CHAPTER 6

VLANs and Trunking

See the following sections for configuration information about these topics:

- **6-1: VLAN Configuration**—Describes the method for configuring, creating, and configuring VLANs on a switch.
- **6-2: VLAN Port Membership**—Explains how to assign a port to a VLAN using static or dynamic methods.
- **6-3: Trunking**—Covers the method for extending a VLAN beyond the boundaries of a single switch through tagging mechanisms.
- **6-4: VLAN Trunking Protocol**—Describes the Cisco proprietary protocol for maintaining a forwarding path between switches that are trunking and how to prune for unused VLANs.
- **6-5: GVRP**—Explains the industry standard process management of traffic across trunk links and how to maintain VLANs on switches for forwarding purposes.
- **6-6: Private VLANs**—Explains the feature that allows for more granular traffic control within the VLAN using the private VLAN structure.

6-1: VLAN Configuration

- *VLANs* are broadcast domains defined within switches to allow control of broadcast, multicast, unicast, and unknown unicast within a Layer 2 device.
- VLANs are defined on a switch in an internal database known as the *VLAN Trunking Protocol* (VTP) *database*. After a VLAN has been created, ports are assigned to the VLAN.
- VLANs are assigned numbers for identification within and between switches. Cisco switches have two ranges of VLANs, the *normal range* and *extended range*.
- VLANs have a variety of configurable parameters, including name, type, and state.
- Several VLANs are reserved, and some can be used for internal purposes within the switch.

Creation of an Ethernet VLAN

VLANs are created on Layer 2 switches to control broadcasts and enforce the use of a Layer 3 device for communications. Each VLAN is created in the local switch's database for use. If a VLAN is not known to a switch, that switch cannot transfer traffic across any of its ports for that VLAN. VLANs are created by number, and there are two ranges of usable VLAN numbers (normal range 1–1000 and extended range 1025–4096). When a VLAN is created, you can also give it certain attributes such as a VLAN name, VLAN type, and its operational state. To create a VLAN, use the following steps.

1 Configure VTP.

VTP is a protocol used by Cisco switches to maintain a consistent database between switches for trunking purposes. VTP is not required to create VLANs; however, Cisco has set it up to act as a conduit for VLAN configuration between switches as a default to make administration of VLANs easier. Because of this, you must first either configure VTP with a domain name or disable VTP on the switch. VTP is explained in detail in section "6-4: VLAN Trunking Protocol."

NOTE For Catalyst 4000 and 6000 switches running IOS Supervisor 12.1(8a) or above (native IOS), you can configure the VTP parameters in global configuration mode as well.

— Specify a VTP name:

COS	**`set vtp domain`** *`domain-name`*
IOS	`(vlan)` **`vtp domain`** *`domain-name`* -OR- `(global)` **`vtp domain`** *`domain-name`*

By default, the VTP is in server mode and must be configured with a domain name before any VLANs can be created. These commands specify the VTP domain name. For IOS switches, you enter vlan database mode, **(vlan)**, by entering the command **vlan database**, at the privileged-level prompt.

NOTE The global configuration command **vtp domain** is not available on all switches that run IOS.

-OR-

— Disable VTP synchronization:

COS	**`set vtp mode transparent`**
IOS	`(vlan)` **`vtp transparent`** -OR- `(global)` **`vtp mode transparent`**

Another option is to disable VTP synchronization of the databases. Disabling it enables you to manage your local VTP database without configuring and relying on VTP. For Catalyst 4000 and 6000 switches running IOS Supervisor 12.1(8a) or above (native IOS), you can configure the VTP parameters in global configuration mode as well.

NOTE The global configuration command **vtp mode transparent** is not available on all switches that run IOS.

-OR-

— Disable VTP:

COS	**`set vtp mode off`**
IOS	N/A

With the introduction of COS version 7.1.1, an option now exists to disable VTP completely. Use the command **set vtp mode off** to turn off VTP. After doing so, you can administer the local VTP database.

2 Create the VLAN.

VLANs are created by number. The two ranges of VLANs are as follows:

— The standard range consists of VLANs 1 to 1000.

— The extended range consists of VLANs 1025 to 4096.

Extended VLANs are currently supported only on switches running COS software version 6.1 or greater. When you create a VLAN, you have many options to consider. Many options are valid only for FDDI and Token Ring VLANs. Some of the items configured deal with options, such as private VLANs, which are discussed in other sections in this book. VLANs are created using the **set vlan** command for COS devices or with the **vlan** command in vlan database mode for IOS switches. For Ethernet VLANs, you can also configure the standard parameters in Table 6-1.

Table 6-1 *Configurable VLAN Parameters*

Parameter	Description
name	A description of the VLAN up to 32 characters. If none is given, it defaults to VLAN00XXX, where xxx is the VLAN number.
mtu	The maximum transmission unit (packet size, in bytes) that the VLAN can use; valid values are from **576** to **18190**. The MTU can extend up to 1500 for Ethernet, but beyond for Token Ring or FDDI. The default is **1500**.
state	Used to specify whether the state of the VLAN is active or suspended. All ports in a suspended VLAN will be suspended and not allowed to forward traffic. The default state is **active**.

NOTE Many other options are available during the VLAN configuration command; however, most of these deal with the configuration of FDDI and Token Ring VLANs. Because these are not widely used topologies, the options and descriptions of Token Ring and FDDI VLAN configuration and parameters have not been included in this book. For information on Token Ring or FDDI VLANs, refer to www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_6_3/config/vlans.htm.

a. Create a VLAN in the standard range:

COS	`set vlan vlan-id [name name] [state state] [mtu mtu]`
IOS	`(vlan) vlan vlan-id [name vlan-name] [state {suspend	active}] [mtu mtu-size]` `(global) vlan vlan-id` `(vlan-config) vlan vlan-id [mtu mtu-size] [name vlan-name] [state {suspend	active}]`

The **vlan-id** specifies the VLAN by number. For COS you can specify a range of VLANs in the *vlan-id* section; you cannot configure the name for a range of VLANs, however, because each VLAN is to have a unique name. For IOS switches, VLANs are created in vlan database mode. For Catalyst 6000 and 4000 switches running Supervisor IOS 12.1(8a) and above, you can create VLANs in global configuration mode if the switch is in VTP transparent mode. To do this, enter the **vlan** *vlan-id* command to move to vlan-config mode. From vlan-config mode, you can manage the parameters of the VLANs.

NOTE You cannot modify any of the parameters for VLAN 1.

b. Create a VLAN in the extended range.

Extended VLANs support VLANs up to 4096 in accordance with the 802.1Q standard. Currently only switches running COS 6.1 or greater can support creation and assignment of VLANs in the extended range. You cannot currently use VTP to manage VLANs in the extended range, and these VLANs cannot be passed over an *Inter-Switch Link* (ISL) trunk link.

1 Enable spanning-tree MAC reduction:

COS	**`set spantree macreduction enable`**
IOS	N/A

To allow these switches to use the extended range, you must first enable **spanningtree macreduction** to allow the switch to support a large number of spanning-tree instances with a very limited number of MAC addresses and still maintain the IEEE 802.1D bridge ID requirement for each STP instance.

NOTE After you have created a VLAN in the extended range, you cannot disable this feature unless you first delete the VLAN.

2 Create a VLAN in the extended range:

COS	**set vlan** *vlan-id* [**name** *name*] [**state** *state*] [**mtu** *mtu*]
IOS	N/A

Here the *vlan-id* would be a number from 1025 to 4096. Numbers 1001 to 1024 are reserved by Cisco and cannot be configured.

CAUTION For Catalyst 6000 series switches with FlexWAN cards, the system identifies these ports internally with VLAN numbers starting with 1025. If you have any FlexWAN modules, be sure to reserve enough VLAN numbers (starting with VLAN 1025) for all the FlexWAN ports you want to install. You cannot use these extended VLANs if you install FlexWAN ports.

Feature Example

In this example, the switches Access_1 and Distribution_1 are going to be configured with VLANs 5, 8, and 10 with the names Cameron, Logan, and Katie, respectively. Also the distribution switch will be configured with VLAN 2112 with the name Rush.

An example of the Catalyst OS configuration for Distribution 1 follows:

```
Distribution_1 (enable)>set vtp mode transparent
Distribution_1 (enable)>set vlan 5 name Cameron
Distribution_1 (enable)>set vlan 8 name Logan
Distribution_1 (enable)>set vlan 10 name Katie
Distribution_1 (enable)>set spantree macreduction enable
Distribution_1 (enable)>set vlan 2112 name Rush
Distribution_1 (enable)>
```

An example of the Supervisor IOS configuration for Distribution 1 follows:

```
Distribution_1#vlan database
Distribution_1(vlan)#vtp transparent
Distribution_1(vlan)#exit
Distribution_1#conf t
Distribution_1(config)#vlan 5
Distribution_1(config-vlan)# name Cameron
Distribution_1(config-vlan)#vlan 8
Distribution_1(config-vlan)# name Logan
Distribution_1(config-vlan)# vlan 10
Distribution_1(config-vlan)# name Katie
Distribution_1(config-vlan)# end
Distribution_1 #copy running-config startup-config
```

NOTE For the Supervisor IOS, extended VLANs such as 2112 are not supported.

An example of the Layer 2 IOS configuration for Access 1 follows:

```
Access_1#vlan database
Access_1 (vlan)#vtp transparent
Access_1 (vlan)#vlan 5 name Cameron
Access_1 (vlan)#vlan 8 name Logan
Access_1 (vlan)#vlan 10 name Katie
Access_1 (vlan)#exit
Access_1#copy running-config startup-config
```

6-2: VLAN Port Assignments

- VLANs are assigned to individual switch ports.
- Ports can be statically assigned to a single VLAN or dynamically assigned to a single VLAN.
- All ports are assigned to VLAN 1 by default

- Ports are active only if they are assigned to VLANs that exist on the switch.
- Static port assignments are performed by the administrator and do not change unless modified by the administrator, whether the VLAN exists on the switch or not.
- Dynamic VLANs are assigned to a port based on the MAC address of the device plugged into a port.
- Dynamic VLAN configuration requires a *VLAN Membership Policy Server* (VMPS) client, server, and database to operate properly.

Configuring Static VLANs

On a Cisco switch, ports are assigned to a single VLAN. These ports are referred to as *access ports* and provide a connection for end users or node devices, such as a router or server. By default all devices are assigned to VLAN 1, known as the *default VLAN*. After creating a VLAN, you can manually assign a port to that VLAN and it will be able to communicate only with or through other devices in the VLAN. Configure the switch port for membership in a given VLAN as follows:

1 Statically assign a VLAN:

COS	**`set vlan`** *`number mod/port`*
IOS	`(global)` **`interface`** *`type mod/port`* `(interface)` **`switchport access vlan`** *`number`*

To change the VLAN for a COS device, use the **set vlan** command, followed by the VLAN *number*, and then the port or ports that should be added to that VLAN. VLAN assignments such as this are considered static because they do not change unless the administrator changes the VLAN configuration.

For the IOS device, you must first select the port (or port range for integrated IOS) and then use the **switchport access vlan** command followed by the VLAN *number*.

CAUTION If the VLAN that the port is assigned to does not exist in the database, the port is disabled until the VLAN is created.

Configuring Dynamic VLANs

Although static VLANs are the most common form of port VLAN assignments, it is possible to have the switch dynamically choose a VLAN based on the MAC address of the device connected to a port. To achieve this, you must have a VTP database file, a VTP server, a

VTP client switch, and a dynamic port. After you have properly configured these components, a dynamic port can choose the VLAN based on whichever device is connected to that port. Use the following steps to configure dynamic VLANs:

1 Create a VTP database file.

Using a text editor, such as WordPad or vi, create a VTP database file and place it on a VMPS or *Remote Copy Protocol* (RCP) server. The VTP database file contains the following elements:

— A header that includes a VMPS domain name

— The VMPS operational mode

— The fallback VLAN name

— A list of MAC address mapped to VLAN names

The basic outline of a VMPS database file is as follows:

```
vmps domain Switchblock1
vmps mode open
vmps fallback default
vmps no-domain-req deny
!
vmps-mac-addrs
!
!
address 0001.0387.0943 vlan-name GroupA
address 0050.0491.F950 vlan-name GroupB
address 0050.DA8F.1134 vlan-name GroupC
```

The very first thing that should be in the VTP database file are the letters **vmps** followed by the word **domain** and a domain name. The domain name matches that of the VTP domain name of the switch(es) sending the VMPS request. (VTP is discussed further in section "6-4: VLAN Trunking Protocol.") This name is used in the request for VMPS mapping information. The next three lines in the file are information about how VMPS should operate. The **mode open** indicates whether a request comes in that is not in the MAC address list. The switch should place that device in a default VLAN. The next line specifies that VLAN by name. The name **default** is that of VLAN 1. You can also configure the mode as **closed**; if this is the case, the port will be suspended if the device is not in the MAC address table. The **no-domain-req deny** option states that any device that sends a request with no domain name should not be given any port VLAN mapping information. Each **!** (exclamation point) is a comment and is ignored by the VMPS server.

The **vmps-mac-addrs** entry indicates the start of the MAC address to VLAN mapping. The entries are entered with the format **address** *address* **vlan-name** *vlan_name*, where the address is in dotted-hexadecimal format and the VLAN name is the exact name (including case) as found in the VLAN database of the requesting switch. When a request is sent, this mapping is returned to the requesting switch. The VLAN assignment is based on the name returned. If the name is not found on the local switch, the assignment is not made.

2 Configure the VMPS server.

a. *(Optional)* Set the VMPS download method:

COS	**set vmps downloadmethod** {**rcp** | **tftp**}
IOS	N/A

Specify how to download the VMPS database file using **rcp** or **tftp**. If you do not choose a method, the default is **tftp**.

b. Set the VMPS download server and filename:

COS	**set vmps downloadserver** *ipaddress* [*filename*]
IOS	N/A

Configure the IP address of the RCP or TFTP server and specify the *filename* of the VMPS database.

c. Enable the VMPS server service:

COS	**set vmps state enable**
IOS	N/A

When you enable the VMPS server service, it will read the file from the server into the memory of the switch and will then be able to respond to request from the VMPS client switches. Use the commands **show vmps**, **show vmps mac**, **show vmps vlan**, and **show vmps statistics** to verify the operation of the VMPS server.

NOTE After the VMPS server service has been enabled and the VMPS information loaded into the memory of the server, the VMPS database file is no longer referenced. If you make changes to the VMPS database file, you must either disable and reenable the server service or reload the file with the command **download vmps**.

3 Configure the VMPS client:

COS	**set vmps server** *ipaddress* [**primary**]
IOS	**(global) vmps server** *ipaddress* **primary**

Any switch that will have dynamic ports is considered a VMPS client. For this switch to request the dynamic VLAN information from the server, you must configure the client with the server address. Use the primary option to specify the IP address of the main VMPS server. You can also specify up to three other IP addresses for VMPS servers. Use the command **show vmps server** for COS and **show vmps** on IOS devices to confirm the server configuration.

NOTE If the a switch is configured as a VMPS server and it will also have dynamic ports, it must also be configured as a client using Step 3 and pointing to its own IP address as server.

4 Configure the port for dynamic VLAN assignments:

COS	`set port membership` *`mod/port`* `dynamic`
IOS	`(interface)` **`switchport access dynamic`**

This places the port in dynamic VLAN mode. The switch must first be configured as a client (Step 3) before you configure a port as dynamic. After this has been configured, the port is assigned to the local switch's VLAN that has a name that matches the one mapped to the MAC address of the attached device in the VMPS database.

Verifying VLAN Assignments

After configuring a port for VLAN assignments, use one of the following commands to verify the VLAN port assignments:

COS	**`show port`**
IOS	`(privileged)` **`show interface`** *`type mod/port`* **`switchport`** -OR- `(privileged)`**`show interface status`**

NOTE The command **show interface status** is not available on all switches that run IOS.

Feature Example

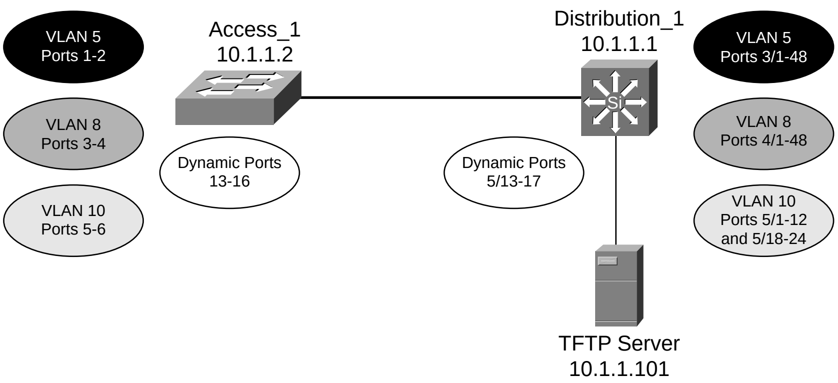
In this example, ports for the switches Access_1 and Distribution_1 are assigned as follows:

- Static assignments for ports 1 and 2 on the access switch and 3/1–48 on the distribution switch into VLAN 5
- Static assignments for ports 3 and 4 on the access switch and 4/1–48 on the distribution switch into VLAN 8
- Static assignments for ports 5 and 6 on the access switch and 5/1–12 and 5/18–24 on the distribution switch into VLAN 10

Distribution_1 will be assigned the IP address 10.1.1.1 and will serve as a VMPS server and get a file called *vmpsconfig.txt* (shown at the end of the example) from the server 10.1.1.101.

Ports 13–16 will be dynamic on the access switch, and ports 5/13-17 will be dynamic on the Distribution_1 server. Figure 6-1 shows the connections and assignments associated with this example.

Figure 6-1 *VLAN Port Assignments on Access_1 and Distribution_1*



An example of the Catalyst OS configuration for Distribution_1 follows:

```
Distribution_1 (enable)>set vlan 5 3/1-48
Distribution_1 (enable)>set vlan 8 4/1-48
Distribution_1 (enable)>set vlan 10 5/1-12,5/18-24
Distribution_1 (enable)>set vmps downloadserver 10.1.1.101 vmpsconfig.txt
Distribution_1 (enable)>set int sc0 10.1.1.1/24
Distribution_1 (enable)>set vmps enable
Distribution_1 (enable)>set vmps server 10.1.1.1
Distribution_1 (enable)> set port membership 5/13-17 dynamic
```

An example of the Supervisor IOS configuration for Distribution_1 follows:

```
Distribution_1(config)#interface range fastethernet 3/1 - 48
Distribution_1(config-if)#switchport
Distribution_1(config-if)#switchport mode access
Distribution_1(config-if)#switchport access vlan 5
Distribution_1(config-if)#no shut
Distribution_1(config)#interface range fastethernet 2/1 - 48
Distribution_1(config-if)#switchport
Distribution_1(config-if)#switchport mode access
Distribution_1(config-if)#switchport access vlan 8
Distribution_1(config-if)#no shut
Distribution_1(config)#interface range fastethernet 5/1 - 12 , 5/18 - 24
Distribution_1(config-if)#switchport
Distribution_1(config-if)#switchport mode access
Distribution_1(config-if)#switchport access vlan 10
Distribution_1(config-if)#no shut
Distribution_1(config-if)# end
Distribution_1 #copy running-config startup-config
```

NOTE For the Supervisor IOS running on a Catalyst 6000 or Catalyst 4000, dynamic VLAN services are currently not supported. These switches cannot be configured with dynamic access ports or to act as a VMPS server.

An example of the Layer 2 IOS configuration for Access_1 follows:

```
Access_1(config)#interface fastethernet 0/1
Access_1(config-if)#switchport access vlan 5
Access_1(config-if)#interface fastethernet 0/2
Access_1(config-if)#switchport access vlan 5
Access_1(config-if)#interface fastethernet 0/3
Access_1(config-if)#switchport access vlan 8
Access_1(config-if)#interface fastethernet 0/4
Access_1(config-if)#switchport access vlan 8
Access_1(config-if)#interface VLAN 1
Access_1(config-if)#ip address 10.1.1.2 255.255.255.0
Access_1(config-if)#vmps server 10.1.1.1
Access_1(config)#interface fastethernet 0/5
Access_1(config-if)#switchport access dynamic
Access_1(config-if)#interface fastethernet 0/6
Access_1(config-if)#switchport access vlan dynamic
Access_1(config-if)# end
Access_1 #copy running-config startup-config
```

An example of the VMPS database file *vmpsconfig.txt* follows:

```
vmps domain Switchblock1
vmps mode open
vmps fallback default
vmps no-domain-req allow
!
vmps-mac-addrs
!
!
address 0001.0387.0943 vlan-name Katie
address 0050.0491.F950 vlan-name Logan
address 0050.DA8F.1134 vlan-name Cameron
```

6-3: Trunking

- VLANs are local to each switch's database, and VLAN information is not passed between switches.
- Trunk links provide VLAN identification for frames traveling between switches.
- Cisco switches have two Ethernet trunking mechanisms: ISL and IEEE 802.1Q.
- Certain types of switches can negotiate trunk links.
- Trunks carry traffic from all VLANs to and from the switch by default but can be configured to carry only specified VLAN traffic.
- Trunk links must be configured to allow trunking on each end of the link.

Enabling Trunking

Trunk links are required to pass VLAN information between switches. A port on a Cisco switch is either an access port or a trunk port. Access ports belong to a single VLAN and do not provide any identifying marks on the frames that are passed between switches. Access ports also carry traffic that comes from only the VLAN assigned to the port. A trunk port is by default a member of *all* the VLANs that exist on the switch and carry traffic for all those VLANs between the switches. To distinguish between the traffic flows, a trunk port must mark the frames with special tags as they pass between the switches. Trunking is a function that must be enabled on both sides of a link. If two switches are connected together, for example, both switch ports must be configured for trunking, and they must both be configured with the same tagging mechanism (ISL or 802.1Q).

To enable trunking between the switches, use the following steps:

1 Enable trunking on a port.

a. Enable the trunk:

COS	**set trunk** *mod/port* [**auto** | **desirable** | **on** | **nonegotiate** | **off**]
IOS	(global) **interface** *type mod/port* (interface) **switchport mode dynamic [auto** | **desirable]** (interface) **switchport mode trunk** (interface) **switchport nonegotiate**

The most basic way to configure a trunk link is using the option **on**. This option enables the trunk and requires that you also specify a tagging mechanism for the trunk. For IOS devices, the command **switchport mode trunk** is equivalent to the **set trunk** *mod/port* **on** command. When specifying the option **on**, you must also choose a tagging mechanism (see Step 1b).

NOTE Some IOS switches do not support Dynamic Trunking Protocol. For these switches, the only command that you can use to configure trunking is **switchport mode trunk**, which essentially turns trunking on.

Many Cisco switches employ an automatic trunking mechanism known as the *Dynamic Trunking Protocol* (DTP), which allows a trunk to be dynamically established between two switches. All COS switches and integrated IOS switches can use the DTP protocol to form a trunk link. The COS options **auto**, **desirable**, and **on** and the IOS options of **dynamic auto**, **dynamic desirable**, and **trunk** configure a trunk link using DTP. If one side of the link is configured to trunk and will send DTP signals, the other side of the link will dynamically begin to trunk if the options match correctly.

If you want to enable trunking and not send any DTP signaling, use the option **nonegotiate** for switches that support that function. If you want to disable trunking completely, use the **off** option for a COS switch or the **no switchport mode trunk** command on an IOS switch.

Table 6-2 shows the DTP signaling and the characteristics of each mode.

TIP It is important to remember that not all switches support DTP and might not establish a trunk without intervention. Also remember that DTP offers no benefit when you are trunking with a non-Cisco switch. To eliminate any overhead associated with DTP, it is useful to use the **nonegotiate** option when DTP is not supported.

NOTE When enabling trunking, it is not possible to specify a range of ports.

Table 6-2 *Trunking Mode Characteristics*

Trunking Mode	Characteristics
COS = **on** IOS = **mode trunk**	Trunking is on for these links. They will also send DTP signals that attempt to initiate a trunk with the other side. This will form a trunk with other ports in the states **on**, **auto**, or **desirable** that are running DTP. A port that is in **on** mode always tags frames sent out the port.

Table 6-2 *Trunking Mode Characteristics (Continued)*

Trunking Mode	Characteristics
COS = **desirable** IOS = **mode dynamic desirable**	These links would like to become trunk links and will send DTP signals that attempt to initiate a trunk. They will only become trunk links if the other side responds to the DTP signal. This will form a trunk with other ports in the states **on**, **auto**, or **desirable** that are running DTP. This is the default mode for the 6000 running Supervisor IOS.
COS = **auto** IOS = **mode dynamic auto**	These links will only become trunk links if they receive a DTP signal from a link that is already trunking or desires to trunk. This will only form a trunk with other ports in the states **on** or **desirable**. This is the default mode for COS switches.
COS = **nonegotiate** IOS = **mode nonegotiate**	Sets trunking on and disables DTP. These will only become trunks with ports in **on** or **nonegotiate** mode.
COS = **off** IOS = **no switchport mode trunk**	This option sets trunking and DTP capabilities off. This is the recommended setting for any access port because it will prevent any dynamic establishments of trunk links.

NOTE Cisco 2950 and 3500XL switches do not support DTP and are always in a mode similar to **nonegotiate**. If you turn trunking on for one of these devices, it will not negotiate with the other end of the link and requires that the other link be configured to **on** or **nonegotiate**.

b. Specify the encapsulation method:

COS	`set trunk mod/port [negotiate	isl	dot1Q]`
IOS	`(global) interface type mod/port` `(interface) switchport trunk encapsulation [negotiate	isl	dot1Q]`

The other option when choosing a trunk link is the encapsulation method. For Layer 2 IOS switches, such as the 2900XL or the 3500XL, the default encapsulation method is **isl**. You can change from the default with the **switchport trunk encapsulation** command. For COS switches or integrated IOS switches, the default encapsulation is **negotiate**. This method signals between the trunked ports to choose an encapsulation method. (ISL is preferred over 802.1Q.) The **negotiate** option is valid for **auto** or **desirable** trunking modes only. If you choose **on** as the mode or if you want to force a particular method or if the other side of the trunk cannot negotiate the trunking type, you must choose the option **isl** or **dot1Q** to specify the encapsulation method.

NOTE Not all switches allow you to negotiate a trunk encapsulation setting. The 2900XL and 3500XL trunks default to **isl** and you must use the **switchport trunk encapsulation** command to change the encapsulation type. The 2950 and some 4000 switches support only 802.1Q trunking and provide no options for changing the trunk type.

c. *(Optional)* Specify the native VLAN:

COS	`set vlan` *number mod/port*
IOS	(global) **interface** *type mod/port* (interface) **switchport trunk native vlan** *number*

For switches running 802.1Q as the trunking mechanism, the native VLAN of each port on the trunk must match. By default all COS ports are in VLAN 1; and the native VLAN on the IOS devices is also configured for VLAN 1, so the native VLAN does match. If you choose to change the native VLAN, use the **set vlan** command for COS switches or the **switchport trunk native vlan** command for IOS switches to specify the native VLAN. Remember that the native VLAN *must* match on both sides of the trunk link for 802.1Q; otherwise the link will not work. If there is a native VLAN mismatch, *Spanning Tree Protocol* (STP) places the port in a *port VLAN ID* (PVID) inconsistent state and will not forward on the link.

NOTE *Cisco Discovery Protocol* (CDP) version 2 passes native VLAN information between Cisco switches. If you have a native VLAN mismatch, you will see CDP error messages on the console output.

Specifying VLANs to Trunk

By default a trunk link carries all the VLANs that exist on the switch. This is because all VLANs are active on a trunk link; and as long as the VLAN is in the switch's local database, traffic for that VLAN is carried across the trunks. You can elect to selectively remove and add VLANs from a trunk link. To specify which VLANs are to be added or removed from a trunk link, use the following commands.

1 *(Optional)* Manually remove VLANs from a trunk link:

COS	**clear trunk** *mod/port vlanlist*
IOS	(global) **interface** *type mod/port* (interface) **switchport trunk allowed vlan remove** *vlanlist*

By specifying VLANs in the *vlanlist* field of this command, the VLANs will not be allowed to travel across the trunk link until they are added back to the trunk using the command **set trunk** *mod/port vlanlist* or **switchport trunk allowed vlan add** *vlanlist*.

Verifying Trunks

After configuring a port for trunking, use one of the following commands to verify the VLAN port assignments:

COS	**show trunk** [*mod*] [*mod/port*]
IOS	(privileged) **show interface** *type mod/port* **switchport** -OR- **show interfaces trunk** -OR- **show interface** [*mod*] [*interface_id*] **trunk**

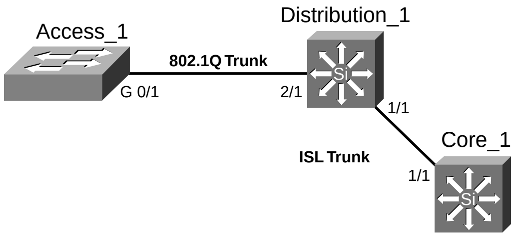
Section 6-3

NOTE The commands **show interfaces trunk** and **show interface** [*mod*] [*interface_id*] **trunk** are not available on all switches that run IOS.

Feature Example

In this example the switches Access_1 and Distribution_1 and Core_1 are connected as shown in Figure 6-2. 802.1Q trunking is configured in the on mode between Access_1 and Distribution_1 switches. ISL is configured in desirable mode on the Distribution_1 switch to the link connecting to the core. The core is configured for autotrunking mode and encapsulation negotiate. The trunk connected between the access switch is configured to only trunk for VLANs 5, 8, and 10. The trunk between the Distribution_1 and Core_1 is configured to carry only VLAN 1 and VLAN 10.

Figure 6-2 *Network Diagram for Trunk Configuration on Access_1, Distribution_1, and Core_1*



An example of the Catalyst OS configuration for Distribution_1 follows:

```
Distribution_1 (enable)>clear trunk 1/1 2-1001
Distribution_1 (enable)>set trunk 1/1 desirable isl 10
Distribution_1 (enable)>clear trunk 2/1 2-1001
Distribution_1 (enable)>set trunk 2/1 on dot1q 5,8,10
```

An example of the Catalyst OS configuration for Core_1 follows:

```
Core_1 (enable)>clear trunk 1/1 2-1001
Core_1 (enable)>set trunk 1/1 10
```

An example of the Supervisor IOS configuration for Core_1 follows:

```
Core_1(config)#interface gigabitethernet 1/1
Core_1(config-if)#switchport encapsulation negotiate
Core_1(config-if)#switchport mode dynamic auto
Core_1(config-if)#switchport trunk allowed vlan remove 2-1001
Core_1(config-if)#switchport trunk allowed vlan add 10
Core_1 (config-if)#end
Core_1#copy running-config startup-config
```

An example of the Layer 2 IOS configuration for Access_1 follows:

```
Access_1 (config)#interface gigabitethernet 0/1
Access_1 (config-if)#switchport mode trunk
Access_1 (config-if)#switchport trunk encapsulation dot1q
Access_1 (config-if)#switchport trunk allowed vlan remove 2-1001
Access_1 (config-if)#switchport trunk allowed vlan add 5,8,10
Access_1 (config-if)#end
Access_1#copy running-config startup-config
```

6-4: VLAN Trunking Protocol

- VTP sends messages between trunked switches to maintain VLANs on these switches in order to properly trunk.
- VTP is a Cisco proprietary method of managing VLANs between switches and runs across any type of trunking mechanism.
- VTP messages are exchanged between switches within a common VTP domain.
- VTP domains must be defined or VTP disabled before a VLAN can be created.
- Exchanges of VTP information can be controlled by passwords.
- VTP manages only VLANs 2 through 1002.
- VTP allows switches to synchronize their VLANs based on a configuration revision number.
- Switches can operate in one of three VTP modes: server, transparent, or client.
- VTP can prune unneeded VLANs from trunk links.

Enabling VTP for Operation

VTP exists to ensure that VLANs exist on the local VLAN database of switches in a trunked path. In addition to making sure the VLANs exist, VTP can further synchronize name settings and can be used to prune VLANs from trunk links that are destined for switches that do not have any ports active in that particular VLAN.

To manage and configure VTP, use the following steps.

1 Activate VTP on a switch.

a. Specify a VTP domain name:

COS	**set vtp domain** *name*
IOS	(privileged) **vlan database** (vlan_database) **vtp domain** *name* -OR- (global) **vtp domain** *name*

By default VTP is in server mode, which is an operational mode that enables you to manage VLANs on the local switch's database and use the information in the database to synchronize with other switches. To configure VTP for operation, you must specify a name. After you enable trunking, this name propagates to switches that have not been configured with a name. If you choose to configure names on your switches, however, remember that VTP names are case-sensitive and must match exactly. Switches that have different VTP names will not exchange VLAN information.

NOTE The global configuration command **vtp domain** is not supported on all switches that run the IOS.

NOTE VTP names are used only in the context of synchronizing VTP databases. VTP domain names do not separate broadcast domains. If VLAN 20 exists on two switches trunked together with different VTP domain names, VLAN 20 is still the same broadcast domain!

b. Enable the trunk:

COS	**set trunk** *mod/port* [**auto** | **desirable** | **on** | **nonegotiate** | **off**]
IOS	(global) **interface** *type mod/port* (interface) **switchport mode dynamic [auto** | **desirable]** (interface) **switchport mode trunk** (interface) **switchport nonegotiate**

VTP information is passed only across trunk links. If you do not enable a trunk, VLAN information is not exchanged between the switches. See section "6-3: Trunking" for more details on trunking.

NOTE Some IOS switches do not support DTP. For these switches, the only command that you can use to configure trunking is **switchport mode trunk**, which essentially turns trunking on.

Setting VTP Passwords

By default, there are no passwords in VTP informational updates, and any switch that has no VTP domain name will join the VTP domain when trunking is enabled. Also any switch that has the same VTP domain name configured will join and exchange VTP information. This could enable an unwanted switch in your network to manage the VLAN database on each of the switches. To prevent this from occurring, set a VTP password on the switches you want to exchange information.

1 *(Optional)* Set the VTP password:

COS	**set vtp passwd** *password*
IOS	(privileged) **vlan database** (vlan_database) **vtp password** *password* -OR- (global)**vtp password** *password*

The password is entered on each switch that will be participating in the VTP domain. The passwords are case-sensitive and must match exactly. If you want to remove the passwords, use the command **set vtp passwd 0** on a COS device or **no vtp password** in the VLAN database mode for the IOS device.

NOTE If you choose to set a password for VTP, it must be between 8 and 32 characters in length.

NOTE The global configuration command **vtp password** is not supported on all switches that run the IOS.

Changing VTP Modes

VTP operates in one of three modes: server, client, and transparent. The modes determine how VTP passes information, how VLAN databases are synchronized, and whether VLANs can be managed for a given switch.

1 *(Optional)* Set the VTP mode:

COS	`set vtp mode [server | client | transparent]`

IOS	`(privileged) vlan database`
	`(vlan_database) vtp [server | client | transparent]`
	-OR-
	`(global)vtp mode [server | client | transparent]`

By default Cisco switches are in VTP server mode. For a VTP server, you can create, delete, or modify a VLAN in the local VLAN database. After you make this change, the VLAN database changes are propagated out to all other switches in server or client mode in the VTP domain. A server will also accept changes to the VLAN database from other switches in the domain. You can also run the VTP in client mode. Switches in client mode cannot create, modify, or delete VLANs in the local VLAN database. Instead, they rely on other switches in the domain to update them about new VLANs. Clients will synchronize their databases, but they will not save the VLAN information and will loose this information if they are powered off. Clients will also advertise information about their database and forward VTP information to other switches. VTP transparent mode works much like server mode in that you can create, delete, or modify VLANs in the local VLAN database. The difference is that these changes are not propagated to other switches. In addition, the local VLAN database does not accept modifications from other switches. VTP transparent mode switches forward or relay information between other server or client switches. A VTP transparent mode switch does not require a VTP domain name.

NOTE The global configuration command **vtp mode** is not supported on all switches that run the IOS.

NOTE As of COS 7.1(1), Cisco introduced a VTP off mode (**set vtp mode off**). This mode is similar to transparent mode; but in VTP off mode, the switch does not relay VTP information between switches. This command is useful when you do not want to send or forward VTP updates—for example, if you are trunking with all non-Cisco switches or if you are using *Generic VLAN Registration Protocol* (GVRP) dynamic VLAN creation to manage your VLAN database.

Enabling VTP Pruning

By default all the VLANs that exist on a switch are active on a trunk link. As noted in section “6-3: Trunking”, you can manually remove VLANs from a trunk link and then add them later. VTP pruning allows the switch to not forward user traffic for VLANs that are not active on a remote switch. This feature dynamically prunes unneeded traffic across trunk links. If the VLAN traffic is needed at a later date, VTP will dynamically add the VLAN back to the trunk.

NOTE Dynamic pruning removes only unneeded user traffic from the link. It does not prevent any management frames such as STP from crossing the link.

1 *(Optional)* Enable VTP pruning.

a. Enable pruning:

COS	`set vtp pruning enable`
IOS	(privileged) **vlan database** (vlan_database) **vtp pruning**

After VTP pruning is enabled on one VTP server in the domain, all other switches in that domain will also enable VTP pruning. VTP pruning can only be enabled on switches that are VTP version 2-capable, so all switches in the domain must be version 2-capable before you enable pruning.

NOTE The switch must be VTP version 2-capable, but does not have to have version 2 enabled, to turn on pruning.

b. *(Optional)* Specify VLANs that are eligible for pruning:

COS	**clear vtp pruneeligible** *vlanlist*
IOS	(global) **interface** *type mod/port* (interface) **switchport trunk pruning vlan remove** *vlanlist*

By default all the VLANs on the trunk are eligible for pruning. You can remove VLANs from the list of eligible VLANs using these commands. After a VLAN has been removed from the eligible list, it cannot be pruned by VTP. To add the VLANs back, use the command **set vtp pruneeligible** *vlanlist* for COS switches or **switchport trunk pruning vlan add** *vlanlist* for IOS.

Changing VTP Versions

VTP supports two versions. By default all switches are in VTP version 1 mode, but most switches can support version 2 mode.

1 *(Optional)* Enable VTP version 2:

COS	**`set vtp v2 enable`**
IOS	`(privileged)` **`vlan database`** `(vlan_database)`**`vtp v2-mode`** -OR- `(global)`**`vtp version 2`**

VTP version 2 is disabled by default. After you have enabled version 2 on one switch, all other switches in the domain also begin to operate in version 2 mode.

NOTE The global configuration command **vtp version 2** is not supported on all switches that run the IOS.

VTP version 2 offers the following support options not available with version 1:

— **Unrecognized *type-length-value* (TLV) support**—A VTP server or client propagates configuration changes to its other trunks, even for TLVs it is not able to parse. The unrecognized TLV is saved in NVRAM.

— **Version-dependent transparent mode**—In VTP version 1, a VTP transparent switch inspects VTP messages for the domain name and version and forwards a message only if the version and domain name match. Because only one domain is supported in the Supervisor engine software, VTP version 2 forwards VTP messages in transparent mode, without checking the version.

— **Consistency checks**—In VTP version 2, VLAN consistency checks (such as VLAN names and values) are performed only when you enter new information through the *command-line interface* (CLI) or *Simple Network Management Protocol* (SNMP). Consistency checks are not performed when new information is obtained from a VTP message or when information is read from NVRAM. If the digest on a received VTP message is correct, its information is accepted without consistency checks.

Verifying VTP Operation

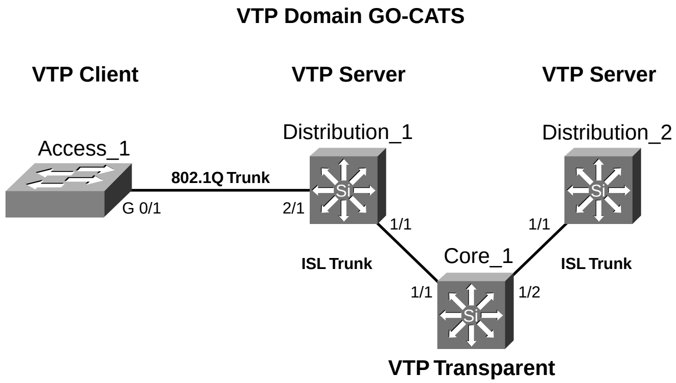
After configuring VTP, use one of the following commands to verify the VLAN port assignments:

COS	**show vtp domain**
IOS	(privileged) **show vtp status**

Feature Example

In this example, Access_1, Distribution_1, and Distribution_2 will be assigned to a VTP domain named GO-CATS. Figure 6-3 shows that Access_1 will be in VTP client mode with an 802.1Q trunk connecting to Distribution_1. Distribution_1 will be configured in VTP server mode with an ISL trunk connecting it to Core_1, which is in VTP transparent mode. Core_1 has an ISL trunk to Distribution_2, which is also in VTP server mode. VTP pruning has also been enabled for the domain, and all switches are configured so that VLAN 10 is not prune-eligible on the trunk links. Because VTP runs across trunk links, it is not necessary to configure the VTP domain name on the Distribution_2 switch or the Access_1 switch. It is also not necessary to configure the pruning on each switch; this is also propagated by VTP.

Figure 6-3 *Network Diagram for VTP Configuration on Access_1, Distribution_1, Distribution_2, and Core_1.*



An example of the Catalyst OS configuration for Core_1 follows:

```
Core_1 (enable)>set vtp mode transparent
Core_1 (enable)>set trunk 1/1 on isl
Core_1 (enable)>set trunk 1/2 on isl
Core_1 (enable)>
```

An example of the Catalyst OS configuration for Distribution_1 follows:

```
Distribution_1 (enable)>set vtp domain  GO-CATS
Distribution_1 (enable)>set trunk 1/1 on isl
Distribution_1 (enable)>set trunk 2/1 on dot1Q
Distribution_1 (enable)>set vtp pruning enable
Distribution_1 (enable)>clear vtp pruneeligible 10
```

An example of the Catalyst OS configuration for Distribution_2 follows:

```
Distribution_2 (enable)>set trunk 1/1 on isl
Distribution_2 (enable)>clear vtp pruneeligible 10
```

An example of the Layer 2 IOS configuration for Access_1 follows:

```
Access_1#vlan database
Access_1 (vlan)#vtp client
Access_1 (vlan)#exit
Access_1 #config t
Access_1 (config)#interface gigabitethernet 0/1
Access_1 (config-if)#switchport mode trunk
Access_1 (config-if)#switchport trunk encapsulation dot1Q
Access_1 (config-if)#switchport trunk pruning vlan remove 10
Access_1 (config-if)#end
Access_1#copy running-config startup-config
```

6-5: GVRP

- *Generic Attribute Registration Protocol* (GARP) *VLAN Registration Protocol* (GVRP) is an application defined in the IEEE 802.1Q standard that allows for the control of VLANs.
- GVRP runs only on 802.1Q trunk links.
- GVRP prunes trunk links so that only active VLANs will be sent across trunk connections.
- GVRP expects to hear join messages from the switches before it will add a VLAN to the trunk.
- GVRP updates and hold timers can be altered.
- GVRP ports run in various modes to control how they will prune VLANs.
- GVRP can be configured to dynamically add and manage VLANS to the VLAN database for trunking purposes.

Configuring GVRP

GVRP is supported only on COS switches. GVRP will run only on 802.1Q trunk ports and is used primarily to prune traffic from VLANs that does not need to be passed between trunking switches. Use the following steps to configure GVRP.

1. Enable GVRP globally:

COS	**set gvrp enable**

By default GVRP is not enabled for the switch. You must first enable GVRP on the switch before you can configure the 802.1Q ports for GVRP operation.

2. Configure the port for 802.1Q operation:

COS	**set trunk** *mod/port* [**auto** | **desirable** | **on**] **dot1q**

GVRP will run only on ports that are configured for 802.1Q trunking. See section “6-3: Trunking” for more information on trunking.

3. Configure the port GVRP:

COS	**set port gvrp** *mod/port* **enable**

This command enables GVRP on the individual 802.1Q trunk port. GVRP must be configured on both sides of the trunk to work correctly.

4. *(Optional)* Configure the port registration mode:

COS	**set gvrp registration** [**normal** | **fixed** | **forbidden**] *mod/port*

By default GVRP ports are in **normal** registration mode. These ports use GVRP join messages from neighboring switches to prune the VLANs running across the 802.1Q trunk link. If the device on the other side is not capable of sending GVRP messages, or if you do not want to allow the switch to prune any of the VLANs, use the **fixed** mode. Fixed mode ports will forward for all VLANs that exist in the switch database. Ports in **forbidden** mode forward only for VLAN 1.

Configuring GVRP for Dynamic VLAN Creation

Like VTP, GVRP can dynamically create VLANs on switches for trunking purposes. By enabling GVRP dynamic VLAN creation, a switch will add VLANs to its database when it receives GVRP join messages about VLANs it does not have.

1 (Optional) Enable dynamic VLAN creation:

COS	**`set gvrp dynamic-vlan-creation enable`**

Dynamic VLAN creation is configured on a switch-by-switch basis. GVRP does not synchronize between switches, but only adds VLANs on devices that have dynamic creation enabled in order to pass traffic between trunks. To enable dynamic VLAN creation, all the trunk ports on the switch have to be 802.1Q and they all must be GVRP-enabled ports. If the switch has any non-802.1Q trunk ports or if the 802.1Q ports that exist are not configured for GVRP, this feature will not be enabled. VLANs will be added only for join messages received across a normal registration port. You must also have configured VTP in transparent or off mode, because VTP and dynamic VLAN creation cannot both be enabled at the same time.

NOTE The trunk ports 15/1 and 16/1 on a 5000 or 6000 series switch do not count as ISL trunks when enabling **dynamic-vlan-creation** and will not prevent the function from operating.

Verifying GVRP Operation

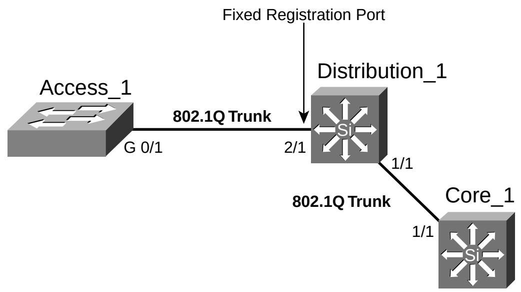
After you have configured GVRP, use the following command to verify operation:

COS	**`show gvrp configuration`**

Feature Example

In this example, the switch Access_1 is connected to Distribution_1 via an 802.1Q trunk shown in Figure 6-4. Distribution_1 is also connected to Core_1 via an 802.1Q trunk. GVRP is enabled on both the distribution and core switches and on each GVRP port on those switches. Dynamic VLAN creation has also been enabled on the switches, and the port from Distribution_1 to Access_1 has been set to GVRP fixed mode because the Access_1 device will not send join messages and the distribution switch would prune all VLANs if it were in the normal default mode.

Figure 6-4 *Network Diagram for GVRP Configuration on Access_1, Distribution_1, and Core_1*



An example of the Catalyst OS configuration for Core_1 follows:

```
Core_1 (enable)>set vtp mode transparent
Core_1 (enable)>set trunk 1/1 on dot1Q
Core_1 (enable)>set gvrp enable
Core_1 (enable)>set port gvrp 1/1 enable
Core_1 (enable)>set gvrp dynamic-vlan-creation enable
```

An example of the Catalyst OS configuration for Distribution_1 follows:

```
Distribution_1 (enable)>set vtp mode transparent
Distribution_1 (enable)>set trunk 1/1 on dot1q
Distribution_1 (enable)>set trunk 2/1 on dot1q
Distribution_1 (enable)>set gvrp enable
Distribution_1 (enable)>set gvrp enable 1/1
Distribution_1 (enable)>set gvrp enable 2/1
Distribution_1 (enable)>set gvrp registration fixed 2/1
Distribution_1 (enable)>set gvrp dynamic-vlan-creation enable
```

An example of the Layer 2 IOS configuration for Access_1 follows:

```
Access_1 #config t
Access_1 (config)#interface gigabitethernet 0/1
Access_1 (config-if)#switchport mode trunk
Access_1 (config-if)#switchport trunk encapsulation dot1Q
Access_1 (config-if)#end
Access_1#copy running-config startup-config
```

6-6: Private VLANs

- Private VLANs allow for additional security between devices in a common subnet.
- Private edge VLANs can be configured to prevent connectivity between devices on access switches.
- Private VLANs can be configured on the Catalyst 6000 and Catalyst 4000 series products.
- Within a private VLAN, you can isolate devices to prevent connectivity between devices within the isolated VLAN.

- Within a private VLAN, communities can be created to allow connection between some devices and to prevent them from communicating with others.
- Promiscuous ports are mapped to private VLANs to allow for connectivity to VLANs outside of this network.

Configuring Private VLANs

Private VLANs provide a mechanism to control which devices can communicate within a single subnet. The private VLAN uses **isolated** and **community** secondary VLANs to control how devices communicate. The secondary VLANs are assigned to the primary VLAN, and ports are assigned to the secondary VLANs. Ports in an isolated VLAN cannot communicate with any device in the VLAN other than the promiscuous port. Ports configured in a community VLAN can communicate with other ports in the same community and the promiscuous port. Ports in different communities cannot communicate with one another. To configure private VLANs, use the following steps.

1 Set VTP transparent mode:

COS	`set vtp mode transparent`
IOS	`(privileged) vlan database` `(vlan_database) vtp transparent`

You must configure VTP to transparent mode before you can create a private VLAN. Private VLANs are configured in the context of a single switch and cannot have members on other switches. Private VLANs also carry TLVs that are not known to all types of Cisco switches.

2 Create the primary private VLAN:

COS	**set vlan** *primary_number* **pvlan-type primary**
IOS	(global) **vlan** *primary_number* (vlan-config) **private-vlan primary**

You must first create a primary private VLAN. The number of the primary VLAN is used in later steps for binding secondary VLANs and mapping promiscuous ports.

3 Create isolated and community VLANs:

COS	**set vlan** *secondary_number* **pvlan-type** [**isolated** | **community** | **twoway-community**]
IOS	(global) **vlan** *secondary_number* (vlan-config) **private-vlan** [**isolated** | **community**]

Section 6-6

Configure isolated or community secondary VLANs for assignment of ports and control of the traffic. The secondary number for each of these VLANs must be unique from one another and the primary number. Members of an isolated VLAN can only communicate with the promiscuous port(s) mapped in Step 6, whereas members of a community VLAN can communicate with members of the same community and the promiscuous ports. A two-way community acts like a regular community, but has the additional aspect of allowing access control lists to check traffic going to and from (two ways) the VLAN and provides enhanced security within a private VLAN.

4 Bind isolated and community VLANs to the primary VLAN:

COS	`set pvlan` *primary_number secondary_number*
IOS	(global) **vlan** *primary_number* (vlan-config) **private-vlan association** *secondary_number_list* [**add** *secondary_number_list*]

This command associates or binds the secondary VLANs to the primary VLAN. For the IOS command, the **add** option allows other VLANs to be associated in the future.

5 Place ports into the isolated and community VLANs:

COS	**set pvlan** *primary_number secondary_number mod/port* [sc0]
IOS	(global) **interface** *type mod/port* (interface) **switchport** (interface) **switchport mode private-vlan host** (interface) **switchport mode private-vlan host-association** *primary_number secondary_number*

After you have created and associated the primary and secondary VLANs, you must assign ports to that VLAN. For COS switches, you can add the **sc0** interface to the private VLAN as well.

6 Map the isolated and community VLANs to promiscuous port(s):

COS	**set pvlan mapping** *primary_number secondary_number mod/port*
IOS	(global) **interface** *type mod/port* (interface) **switchport** (interface) **switchport mode private-vlan promiscuous** (interface) **switchport mode private-vlan mapping** *primary_number secondary_number*

After you have assigned ports to the secondary VLANs, you must map the VLANs to a promiscuous port for access outside of the isolated or community VLAN.

7 *(Optional)* Map the isolated and community VLANs a *Multilayer Switch Feature Card* (MSFC) interface:

COS	**set pvlan mapping** *primary_number secondary_number* **15/1** **session 15** (privileged)**config t** (global)**interface vlan** *primary_number* (interface)**ip address** *address mask*
IOS	(global) **interface** *primary_number* (interface) **ip address** *address mask* (interface) **private-vlan mapping** *primary_number secondary_number*

If your switch has an MSFC, you can map the private VLANs to the MSFC. For a switch running COS, you map the VLAN to port 15/1 (or 16/1 for the MSFC in slot 2), and then configure the IP address on the VLAN interface with the number of the primary VLAN. For an IOS switch, you go to the VLAN interface with the primary number, and then map the primary and secondary VLANs to that port.

Configuring Private Edge VLANs

The 3500XL switch uses the concept of a protected port to allow for control of traffic on the switch. A protected port on a 3500XL will not forward traffic to another protected port on the same switch. This behavior is similar to an isolated VLAN in that protected ports cannot communicate with one another. Use the following command to configure a protected port.

1 *(Optional)* Configure a protected port:

COS	—
IOS	(global) **interface** *type mod/port* (interface) **port protected**

To configure a private edge VLAN, select the interface and type the command **port protected**. To verify that a port is in protected mode, use the command **show port protected**.

Verifying Private VLAN Operation

After configuring private VLANs, use the following command to verify operation:

COS	**show pvlan** *number* **show pvlan mapping** **show pvlan capability** *mod/port*

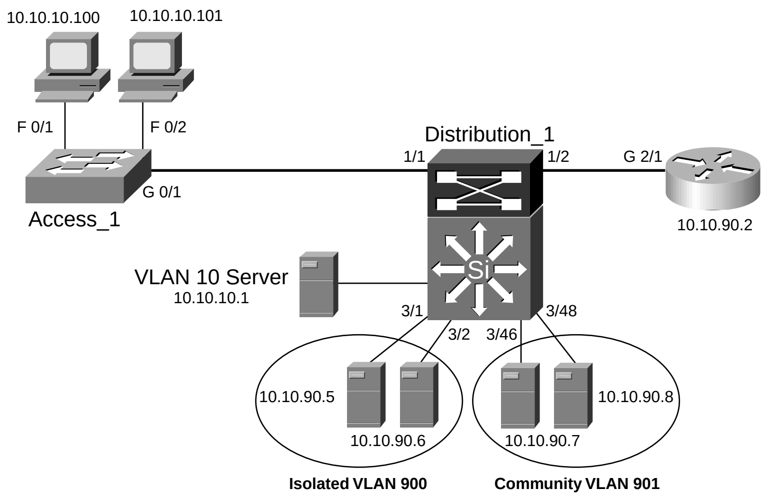
IOS	**show vlan private-vlan** *[type]*
	show interface private-vlan mapping
	show interface *type mod/port* **switchport**

NOTE A number of guidelines and restrictions apply to private VLANs. For a complete list of these items, go to www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_7_2/confg_gd/vlans.htm#xtocid21.

Feature Example

Figure 6-5 shows the network diagram for a working private VLAN configuration example. In this example, the switch Access_1 is configured with ports 1 and 2 as protected ports both in VLAN 10. The VLAN 10 server on Distribution_1 is also in VLAN 10. This allows the PCs to connect to the server but not one another. Also on the distribution switch, private VLAN 90 has been created with a community VLAN 901 and an isolated VLAN 900. Server 2 in port 3/46 and Server 3 in port 3/48 are placed in the community VLAN, and servers connected to ports 3/1 and 3/2 are to be placed in the isolated VLAN. All these devices are mapped to the router connected to port 1/2 and the MSFC port 15/1 for interface VLAN 90.

Figure 6-5 *Network Diagram for Private VLAN Configuration*



An example of the Catalyst OS configuration for Distribution_1 follows:

```
Distribution_1 (enable)>set vtp mode transparent
Distribution_1 (enable)>set vlan 90 pvlan-type primary
Distribution_1 (enable)>set vlan 900 pvlan-type isolated
Distribution_1 (enable)>set vlan 901 pvlan-type community
Distribution_1 (enable)>set pvlan 90 900
Distribution_1 (enable)>set pvlan 90 901
Distribution_1 (enable)>set pvlan 90 900 3/1-2
Distribution_1 (enable)>set pvlan 90 901 3/46,3/48
Distribution_1 (enable)>set pvlan mapping 90 900 1/2,15/1
Distribution_1 (enable)>set pvlan mapping 90 901 1/2,15/1
Distribution_1 (enable)>session 15
MSFC_Dist1>enable
MSFC_Dist1#config t
MSFC_Dist1(config)#interface vlan 90
MSFC_Dist1(config-if)#ip address 10.10.90.1 255.255.255.0
MSFC_Dist1(config-if)#no shut
MSFC_Dist1(config-if)#end
MSFC_Dist1#copy running-config startup-config
```

An example of the Supervisor IOS configuration for Distribution_1 follows:

```
Distribution_1#vlan database
Distribution_1(vlan)#vtp transparent
Distribution_1(vlan)#exit
Distribution_1#conf t
Distribution_1(config)#vlan 90
Distribution_1(config-vlan)#private-vlan primary
Distribution_1(config-vlan)#vlan 900
Distribution_1(config-vlan)#private-vlan isolated
Distribution_1(config-vlan)#vlan 901
Distribution_1(config-vlan)#private-vlan community
Distribution_1(config-vlan)#vlan 90
Distribution_1(config-vlan)#private-vlan association 900,901
Distribution_1(config-vlan)#interface range fastethernet 3/1 - 2
Distribution_1(config-if)#switchport
Distribution_1(config-if)#switchport mode private-vlan host
Distribution_1(config-if)#switchport mode private-vlan host-association 90 900
Distribution_1(config-if)#no shut
Distribution_1(config-if)#interface range fastethernet 3/46 , 3/48
Distribution_1(config-if)#switchport
Distribution_1(config-if)#switchport mode private-vlan host
Distribution_1(config-if)#switchport mode private-vlan host-association 90 901
Distribution_1(config-if)#no shut
Distribution_1(config-if)#interface gigabitethernet 1/2
Distribution_1(config-if)#switchport
Distribution_1(config-if)#switchport mode private-vlan promiscuous
Distribution_1(config-if)#switchport mode private-vlan mapping 90 900,901
Distribution_1(config-if)#no shut
Distribution_1(config-vif)#interface vlan 90
Distribution_1(config-if)#ip address 10.10.90.1 255.255.255.0
Distribution_1(config-if)#private-vlan mapping 90 900,901
Distribution_1(config-if)#no shut
Distribution_1(config-if)#end
Distribution_1 #copy running-config startup-config
```

An example of the Layer 2 IOS configuration for Access_1 follows:

```
Access_1 #config t
Access_1 (config)#interface fastethernet 0/1
Access_1 (config-if)#switchport access vlan 10
Access_1 (config-if)#port protected
Access_1 (config)#interface fastethernet 0/2
```

```
Access_1 (config-if)#switchport access vlan 10
Access_1 (config-if)#port protected
Access_1 (config)#interface gigabitethernet 0/1
Access_1 (config-if)#switchport mode trunk
Access_1 (config-if)#switchport trunk encapsulation dot1Q
Access_1 (config-if)#end
Access_1#copy running-config startup-config
```

Further Reading

Refer to the following recommended sources for further information about the topics covered in this chapter.

Cisco LAN Switching by Kennedy Clark and Kevin Hamilton, Cisco Press, ISBN 1-57870-094-9

Building Cisco Multilayer Switched Networks by Karen Webb, Cisco Press, ISBN 1-57870-093-0

CCNP Switching Exam Certification Guide by Tim Boyles and David Hucaby, Cisco Press, ISBN 1-57870-xxx-x

Securing Networks with Private VLANs and VLAN Access Control Lists at: www.cisco.com/warp/public/473/90.shtml

GVRP (802.1Q) Standard at: http://standards.ieee.org/reading/ieee/std/lanman/802.1Q-1998.pdf