CHAPTER 1

Using the Command-Line Interface

The Catalyst 2900 series XL switches, hereafter referred to as the Catalyst 2900 series switches, are supported by Cisco IOS software. The current release is Cisco IOS Release 11.2(8)SA4. This chapter describes how to use the switch command-line interface (CLI) to configure those features that have been added for the switch. For a complete description of the commands that support these features, see Chapter 2, "Cisco IOS Commands." For more information on Cisco IOS Release 11.2(8), refer to the *Cisco IOS Release 11.2 Command Summary.*

The switches are preconfigured and begin forwarding packets as soon as they are attached to compatible devices.

All ports belong by default to virtual LAN (VLAN) 1. Access to the switch itself is also through VLAN 1. For management purposes, only devices connected to ports assigned to VLAN 1 can communicate with the switch. This applies to Telnet, web-based management, and SNMP.

Note This manual describes commands used in the standard and Enterprise Edition Software packages. Commands and features that are available only in the Enterprise Edition Software are identified; otherwise, the command and feature is supported in both the standard and Enterprise Edition Software.

Configuration Tasks

This chapter describes how to complete the following configuration tasks:

- Assigning IP information to the switch
- Setting port features, including creating Fast EtherChannel and Gigabit EtherChannel port groups
- Managing the switch MAC-address table
- Enabling the Spanning-Tree Protocol (STP) Port Fast feature
- Enabling the Cisco Group Management Protocol (CGMP) Fast Leave feature
- Assigning ports for static-access VLAN membership
- Assigning ports for multi-VLAN membership

Using the Enterprise Edition Software, you can complete the following configuration tasks:

- Configuring VLAN Trunk Protocol (VTP)
- Adding a VLAN to the database
- Modifying a VLAN in the database

- Removing a VLAN from the database
- Configuring a VLAN trunk
- Assigning ports for dynamic VLAN membership

Type of Memory

The switch Flash memory stores the Cisco IOS software image, the startup configuration file, and helper files.

Platforms

Cisco IOS Release 11.2(8)SA4-A and SA4-EN run on a variety of Catalyst 2900 series switches and modules. For a complete list, see the *Release Notes for the Catalyst 2900 Series XL Cisco IOS Release 11.2(8)SA4*.

Assigning IP Information to the Switch

If no IP information has been entered for the switch, the setup program prompts you for the IP address, subnet mask, and default gateway the first time you access the CLI. You can enter or change this information at any time through the CLI.

For management purposes, the switch belongs to VLAN 1, and the switch IP address and subnet mask are associated with VLAN 1.

Beginning in privileged EXEC mode, follow these steps to enter the IP information:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port to which the IP information is assigned. VLAN 1 is the switch interface.	**interface vlan 1**
Step 3	Enter the IP address and subnet mask.	**ip address** *ip_address subnet_mask*
Step 4	Enter the IP address of the default router.	**ip default-gateway** *ip_address*
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify that the information was entered correctly by displaying the running configuration. If the information is incorrect, repeat the procedure.	**show running-config**

Setting Port Features

The port commands control switch features that manage packet flooding, port security, EtherChannel port groups, and other switch activities. This section describes how to use the port commands to complete the following tasks:

- Blocking flooded unicast and multicast packets
- Entering the speed and duplex settings
- Enabling broadcast-storm control
- Defining a network port
- Enabling port security
- Creating a source-based or destination-based Fast EtherChannel or Gigabit EtherChannel port group

Blocking Unicast and Multicast Flooding

By default, the switch floods unknown unicast and multicast packets to all ports in a VLAN. Although flooding ensures that packets always reach their destinations, it is unnecessary in configurations where there are no unknown addresses. For example, it is unnecessary when a workstation is connected to a port and the workstation is initiating all network activity (that is, between the workstation and other devices) or when the port is a secure port.

Note For information on configuration restrictions and usage guidelines, see the "port block" section on page 2-24.

Beginning in privileged EXEC mode, follow these steps to disable the flooding of multicast and unicast packets to a port:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port to configure.	**interface** *interface*
Step 3	Block multicast forwarding to the port.	**port block multicast**
Step 4	Block unicast flooding to the port.	**port block unicast**
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries by entering the appropriate command once for the **multicast** option and once for the **unicast** option.	**show port block** {**multicast** | **unicast**} *interface*

Entering the Speed and Duplex Settings for a Port

You can enter the speed (10 or 100 Mbps) on Fast Ethernet ports and duplex (half or full) settings on Fast Ethernet and Gigabit Ethernet ports, or you can let the switch configure the port by using the IEEE 802.3u autonegotiation protocol.

Autonegotiation is still enabled when one of the parameters has been manually set. The mix of autonegotiation and explicitly set parameters can produce unexpected results that affect performance. To maximize the performance of your switch, follow one of these guidelines when setting the speed and duplex parameters:

- Let both ends of a connection autonegotiate the speed and duplex parameters.
- Manually set both parameters at both ends of the connection.

Beginning in privileged EXEC mode, follow these steps to set the speed and duplex parameters on a port:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port to be configured.	**interface** *interface*
Step 3	Enter the speed parameter for the port. You cannot enter the speed on Gigabit Ethernet ports.	**speed** {**10** | **100** | **auto**}
Step 4	Enter the duplex parameter for the port.	**duplex** {**full** | **half** | **auto**}
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries.	**show running-config**

Enabling Broadcast-Storm Control

Broadcast-storm control blocks the forwarding of packets created by broadcast storms, the bursts of broadcast traffic that ports can generate. When you enable broadcast-storm control on a port, two threshold parameters define the beginning and the end of a broadcast storm. The **rising** parameter determines when the forwarding of broadcast packets from the port is blocked. The **falling** parameter determines when normal forwarding resumes. You can set the port to generate a trap when these thresholds are crossed, and you can disable the port during a broadcast storm.

Beginning in privileged EXEC mode, follow these steps to enable broadcast-storm control:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port to configure.	**interface** *interface*
Step 3	Enter the rising and falling thresholds. Thresholds can be from 0 to 4294967295 broadcast packets per second.	**port storm-control** [**threshold** {**rising** *rising-number* **falling** *falling-number*}]
Step 4	Disable the port during a broadcast storm, or generate an SNMP trap when the traffic on the port crosses the rising or falling threshold.	**port storm-control filter** or **port storm-control trap**
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries.	**show port storm-control** [*interface*]

Defining a Network Port

Enabling a network port can reduce flooded traffic on your network. The network port receives all traffic with unknown destination addresses instead of the switch flooding them to all ports in the same VLAN. Space is then conserved in the dynamic address table because a network port does not learn source addresses from received packets.

Note For information on configuration restrictions and usage guidelines, see the “port network” section on page 2-28.

Beginning in privileged EXEC mode, complete these tasks to define a port as the network port:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port to be configured.	**interface** *interface*
Step 3	Define the port as the network port.	**port network**
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entry.	**show running-config**

Enabling Port Security

Secured ports restrict the use of a port to a user-defined group of stations. When you assign secure addresses to a secure port, the switch does not forward any packets with source addresses outside the group. A secure address is associated with one port per VLAN. You can enter these addresses, or the switch can learn them. See "Adding Secure Addresses" section on page 1-9 for more information.

When you secure a port, you can also define the number of addresses that the switch can learn. The switch does not learn addresses on this port after it has reached the number you enter.

Note For information on configuration restrictions and usage guidelines, see the "port security" section on page 2-29.

Beginning in privileged EXEC mode, follow these steps to enable security on a port:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port to configure.	**interface** *interface*
Step 3	Enter the maximum number of addresses this port can learn. You can enter a number between 1 and 132.	**port security max-mac-count** *address-number*
Step 4	Enable port security, and define the action to take for an address violation.	**port security action** {**shutdown** | **trap**}
Step 5	Return to global configuration mode.	**exit**
Step 6	Enter the IP address and community string of the SNMP trap host, and enable it to receive traps.	**snmp-server host** *host-address community-string* **c2900**
Step 7	Return to privilege EXEC mode.	**end**
Step 8	Verify your entries.	**show port security** [*interface*]

Creating Fast EtherChannel or Gigabit EtherChannel Port Groups

Fast EtherChannel and Gigabit EtherChannel port groups are high-speed links. The switch considers the group to be a single port, and protocols such as STP enable and disable the group as if it were a single port. All ports in the group have the same VLAN configuration.

You can create a port group that forwards based on the source or destination address of the received packet. Source-based forwarding groups can have up to eight ports. Destination-based forwarding groups can have any number of ports.

For more information on the difference between these two methods, see the *Catalyst 2900 Series XL Installation and Configuration Guide*.

Note For information on configuration restrictions and usage guidelines, see the "port group" section on page 2-25.

Beginning in privileged EXEC mode, complete these tasks to create a two-port group:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port of the first port to be added to the group.	**interface** *interface*
Step 3	Assign the port to group 1 with destination-based forwarding.	**port group 1 distribution destination**
Step 4	Enter the second port to be added to the group.	**interface** *interface*
Step 5	Assign the port to group 1 with destination-based forwarding.	**port group 1 distribution destination**
Step 6	Return to privileged EXEC modes.	**end**
Step 7	Verify your entries.	**show running-config**

Managing the Switch Address Table

The switch uses the MAC address tables to forward traffic between ports. These MAC tables include dynamic, secure, and static addresses. The address tables list the destination MAC address and the associated VLAN ID, module, and port number associated with the address.

Each switch maintains an address table of ports that belong to the VLAN and their associated addresses. An address can be learned in more than one VLAN, and a dynamic address learned in one VLAN can be entered as a secure address in another VLAN. An address that is learned in one VLAN is unknown in another VLAN until it is entered or learned.

You can also enter addresses and their ports and VLANs in the address table. The switch supports three kinds of MAC addresses:

- *Dynamic* addresses are learned by each VLAN and dropped (aged out) when not in use.
- *Secure* addresses do not age and are retained when the switch resets. Secure addresses are always unicast addresses that are forwarded to only one port per VLAN. You can enter secure addresses, or the port can learn them.

- *Static* addresses are entered into the address table on a per-VLAN basis and accompanied by a *forwarding map*. The forwarding map describes how the switch forwards a packet destined for the static address based on the VLAN and the source port that the packet arrived on.

  When an address is statically entered in an address table for one VLAN, it must be a static address in all other VLANs. Static addresses are retained when the switch reboots.

  For more information on the switch learning capabilities, see the "Concepts" chapter of the *Catalyst 2900 Series XL Installation and Configuration Guide*.

This section describes how to use the CLI to complete the following address-table tasks:

- Displaying the contents of the address table
- Adding secure addresses
- Adding static addresses
- Defining the aging time

Displaying the Contents of the Address Table

To display the contents of the address table, enter the **show mac-address-table** command in privileged EXEC mode:

```
switch# show mac-address-table

Dynamic Addresses Count:                45
Secure Addresses (User-defined) Count: 1
Static Addresses (User-defined) Count: 0
System Self Addresses Count:            37
Total MAC addresses:                    83
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0000.0c07.ac01       Dynamic          1  FastEthernet0/16
0000.0c07.ac01       Dynamic          2  FastEthernet0/16
0000.0c07.ac01       Dynamic          3  FastEthernet0/16
0010.0b3f.ac80       Dynamic          1  FastEthernet0/5
0010.0b3f.ac85       Dynamic          1  FastEthernet0/5
0010.0de1.c9c0       Dynamic          1  FastEthernet0/3
0010.0de1.c9c3       Dynamic          1  FastEthernet0/3
0020.afd0.ea97       Dynamic          1  FastEthernet0/16
```

Adding Secure Addresses

A secure address is forwarded to one port per VLAN. Secure addresses do not age and can be either manually entered into the address table or learned.

You can enter a secure port address even when the port does not yet belong to the VLAN. When the port is later assigned to the VLAN, packets destined for that address are forwarded to the port.

Note For information on configuration restrictions and usage guidelines, see the "mac-address-table secure" section on page 2-21.

Beginning in privileged EXEC mode, follow these steps to enter a secure address:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter the MAC address, its associated port, and the VLAN ID.	**mac-address-table secure** *hw-addr interface* **vlan** *vlan-id*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry.	**show mac-address-table secure**

Adding Static Addresses

Static addresses are entered in the address table with an *in-port-list* and an *out-port-list* and, as needed, a VLAN definition. Packets received from the in-port are forwarded to ports listed in the out-port-list.

Note If the in-port and out-port-list parameters are all access ports in a single VLAN, you can omit the VLAN identification. In this case, the switch recognizes the VLAN as that associated with the in-port VLAN. Otherwise, you must supply the VLAN ID.

Note For information on configuration restrictions and usage guidelines, see the "mac-address-table static" section on page 2-22.

Beginning in privileged EXEC mode, follow these steps to enter a static address in the address table:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter the MAC address, the input port, the ports to which it can be forwarded, and the VLAN ID of those ports.	**mac-address-table static** *hw-addr in-port out-port-list* **vlan** *vlan-id*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry.	**show mac-address-table static**

Defining the Aging Time

The address table retains dynamic addresses for a configurable amount of time (the aging time). This value is valid for all dynamic addresses in all VLANs, and the default is 300 seconds. Beginning in privileged EXEC mode, complete the following tasks to define the aging time for the address table.

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter the number of seconds that dynamic addresses are to be retained in the address table. You can enter a number from 10 to 1000000.	**mac-address-table aging-time** *seconds*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry.	**show mac-address-table aging-time**

Entering Spanning-Tree Protocol Parameters

STP is enabled by default on the switch. You can use the **spanning-tree** commands to change the global and port-based STP parameters.

The following parameters are entered in global configuration mode per VLAN:

- spanning-tree
- forward-time
- hello-time
- max-age
- priority
- protocol

The following parameters are entered on a per-port, per-VLAN basis in interface configuration mode:

- cost
- port-priority
- portfast (operates on a per-port, VLAN-independent basis)

Enabling STP Port Fast

The STP Port Fast option accelerates the process of bringing a port into the forwarding state. Use this option when a port is connected to a workstation or server and cannot contribute to bridging loops.

Caution Enabling this option on a port connected to a switch or hub could prevent STP from detecting and disabling loops in your network.

Note For information on configuration restrictions and usage guidelines, see the "spanning-tree portfast" section on page 2-77.

Disable Port Fast with the **no** version of this command. Beginning in privileged EXEC mode, follow these steps to enable Port Fast option:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port to be configured.	**interface** *interface*
Step 3	Enable the Port Fast feature for the port.	**spanning-tree portfast**
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entry.	**show running-config**

Enabling CGMP Fast Leave

CGMP reduces flooding by limiting the forwarding of IP multicast and broadcast packets. The Fast Leave option reduces the amount of time required for CGMP to remove groups that are no longer active.

Beginning in privileged EXEC mode, complete these tasks to enable CGMP Fast Leave option:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable CGMP and CGMP Fast Leave.	**cgmp leave-processing**
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry.	**show running-config**

Configuring VLANs

A VLAN is an administratively defined broadcast domain. Stations can receive packets sent by other stations in the same VLAN. A VLAN enhances performance by limiting traffic; it allows the transmission of traffic among stations that belong to it and blocks traffic from stations in other VLANs. The Catalyst 2900 series switch locally supports up to 64 active VLANs with IDs from 1 to 1001.

Table 1-1 shows the VLAN features supported in this IOS software release.

Table 1-1 VLAN Features Supported by the IOS Software

Feature	IOS Release11.2(8)SA4-A	IOS Release11.2(8)SA4-EN
Assign ports for static-access VLAN membership.	Yes	Yes
Assign ports for multi-VLAN membership.	Yes	Yes
Add, modify, and delete VLANs from VLAN Trunk Protocol (VTP) database.	No	Yes
Configure VLAN trunk ports.	No	Yes
Assign ports for dynamic VLAN membership.	No	Yes
Supports Inter-Switch Link and IEEE 802.1Q VLAN tagging.	No	Yes

In the standard edition software, all ports are static-access ports and are assigned to VLAN 1 by default. Static-access ports can belong to only one VLAN; multi-VLAN ports can belong to more than one VLAN. You use the **switchport mode**, **switchport access**, and **switchport multi** commands to assign ports to VLANs. These VLANs exist without the use of the VTP database.

Using Enterprise Edition Software, you can assign ports as static-access, multi-VLAN, dynamic-access, or trunks. A dynamic-access port can belong only to one VLAN at a time. A trunk port is by default a member of every VLAN known to VTP and carries the traffic of multiple VLANs. Unlike in the standard edition software, you should use the **vlan** command to create a new VLAN (except for the default VLANs 1 and 1002 to 1005) in the VTP database. If you use the **switchport** command to add a static-access or multi-VLAN port to a VLAN, the new VLAN is automatically added to the database. However, trunk ports are not automatically added to the database using the **switchport** command.

For a dynamic-access port, you must configure a VLAN Membership Policy Server (VMPS) on another switch, such as a Catalyst 5000, to hold a database of MAC address-to-VLAN mappings. You must also use **vmps** commands to locally configure the VMPS server address. When the Catalyst 2900 series switch receives the first packet from a new host on its dynamic-access port, the switch uses the VLAN Query Protocol (VQP) to send the source MAC address to the VMPS. The VMPS provides the VLAN name to which this port must be assigned. The VLAN name must exist in the local VTP database before the dynamic-access port can be assigned to the VLAN.

Trunk ports become a member of a VLAN if the VLAN is in both the allowed list and in the VTP database. The allowed VLAN list contains the VLAN IDs that receive and transmit traffic on the trunk. By default, all possible VLANs (VLAN IDs 1-1005) are allowed in the list, but the trunk port can only transmit and receive packets on 64 of these VLANs at once. You can configure the allowed VLAN list for more control over VLAN membership of a trunk port.

This section describes how to use the CLI to complete the following VLAN tasks:

- Assigning ports for static-access VLAN membership
- Assigning ports for multi-VLAN membership
- Adding VLANs to the VTP database
- Modifying VLANs in the VTP database
- Deleting VLANs from the VTP database
- Configuring a VLAN trunk
- Assigning ports for dynamic VLAN membership

Assigning Ports for Static-Access VLAN Membership

All ports are static-access ports. A static-access port belongs to VLAN 1 by default.

Beginning in privileged EXEC mode, follow these steps to assign a port for static-access VLAN membership:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port to be added to the VLAN.	**interface** *interface*
Step 3	Enter the VLAN membership mode for static-access ports.	**switchport mode access**
Step 4	Assign the port to a VLAN.	**switchport access vlan 2**
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries.	**show interface** *interface-id* **switchport**

Assigning Ports for Multi-VLAN Membership

A multi-VLAN port belongs to more than one VLAN. The switch does not encapsulate packets on a multi-VLAN port.

Note A multi-VLAN port and trunk port cannot coexist on the same switch.

Caution To avoid loss of connectivity, do not connect multi-VLAN ports to hubs or switches. Connect multi-VLAN ports to routers or servers.

Note For information on configuration restrictions and usage guidelines, see the "switchport multi" section on page 2-87.

Beginning in privileged EXEC mode, follow these steps to assign ports for multi-VLAN membership:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port to be added to the VLAN.	**interface** *interface*
Step 3	Enter the VLAN membership mode for multi-VLAN ports.	**switchport mode multi**
Step 4	Assign the port to more than one VLAN. Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.	**switchport multi vlan add** *vlan-list*
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries.	**show interface** *interface-id* **switchport**

Configuring VLAN Trunk Protocol

VTP is a Layer-2 messaging protocol that maintains VLAN configuration consistency throughout the network. VTP manages the addition, deletion, and modification of VLANs network-wide by allowing each device to send advertisements on its trunk ports. These advertisements include the VTP management domain of the device, its configuration revision number, the VLANs it received advertisements about, and certain VLAN parameters. By receiving these advertisements, all devices in the same management domain learn about new VLANs now configured in the transmitting device. These advertisements automatically communicate the changes you make to all the other switches in the network.

VTP minimizes configuration inconsistencies that can arise when changes are made. These inconsistencies can result in security violations because VLANs cross-connect when duplicate names are used and internally disconnect when VLANs are incorrectly mapped between one LAN type and another.

Note This feature is available only in the Enterprise Edition Software. For more information, see the *Catalyst 2900 Series XL Enterprise Edition Software Configuration Guide*.

Beginning in privileged EXEC mode, follow these steps to configure VTP:

Task		Command
Step 1	Enter VLAN database mode.	**vlan database**
Step 2	Enter a unique VTP domain name, and optionally enter a password. The domain name can be from 1 to 32 characters; the password can be from 8 to 64 characters. Both are case sensitive. Passwords should match on all switches in the same domain.	**vtp domain** *domain-name* **password** *password-value*
Step 3	Enable the switch to run in server mode.	**vtp server**
Step 4	Enable the VTP administrative domain to operate with VTP version 2. To use V2 mode, all VTP switches in the network must support version 2; otherwise, you must configure them to operate in VTP V2-mode disabled.	**vtp v2-mode**
Step 5	Enable VTP pruning globally in the administrative domain. Pruning restricts flooded traffic to those trunk links that the traffic must use to access ports assigned to those VLANs. For Catalyst 2900 series switches, no VLANs are pruning eligible on the trunk ports.	**vtp pruning**
Step 6	Return to privileged EXEC mode.	**exit**
Step 7	Enter global configuration mode.	**configure terminal**
Step 8	Enable SNMP VTP trap notification if you want to receive these traps.	**snmp-server enable traps vtp**
Step 9	Enter the IP address and community string of the SNMP trap host, and enter it to receive VTP traps.	**snmp-server host** *host-address community-string* **vtp**
Step 10	Return to privileged EXEC mode.	**end**
Step 11	Verify your entries.	**show vtp status**

Adding VLANs to the Database

The VLAN database includes VLAN 1 and 1002 through 1005 by default. You can add VLAN configurations to the database by entering the VLAN database configuration mode.

Note This feature is available only in the Enterprise Edition Software. For more information, see the *Catalyst 2900 Series XL Enterprise Edition Software Configuration Guide*.

Beginning in privileged EXEC mode, follow these steps to add Ethernet VLANs to the database:

Task		Command
Step 1	Enter VLAN database mode.	**vlan database**
Step 2	Add an Ethernet VLAN with default media characteristics. The default *vlan-name* is "VLANxxxx," where "xxxx" represents four numeric digits (including leading zeroes) equal to the VLAN ID number.	**vlan** *vlan-id* **name** *vlan-name*
Step 3	Add an Ethernet VLAN with a specific MTU size.	**vlan** *vlan-id* **name** *vlan-name* **mtu** *mtu-size*
Step 4	Add an Ethernet VLAN in a suspended state.	**vlan** *vlan-id* **name** *vlan-name* **state** *suspend*
Step 5	Implement the proposed new database, propagate it throughout the administrative domain, and return to privileged EXEC mode.	**exit**
Step 6	Verify your entries.	**show vlan id** *vlan-id*

Modifying VLANs in the Database

You can modify VLAN characteristics in the database.

Note This feature is available only in the Enterprise Edition Software. For more information, see the *Catalyst 2900 Series XL Enterprise Edition Software Configuration Guide*.

Beginning in privileged EXEC mode, follow these steps to modify an existing Ethernet VLAN in the database:

Task		Command
Step 1	Enter VLAN database mode.	**vlan database**
Step 2	Modify an existing Ethernet VLAN by changing its MTU size and SAID value.	**vlan** *vlan-id* **mtu** *mtu-size* **said** *said-value*
Step 3	Implement the proposed new database, propagate it throughout the administrative domain, and return to privileged EXEC mode.	**exit**
Step 4	Verify your entries.	**show vlan id** *vlan-id*

Deleting VLANs from the Database

You can remove VLANs from the database. However, you cannot delete VLAN 1 or 1002 to 1005.

Note This feature is available only in the Enterprise Edition Software. For more information, see the *Catalyst 2900 Series XL Enterprise Edition Software Configuration Guide*.

Beginning in privileged EXEC mode, follow these steps to remove an Ethernet VLAN from the database:

Task		Command
Step 1	Enter VLAN database mode.	**vlan database**
Step 2	Remove an existing VLAN by its VLAN ID.	**no vlan** *vlan-id*
Step 3	Implement the proposed new database, propagate it throughout the administrative domain, and return to privileged EXEC mode.	**exit**
Step 4	Verify your entries.	**show vlan brief**

Configuring a VLAN Trunk

A trunk is a point-to-point link between two switches or between a switch and a router. Trunks carry the traffic of multiple VLANs and allow you to extend VLANs from one switch to another. On a trunk port, the switch encapsulates all packets to identify (or tag) the VLAN to which the traffic belongs.

By default, a Catalyst 2900 series trunk port is a member of all active Ethernet VLANs up to 64 VLANs. You can further control the VLAN membership of a trunk port by modifying the allowed list to restrict the traffic a trunk carries. This list of allowed VLANs does not affect any port but the trunk port associated with it.

Note This feature is available only in the Enterprise Edition Software. For more information, see the *Catalyst 2900 Series XL Enterprise Edition Software Configuration Guide*.

Note Trunk ports and multi-VLAN ports cannot coexist on the same switch. For information on configuration restrictions and usage guidelines, see the“switchport mode” section on page 2-85 and the “switchport trunk encapsulation” section on page 2-91.

Beginning in privileged EXEC mode, follow these steps to configure a VLAN trunk:

Task		Command
Step 1	Add a VLAN to the database.	See “Adding VLANs to the Database” section on page 1-16.
Step 2	Enter global configuration mode.	**configure terminal**
Step 3	Enter interface configuration mode, and enter the port to be added to the VLAN.	**interface** *interface*
Step 4	Enter the VLAN membership mode for trunk ports.	**switchport mode trunk**

Step 5	Enter the encapsulation format on the trunk port.	**switchport trunk encapsulation** {**isl** | **dot1q**}
Step 6	Restrict the list of VLANs enabled to receive and transmit traffic on the trunk. By default, VLANs 1 through 1005 are included in the allowed list. Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.	**switchport trunk allowed vlan remove** *vlan-list*
Step 7	For 802.1Q trunks, enter the native VLAN for untagged traffic.	**switchport trunk native vlan** *vlan-id*
Step 8	Return to privileged EXEC mode.	**end**
Step 9	Verify your entries.	**show interface** *interface-id* **switchport**

Assigning Ports for Dynamic VLAN Membership

By assigning ports to dynamic VLAN membership, you can move a connection from a port on one switch to a port on another switch in the network without reconfiguring the port. Before configuring dynamic-access ports, you must configure a VLAN Membership Policy Server (VMPS), such as the Catalyst 5000 switch, so that it is active and accessible by the Catalyst 2900 series switches.

A dynamic-access port can only belong to only one VLAN at a time.

Caution Dynamic-access ports are designed to work with end stations. Loss of connectivity can occur if you connect dynamic-access ports to switches or routers running bridging protocols.

Note This feature is available only in the Enterprise Edition Software. For more information, see the *Catalyst 2900 Series XL Enterprise Edition Software Configuration Guide*.

Note For information on configuration restrictions and usage guidelines, see the "switchport access" section on page 2-83.

Beginning in privileged EXEC mode, follow these steps to configure dynamic VLAN membership:

Task		Command
Step 1	Add a VLAN to the database.	See "Adding VLANs to the Database" section on page 1-16.
Step 2	Enter global configuration mode.	**configure terminal**
Step 3	Enter the primary VMPS IP address to be queried.	**vmps server** *ipaddress* **primary**
Step 4	Enter the secondary VMPS IP addresses that the switch queries if no responses are received from the primary VMPS.	**vmps server** *ipaddress*
Step 5	Enter the interface configuration mode, and enter the port to be added to the VLAN.	**interface** *interface*
Step 6	Enter the VLAN membership mode for static-access ports.	**switchport mode access**
Step 7	Configure the port to be a dynamic-access port.	**switchport access vlan dynamic**
Step 8	Return to global configuration mode.	**exit**

Task		Command
Step 9	Enable SNMP VMPS trap notification, if you want to receive these traps.	**snmp-server enable traps vlan-membership**
Step 10	Enter the IP address and community string of the SNMP trap host, and enable it to receive VMPS traps.	**snmp-server host** *host-address community-string* **vlan-membership**
Step 11	Return to privileged EXEC mode.	**end**
Step 12	Verify your entries.	**show vmps** **show interface** *interface* **switchport**