

# Virtual LANs

---

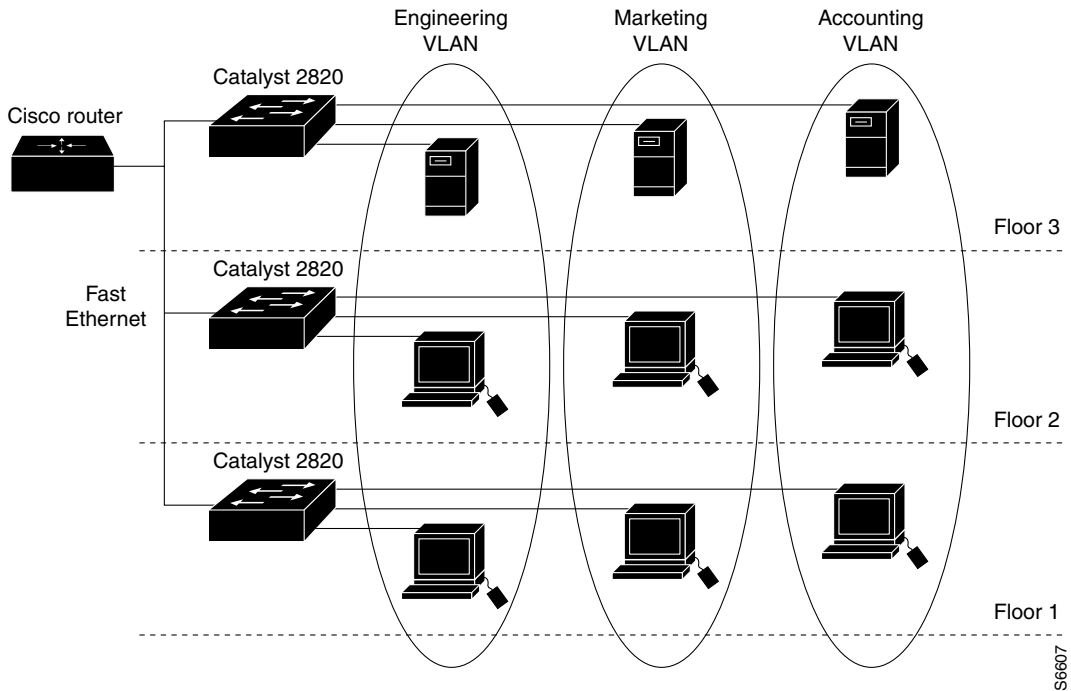
This chapter describes virtual LAN (VLAN) features and functionality, the Virtual LAN Menu of the Catalyst 2820 and Catalyst 1900 switches, procedures for creating VLANs, and the assignment of ports to VLANs.

## VLAN Features and Components

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 located close to one another, you can group them into a LAN segment. But if any of the end stations are in different buildings, you can then group them into a VLAN with the same attributes as a LAN, even though the end stations are not all on the same physical LAN segment.

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. This segmentation improves the overall performance of the network. Figure 2-1 shows an example of VLANs segmented into logically defined networks.

**Figure 2-1 VLANs as Logically Defined Networks**



## VLAN Features

VLANs provide the following features:

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

The VLANs on a Catalyst 2820 or Catalyst 1900 switch simplify adding and moving end stations on a network. For example, 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.

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 Catalyst 2820 or Catalyst 1900 switch to any VLAN. A network management station and workstations on any Catalyst series switch VLAN then have direct access to other Catalyst 2820 and Catalyst 1900 switches on the same VLAN, without needing a router. Only one IP address can be assigned to a Catalyst 2820 or Catalyst 1900 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. You can create VLANs for an entire management domain from a single Catalyst 2820 or Catalyst 1900 switch. The management domain is a group of VLANs that are managed by a single administrative authority.

- Workgroup and network security

You can increase security by segmenting the network into distinct broadcast groups. To this end, VLANs can restrict the number of users in a VLAN or prevent another user from joining a VLAN without first receiving approval. You can also control the size and composition of the broadcast domain by controlling the size of a VLAN group. To implement this type of segmentation, you can group switch ports based on the type of applications and the access privilege.

The Catalyst 2820 and Catalyst 1900 VLAN features might differ from the VLAN capability of other Catalyst series switches. Table 2-1 shows the capability and defaults for the Catalyst 2820 and Catalyst 1900 VLAN features.

**Table 2-1 Catalyst 2820 and Catalyst 1900 VLAN Features**

<b>Feature</b>	<b>Capability</b>	<b>Default</b>
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.	No trunk ports are enabled.
Load sharing	Supports Spanning-Tree Protocol (STP) on VLAN trunks to load share. Supports STP on a maximum of 64 VLANs at one time.	No load sharing is set up.
VLAN Trunk Protocol (VTP)	Supports server, client, and transparent modes. However, you can only configure server and transparent modes. Server and transparent modes support a maximum of 128 VLANs. The switch automatically transitions to client mode from server 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 1-64 are enabled with STP.

## VLAN Components

VLANs are composed 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 extend 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, 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 Steps

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.
- Configure STP on different VLANs.

## Accessing the Virtual LAN Menu

To access the Virtual LAN Menu, enter **V** at the selection prompt on the Main Menu. After you enter **V**, 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.

# Assigning a Management Domain

A management domain is a group of VLANs that is under the same administrative responsibility. You need to assign a management domain to the switch before you create a VLAN.

By default, a Catalyst 2820 or Catalyst 1900 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] <b>Virtual LAN Menu</b> from the Main Menu.
2 Define the VLAN management domain of the switch.	<ol style="list-style-type: none"><li>Select [N] <b>Domain Name Menu</b> from the Virtual LAN Menu.</li><li>Enter the management domain name at the selection prompt.</li><li>Press <b>Return</b>. The Virtual LAN Menu reappears.</li></ol>

## Verifying the Management Domain Assignment

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

## Concepts About 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 2820 and Catalyst 1900 switches support only one management domain for each switch.

Catalyst 2820 and Catalyst 1900 switches operate in one of three modes: server, client, or transparent mode. By default, a Catalyst 2820 or Catalyst 1900 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. In server mode, you can add or delete VLANs by using either the VTP Management Information Base (MIB) Simple Network Management Protocol (SNMP) management station or the console.

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 or the console. 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.

A switch automatically changes from VTP server mode to VTP client mode when it receives an advertisement with more than 128 VLANs. You cannot configure a 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 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.

# 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 [ <b>V</b> ] <b>Virtual LAN Menu</b> from the Main Menu.
2 Add the specified VLAN to the VLAN list for the trunk.	Select [ <b>A</b> ] <b>Add VLAN</b> 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 [ <b>1</b> ]. Press <b>Return</b> .
4 Define the VLAN number.	At the next menu, select [ <b>N</b> ] <b>VLAN Number</b> , and enter the number of the VLAN to be added. Press <b>Return</b> .
5 Define the VLAN name.	At the next menu, select [ <b>V</b> ] <b>VLAN Name</b> , and enter the name of the VLAN to be added. Press <b>Return</b> .
6 Set the IEEE 802.10 SAID value.	At the next menu, select [ <b>I</b> ] <b>802.10 SAID</b> , 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 <b>Return</b> .
7 Set the MTU size.	At the next menu, select [ <b>M</b> ] <b>MTU Size</b> , and enter the appropriate value. Press <b>Return</b> .
8 Enable the VLAN.	At the next menu, select [ <b>T</b> ] <b>VLAN State</b> , and select Enabled. Press <b>Return</b> .
9 Save the configuration.	Select [ <b>S</b> ] <b>Save</b> .

## 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] 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**.

## Concepts about VLAN Definition

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 permanent virtual connections (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.

## Grouping Switch Ports to VLANs

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] from the Main Menu.
2 Access the VLAN Membership screen.	Select [E] <b>VLAN Membership</b> .
3 Access the VLAN Assignment screen.	Select [V] <b>VLAN Assignment</b> .
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 <b>Return</b> .

---

**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 port. An ATM module can function as a LANE trunk or a static VLAN member port. You can group a Fast Ethernet port into different VLANs (that is, if it is not a trunk) by following the steps listed in this section. For ATM, you must configure a LANE client in addition to performing the steps listed in this section. 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, view the contents of the VLAN Membership Configuration Menu.

## Concepts about Port Grouping

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**

## 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 and allow you to extend VLANs from one Catalyst series switch to another.

To establish a trunk, you must configure a Fast Ethernet port or an ATM module on each Catalyst 2820 or Catalyst 1900 switch as a trunk port. The Enterprise Edition software for Catalyst 2820 or Catalyst 1900 switches supports a maximum of 27 switched ports. A maximum of 2 of these ports can be configured as trunk ports. On the Catalyst 2820 switch, you can configure only the single-port Fast Ethernet TX or FX and ATM modules as trunks. (Refer to the *Catalyst 2820 ATM Modules Installation and Configuration Guide* to determine the firmware version that supports trunking.) On the Catalyst 1900 switch, you can configure the 100BaseTX or 100BaseFX ports as trunks.

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 automatically learns the management domain and the VLANs within it that are defined on all other switches.

The remainder of this section describes how to configure VLAN trunks and establish load sharing by assigning port priorities.

## Configuring Trunks

To configure a trunk, do the following:

Step	Action
1	Access the Virtual LAN Menu. Select [V] from the Main Menu.
2	Access the Trunk Configuration Menu. Enter [T] <b>Trunk Configuration</b> .
3	Select the appropriate trunk port. At the next menu, enter [A] or [B] at the selection prompt, and press <b>Return</b> .
4	Access the Trunking setting. Enter [T] <b>Trunking</b> .
5	Turn on trunking for the selected port. At the next menu, select [1] <b>On</b> , and press <b>Return</b> .

---

**Note** If you have installed an ATM module, it resets when you change the trunking status.

---

## 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. (A Fast Ethernet trunk shows ISL encapsulation. An ATM module shows LANE as the encapsulation type.) From the Main Menu, access the Port Configuration 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 have been enabled to receive and transmit all types of traffic on that trunk. For a VLAN to receive traffic on a trunk, you must configure the VLAN and add it to the allowed list for the trunk. 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] from the Main Menu.
2	Access the Trunk Configuration Menu. Enter [T] <b>Trunk Configuration</b> .

## Configuring VLAN Trunks

---

Step	Action
3 Select the appropriate trunk port.	At the next menu, enter [A] or [B] at the selection prompt, and press <b>Return</b> .
4 Add the VLAN to the allowed list for the trunk.	<p>a. Enter [A] <b>Add Allowed VLANs</b> 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 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 for a trunk, do the following:

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

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

### 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 enables you to restrict 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] from the Main Menu.
2	Access the Trunk Configuration Menu. Enter [T] <b>Trunk Configuration</b> .
3	Select the appropriate trunk port. At the next menu, enter [A] or [B] at the selection prompt, and press <b>Return</b> .
4	Add the pruning eligible VLAN. <ul style="list-style-type: none"> <li>a. Enter [E] <b>Pruning Eligible VLANs</b> at the selection prompt.</li> <li>b. Enter the appropriate VLAN number at the selection prompt in the next menu. The Trunk Configuration Menu reappears.</li> </ul>

### 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] from the Main Menu.
2	Access the Trunk Configuration Menu. Enter [T] <b>Trunk Configuration</b> .
3	Delete the VLAN number. <b>a.</b> Select [C] <b>Delete Pruning Eligible VLAN(s)</b> . <b>b.</b> Enter the appropriate VLAN number at the selection prompt in the next menu, and press <b>Return</b> .

### 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 that Transmit and Receive 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**.

## Assigning STP Port Priority for Load Sharing

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

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 designated as option 1 and option 2 in the Port 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 <b>[P] Port Configuration</b> at the selection prompt in the Main Menu.
2 Specify the port to be prioritized.	Enter the port number at the selection prompt, and press <b>Return</b> .
3 Select first and second priorities for the port.	<ul style="list-style-type: none"> <li>a. Select <b>[I] Port Priority (spanning tree) - option 1</b>.</li> <li>b. Enter the port priority at the selection prompt. Press <b>Return</b>.</li> <li>c. Select <b>[J] Port Priority (spanning tree) - option 2</b>.</li> <li>d. Enter the port priority at the selection prompt. Press <b>Return</b>.</li> </ul>
4 Assign the VLANs to the prioritized ports.	<ul style="list-style-type: none"> <li>a. Select <b>[M] Assign VLANs to option 1 port priority</b>.</li> <li>b. Enter the VLAN numbers to which the port is assigned at the selection prompt. Press <b>Return</b>.</li> <li>c. Select <b>[O] Assign VLANs to option 2 port priority</b>.</li> <li>d. Enter the VLAN numbers to which the port is assigned at the selection prompt. Press <b>Return</b>.</li> </ul>

### Verifying the STP Port Priority for Load Sharing

To verify there is an STP port for load sharing, access the Port Configuration Menu, and view the contents of this display.

## Concepts about VLAN Trunking

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

A Catalyst 1900 switch supports up to two Fast Ethernet ISL trunks. A Catalyst 2820 switch supports up to two 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 allows you to extend 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 permanent virtual connection (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.

### VLAN Trunking With Load Sharing

To use load sharing, 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.

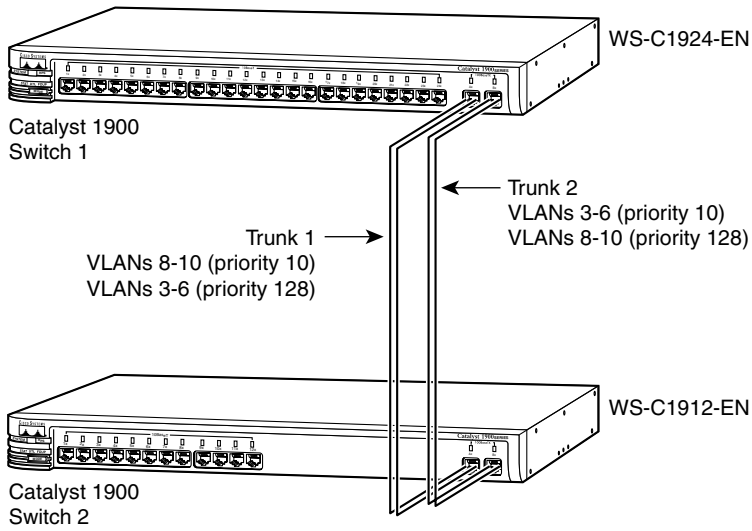
Each trunk port supports two STP port priorities. You can assign one of the two priorities to each VLAN. As a result, the trunk port with the higher priority (lower integer values) for a VLAN remains in the forwarding state. The trunk port with the lower priority (higher integer values) for the same VLAN remains in the blocking state. All traffic for the VLAN is transmitted or received on only one trunk port.

Figure 2-3 illustrates 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 2-3 Load Sharing Using VLAN Trunks



H10750

## Configuring VLAN Trunk Protocol

VLAN Trunk Protocol (VTP) maintains VLAN consistency throughout the network and manages the modification of VLANs 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] from the Main Menu.
2 Verify the setting of a management domain name.	Access [N] <b>Domain Name</b> 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 <b>Return</b> to view the Virtual Lan Menu.
3 Access the VTP Mode Control Menu.	Select [V] <b>VTP Mode Control</b> from the VLAN Configuration Menu.
4 Select the server mode.	Enter [S] <b>Server</b> at the selection prompt. The VLAN Configuration Menu reappears on the screen.

---

**Note** The switch learns advertisements only if other VTP devices reside on the network. In addition, at least one trunk port must be configured on the switch. VTP can learn 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 [ <b>V</b> ] from the Main Menu.
2 Access the list of defined LANs.	Select [ <b>L</b> ] from the Virtual LAN Menu.
3 View the VTP statistics.	Select [ <b>P</b> ] <b>VTP Statistics</b> 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. To configure a password, do the following:

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

The same password must be set on all VTP devices in a management domain.

## Concepts about VTP

VTP maintains VLAN configuration consistency throughout the network. VTP manages the addition, deletion, and renaming 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 2820 and Catalyst 1900 switches when the switch is in VTP server or transparent mode. You can use the console or the MIB (when using a Simple Network Management Protocol (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 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 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 or the MIB.

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

**Table 2-2 Catalyst 2820 and Catalyst 1900 VTP Modes**

<b>Mode</b>	<b>Maximum Number of VLANs in NVRAM</b>	<b>MIB or Console Configuration</b>	<b>Switch Receives Advertisements</b>	<b>Maximum Number of VLANs</b>
VTP server	128	Configure using MIB or console for up to 128 VLANs.	Yes	128
VTP client	0	Cannot configure using MIB or console.	Yes	1005
VTP transparent	128	Configure using console for up to 128 VLANs.	No	128

---

**Note** If a switch in VTP server mode receives advertisements containing more than 128 VLANs, the switch automatically transitions to VTP client mode. You cannot configure the Catalyst 1900 and Catalyst 2820 switches to operate in VTP client mode.

---

---

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

---

### VTP Information Transmission

Using VTP, each Catalyst 2820 and Catalyst 1900 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 nonvolatile RAM (NVRAM).

VTP also dynamically maps VLANs across multiple LAN types with unique names and internal index associations. VTP 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

## Enabling VTP Pruning

### Enabling VTP Pruning

To enable VTP pruning, do the following:

Step	Action
1 Access the Virtual LAN Menu.	Select [V] from the Main Menu.
2 Access the VTP Pruning Mode screen.	Select [F] <b>VTP Pruning Mode</b> .
3 Enable VTP pruning.	Enter <b>Enable</b> 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.

## Concepts about VTP Pruning

# Configuring Dynamic Port VLAN Membership

With dynamic ports, you can move a connection from a port on one switch to a port on another switch in the network without reconfiguring the 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

---

To configure dynamic port VLAN membership, you must configure the VMPS addresses and dynamic ports as described in the following sections.

## Configuring the VMPS Addresses

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

Step	Action
1 Access the Virtual LAN Menu.	Select [V] from the Main Menu.
2 Configure the primary VMPS IP address to be queried.	<p>a. Select [S] <b>VLAN Membership Servers</b>.</p> <p>b. Select [1] <b>1st VMPS IP Address</b>.</p> <p>c. Enter the IP address of the server to be queried, and press <b>Return</b>.</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] <b>VLAN Membership Servers</b></p> <p>b. Select [2], [3], or [4], enter the appropriate IP addresses, and press <b>Return</b>.</p>
4 Select the primary VMPS.	<p>a. Select [S] <b>VLAN Membership Servers</b>.</p> <p>b. Select [P] <b>Primary Server</b>.</p> <p>c. Select the number of the server to be used as the primary VMPS.</p>

Step	Action
5 Set the number of attempts to contact a VMPS before the switch queries the next VMPS in the list.	Select <b>[R] Number of retries before changing server</b> , enter the appropriate number, and press <b>Return</b> .

### 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 <b>[V]</b> from the Main Menu.
2 Access the VLAN Membership Menu.	Select <b>[E]</b> from the VLAN Configuration Menu.
3 Access the Membership Type Menu.	Select <b>[M] Membership Type</b> 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 <b>[D] ynamic</b> 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 indicates a port status change from static to dynamic.

### Concepts about Dynamic Port VLAN Membership

without reconfiguring the port. Until a valid VLAN is assigned to a dynamic port, no connectivity is allowed, and the port belongs to VLAN 0. If the Catalyst 2820 or the Catalyst 1900 switch receives an *access-denied* response from the VMPS, it continues to disallow the forwarding of 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 Catalyst 2820 or the Catalyst 1900 switch receives a *port-shutdown* response from the VMPS, it changes the port status to disabled-management. Traffic is not forwarded to or from the port. You must use SNMP or the console to enable the port.

---

**Note** Dynamic ports must be used only to connect end stations. If dynamic ports are connected to switches or routers, you may lose connectivity.

---

---

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

---

## 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 2820 and Catalyst 1900 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 remainder of the VLANs with STP disabled. By default, STP is enabled on VLANs 1 through 64.

## Accessing the STP Menu

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

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

You can use the Spanning-Tree Configuration Menu to do the following tasks:

- Enable or disable STP for different VLANs.
- Configure STP options with these parameters:
  - Bridge priority
  - Max age
  - Hello time
  - Forward delay
- Assign an STP instance to parameters defined by a specific option.

### Enabling and Disabling STP

To enable or disable STP, do the following:

Step	Action
1 Access the Network Management Configuration Menu.	Enter <b>N</b> at the selection prompt in the Main Menu.
2 Access the Bridge Configuration menu.	Select <b>[B] Bridge Configuration</b> .
3 Enable STP on a specified VLAN, if desired.	Enter <b>[E]</b> at the selection prompt. Press <b>Return</b> .
4 Disable STP on a specified VLAN, if desired.	Enter <b>[D]</b> at the selection prompt. Press <b>Return</b> .

### Configuring STP Options

The Enterprise Edition software contains four STP configuration options. These options are relevant only 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 that option 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 <b>N</b> at the selection prompt in the Main Menu.
2 Access the Bridge Configuration Menu.	Select <b>[B] Bridge Configuration</b> .
3 Specify an option to be configured.	At the selection prompt, enter <b>[1]</b> , <b>[2]</b> , <b>[3]</b> , or <b>[4]</b> to access the option screen.
4 Modify the Bridge Priority parameter.	Enter <b>[B]</b> at the selection prompt, and enter the appropriate modifications.
5 Modify the Max Age parameter.	Enter <b>[M]</b> at the selection prompt, and enter the appropriate modifications.

Step	Action
6 Modify the Hello Time parameter.	Enter [ <b>H</b> ] at the selection prompt, and enter the appropriate modifications.
7 Modify the Forward Delay parameter.	Enter [ <b>F</b> ] at the selection prompt, and enter the appropriate modifications.
8 Select the next option to be configured, if desired.	Enter [ <b>N</b> ] at the selection prompt to access another option.

### Assigning an STP Instance

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

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

### Verifying STP Configuration

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

Step	Action
1 Access the Network Management Configuration Menu.	Enter <b>N</b> at the selection prompt in the Main Menu
2 Access the Bridge Configuration screen.	Select <b>[B] Bridge Configuration</b> .
3 Check the STP status of a VLAN.	Select <b>[0] VLAN Bridge Operating Parameters</b> .
4 Specify the VLAN.	Enter the VLAN number at the selection prompt. Press <b>Return</b> .

### Concepts About 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 confuses the forwarding algorithm and allows forwarding of duplicate frames.

To provide path redundancy, STP defines a tree that spans all switches in an extended network. STP 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 a switched LAN of multiple segments.

## VLAN Example

This section contains an example of a VLAN configuration for ISLs on Fast Ethernet ports and multiple Catalyst 2820 and Catalyst 1900 switches using STP.

### Inter-Switch Links on Fast Ethernet Ports

Any Fast Ethernet port can be configured as a trunk. Trunks use the ISL Protocol to support multiple VLANs. An ISL trunk is like a continuation of the switching backplane. It allows the Catalyst switch to multiplex up to 1005 VLANs between switches and routers.

Figure 2-4 and Figure 2-5 show examples of Fast Ethernet ISL configurations.

**Figure 2-4 Catalyst 2820 Switches and Catalyst 1900 Switches in a Fast Ethernet ISL Configuration**

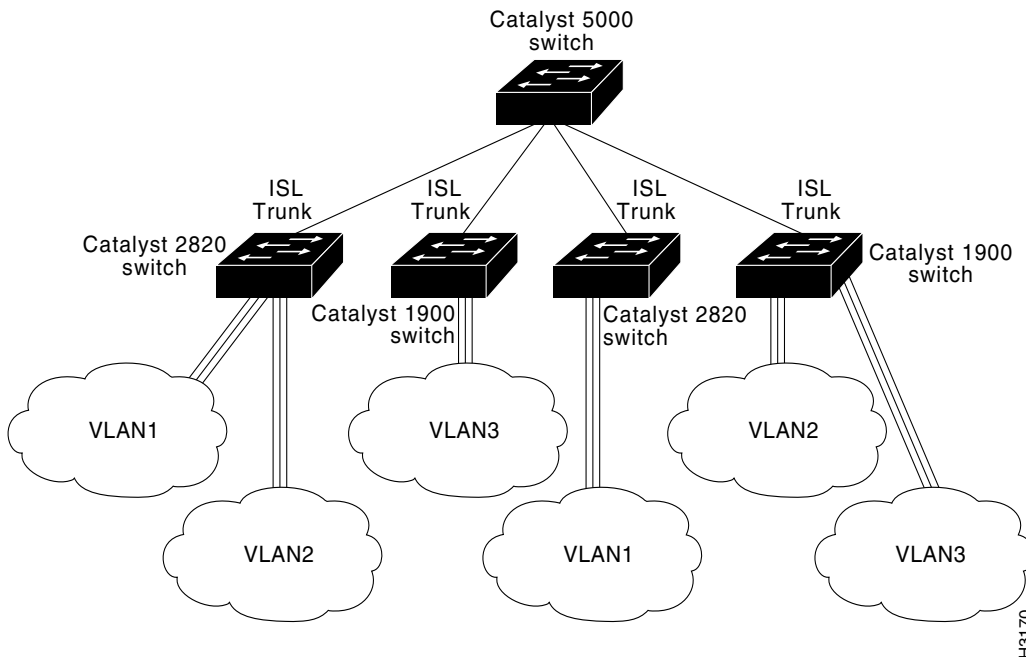


Figure 2-5 Catalyst 2820 ATM ELAN Configuration with a Router

