CHAPTER 6

# Configuring the System

This chapter provides information about changing switch-wide configuration settings. It includes command-line interface (CLI) procedures for using commands that have been specifically created or changed for the Catalyst 2900 XL or Catalyst 3500 XL switches. For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.

This chapter does not repeat the concepts and CLI procedures provided in the standard Cisco IOS Release 12.0 documentation. For switch features that use standard Cisco IOS Release 12.0 commands, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

For information about configuring these settings from Cluster Management Suite (CMS), refer to the online help.

**Note** Some features can be implemented only by using the CLI.

# Changing IP Information

You can assign and change the IP information of your switch in the following ways:

- Using the setup program, as described in the release notes
- Manually assigning an IP address, as described in this section
- Using Dynamic Host Configuration Protocol (DHCP)-based autoconfiguration, as described in this section

**Caution** Changing the switch IP address ends any CMS, Telnet, or Simple Network Management Protocol (SNMP) session. To restart your CMS session, enter the new IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer). To restart your CLI session through Telnet, follow the steps described in the "Accessing the CLI" section on page 3-8.

**Note** If you enabled the DHCP feature, the switch assumes you are using an external server for IP address allocation. While this feature is enabled, any values you manually enter (from the CMS or from the **ip address** command) are ignored.

## Manually Assigning and Removing Switch IP Information

You can manually assign an IP address, mask, and default gateway to the switch. The mask identifies the bits that denote the network number in the IP address. When you use the mask to subnet a network, the mask is then referred to as a subnet mask. The broadcast address is reserved for sending messages to all hosts. The CPU sends traffic to an unknown IP address through the default gateway.

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

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **interface vlan 1** | Enter interface configuration mode, and enter the VLAN to which the IP information is assigned. VLAN 1 is the default management VLAN, but you can configure any VLAN from IDs 1 to 1001. |
| Step 3 | **ip address** *ip_address subnet_mask* | Enter the IP address and subnet mask. |
| Step 4 | **exit** | Return to global configuration mode. |
| Step 5 | **ip default-gateway** *ip_address* | Enter the IP address of the default router. |
| Step 6 | **end** | Return to privileged EXEC mode. |
| Step 7 | **show running-config** | Verify that the information was entered correctly by displaying the running configuration. If the information is incorrect, repeat the procedure. |

Use the following procedure to remove the IP information from a switch.

**Note** Using the **no ip address** command in configuration mode disables the IP protocol stack as well as removes the IP information. Cluster members without IP addresses rely on the IP protocol stack being enabled.

Beginning in privileged EXEC mode, follow these steps to remove an IP address:

| | Command | Purpose |
|---|---|---|
| Step 1 | **clear ip address vlan 1** *ip_address subnet_mask* | Remove the IP address and subnet mask. |
| Step 2 | **end** | Return to privileged EXEC mode. |
| Step 3 | **show running-config** | Verify that the information was removed by displaying the running configuration. |

# Using DHCP-Based Autoconfiguration

The Dynamic Host Configuration Protocol (DHCP) provides configuration information to Internet hosts and internetworking devices. With DHCP-based autoconfiguration, your switch (DHCP client) can be automatically configured during bootup with IP address information and a configuration file that it receives during DHCP-based autoconfiguration.

**Note** DHCP replaces the Bootstrap Protocol (BOOTP) feature autoconfiguration to ensure retrieval of configuration files by unicast TFTP messages. BOOTP is available in earlier software releases for this switch.

## Understanding DHCP-Based Autoconfiguration

The DHCP provides configuration information to internet hosts and internetworking devices. This protocol consists of two components: one for delivering configuration parameters from a DHCP server to a device and one for allocating network addresses to devices. DHCP is built on a client-server model, where designated DHCP servers allocate network addresses and deliver configuration parameters to dynamically configured devices.

With DHCP-based autoconfiguration, your switch (DHCP client) can be automatically configured at startup with IP address information and a configuration file that it receives during DHCP-based autoconfiguration. No DHCP client-side configuration is required on your switch.

However, you need to configure the DHCP server for various lease options. You might also need to configure a TFTP server, a Domain Name System (DNS) server, and possibly a relay device if the servers are on a different LAN than your switch. A relay device forwards broadcast traffic between two directly connected LANs. A router does not forward broadcast packets, but it forwards packets based on the destination IP address in the received packet. DHCP-based autoconfiguration replaces the BOOTP client functionality on your switch.

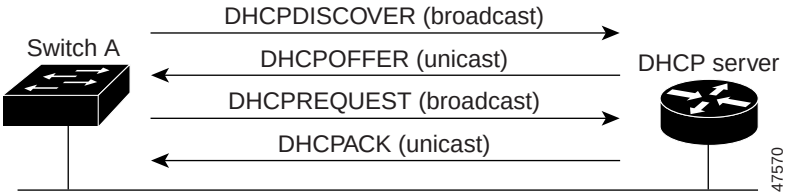
## DHCP Client Request Process

When you boot your switch, the DHCP client can be invoked and automatically request configuration information from a DHCP server under the following conditions:

- The configuration file is not present on the switch.
- The configuration file is present, but the IP address is not specified in it.
- The configuration file is present, the IP address is not specified in it, and the **service config** global configuration command is included. This command enables the autoloading of a configuration file from a network server.

Figure 6-1 shows the sequence of messages that are exchanged between the DHCP client and the DHCP server.

***Figure 6-1 DHCP Request for IP Information from a DHCP Server***




The client, Switch A, broadcasts a DHCPDISCOVER message to locate a DHCP server. The DHCP server offers configuration parameters (such as an IP address, subnet mask, gateway IP address, DNS IP address, a lease for the IP address, and so forth) to the client in a DHCPOFFER unicast message.

In a DHCPREQUEST broadcast message, the client returns a request for the offered configuration information to the DHCP server. The request is broadcast so that all other DHCP servers that received the DHCPDISCOVER broadcast message from the client can reclaim the IP addresses that they offered to the client.

The DHCP server confirms that the IP address has been allocated to the client by returning a DHCPACK unicast message to the client. With this message, the client and server are bound, and the client uses configuration information received from the server. The amount of information the switch receives depends on how you configure the DHCP server. For more information, see the "Configuring the DHCP Server" section on page 6-6.

If the configuration parameters sent to the client in the DHCPOFFER unicast message by the DHCP server are invalid (a configuration error exists), the client returns a DHCPDECLINE broadcast message to the DHCP server.

The DHCP server sends the client a DHCPNAK denial broadcast message, which means the offered configuration parameters have not been assigned, an error has occurred during the negotiation of the parameters, or the client has been slow in responding to the DHCPOFFER message (the DHCP server assigned the parameters to another client) of the DHCP server.

A DHCP client might receive offers from multiple DHCP or BOOTP servers and can accept any one of the offers; however, the client usually accepts the first offer it receives. The offer from the DHCP server is not a guarantee that the IP address will be allocated to the client; however, the server usually reserves the address until the client has had a chance to formally request the address. If the switch accepts replies from a BOOTP server and configures itself, the switch will broadcast, instead of unicast, TFTP requests to obtain the switch configuration file.

## Configuring the DHCP Server

You should configure the DHCP servers with reserved leases that are bound to each switch by the switch hardware address. If the DHCP server does not support reserved leases, the switch can obtain different IP addresses and configuration files at different boot instances. You should configure the DHCP server with the following lease options:

- IP address of the client (required)
- Subnet mask of the client (required)
- DNS server IP address (required)
- Router IP address (default gateway address to be used by the switch) (required)
- TFTP server name (required)
- Boot filename (the name of the configuration file that the client needs) (recommended)
- Host name (optional)

If you do not configure the DHCP server with the lease options described earlier, then it replies to client requests with only those parameters that have available values. If the IP address and subnet mask are not in the reply, the switch is not configured. If the DNS server IP address, router IP address, or TFTP server name are not found, the switch might broadcast TFTP requests. Unavailability of other lease options does not affect autoconfiguration.

**Note** If the configuration file on the switch does not contain the IP address, the switch obtains its address, mask, gateway IP address, and host name from DHCP. If the **service config** global configuration command is specified in the configuration file, the switch receives the configuration file through TFTP requests. If the **service config** global configuration command and the IP address are both present in the configuration file, DHCP is not used, and the switch obtains the default configuration file by broadcasting TFTP requests.

The DHCP server can be on the same or a different LAN as the switch. If it is on a different LAN, the switch must be able to access it through a relay device. The DHCP server can be running on a UNIX or Linux operating system; however, the Windows NT operating system is not supported in this release.

For more information, see the "Configuring the Relay Device" section on page 6-9. You must also set up the TFTP server with the switch configuration files; for more information, see the next section.

For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

## Configuring the TFTP Server

The TFTP server must contain one or more configuration files in its base directory. The files can include the following:

- The configuration file named in the DHCP reply (the actual switch configuration file)
- The network-confg or the cisconet.cfg file (known as the default configuration files)
- The router-confg or the ciscortr.cfg file (These files contain commands common to all switches. Normally, if the DHCP and TFTP servers are properly configured, these files are not accessed.)

You must specify the TFTP server name in the DHCP server lease database. You must also specify the TFTP server name-to-IP-address mapping in the DNS server database.

The TFTP server can be on the same or a different LAN as the switch. If it is on a different LAN, the switch must be able to access it through a relay device or a router. For more information, see the "Configuring the Relay Device" section on page 6-9.

If the configuration filename is provided in the DHCP server reply, the configuration files for a switch can be spread over multiple TFTP servers. However, if the configuration filename is not provided, then the configuration files must reside on a single TFTP server.

For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

## Configuring the Domain Name and the DNS

Each unique IP address can have a host name associated with it. The IOS software maintains a cache of host name-to-address mappings for use by the EXEC mode **connect**, **telnet**, and **ping** commands, and related Telnet support operations. This cache speeds the process of converting names to addresses.

IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco Systems is a commercial organization that IP identifies by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, the File Transfer Protocol (FTP) system for example, is identified as *ftp.cisco.com*.

To keep track of domain names, IP has defined the concept of a Domain Name Server (DNS), which holds a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the host names and then specify a name server and enable the DNS, the Internet's global naming scheme that uniquely identifies network devices.

You can specify a default domain name that the software uses to complete domain name requests. You can specify either a single domain name or a list of domain names. When you specify a domain name, any IP host name without a domain name will have that domain name appended to it before being added to the host table.

If your network devices require connectivity with devices in networks for which you do not control name assignment, you can assign device names that uniquely identify your devices within the entire internetwork. The Internet's global naming scheme, the DNS, accomplishes this task. This service is enabled by default.

The switch uses the DNS server to resolve the TFTP server name to a TFTP server IP address. You must configure the TFTP server name-to-IP address map on the DNS server. The TFTP server contains the configuration files for the switch.

You must configure the IP addresses of the DNS servers in the lease database of the DHCP server from where the DHCP replies will retrieve them. You can enter up to two DNS server IP addresses in the lease database.

The DNS server can be on the same or a different LAN as the switch. If it is on a different LAN, the switch must be able to access it through a relay device or router. For more information, see the "Configuring the Relay Device" section on page 6-9.

For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

## Configuring the Relay Device

You need to use a relay device if the DHCP, DNS, or TFTP servers are on a different LAN than the switch. You must configure this relay device to forward received broadcast packets on an interface to the destination host. This configuration ensures that broadcasts from the DHCP client can reach the DHCP, DNS, and TFTP servers and that broadcasts from the servers can reach the DHCP client.

If the relay device is a Cisco router, you enable IP routing (**ip routing** global configuration command) and configure it with helper addresses by using the **ip helper-address** interface configuration command.

For example, in Figure 6-2, you configure the router interfaces as follows:

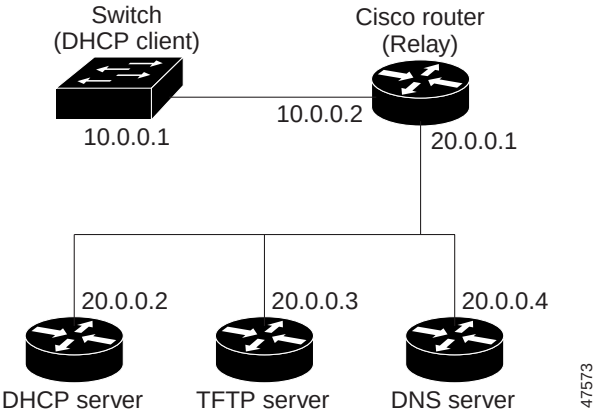
On interface 10.0.0.2:

```
router(config-if)# ip helper-address 20.0.0.2
router(config-if)# ip helper-address 20.0.0.3
router(config-if)# ip helper-address 20.0.0.4
```

On interface 20.0.0.1

```
router(config-if)# ip helper-address 10.0.0.1
```

***Figure 6-2 Relay Device Used in Autoconfiguration***




For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

## Obtaining Configuration Files

Depending on the availability of the IP address and the configuration filename in the DHCP reserved lease, the switch obtains its configuration information in the following ways:

- The IP address and the configuration filename is reserved for the switch and provided in the DHCP reply (one-file read method).

  The switch receives its IP address, subnet mask, and configuration filename from the DHCP server. It also receives a DNS server IP address and a TFTP server name. The switch sends a DNS request to the DNS server, specifying the TFTP server name, to obtain the TFTP server address. Then the switch sends a unicast message to the TFTP server to retrieve the named configuration file from the base directory of the server, and upon receipt, completes its boot-up process.

- Only the configuration filename is reserved for the switch. The IP address is dynamically allocated to the switch by the DHCP server (one-file read method).

  The switch follows the same configuration process described above.

- Only the IP address is reserved for the switch and provided in the DHCP reply. The configuration filename is not provided (two-file read method).

  The switch receives its IP address and subnet mask from the DHCP server. It also receives a DNS server IP address and a TFTP server name. The switch sends a DNS request to the DNS server, specifying the TFTP server name, to obtain the TFTP server address.

  The switch sends a unicast message to the TFTP server to retrieve the network-confg or cisconet.cfg default configuration file. (If the network-confg file cannot be read, the switch reads the cisconet.cfg file.)

  The default configuration file contains the host names-to-IP-address mapping for the switch. The switch fills its host table with the information in the file and obtains its host name. If the host name is not found in the file, the switch uses the host name in the DHCP reply. If the host name is not specified in the DHCP reply, the switch uses the default "Switch" as its host name.

  After obtaining its host name from the default configuration file or the DHCP reply, the switch reads the configuration file that has the same name as its host name (*hostname*-confg or *hostname*.cfg, depending on whether network-confg or cisconet.cfg was read earlier) from the TFTP server. If the cisconet.cfg file is read, the filename of the host is truncated to eight characters.

  If the switch cannot read the network-confg, cisconet.cfg, or the host-name file, it reads the router-confg file. If the switch cannot read the router-confg file, it reads the ciscortr.cfg file.

**Note** The switch broadcasts TFTP server requests if the TFTP server name is not obtained from the DHCP replies, if all attempts to read the configuration file through unicast transmissions fail, or if the TFTP server name cannot be resolved to an IP address.

## Example Configuration

Figure 6-3 shows a sample network for retrieving IP information using DHCP-based autoconfiguration.

***Figure 6-3 DHCP-Based Autoconfiguration Network Example***

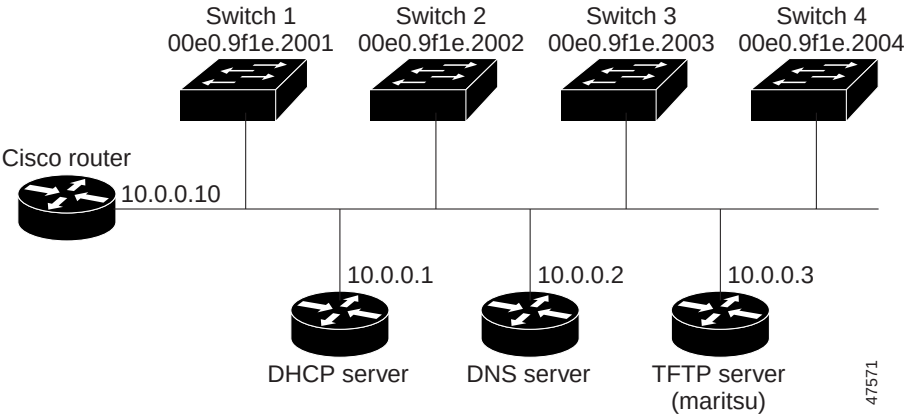



Table 6-1 shows the configuration of the reserved leases on the DHCP server.

*Table 6-1 DHCP Server Configuration*

| | Switch-1 | Switch-2 | Switch-3 | Switch-4 |
|---|---|---|---|---|
| Binding key (hardware address) | 00e0.9f1e.2001 | 00e0.9f1e.2002 | 00e0.9f1e.2003 | 00e0.9f1e.2004 |
| IP address | 10.0.0.21 | 10.0.0.22 | 10.0.0.23 | 10.0.0.24 |
| Subnet mask | 255.255.255.0 | 255.255.255.0 | 255.255.255.0 | 255.255.255.0 |
| Router address | 10.0.0.10 | 10.0.0.10 | 10.0.0.10 | 10.0.0.10 |
| DNS server address | 10.0.0.2 | 10.0.0.2 | 10.0.0.2 | 10.0.0.2 |
| TFTP server name | *maritsu* or *10.0.0.3* | *maritsu* or *10.0.0.3* | *maritsu* or *10.0.0.3* | *maritsu* or *10.0.0.3* |
| Boot filename (configuration file) (optional) | switch1-confg | switch2-confg | switch3-confg | switch4-confg |
| Host name (optional) | switch1 | switch2 | switch3 | switch4 |

### DNS Server Configuration

The DNS server maps the TFTP server name *maritsu* to IP address 10.0.0.3.

### TFTP Server Configuration (on UNIX)

The TFTP server base directory is set to /tftpserver/work/. This directory contains the network-confg file used in the two-file read method. This file contains the host name to be assigned to the switch based on its IP address. The base directory also contains a configuration file for each switch (switch1-confg, switch2-confg, and so forth) as shown in this display:

```
prompt> cd /tftpserver/work/
prompt> ls
network-confg
switch1-confg
switch2-confg
switch3-confg
switch4-confg
prompt> cat network-confg
ip host switch1 10.0.0.21
ip host switch2 10.0.0.22
ip host switch3 10.0.0.23
ip host switch4 10.0.0.24
```

### DHCP Client Configuration

No configuration file is present on Switch 1 through Switch 4.

### Configuration Explanation

In Figure 6-3, Switch 1 reads its configuration file as follows:

- It obtains its IP address 10.0.0.21 from the DHCP server.
- If no configuration filename is given in the DHCP server reply, Switch 1 reads the network-confg file from the base directory of the TFTP server.
- It adds the contents of the network-confg file to its host table.
- It reads its host table by indexing its IP address 10.0.0.21 to its host name (switch1).
- It reads the configuration file that corresponds to its host name; for example, it reads switch1-confg from the TFTP server.

Switches 2 through 4 retrieve their configuration files and IP addresses in the same way.

# Changing the Password

You can assign the password of your switch in the following ways:

- Using the setup program, as described in the release notes
- Manually assigning a password, as described in this section

**Note** You can change a password only by using the CLI. Your connection with the switch ends when you change the enable secret password. You will then need to reopen the session with the new password. If you have forgotten your password, see the "Recovering from a Lost or Forgotten Password" section on page 9-22.

Because many privileged EXEC commands are used to set operating parameters, you should password-protect these commands to prevent unauthorized use. Catalyst 2900 XL and Catalyst 3500 XL switches have two commands for setting passwords:

- **enable secret** *password* (a very secure, encrypted password)
- **enable password** *password* (a less secure, unencrypted password)

You must enter one of these passwords to gain access to privileged EXEC mode. We recommend that you use the enable secret password.

**Note** When set, the enable secret password takes precedence, and the enable password serves no purpose.

If you enter the **enable secret** command, the text is encrypted before it is written to the config.text file, and it is unreadable. If you enter the **enable password** command, the text is written as entered to the config.text file where you can read it.

You can also specify up to 15 privilege levels and define passwords for them by using the **enable password** [**level** *level*] {*password*} or the **enable secret** [**level** *level*] {*password*} command. Level 1 is EXEC-mode user privileges. If you do not specify a level, the privilege level defaults to 15 (privileged EXEC-mode privileges).

You can specify a level, set a password, and give the password only to users who need to have access at this level. Use the **privilege level** global configuration command to specify commands accessible at various levels.

**Note** You need an enable secret password with a privilege level 15 to access CMS. You must also use this password if you configure the Terminal Access Controller Access Control System Plus (TACACS+) protocol from the CLI so that all your HTTP connections are authenticated through the TACACS+ server. The Telnet password must be an enable secret password.

For information about managing passwords in switch clusters, see the "Passwords" section on page 5-8.

Both types of passwords can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and both can start with a number. Spaces are also valid password characters; for example, *two words* is a valid password. Leading spaces are ignored; trailing spaces are recognized. The password is case sensitive.

To remove a password, use the **no** version of the commands: **no enable secret** or **no enable password**. If you lose or forget your enable password, see the "Recovering from a Lost or Forgotten Password" section on page 9-22.

For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

# Setting the System Date and Time

You can change the date and a 24-hour clock time setting on the switch. If you are entering the time for an American time zone, enter the three-letter abbreviation for the time zone, such as PST for Pacific standard time. If you are identifying the time zone by referring to Greenwich mean time, enter UTC (universal coordinated time). You then must enter a negative or positive number as an offset to indicate the number of time zones between the switch and Greenwich, England. Enter a negative number if the switch is west of Greenwich, England, and east of the international date line. For example, California is eight time zones west of Greenwich, so you would enter –8. Enter a positive number if the switch is east of Greenwich. You can also enter negative and positive numbers for minutes.

## Configuring Daylight Saving Time

You can configure the switch to change to daylight saving time on a particular day every year, on a day that you enter, or not at all.

For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

## Configuring the Network Time Protocol

In complex networks, it is often prudent to distribute time information from a central server. The Network Time Protocol (NTP) can distribute time information by responding to requests from clients or by broadcasting time information.

For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

### Configuring the Switch as an NTP Client

You configure the switch as an NTP client by entering the IP addresses of up to ten NTP servers and specifying which server should be used first. You can also enter an authentication key to be used as a password when requests for time information are sent to the server.

### Enabling NTP Authentication

To ensure the validity of information received from NTP servers, you can authenticate NTP messages with public-key encryption. This procedure must be coordinated with the administrator of the NTP servers: the information you enter will be matched by the servers to authenticate it.

### Configuring the Switch for NTP Broadcast-Client Mode

You can configure the switch to receive NTP broadcast messages if there is an NTP broadcast server, such as a router, broadcasting time information on the network. You can also enter a value to account for any round-trip delay between the client and the NTP broadcast server.

# Configuring SNMP

If your switch is part of a cluster, the clustering software can change Simple Network Management Protocol (SNMP) parameters (such as host names) when the cluster is created. If you are configuring a cluster for SNMP, see the "SNMP Community Strings" section on page 5-10.

## Disabling and Enabling SNMP

SNMP is enabled by default and must be enabled for Cluster Management features to work properly.

SNMP is always enabled for Catalyst 1900 and Catalyst 2820 switches.

For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

# Entering Community Strings

Community strings serve as passwords for SNMP messages, permitting access to the agent on the switch. If you are entering community strings for a cluster member, see the "SNMP Community Strings" section on page 5-10. You can enter community strings with the following characteristics:

Read-only (RO)—Requests accompanied by the string can display MIB-object information.

Read-write (RW)—Requests accompanied by the string can display MIB-object information and set MIB objects.

For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

# Adding Trap Managers

A trap manager is a management station that receives and processes traps. When you configure a trap manager, the community strings for each member switch must be unique. If a member switch has an assigned IP address, the management station accesses the switch by using that IP address.

By default, no trap manager is defined, and no traps are issued. Table 6-2 describes the Catalyst 2900 XL and Catalyst 3500 XL switch traps. You can enable any or all of these traps and configure a trap manager on these switches to receive them.

***Table 6-2 Catalyst 2900 XL and Catalyst 3500 XL Switch Traps***

| | |
|---|---|
| Config | Generate traps whenever the switch configuration changes. |
| SNMP | Generate the supported SNMP traps. |
| TTY | Generate traps when the switch starts a management console CLI session. |
| VLAN membership | Generate a trap for each VLAN Membership Policy Server (VMPS) change. |
| VTP | Generate a trap for each VLAN Trunk Protocol (VTP) change. |
| C2900/C3500 | Generate the switch-specific traps. These traps are in the private enterprise-specific Management Information Base (MIB). |

Catalyst 1900 and Catalyst 2820 switches support up to four trap managers. When you configure community strings for these switches, limit the string length to 32 characters. When configuring traps on these switches, you cannot configure individual trap managers to receive specific traps.

Table 6-3 describes the Catalyst 1900 and Catalyst 2820 switch traps. You can enable any or all of these traps, but these traps are received by all configured trap managers.

***Table 6-3 Catalyst 1900 and Catalyst 2820 Switch Traps***

| Trap Type | Description |
|---|---|
| Address-violation | Generates a trap when the address violation threshold is exceeded. |
| Authentication | Generates a trap when an SNMP request is not accompanied by a valid community string. |
| BSC | Generates a trap when the broadcast threshold is exceeded. |
| Link-up-down | Generates a link-down trap when a port is suspended or disabled for any of these reasons:<br>• Secure address violation (address mismatch or duplication)<br>• Network connection error (loss of linkbeat or jabber error)<br>• User disabling the port<br>Generates a link-up trap when a port is enabled for any of these reasons:<br>• Presence of linkbeat<br>• Management intervention<br>• Recovery from an address violation or any other error<br>• STP action |
| VTP | Generates a trap when VTP changes occur. |

Beginning in privileged EXEC mode, follow these steps to add a trap manager and a community string:

| | Command | Purpose |
|---|---|---|
| Step 1 | **config terminal** | Enter global configuration mode. |
| Step 2 | **snmp-server host 172.2.128.263 traps1 snmp vlan-membership** | Enter the trap manager IP address, the community string, and the traps to generate. |
| Step 3 | **end** | Return to privileged EXEC mode. |
| Step 4 | **show running-config** | Verify that the information was entered correctly by displaying the running configuration. |

# Configuring CDP

Use the Cisco IOS CLI and Cisco Discovery Protocol (CDP) to enable CDP for the switch, set global CDP parameters, and display information about neighboring Cisco devices.

CDP enables the Cluster Management Suite to display a graphical view of the network. For example, the switch uses CDP to find cluster candidates and to maintain information about cluster members and other devices up to three cluster-enabled devices away from the command switch.

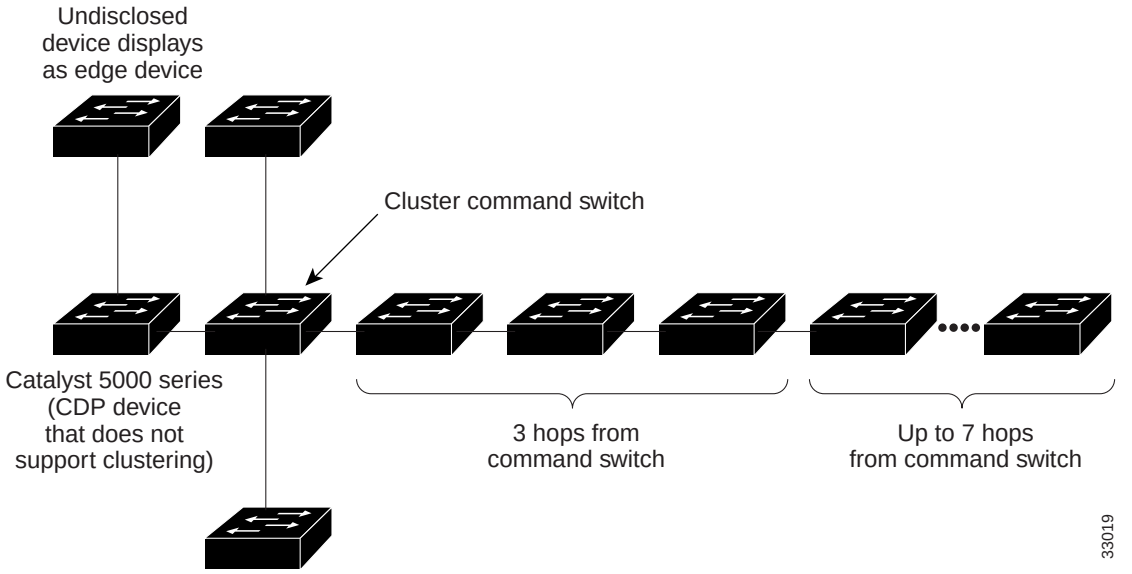
If necessary, you can configure CDP to discover switches running the Cluster Management Suite up to seven devices away from the command switch. Devices that do not run clustering software display as edge devices, and CDP cannot discover any device connected to them.

**Note** Creating and maintaining switch clusters is based on the regular exchange of CDP messages. Disabling CDP can interrupt cluster discovery. For more information about the role that CDP plays in clustering, see the "Automatic Discovery of Cluster Candidates" section on page 5-4.

## Configuring CDP for Extended Discovery

You can change the default configuration of CDP on the command switch to continue discovering devices up to seven *hops* away. Figure 6-4 shows a command switch that can discover candidates and cluster members up to seven devices away from it. Figure 6-4 also shows the command switch connected to a Catalyst 5000 series switch. Although the Catalyst 5000 supports CDP, it does not support clustering, and the command switch cannot learn about connected candidate switches connected to it, even if they are running CMS.

*Figure 6-4 Discovering Cluster Candidates through CDP*




Beginning in privileged EXEC mode, follow these steps to configure the number of hops that CDP uses to discover candidate switches and cluster members.

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **cluster discovery hop-count** *number* | Enter the number of hops that you want CDP to search for cluster candidates and cluster members. |
| Step 3 | **end** | Return to privileged EXEC mode. |
| Step 4 | **show running-config** | Verify the change by displaying the running configuration file. The hop count is displayed in the file. |

# Configuring STP

Spanning Tree Protocol (STP) provides path redundancy while preventing undesirable loops in the network. Only one active path can exist between any two stations. STP calculates the best loop-free path throughout the network.

## Supported STP Instances

You create an STP instance when you assign an interface to a VLAN. The STP instance is removed when the last interface is moved to another VLAN. You can configure switch and port parameters before an STP instance is created. These parameters are applied when the STP instance is created. You can change all VLANs on a switch by using the **stp-list** parameter when you enter STP commands through the CLI. For more information, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.

All Catalyst 3500 XL switches and most Catalyst 2900 XL switches support 250 VLANs. The Catalyst 2912 XL, Catalyst 2924 XL, and Catalyst 2924C XL support only 64 VLANs. For more information about VLANs, see Chapter 8, "Configuring VLANs."

Each VLAN is a separate STP instance. If you have already used up all available STP instances on a switch, adding another VLAN anywhere in the VLAN Trunk Protocol (VTP) domain creates a VLAN that is not running STP on that switch. For example, if 250 VLANs are defined in the VTP domain, you can enable STP on those 250 VLANs. The remaining VLANs must operate with STP disabled.

You can disable STP on one of the VLANs where it is running, and then enable it on the VLAN where you want it to run. Use the **no spanning-tree vlan** *vlan-id* global configuration command to disable STP on a specific VLAN, and use the **spanning-tree vlan** *vlan-id* global configuration command to enable STP on the desired VLAN.

**Caution** Switches that are not running spanning tree still forward Bridge Protocol Data Units (BPDUs) that they receive so that the other switches on the VLAN that have a running STP instance can break loops. Therefore, spanning tree must be running on enough switches so that it can break all the loops in the network. For example, at least one switch on each loop in the VLAN must be running spanning tree. It is not absolutely necessary to run spanning tree on all

switches in the VLAN; however, if you are running STP only on a minimal set of switches, an incautious change to the network that introduces another loop into the VLAN can result in a broadcast storm.

**Note** If you have the default allowed list on the trunk ports of that switch, the new VLAN is carried on all trunk ports. Depending on the topology of the network, this could create a loop in the new VLAN that will not be broken, particularly if there are several adjacent switches that all have run out of STP instances. You can prevent this by setting allowed lists on the trunk ports of switches that have used up their allocation of STP instances. Setting up allowed lists is not necessary in many cases and makes it more labor-intensive to add another VLAN to the network.

# Using STP to Support Redundant Connectivity

You can create a redundant backbone with STP by connecting two of the switch ports to another device or to two different devices. STP automatically disables one port but enables it if the other port is lost. If one link is high-speed and the other low-speed, the low-speed link is originally disabled. If the two link speeds are the same, the port priority and the port ID are added together, and STP disables the link with the lowest value.

You can also create redundant links between switches by using EtherChannel port groups. For more information about creating port groups, see the "Creating EtherChannel Port Groups" section on page 7-10.

## Disabling STP

STP is enabled by default. Disable STP only if you are sure there are no loops in the network topology.

**Caution** When STP is disabled and loops are present in the topology, excessive traffic and indefinite packet duplication can severely reduce network performance.

Beginning in privileged EXEC mode, follow these steps to disable STP:

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **no spanning-tree vlan** *stp-list* | Disable STP on a VLAN. |
| Step 3 | **end** | Return to privileged EXEC mode. |
| Step 4 | **show spanning-tree** | Verify your entry. |

# Accelerating Aging to Retain Connectivity

The default for aging dynamic addresses is 5 minutes. However, a reconfiguration of the spanning tree can cause many station locations to change. Because these stations could be unreachable for 5 minutes or more during a reconfiguration, the address-aging time is accelerated so that station addresses can be dropped from the address table and then relearned. The accelerated aging is the same as the forward-delay parameter value when STP reconfigures.

Because each VLAN is a separate instance of STP, the switch accelerates aging on a per-VLAN basis. A reconfiguration of STP on one VLAN can cause the dynamic addresses learned on that VLAN to be subject to accelerated aging. Dynamic addresses on other VLANs can be unaffected and remain subject to the aging interval entered for the switch.

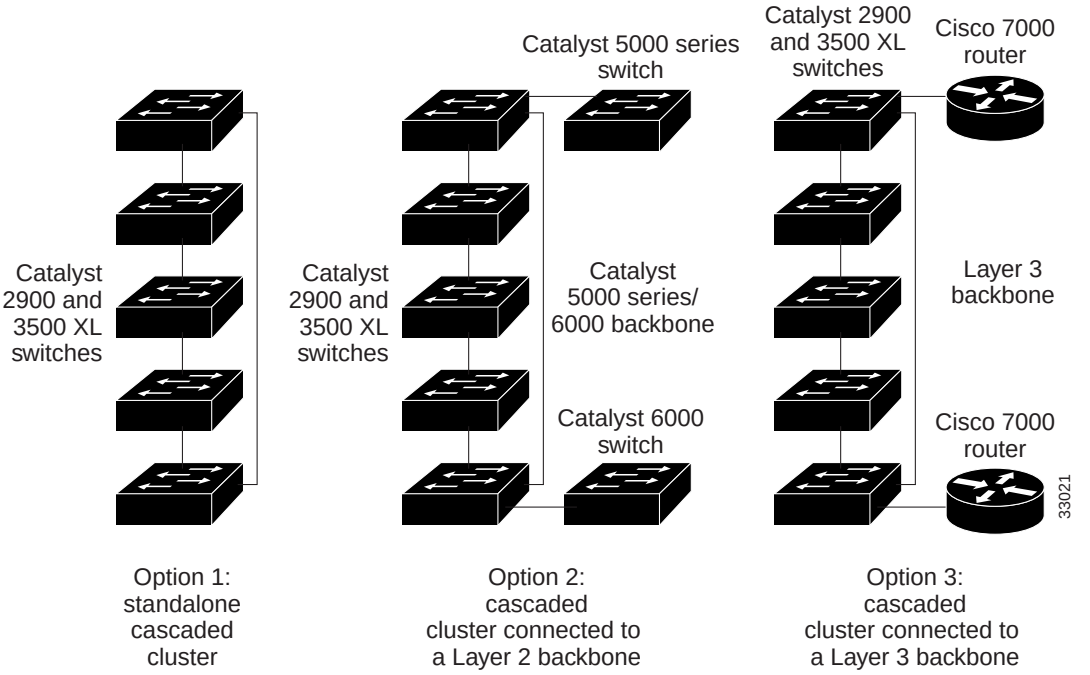
# Configuring STP and UplinkFast in a Cascaded Cluster

STP uses default values that can be reduced when configuring Catalyst 2900 XL and Catalyst 3500 XL switches in cascaded configurations. If an STP root switch is part of a cluster that is one switch from a cascaded stack, you can customize STP to reconverge more quickly after a switch failure. Figure 6-5 shows modular Catalyst 2900 XL and Catalyst 3500 XL switches in three cascaded clusters that use the GigaStack GBIC. Table 6-4 shows the default STP settings and those that are acceptable for these configurations.

*Table 6-4 Default and Acceptable STP Parameter Settings (in Seconds)*

| STP Parameter | STP Default (IEEE) | Acceptable for Option 1 | Acceptable for Option 2 | Acceptable for Option 3 |
|---|---|---|---|---|
| Hello Time | 2 | 1 | 1 | 1 |
| Max Age | 20 | 6 | 10 | 6 |
| Forwarding delay | 15 | 4 | 7 | 4 |

*Figure 6-5 Gigabit Ethernet Clusters*




Enabling UplinkFast on all cluster switches can further reduce the time it takes cluster switches to begin forwarding after a new root switch is selected.

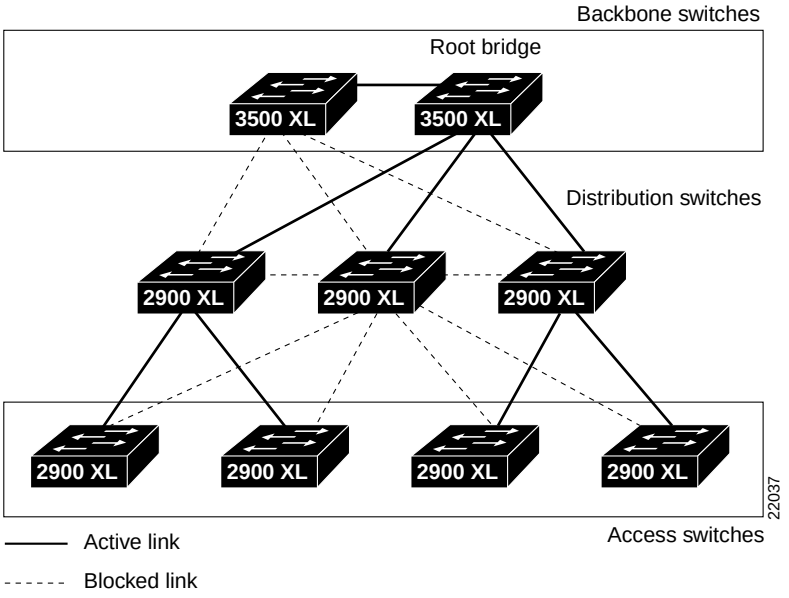
# Configuring Redundant Links By Using STP UplinkFast

Switches in hierarchical networks can be grouped into backbone switches, distribution switches, and access switches. Figure 6-6 shows a complex network where distribution switches and access switches each have at least one redundant link that STP blocks to prevent loops.

If a switch looses connectivity, the switch begins using the alternate paths as soon as STP selects a new root port. When STP reconfigures the new root port, other ports flood the network with multicast packets, one for each address that was learned on the port. You can limit these bursts of multicast traffic by reducing the max-update-rate parameter. The default for this parameter is 150 packets per second. However, if you enter zero, station-learning frames are not generated, so the STP topology converges more slowly after a loss of connectivity.

STP UplinkFast is a Cisco enhancement that accelerates the choice of a new root port when a link or switch fails or when STP reconfigures itself. The root port transitions to the forwarding state immediately without going through the listening and learning states, as it would with normal STP procedures. UplinkFast is most useful in edge or access switches and might not be appropriate for backbone devices.

*Figure 6-6 Switches in a Hierarchical Network*



## Enabling STP UplinkFast

When you enable UplinkFast, it is enabled for the entire switch and cannot be enabled for individual VLANs.

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

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **spanning-tree uplinkfast max-update-rate** *pkts-per-second* | Enable UplinkFast on the switch.<br>The range is from 0 to 1000 packets per second. The default is 150.<br>If you set the rate to 0, station-learning frames are not generated, so the STP topology converges more slowly after a loss of connectivity. |
| Step 3 | **exit** | Return to privileged EXEC mode. |
| Step 4 | **show spanning-tree** | Verify your entries. |

When UplinkFast is enabled, the bridge priority of all VLANs is set to 49152, and the path cost of all ports and VLAN trunks is increased by 3000. This change reduces the chance that the switch will become the root switch. When UplinkFast is disabled, the bridge priorities of all VLANs and path costs of all ports are set to default values.

# Configuring Cross-Stack UplinkFast

Cross-stack UplinkFast (CSUF) provides a fast spanning-tree transition (fast convergence in less than 2 seconds under normal network conditions) across a stack of switches that use the GigaStack GBICs connected in a shared cascaded configuration (multidrop backbone). During the fast transition, an alternate redundant link on the stack of switches is placed into the forwarding state without causing temporary spanning-tree loops or loss of connectivity to the backbone. With this feature, you can have a redundant and resilient network in some configurations.

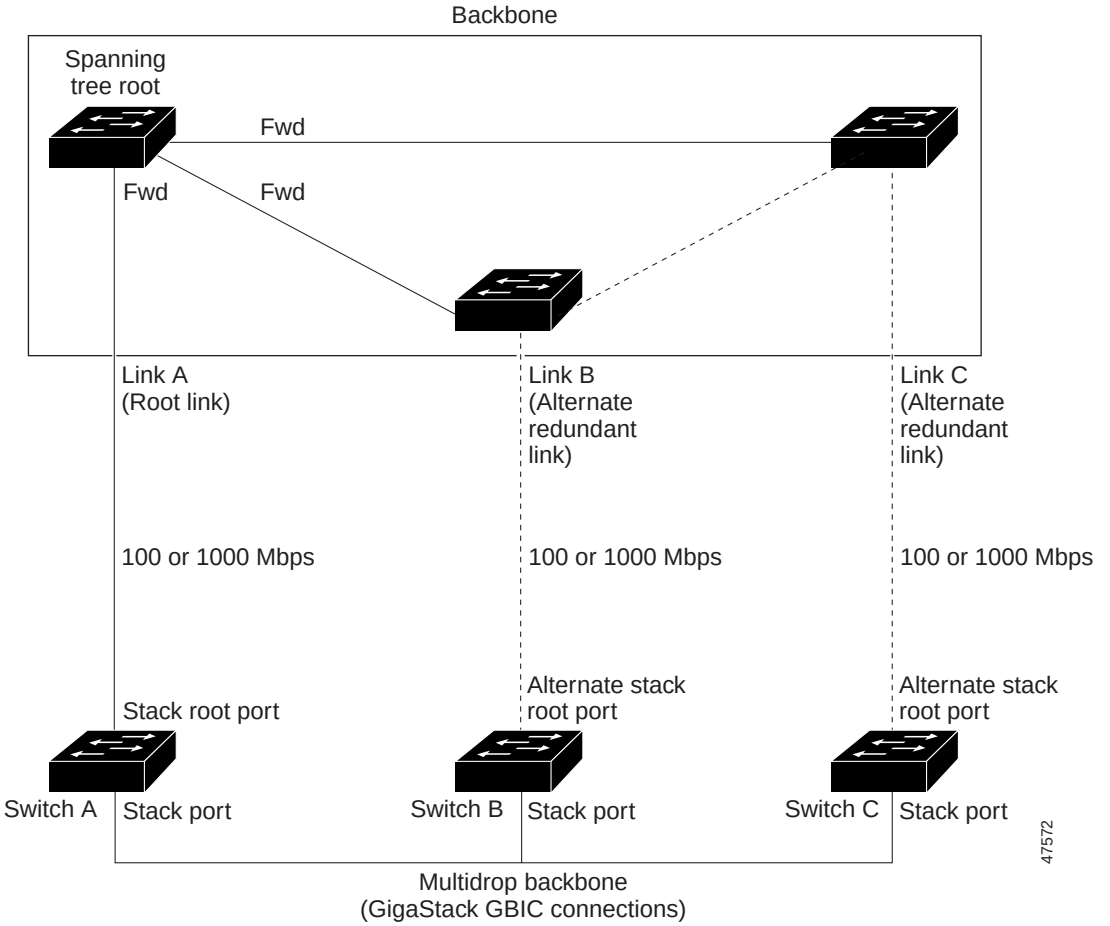
CSUF might not provide a fast transition all the time; in these cases, the normal STP transition occurs, which completes in 30 to 40 seconds. For more information, see the "Events that Cause Fast Convergence" section on page 6-33.

## How CSUF Works

CSUF ensures that one link in the stack is elected as the path to the root. As shown in Figure 6-7, Switches A, B, and C are cascaded through the Gigastack GBIC to form a multidrop backbone, which communicates control and data traffic across the switches at the access layer. The switches in the stack use their stack ports to communicate with each other and to connect to the stack backbone; stack ports are always in the STP forwarding state. The stack root port on Switch A provides the path to the root of the spanning tree; the alternate stack root ports on Switches B and C can provide an alternate path to the spanning-tree root if the current stack root switch fails or its link to the spanning-tree root fails.

Link A, the root link, is in the STP forwarding state; Links B and C are alternate redundant links that are in the STP blocking state. If Switch A fails, if its stack root port fails, or if Link A fails, CSUF selects either the Switch B or Switch C alternate stack root port and puts it into the forwarding state in less than 1 second.

***Figure 6-7 Cross-Stack UplinkFast Topology***




CSUF implements the Stack Membership Discovery Protocol and the Fast Uplink Transition Protocol. Using the Stack Membership Discovery Protocol, all stack switches build a neighbor list of stack members through the receipt of discovery hello packets. When certain link loss or STP events occur (described in the "Events that Cause Fast Convergence" section on page 6-33), the Fast Uplink Transition Protocol uses the neighbor list to send fast-transition requests on the stack port to stack members.

The switch sending the fast-transition request needs to do a fast transition to the forwarding state of a port that it has chosen as the root port, and it must obtain an acknowledgement from each stack switch before performing the fast transition.

Each switch in the stack determines if the sending switch is a better choice than itself to be the stack root of this STP instance by comparing STP root, cost, and bridge ID. If the sending switch is the best choice as the stack root, the switch in the stack returns an acknowledgement; otherwise, it does not respond to the sending switch (drops the packet) and prevents the sending switch from receiving acknowledgements from all stack switches.

When acknowledgements are received from all stack switches, the Fast Uplink Transition Protocol on the sending switch immediately transitions its alternate stack root port to the forwarding state. If acknowledgements from all stack switches are not obtained by the sending switch, the normal STP transitions (blocking, listening, learning, forwarding) take place, and the spanning-tree topology converges at its normal rate (2 * forward-delay time + max-age time).

The Fast Uplink Transition Protocol is implemented on a per-VLAN basis and affects only one STP instance at a time.

## Events that Cause Fast Convergence

Depending on the network event or failure, fast convergence provided by CSUF might or might not occur.

Fast convergence (within 2 seconds under normal network conditions) occurs under these circumstances:

- The stack root port link goes down.

  If two switches in the stack have alternate paths to the root, only one of the switches performs the fast transition.

- The failed link, which connected the stack root to the STP root, comes back up.
- A network reconfiguration causes a new stack root switch to be selected.

- A network reconfiguration causes a new port on the current stack root switch to be chosen as the stack root port.

**Note** The fast transition might not occur if multiple events occur simultaneously. For example, if a stack member switch is powered down, and at the same time, a link connecting the stack root to the STP root comes back up, the normal STP convergence occurs.

Normal STP convergence (30 to 40 seconds) occurs under these conditions:

- The stack root switch is powered down or the software failed.
- The stack root switch, which was powered down or failed, is powered up.
- A new switch, which might become the stack root, is added to the stack.
- A switch other than the stack root is powered down or failed.
- A link fails between stack ports on the multidrop backbone.

**Note** The fast transition of CSUF depends on the amount of network traffic and how you connect the GigaStack GBICs across the stack switches. Because the Fast Uplink Transition Protocol only waits 2 seconds to receive acknowledgements from all stack switches, heavy network traffic might prevent the fast transition from occurring within this time frame. Instead of a fast transition, the normal STP convergence then occurs.

## Limitations

The following limitations apply to CSUF:

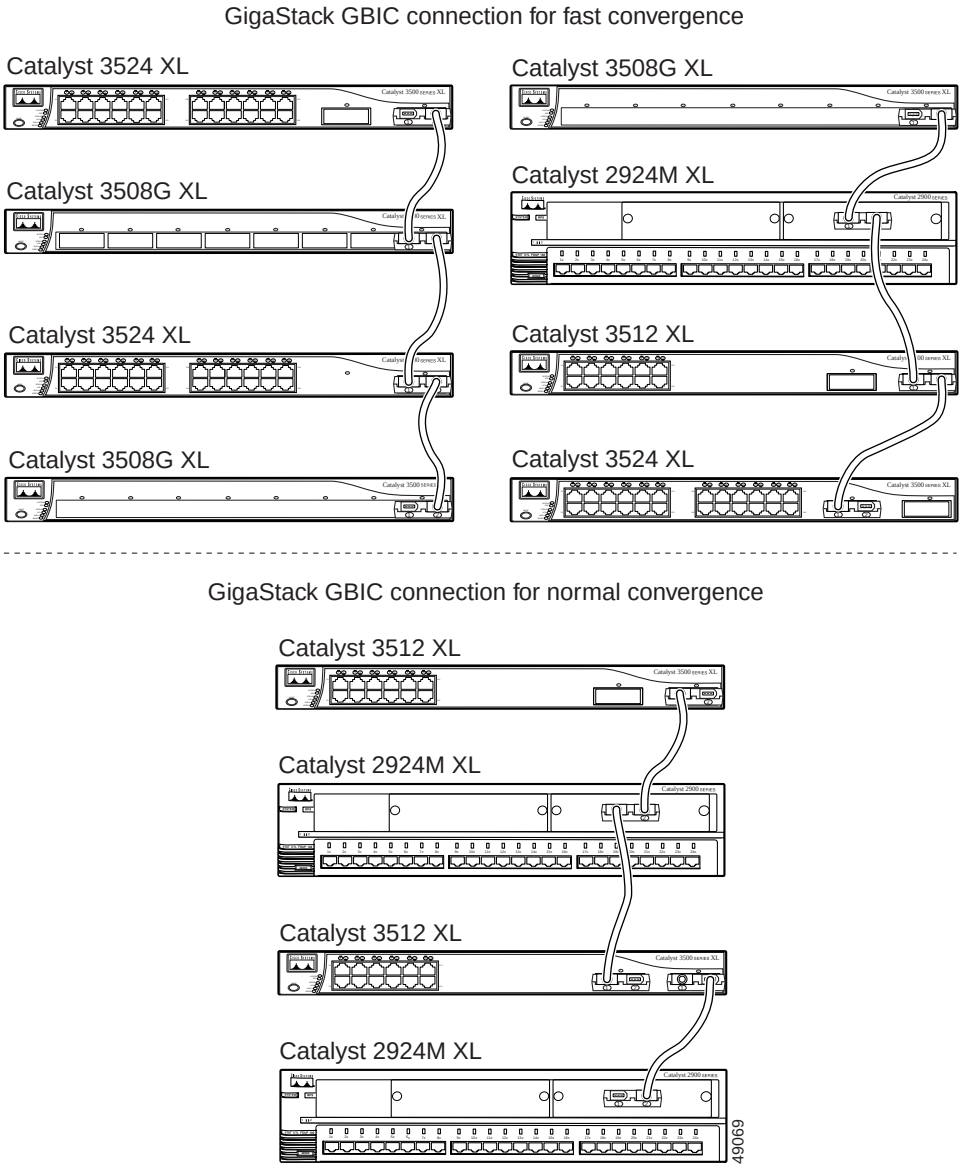
- CSUF uses the Gigastack GBIC and runs on all Catalyst 3500 XL switches but only on modular Catalyst 2900 XL switches.
- Up to nine stack switches can be connected through their stack ports to the multidrop backbone. Only one stack port per switch is supported.
- Each stack switch can be connected to the STP backbone through one uplink.
- Up to 64 VLANs are supported.

## Connecting the Stack Ports

A fast transition occurs across the stack of switches if the multidrop backbone connections are a continuous link from one GigaStack GBIC to another as shown in Figure 6-8. In addition, follow these guidelines:

- Do not connect alternate stack root ports to stack ports.
- Only one stack port is supported per switch.
- All stack ports on the stack of switches must be connected to the multidrop backbone.
- You can connect the open ports on the top and bottom GigaStack GBICs within the same stack to form a redundant link.

***Figure 6-8 GigaStack GBIC Connections and STP Convergence***



## Configuring Cross-Stack UplinkFast

Before enabling CSUF, make sure your stack switches are properly connected. For more information, see the "Connecting the Stack Ports" section on page 6-35.

Beginning in privileged EXEC mode, follow these steps to enable CSUF:

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **spanning-tree uplinkfast [max-update-rate** *pkts-per-second*] | Enable UplinkFast on the switch.<br>(Optional) For **max-update-rate** *pkts-per-second*, specify the number of packets per second at which update packets are sent. The range is 0 to 65535; the default is 150 packets per second. |
| Step 1 | **interface** *interface-id* | Enter interface configuration mode, and specify the GBIC interface on which to enable CSUF. |
| Step 2 | **spanning-tree stack-port** | Enable CSUF on only one stack-port GBIC interface.<br>The stack port connects to GigaStack GBIC multidrop backbone. If you try to enable CSUF on a Fast Ethernet or a copper-based Gigabit Ethernet port, you receive an error message.<br>If CSUF is already enabled on an interface and you try to enable it on another interface, you receive an error message. You must disable CSUF on the first interface before enabling it on a new interface.<br>Use this command only on access switches. |
| Step 3 | **end** | Return to privileged EXEC mode. |
| Step 4 | **show spanning-tree** | Verify your entries. |
| Step 5 | **copy running-config startup-config** | (Optional) Save your entries in the configuration file. |

To disable CSUF on an interface, use the **no spanning-tree stack-port** interface configuration command. To disable UplinkFast on the switch, use the **no spanning-tree uplinkfast** global configuration command.

# Changing the STP Parameters for a VLAN

The root switch for each VLAN is the switch with the highest priority and transmits topology frames to other switches in the spanning tree. You can change the root parameters for the VLANs on a selected switch. The following options define how your switch responds when STP reconfigures itself.

| | |
|---|---|
| Protocol | Implementation of STP to use: IBM or IEEE. The default is IEEE. |
| Priority | Value (0 to 65535) used to identify the root switch. The switch with the **lowest value** has the highest priority and is selected as the root. |
| Max age | Number of seconds (6 to 200) a switch waits without receiving STP configuration messages before attempting a reconfiguration. This parameter takes effect when a switch is operating as the root switch. Switches not acting as the root use the root-switch Max age parameter. |
| Hello Time | Number of seconds (1 to 10) between the transmission of hello messages, which indicate that the switch is active. Switches not acting as a root switch use the root-switch Hello-time value. |
| Forward Delay | Number of seconds (4 to 200) a port waits before changing from its STP learning and listening states to the forwarding state. This wait is necessary so that other switches on the network ensure that no loop is formed before they allow the port to forward packets. |

## Changing the STP Implementation

Beginning in privileged EXEC mode, follow these steps to change the STP implementation. The *stp-list* is the list of VLANs to which the STP command applies.

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **spanning-tree** [**vlan** *stp-list*] **protocol** {**ieee** \| **ibm**} | Specify the STP implementation to be used for a spanning-tree instance. |
| Step 3 | **end** | Return to privileged EXEC mode. |
| Step 4 | **show spanning-tree** | Verify your entry. |

## Changing the Switch Priority

Beginning in privileged EXEC mode, follow these steps to change the switch priority and affect which switch is the root switch. The *stp-list* is the list of VLANs to which the STP command applies.

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **spanning-tree** [**vlan** *stp-list*] **priority** *bridge-priority* | Configure the switch priority for the specified spanning-tree instance.<br>Enter a number from 0 to 65535; the lower the number, the more likely the switch will be chosen as the root switch. |
| Step 3 | **end** | Return to privileged EXEC mode. |
| Step 4 | **show spanning-tree** | Verify your entry. |

## Changing the BPDU Message Interval

Beginning in privileged EXEC mode, follow these steps to change the BPDU message interval (max age time). The *stp-list* is the list of VLANs to which the STP command applies.

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **spanning-tree** [**vlan** *stp-list*] **max-age** *seconds* | Specify the interval between messages the spanning tree receives from the root switch.<br>The maximum age is the number of seconds a switch waits without receiving STP configuration messages before attempting a reconfiguration. Enter a number from 6 to 200. |
| Step 3 | **end** | Return to privileged EXEC mode. |
| Step 4 | **show spanning-tree** | Verify your entry. |

## Changing the Hello BPDU Interval

Beginning in privileged EXEC mode, follow these steps to change the hello BPDU interval (hello time). The *stp-list* is the list of VLANs to which the STP command applies.

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **spanning-tree** [**vlan** *stp-list*] **hello-time** *seconds* | Specify the interval between hello BPDUs.<br>Hello messages indicate that the switch is active. Enter a number from 1 to 10. |
| Step 3 | **end** | Return to privileged EXEC mode. |
| Step 4 | **show spanning-tree** | Verify your entry. |

## Changing the Forwarding Delay Time

Beginning in privileged EXEC mode, follow these steps to change the forwarding delay time. The *stp-list* is the list of VLANs to which the STP command applies.

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **spanning-tree** [**vlan** *stp-list*] **forward-time** *seconds* | Specify the forwarding time for the specified spanning-tree instance.<br>The forward delay is the number of seconds a port waits before changing from its STP learning and listening states to the forwarding state. Enter a number from 4 to 200.<br>The default for IEEE is 15 seconds; the default for IBM is 4 seconds. |
| Step 3 | **end** | Return to privileged EXEC mode. |
| Step 4 | **show spanning-tree** | Verify your entry. |

# STP Port States

When a port is not forwarding due to STP, it can be in one of these states:

- Blocking—Port is not participating in the frame-forwarding process and is not learning new addresses.
- Listening—Port is not participating in the frame-forwarding process, but is progressing towards a forwarding state. The port is not learning addresses.
- Learning—Port is not forwarding frames but is learning addresses.
- Forwarding—Port is forwarding frames and learning addresses.
- Disabled—Port has been removed from STP operation.
- Down—Port has no physical link.
- Broken—One end of the link is configured as an access port, and the other end is configured as an 802.1Q trunk port, or both ends of the link are configured as 802.1Q trunk ports but have different native VLAN IDs.

## Enabling the Port Fast Feature

The Port Fast feature brings a port directly from a blocking state into a forwarding state. This feature is useful when a connected server or workstation times out because its port is going through the normal cycle of STP status changes. A port with Port Fast enabled only goes through the normal cycle of STP status changes when the switch is restarted.

**Caution** Enabling this feature on a port connected to a switch or hub could prevent STP from detecting and disabling loops in your network, and this could cause broadcast storms and address-learning problems.

You can modify the following Port Fast parameters:

- Port Fast—Enable to bring the port more quickly to an STP forwarding state.
- Path Cost —A lower path cost represents higher-speed transmission. This can affect which port remains enabled in the event of a loop.

  Enter a number from 1 to 65535. The default is 100 for 10 Mbps, 19 for 100 Mbps, 14 for 155 Mbps (ATM), 4 for 1 Gbps, 2 for 10 Gbps, and 1 for interfaces with speeds greater than 10 Gbps.
- Priority —Number used to set the priority for a port. A higher number has higher priority. Enter a number from 0 to 65535.

Enabling this feature on a port connected to a switch or hub could prevent STP from detecting and disabling loops in your network. Beginning in privileged EXEC mode, follow these steps to enable the Port Fast feature:

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

## Changing the Path Cost

Beginning in privileged EXEC mode, follow these steps to change the path cost for STP calculations. The STP command applies to the *stp-list*.

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **interface** *interface* | Enter interface configuration mode, and enter the port to be configured. |
| Step 3 | **spanning-tree** [**vlan** *stp-list*] **cost** *cost* | Configure the path cost for the specified spanning-tree instance.<br>Enter a number from 1 to 65535. |
| Step 4 | **end** | Return to privileged EXEC mode. |
| Step 5 | **show running-config** | Verify your entry. |

## Changing the Port Priority

Beginning in privileged EXEC mode, follow these steps to change the port priority, which is used when two switches tie for position as the root switch. The *stp-list* is the list of VLANs to which the STP command applies.

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **interface** *interface* | Enter interface configuration mode, and enter the port to be configured. |
| Step 3 | **spanning-tree** [**vlan** *stp-list*] **port-priority** *port-priority* | Configure the port priority for a specified instance of STP.<br>Enter a number from 0 to 255. The lower the number, the higher the priority. |
| Step 4 | **end** | Return to privileged EXEC mode. |
| Step 5 | **show running-config** | Verify your entry. |

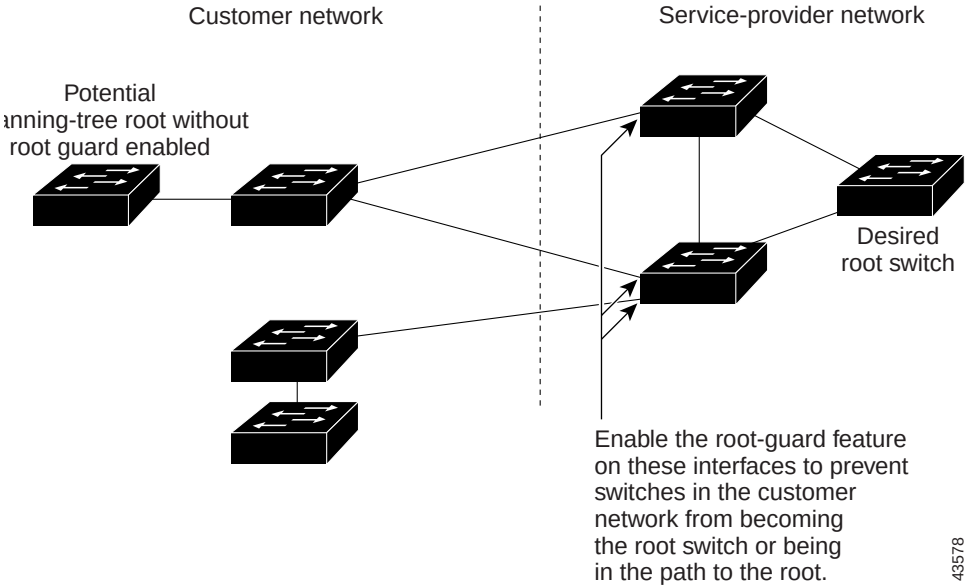
# Configuring STP Root Guard

The Layer 2 network of a service provider (SP) can include many connections to switches that are not owned by the SP. In such a topology, STP can reconfigure itself and select a *customer switch* as the STP root switch, as shown in Figure 6-9. You can avoid this situation by configuring the root-guard feature on interfaces that connect to switches outside of your customer's network. If STP calculations cause an interface in the customer network to be selected as the root port, root guard then places the interface into the root-inconsistent (blocked) state to prevent the customer switch from becoming the root switch or being in the path to the root.

If a switch outside the network becomes the root switch, the interface is blocked (root-inconsistent state), and STP selects a new root switch. The customer switch does not become the root switch and is not in the path to the root.

**Caution** Misuse of this feature can cause a loss of connectivity.

***Figure 6-9 STP in a Service Provider Network***



Root guard enabled on a port applies to all the VLANs that the port belongs to. Each VLAN has its own instance of STP.

Beginning in privileged EXEC mode, follow these steps to set root guard on a port:

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **interface** *interface* | Enter interface configuration mode, and enter the port to be configured. |
| Step 3 | **spanning-tree rootguard** | Enable root guard on the port. |
| Step 4 | **end** | Return to privileged EXEC mode. |
| Step 5 | **show running-config** | Verify that the port is configured for root guard. |

Use the **no** version of the **spanning-tree rootguard** command to disable the root guard feature.

# Managing the ARP Table

To communicate with a device (over Ethernet, for example), the software first must determine the 48-bit MAC or the local data link address of that device. The process of determining the local data link address from an IP address is called *address resolution*.

The Address Resolution Protocol (ARP) associates a host IP address with the corresponding media or MAC addresses and the VLAN ID. Taking an IP address as input, ARP determines the associated MAC address. Once a MAC address is determined, the IP-MAC address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network. Encapsulation of IP datagrams and ARP requests and replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP). By default, standard Ethernet-style ARP encapsulation (represented by the **arpa** keyword) is enabled on the IP interface.

ARP entries added manually to the table do not age and must be manually removed.

For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

# Controlling IP Multicast Packets through CGMP

CGMP reduces the unnecessary flooding of IP multicast packets by limiting the transmission of these packets to CGMP clients that request them. The Fast Leave feature accelerates the removal of unused CGMP groups. By default, CGMP is enabled, and the Fast Leave feature is disabled.

End stations issue join messages to become part of a CGMP group and issue leave messages to leave the group. The membership of these groups is managed by the switch and by connected routers through the further exchange of CGMP messages.

CGMP groups are maintained on a per-VLAN basis: a multicast IP address packet can be forwarded to one list of ports in one VLAN and to a different list of ports in another VLAN. When a CGMP group is added, it is added on a per-VLAN, per-group basis. When a CGMP group is removed, it is only removed in a given VLAN.

**Note** The same multicast MAC addresses cannot belong to both CGMP and Multicast VLAN Registration (MVR) groups. CGMP does not dynamically learn addresses that are MVR group members. If you want CGMP to learn an address that is already an MVR group member, remove the address from the MVR group.

Conversely, you cannot add an address to an MVR group if it is already a CGMP group member. If you want an address that is already a CGMP group member to be an MVR group member, remove the address from the CGMP group, and then statically add it to the MVR group. For information about MVR, see the "Configuring MVR" section on page 6-49.

# Enabling the Fast Leave Feature

The CGMP Fast Leave feature reduces the delay when group members leave groups. When an end station requests to leave a CGMP group, the group remains enabled for that VLAN until all members have requested to leave. With the Fast Leave feature enabled, the switch immediately verifies if there are other group members attached to its ports. If there are no other members, the switch removes the port from the group. If there are no other ports in the group, the switch sends a message to routers connected to the VLAN to delete the entire group.

The Fast Leave feature functions only if CGMP is enabled. The client must be running IGMP version 2 for the Fast Leave feature to function properly.

Beginning in privileged EXEC mode, follow these steps to enable the CGMP Fast Leave feature:

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

# Disabling the CGMP Fast Leave Feature

Beginning in privileged EXEC mode, follow these steps to disable the CGMP Fast Leave feature:

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **no cgmp leave-processing** | Disable CGMP and CGMP Fast Leave. |
| Step 3 | **end** | Return to privileged EXEC mode. |
| Step 4 | **show running-config** | Verify your entry. |

# Changing the CGMP Router Hold-Time

The router hold-time is the number of seconds the switch waits before removing (aging) a router entry and ceasing to exchange messages with the router. If it is the last router entry in a VLAN, all CGMP groups on that VLAN are removed. You can thus enter a lower router hold-time to accelerate the removal of CGMP groups.

**Note** You can remove router ports before the router hold-time has expired.

Beginning in privileged EXEC mode, follow these steps to change the router hold-time.

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **cgmp holdtime 400** | Configure the number of seconds the switch waits before dropping a router entry. |
| Step 3 | **end** | Return to privileged EXEC mode. |
| Step 4 | **show running-config** | Verify your entry. |

# Removing Multicast Groups

You can reduce the forwarding of IP multicast packets by removing groups from the Current Multicast Groups table. Each entry in the table consists of the VLAN, IGMP multicast address, and ports.

You can use the CLI to clear all CGMP groups, all CGMP groups in a VLAN, or all routers, their ports, and their expiration times. Beginning in privileged EXEC mode, follow these steps to remove all multicast groups.

| | Command | Purpose |
|---|---|---|
| Step 1 | **clear cgmp group** | Clear all CGMP groups on all VLANs on the switch. |
| Step 2 | **show cgmp** | Verify your entry by displaying CGMP information. |

# Configuring MVR

Multicast VLAN Registration (MVR) is designed for applications using wide-scale deployment of multicast traffic (for example, broadcast of multiple television channels) across an Ethernet ring-based service provider network. MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the network-wide multicast VLAN. It allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. This provides the ability to continuously send multicast streams in the multicast VLAN, but to isolate the streams from the subscriber VLANs for bandwidth and security reasons.

MVR assumes that subscriber ports subscribe and unsubscribe (join and leave) these multicast streams by sending out Internet Group Management Protocol (IGMP) join and leave messages. These messages can originate from an IGMP version-2-compatible set-top box with an Ethernet connection or from a PC capable of generating IGMP version-2 messages. The switch CPU identifies IP multicast streams and their associated MAC addresses in the switch forwarding table, intercepts the IGMP messages, and modifies the forwarding table to include or remove the subscriber as a receiver of the multicast stream. This forwarding behavior selectively allows traffic to cross between the two VLANs.

Because MVR does not support IGMP dynamic joins, the user or administrator must configure static multicast addresses on the router.

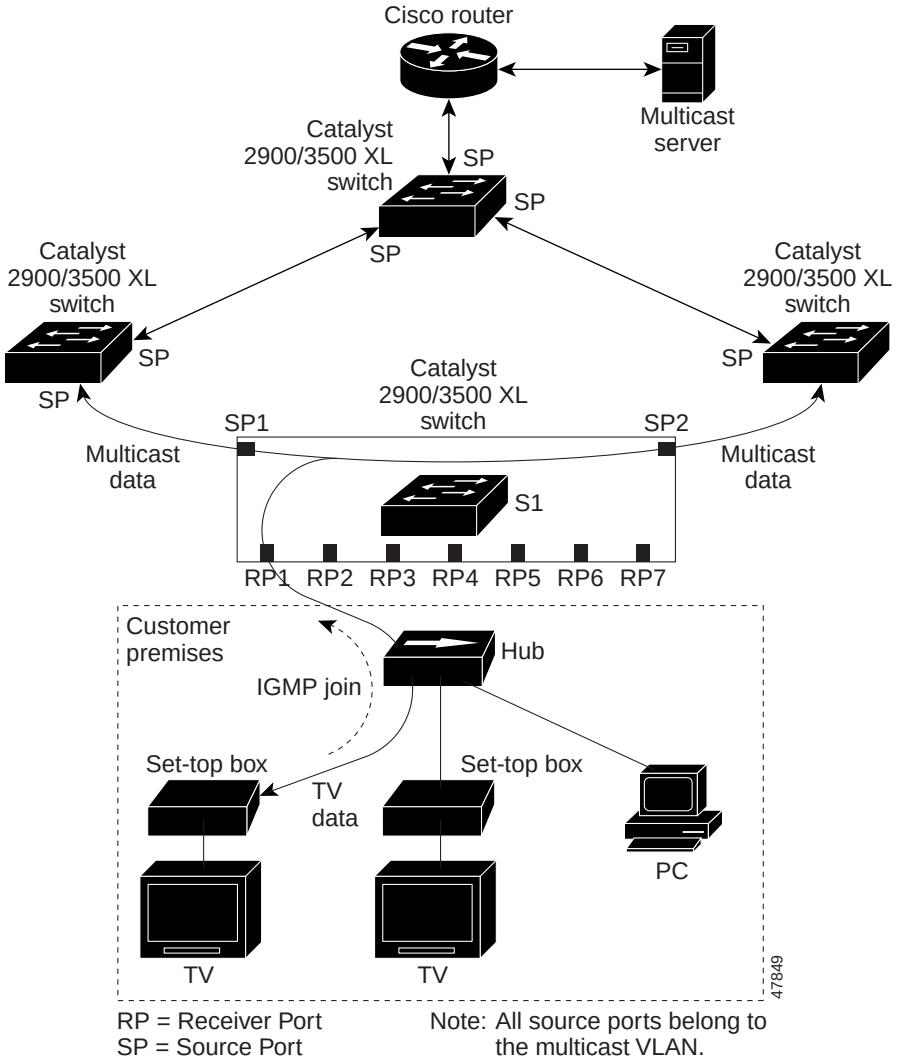
## Using MVR in a Multicast Television Application

In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port. (See Figure 6-10.) DHCP assigns an IP address to the set-top box or the PC. When a subscriber selects a channel, the set-top box or PC sends an IGMP report to the access layer switch (S1 switch) to join the appropriate multicast. If the IGMP report matches one of the configured multicast MAC addresses, the switch CPU modifies the hardware address table to include this receiver port and VLAN as a forwarding destination of the specified multicast stream when it is received from the multicast VLAN over the source port.

When a subscriber changes channels or turns off the television, the set-top box sends an IGMP leave message for the multicast stream. The switch CPU sends an IGMP group-specific query through the receiver port VLAN. If there is another

set-top box in the VLAN still subscribing to this group, that set-top box must respond within the maximum response time. If the CPU does not receive a response, it eliminates the receiver port as a forwarding destination for this group.

***Figure 6-10 Multicast VLAN Registration Example***



MVR eliminates the need to duplicate television-channel multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only once around the VLAN trunk—only on the multicast VLAN. Although the IGMP leave and join messages originate with a subscriber, they appear to be initiated by a port in the multicast VLAN rather than in the VLAN to which the subscriber port is assigned. These messages dynamically register for streams of multicast traffic in the multicast VLAN on the switch. The access layer switch (S1 switch) modifies the forwarding behavior to allow the traffic to be forwarded from the multicast VLAN to the subscriber port in a different VLAN, selectively allowing traffic to cross between two VLANs.

IGMP reports are sent to the same MAC addresses as the multicast data. The S1 CPU must capture all IGMP join and leave messages from subscriber ports. Because the Catalyst 2900 and Catalyst 3500 hardware cannot distinguish IP multicast data packets from IP multicast packets carrying IGMP protocol data, all packets from subscriber ports destined for the configured multicast MAC addresses are forwarded to the switch CPU, which distinguishes IGMP packets from regular multicast traffic.

# Configuration Guidelines and Limitations

Follow these guidelines when configuring MVR:

- All receiver ports on a switch must belong to the same VLAN and must not be trunk ports.
- In applications where the receiver ports represent subscribers to a service, we recommend configuring receiver ports as follows:
  - Enable protected port on all receiver ports to isolate the ports from one another.
  - Enable port blocking on all receiver ports to prevent unknown unicast and multicast packets.
- Before configuring MVR groups, configure all MVR parameters, including the multicast VLAN. If you want to change the MVR parameters after MVR groups have been configured, follow these steps:
  a. Enter the **no mvr** command to disable MVR.
  b. Enter the **mvr vlan** <*vlan-id*> command to change the multicast VLAN.

c. The maximum number of mvr entries is determined by the switch hardware. Each MVR group represents a TV channel.

d. Enter the **mvr** command to enable MVR. You do not need to reconfigure the MVR groups. The switch uses the MVR groups when you re-enable MVR.

- Each channel is one multicast stream destined for a unique IP multicast address.
- Make sure the router is statically configured to forward multicast traffic for the MVR groups to the switch. The router should not depend on IGMP join requests from hosts (forwarded by the switch) to forward multicast traffic to the switch.
- The receiver VLAN is the VLAN to which the first configured receiver port belongs. If the first receiver port is a dynamic port with an unassigned VLAN, it becomes an inactive receiver port and does not take part in MVR unless it is assigned to the receiver VLAN. The receiver VLAN is reset whenever there are no remaining receiver ports on the switch (active or inactive), which means that the receiver VLAN might change every time the first receiver port is configured.

MVR implementation has the following limitations:

- MVR is supported on only modular Catalyst 2900 XL switches.
- Unknown multicast packets, unknown unicast packets, and broadcast packets are leaked from the multicast VLAN to the receiver ports.
- MVR does not support IP-address aliasing and therefore requires that each IP multicast address maps to only one Layer 2 MAC address. In MVR, you cannot configure multiple IP addresses that map to the same MAC address.
- The same multicast MAC addresses cannot belong to both CGMP and MVR groups. CGMP does not dynamically learn addresses that are MVR group members. If you want CGMP to learn an address that is already an MVR group member, remove the address from the MVR group.

  Conversely, you cannot add an address to an MVR group if it is already a CGMP group member. If you want an address that is already a CGMP group member to be an MVR group member, remove the address from the CGMP group, and then statically add it to the MVR group. For information about CGMP, see the "Controlling IP Multicast Packets through CGMP" section on page 6-46.

# Setting MVR Parameters

You do not need to set MVR parameters if you choose to use the default settings. If you do want to change the default parameters, you must do so before enabling MVR.

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

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **mvr querytime** *value* | (Optional) Define the maximum time to wait for IGMP report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a second. The default is 5 tenths or one-half second. |
| Step 3 | **mvr vlan** *vlan-id* | (Optional) Specify the VLAN in which multicast data will be received; all source ports must belong to this VLAN. The default is VLAN 1. |
| Step 4 | **interface** *interface* | Enter interface configuration mode, and enter the type and number of the port to configure, for example, fastethernet 0/1. |
| Step 5 | **mvr threshold** *value* | (Optional) Define the maximum of multicast data packets received on a receiver port before it is administratively shut down. The default is 20. |
| Step 6 | **end** | Exit configuration mode. |
| Step 7 | **show mvr**<br>**show mvr interface** | Verify the configuration. |
| Step 8 | **copy running-config startup-config** | Save your configuration changes to nonvolatile RAM (NVRAM). |

# Configuring MVR

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

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **mvr** | Enable MVR on the switch. |
| Step 3 | **mvr group** *ip-address* [*count*] | Configure an IP multicast address on the switch or use the *count* parameter to configure a contiguous series of IP addresses. Any multicast data sent to this address is sent to all source ports on the switch and all receiver ports that have elected to receive data on that multicast address. Each multicast address would correspond to one television channel.<br>**Note** Each IP address translates to a multicast 48-bit MAC address. If an IP address being configured translates (aliases) to a previously configured MAC address, the command fails. |
| Step 4 | **interface** *interface* | Enter interface configuration mode, and enter the type and number of the port to configure, for example, fastethernet 0/1. |
| Step 5 | **mvr type** *value* | Configure the port as either an MVR receiver port or an MVR source port.<br>• Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by using IGMP leave and join messages.<br>All receiver ports on a switch must belong to the same VLAN. In most cases, you should configure receiver ports as protected ports with port blocking enabled.<br>• Configure uplink ports that receive and send multicast data as source ports. All source ports on a switch belong to the single multicast VLAN. |

| | Command | Purpose |
|---|---|---|
| Step 6 | **mvr immediate** | (Optional) Enables the Immediate Leave feature of MVR on the port.<br>**Note** This command applies only to receiver ports and should only be enabled on receiver ports to which a single receiver device is connected. |
| Step 7 | **end** | Exit configuration mode. |
| Step 8 | **show mvr**<br>**show mvr interface**<br>**show mvr members** | Verify the configuration. |
| Step 9 | **copy running-config startup-config** | Save your configuration changes to NVRAM. |

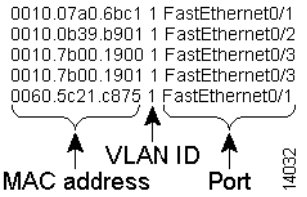
# Managing the MAC Address Tables

You can manage the MAC address tables that the switch uses to forward traffic between ports. All MAC addresses in the address tables are associated with one or more ports. These MAC tables include the following types of addresses:

- Dynamic address: a source MAC address that the switch learns and then drops when it is not in use.
- Secure address: a manually entered unicast address that is usually associated with a secured port. Secure addresses do not age.
- Static address: a manually entered unicast or multicast address that does not age and that is not lost when the switch resets.

The address tables list the destination MAC address and the VLAN ID, module, and port number associated with the address. Figure 6-11 shows an example list of addresses as they would appear in the dynamic, secure, or static address table.

***Figure 6-11 Contents of the Address Table***




# MAC Addresses and VLANs

All addresses are associated with a VLAN. An address can exist in more than one VLAN and have different destinations in each. Multicast addresses, for example, could be forwarded to port 1 in VLAN 1 and ports 9, 10, and 11 in VLAN 5.

Each VLAN maintains its own logical address table. A known address in one VLAN is unknown in another until it is learned or statically associated with a port in the other VLAN. An address can be secure in one VLAN and dynamic in another. Addresses that are statically entered in one VLAN must be static addresses in all other VLANs.

# Changing the Address Aging Time

Dynamic addresses are source MAC addresses that the switch learns and then drops when they are not in use. The aging time parameter defines how long the switch retains unseen addresses in the table. This parameter applies to all VLANs.

Setting too short an aging time can cause addresses to be prematurely removed from the table. Then when the switch receives a packet for an unknown destination, it floods the packet to all ports in the same VLAN as the receiving port. This unnecessary flooding can impact performance. Setting too long an aging time can cause the address table to be filled with unused addresses; it can cause delays in establishing connectivity when a workstation is moved to a new port.

Beginning in privileged EXEC mode, follow these steps to configure the dynamic address table aging time.

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **mac-address-table aging-time** *seconds* | 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. |
| Step 3 | **end** | Return to privileged EXEC mode. |
| Step 4 | **show mac-address-table aging-time** | Verify your entry. |

# Removing Dynamic Address Entries

Beginning in privileged EXEC mode, follow these steps to remove a dynamic address entry:

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **no mac-address-table dynamic** *hw-addr* | Enter the MAC address to be removed from dynamic MAC address table. |
| Step 3 | **end** | Return to privileged EXEC mode. |
| Step 4 | **show mac-address-table** | Verify your entry. |

You can remove all dynamic entries by using the **clear mac-address-table dynamic** command in privileged EXEC mode.

# Adding Secure Addresses

The secure address table contains secure MAC addresses and their associated ports and VLANs. A secure address is a manually entered unicast address that is forwarded to only one port per VLAN. If you enter an address that is already assigned to another port, the switch reassigns the secure address to the new port.

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

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

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

# Removing Secure Addresses

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

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **no mac-address-table secure** *hw-addr* **vlan** *vlan-id* | Enter the secure MAC address, its associated port, and the VLAN ID to be removed. |
| Step 3 | **end** | Return to privileged EXEC mode. |
| Step 4 | **show mac-address-table secure** | Verify your entry. |

You can remove all secure addresses by using the **clear mac-address-table secure** command in privileged EXEC mode.

# Adding Static Addresses

A static address has the following characteristics:

- It is manually entered in the address table and must be manually removed.
- It can be a unicast or multicast address.
- It does not age and is retained when the switch restarts.

You can determine how a port that receives a packet forwards it to another port for transmission. Because all ports are associated with at least one VLAN, the switch acquires the VLAN ID for the address from the ports that you select on the forwarding map.

A static address in one VLAN must be a static address in other VLANs. A packet with a static address that arrives on a VLAN where it has not been statically entered is flooded to all ports and not learned.

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

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

Beginning in privileged EXEC mode, follow these steps to add a static address:

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

# Removing Static Addresses

Beginning in privileged EXEC mode, follow these steps to remove a static address:

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **no mac-address-table static** *hw-addr* **in-port** *in-port* **out-port-list** *out-port-list* **vlan** *vlan-id* | Enter the static MAC address, the input port, the ports to which it can be forwarded, and the VLAN ID to be removed. |
| Step 3 | **end** | Return to privileged EXEC mode. |
| Step 4 | **show mac-address-table static** | Verify your entry. |

You can remove all secure addresses by using the **clear mac-address-table static** command in privileged EXEC mode.

## Configuring Static Addresses for EtherChannel Port Groups

Follow these rules if you are configuring a static address to forward to ports in an EtherChannel port group:

- For default source-based port groups, configure the static address to forward to *all ports* in the port group to eliminate lost packets.
- For destination-based port groups, configure the address to forward to *only one port* in the port group to avoid the transmission of duplicate packets.

# Configuring TACACS+

The Terminal Access Controller Access Control System Plus (TACACS+) provides the means to manage network security (authentication, authorization, and accounting [AAA]) from a server. This section describes how TACACS+ works and how you can configure it. For complete syntax and usage information for the commands described in this chapter, refer to the *Cisco IOS Release 12.0 Security Command Reference*.

You can only configure this feature by using the CLI; you cannot configure it through the Cluster Management Suite.

In large enterprise networks, the task of administering passwords on each device can be simplified by centralizing user authentication on a server. TACACS+ is an access-control protocol that allows a switch to authenticate all login attempts through a central server. The network administrator configures the switch with the address of the TACACS+ server, and the switch and the server exchange messages to authenticate each user before allowing access to the management console.

TACACS+ consists of three services: authentication, authorization, and accounting. Authentication determines who the user is and whether or not the user is allowed access to the switch. Authorization is the action of determining what the user is allowed to do on the system. Accounting is the action of collecting data related to resource usage.

The TACACS+ feature is disabled by default. However, you can enable and configure it by using the CLI. You can access the CLI through the console port or through Telnet. To prevent a lapse in security, you cannot configure TACACS+ through a network-management application. When enabled, TACACS+ can authenticate users accessing the switch through the CLI.

**Note** Although the TACACS+ configuration is performed through the CLI, the TACACS+ server authenticates HTTP connections that have been configured with a privilege level of 15.

# Configuring the TACACS+ Server Host

Use the **tacacs-server host** command to specify the names of the IP host or hosts maintaining an AAA/TACACS+ server. On TACACS+ servers, you can configure the following additional options:

- Number of seconds that the switch waits while trying to contact the server before timing out.
- Encryption key to encrypt and decrypt all traffic between the router and the daemon.
- Number of attempts that a user can make when entering a command that is being authenticated by TACACS+.

Beginning in privileged EXEC mode, follow these steps to configure the TACACS+ server:

| | Command | Purpose |
|---|---|---|
| Step 1 | **tacacs-server host** *name* [**timeout** *integer*] [**key** *string*] | Define a TACACS+ host.<br>Entering the **timeout** and **key** parameters with this command overrides the global values that you can enter with the **tacacs-server timeout** (Step 3) and the **tacacs-server key** commands (Step 5). |
| Step 2 | **tacacs-server retransmit** *retries* | Enter the number of times the server searches the list of TACACS+ servers before stopping.<br>The default is two. |
| Step 3 | **tacacs-server timeout** *seconds* | Set the interval that the server waits for a TACACS+ server host to reply.<br>The default is 5 seconds. |
| Step 4 | **tacacs-server attempts** *count* | Set the number of login attempts that can be made on the line. |
| Step 5 | **tacacs-server key** *key* | Define a set of encryption keys for all of TACACS+ and communication between the access server and the TACACS daemon.<br>Repeat the command for each encryption key. |
| Step 6 | **exit** | Return to privileged EXEC mode. |
| Step 7 | **show tacacs** | Verify your entries. |

# Configuring Login Authentication

Beginning in privileged EXEC mode, follow these steps to configure login authentication by using AAA/TACACS+:

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **aaa new-model** | Enable AAA/TACACS+. |
| Step 3 | **aaa authentication login** {**default** \| *list-name*} *method1* [*method2...*] | Enable authentication at login, and create one or more lists of authentication methods. |
| Step 4 | **line** [**aux** \| **console** \| **tty** \| **vty**] *line-number* [*ending-line-number*] | Enter line configuration mode, and configure the lines to which you want to apply the authentication list. |
| Step 5 | **login authentication** {**default** \| *list-name*} | Apply the authentication list to a line or set of lines. |
| Step 6 | **exit** | Return to privileged EXEC mode. |
| Step 7 | **show running-config** | Verify your entries. |

The variable *list-name* is any character string used to name the list you are creating. The *method* variable refers to the actual methods the authentication algorithm tries, in the sequence entered. You can choose one of these methods:

- **line**—Uses the line password for authentication. You must define a line password before you can use this authentication method. Use the **password** *password* line configuration command.
- **local**—Uses the local username database for authentication. You must enter username information into the database. Use the **username** *password* global configuration command.
- **tacacs+—**Uses TACACS+ authentication. You must configure the TACACS+ server before you can use this authentication method. For more information, see the "Configuring the TACACS+ Server Host" section on page 6-62.

To create a default list that is used if **no list** is specified in the **login authentication** line configuration command, use the **default** keyword followed by the methods you want used in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication succeed even if all methods return an error, specify **none** as the final method in the command line.

# Specifying TACACS+ Authorization for EXEC Access and Network Services

You can use the **aaa authorization** global configuration command with the **tacacs+** keyword to set parameters that restrict a user's network access to Cisco IOS privilege mode (EXEC access) and to network services such as Serial Line Internet Protocol (SLIP), Point-to-Point Protocol (PPP) with Network Control Protocols (NCPs), and AppleTalk Remote Access (ARA).

The **aaa authorization exec tacacs+ local** command sets the following authorization parameters:

- Uses TACACS+ for EXEC access authorization if authentication was done using TACACS+.
- Uses the local database if authentication was not done using TACACS+.

**Note** Authorization is bypassed for authenticated users who login through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify TACACS+ authorization for EXEC access and network services:

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **aaa authorization network tacacs+** | Configure the switch for user TACACS+ authorization for all network-related service requests, including SLIP, PPP NCPs, and ARA protocols. |
| Step 3 | **aaa authorization exec tacacs+** | Configure the switch for user TACACS+ authorization to determine if the user is allowed EXEC access.<br>The **exec** keyword might return user profile information (such as **autocommand** information). |
| Step 4 | **exit** | Return to privileged EXEC mode. |

# Starting TACACS+ Accounting

You use the **aaa accounting** command with the **tacacs+** keyword to turn on TACACS+ accounting for each Cisco IOS privilege level and for network services.

Beginning in privileged EXEC mode, follow these steps to enable TACACS+ accounting:

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **aaa accounting exec start-stop tacacs+** | Enable TACACS+ accounting to send a start-record accounting notice at the beginning of an EXEC process and a stop-record at the end. |
| Step 3 | **aaa accounting network start-stop tacacs+** | Enable TACACS+ accounting for all network-related service requests, including SLIP, PPP, and PPP NCPs. |
| Step 4 | **exit** | Return to privileged EXEC mode. |

**Note** These commands are documented in the "Accounting and Billing Commands" chapter of the *Cisco IOS Release 12.0 Security Command Reference*.

# Configuring a Switch for Local AAA

You can configure AAA to operate without a server by setting the switch to implement AAA in local mode. The switch then verifies authentication and authorization. No accounting is available in this configuration.

Beginning in privileged EXEC mode, follow these steps to configure the switch for local AAA:

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **aaa new-model** | Enable AAA. |
| Step 3 | **aaa authentication login default local** | Set the login authorization to default to local. |
| Step 4 | **aaa authorization exec local** | Configure user AAA authorization for all network-related service requests, including SLIP, PPP NCPs, and ARA protocols. |
| Step 5 | **aaa authorization network local** | Configure user AAA authorization to determine if the user is allowed to run an EXEC shell. |
| Step 6 | **username** *name* **password** *password* **privilege** *level* | Enter the local database.<br>Repeat this command for each user. |