name, the current VTP revision, and the number of VLANs. You can also display statistics about the advertisements sent and received by the switch.

To monitor VTP activity, perform this task from the CLI privileged EXEC mode:

Step	Action
1 Display the VTP switch configuration information.	show vtp
2 Display VTP counters about VTP messages being sent and received.	show vtp statistics

This example shows how to display VTP configuration information:

```
hostname# show vtp

                VTP version: 1
Configuration revision : 3
Maximum VLANs supported locally: 1005
Number of existing VLANs: 5
VTP domain name      : Zorro
VTP password         : vtp_server
VTP operating mode   : Server
VTP pruning mode     : Enabled
VTP traps generation : Enabled
Configuration last modified by: 10.1.126.45 at 9-4-99 00:12:24
```

This example shows how to display VTP messages and pruning statistics:

```
hostname# show vtp statistics

Receive Statistics                      Transmit Statistics
-----
Summary Adverts                        0      Summary Adverts
0
Subset Adverts                          0      Subset Adverts
0
Advert Requests                         0      Advert Requests
0
Configuration Errors:
  Revision Errors                       0
  Digest Errors                         0

VTP Pruning Statistics:
Port      Join Received      Join Transmitted      Summary Adverts received
with no pruning support
-----
A         0                    0                    0
B         0                    0                    0
```

Dynamic Port VLAN Membership

Note without reconfiguring the portCatalyst 1900 and Catalyst 2820 switchesThe switch VTP management domain name must match the VMPS server domain name.

Dynamic Port VLAN Membership

- switchswitchIf the assigned VLAN is restricted to a group of ports, the VMPS verifies the requesting port against this group.
 - If the VLAN is legal on this port, the VLAN name is passed in the response.
 - If the VLAN is illegal on this port, and the VMPS is not in secure mode, the VMPS sends an *access-denied* response.
 - If the VLAN is illegal on this port, and the VMPS is in secure mode, the VMPS sends a *port-shutdown* response.
- If the VLAN from the table does not match the current VLAN on the port, there are active hosts on the port, and the VMPS is not in secure mode, the VMPS sends an *access-denied* response.
- If the VLAN from the table does not match the current VLAN on the port, there are active hosts on the port, and the VMPS is in secure mode, the VMPS sends a *port-shutdown* response.

Note If the Catalyst 1900 or Catalyst 2820 switch receives an *access-denied* response from the VMPS, it continues to block traffic to or from the port. The switch continues to monitor the packets directed to the port and sends a query to the VMPS when it identifies a new address. If the switch receives a *port-shutdown* response from the VMPS, it changes the port status to disabled-management. You must use SNMP or the console to enable the port.

Note switchUntil a valid VLAN is assigned to a dynamic port, no connectivity is allowed. Use dynamic ports only to connect end stations. If dynamic ports are connected to switches or routers, you could lose connectivity.

Note The ATM modules do not support dynamic port VLAN membership.

Configuring Dynamic Port VLAN Membership

You can move a connection from a dynamic port on one switch to a dynamic port on another switch in the network without reconfiguring either port. When you configure dynamic ports, the switch automatically assigns VLAN membership to a dynamic VLAN port based on the source MAC address of the received packets.

Note Catalyst 1900 and Catalyst 2820 switches

Configuring the VMPS Addresses

To configure dynamic port VLAN membership, you configure the addresses of the VMPSs by doing the following:

Step	Action
1 Access the Virtual LAN Menu.	Select [V] Virtual LAN from the Main Menu.
2 Configure the primary VMPS IP address to be queried.	<p>a. Select [S] VLAN Membership Servers.</p> <p>b. Select [1] 1st VMPS IP Address.</p> <p>c. Enter the IP address of the server, and press Return.</p>
3 Configure the secondary VMPS IP addresses that the switch queries if no responses are received from the primary VMPS.	<p>a. Select [S] VLAN Membership Servers.</p> <p>b. Select [2], [3], or [4], enter the appropriate IP addresses, and press Return.</p>
4 Select the primary VMPS.	<p>a. Select [S] VLAN Membership Servers.</p> <p>b. Select [P] Primary Server.</p> <p>c. Select the number of the server to be used as the primary VMPS.</p>
5 Set the number of attempts to contact a VMPS before the switch queries the next VMPS in the list.	Select [R] Number of retries before changing server , enter the appropriate number, and press Return .

Spanning-Tree Protocol

Verifying VMPS Addresses

To verify that you have configured the VMPS addresses, access the VLAN Membership Servers Menu, and view the contents of this display.

Configuring Dynamic Ports

After configuring the addresses of the VMPS, configure the ports as dynamic.

Step	Action
1 Access the Virtual LAN Menu.	Select [V] Virtual LAN from the Main Menu.
2 Access the VLAN Membership Menu.	Select [E] VLAN Membership from the VLAN Configuration Menu.
3 Access the Membership Type Menu.	Select [M] Membership Type from the VLAN Membership Menu.
4 Specify the port on which you want to configure dynamic VLAN membership.	Enter the port number at the selection prompt.
5 Change the specified port from static to dynamic.	Select [D] Dynamic at the selection prompt.

Verifying Dynamic Port Configuration

To verify that you have configured the port as a dynamic port, select **[E] VLAN Membership** to see the VLAN membership configuration display for all ports. The display shows a port status change from static to dynamic.

Spanning-Tree Protocol

STP provides path redundancy while preventing undesirable loops that are caused by multiple active paths. For an Ethernet network to function properly, only one active path must exist between two stations.

Loops result in some switches seeing stations appear on both sides of the switch. This condition voids the forwarding algorithm and allows forwarding of duplicate frames.

STP defines a tree that spans all switches in an extended network and forces certain redundant data paths into a standby (blocked) state. If one of the network segments in the spanning tree becomes unreachable, or if STP costs change, the spanning-tree algorithm reconfigures the spanning-tree topology and reestablishes the link by activating the standby path. The STP operation is transparent to end stations, which do not recognize whether they are connected to a single LAN segment or to a switched LAN of multiple segments.

Configuring Spanning-Tree Protocol on Different VLANs

When creating fault-tolerant internetworks, a loop-free path must exist between all nodes in a network. The spanning-tree algorithm calculates the best loop-free path throughout the switched network.

Because each VLAN is a logical LAN segment, one instance of STP maintains a loop-free topology in each VLAN. Although the Catalyst 1900 and Catalyst 2820 switches support a maximum of 1005 VLANs, you can enable STP on a maximum of 64 VLANs at one time. If you configure more than 64 VLANs, you can still operate the other VLANs with STP disabled. By default, STP is enabled on VLANs 1 through 64.

Note If VLANs or bridge groups are configured on the switch, the web interface displays the spanning-tree values for VLAN 1 or bridge group 1, respectively.

Accessing the STP Menu

To access the Spanning Tree Configuration Menu, do the following:

Step	Action
1	Access the Network Management Menu. Select [N] Network Management from the Main Menu.
2	Access the Bridge - Spanning Tree Menu. Enter [B] Bridge - Spanning Tree from the Network Management Menu.

Enabling and Disabling STP

To enable or disable STP, do the following:

Step	Action
1 Access the Network Management Menu.	Select [N] Network Management from the Main Menu.
2 Access the Bridge - Spanning Tree Menu.	Enter [B] Bridge - Spanning Tree from the Network Management Menu.
3 Enable STP on a specified VLAN, if desired.	Enter [E] at the selection prompt, and press Return .
4 Disable STP on a specified VLAN, if desired.	Enter [D] at the selection prompt, and press Return .

Verifying STP Configuration

To check the STP status of a VLAN, do the following:

Step	Action
1 Access the Network Management Menu.	Select [N] Network Management from the Main Menu.
2 Access the Bridge - Spanning Tree Menu.	Enter [B] Bridge - Spanning Tree from the Network Management Menu.
3 Check the STP status of a VLAN.	Select [O] VLAN Bridge Operating Parameters .
4 Specify the VLAN.	Enter the VLAN number at the selection prompt. Press Return .

The following VLAN STP operating parameters are displayed:

- Designated root
- Number of member ports
- Max age
- Forward delay

- Number and time of topology changes that have occurred
- Root port
- Root path-cost
- Hello time
- Last topology change

Configuring STP Options

The Enterprise Edition software contains four configuration options for VLANs enabled with STP. For each option, you can configure a unique bridge priority, max age, hello time, and forward delay. After configuring an option, you can assign it to one STP instance or to several STP instances. By default, option 1 is assigned to all STP instances.

For more information about the bridge priority, max age, hello time, and forward delay options, refer to the *Catalyst 1900 Series Installation and Configuration Guide* or the *Catalyst 2820 Series Installation and Configuration Guide*.

To configure bridge priority, max age, hello time, and forward delay, do the following:

Step	Action
1 Access the Network Management Configuration Menu.	Enter [N] Network Management at the selection prompt in the Main Menu.
2 Access the Bridge - Spanning Tree Menu.	Enter [B] Bridge - Spanning Tree from the Network Management Menu.
3 Specify an option to be configured.	At the selection prompt, enter [1], [2], [3], or [4] to access the option screen.
4 Modify the Bridge Priority parameter.	Enter [B] Bridge Priority at the selection prompt, and enter the Bridge Priority value.
5 Modify the Max Age parameter.	Enter [M] Max Age at the selection prompt, and enter the Max Age value.
6 Modify the Hello Time parameter.	Enter [H] Hello Time at the selection prompt, and enter the Hello Time value.
7 Modify the Forward Delay parameter.	Enter [F] Forward Delay at the selection prompt, and enter the Forward Delay value.

Spanning-Tree Protocol

Step	Action
8 Select the next option to be configured, if desired.	Enter [N] Next Option at the selection prompt to access another option.

Assigning an STP Instance

To assign an STP instance to a specific option, do the following:

Step	Action
1 Access the Network Management Configuration Menu.	Enter [N] Network Management at the selection prompt in the Main Menu.
2 Access the Bridge - Spanning Tree Menu.	Enter [B] Bridge - Spanning Tree from the Network Management Menu.
3 Assign an STP instance operating on a VLAN to use a specified option.	<ol style="list-style-type: none">Enter option 1, 2, 3, or 4 at the selection prompt.Select [A] Assign VLANs to option.Enter the VLAN number at the selection prompt, and press Return. You see the spanning-tree option menu.Select [X] Exit to the Bridge STP Configuration Menu.

