

Additional Features

This chapter describes these features:

- Fast EtherChannel Feature
- Spanning-Tree Protocol UplinkFast
- Bridge Groups
- TACACS+
- Configuration File Upload and Download

Fast EtherChannel Feature

The Fast EtherChannel feature provides parallel bandwidth of up to 400 Mbps (in full-duplex mode) between a Catalyst 1900 or Catalyst 2820 switch and another switch or host. It groups two Fast Ethernet interfaces into a single, logical transmission path. VLANs must be enabled to configure the Fast EtherChannel feature.

You can configure channels by using the standard command-line interface (CLI), the Simple Network Management Protocol (SNMP), or the switch web console.

Note The Fast EtherChannel feature is not available if you configured bridge groups on the switch. For more information on bridge groups, see the “Bridge Groups” section on page 3-15.

When a Fast EtherChannel link is formed, the port-channel interface is enabled. You can verify this by using the **show interfaces port-channel** command. The port-channel remains enabled until both ports lose the link.

Note The port status LEDs are amber during DISL negotiation and while the Fast EtherChannel links are forming.

Port Aggregation Protocol

The Port Aggregation Protocol (PAgP) facilitates the automatic creation of Fast EtherChannel links by sending packets between Fast EtherChannel-capable ports. The protocol allows directly connected devices to exchange information regarding the ability of ports to form a channel. Once PAgP identifies correctly paired Fast EtherChannel links, it groups the ports into a channel. The channel is then added to the spanning tree as a single bridge port.

The Fast EtherChannel feature includes four user-configurable channel modes: on, off, auto, and desirable. Each mode affects the way a port handles PAgP packets. By default, ports are in off mode. Table 3-1 describes each of the four modes.

Table 3-1 Channel Modes

Mode	Description
On	Forces the port to aggregate without negotiation.
Off	Prevents the port from aggregating without negotiation. (Default)
Auto	The port responds to PAgP packets it receives, but does not initiate PAgP packet negotiation.
Desirable	The port initiates negotiations with other ports by sending PAgP packets.

Both the auto and desirable modes allow ports to negotiate with connected ports to determine if they can form a channel, based on criteria such as trunking state, VLAN numbers, and so on.

The Fast EtherChannel mode only affects the two Fast Ethernet ports and is always the same on both of the Fast Ethernet ports.

Using a Template Port

Because port channel parameters are not stored separately from physical port parameters, you must use the parameters of one of the physical ports as a template for the parameters of the port channel. This is done by using the **port-channel template-port** command.

Note For more information on the command-line interface, see the *Catalyst 1900 Series and Catalyst 2820 Series Command Reference* (online only).

Once aggregated, the following template port parameters are applied to both ports automatically:

- For nontrunk ports:
 - VLAN number
 - Spanning-tree path cost
 - Spanning-tree port priority
- For trunk ports:
 - VLAN allowed list
 - VTP pruning-eligible list
 - Two spanning-tree path cost options and the VLAN assignment for each
 - Two spanning-tree port priority options and the VLAN assignment for each
 - DISL state

When a port-channel is enabled, the parameters of the template port are applied to both physical ports (port A and port B). Any changes made to the port-channel or either of the physical ports are applied to both member ports and the port-channel.

Frame Ordering and Load Balancing

When configuring the Fast EtherChannel feature with PAgP enabled, you can preserve the order of frames or maximize load balancing between the Fast EtherChannel links. If you preserve the order of the frames, the switch indicates to its Fast EtherChannel partner that it is a physical learner device.

A physical learner device learns MAC addresses by physical ports, and it selects those ports based on that information for its subsequent transmissions. The Fast EtherChannel partner is therefore required to use source-based distribution for frame transmission. This requirement means that the frames with the same source MAC address transmitted from the partner always use the same Fast EtherChannel physical port and that the same MAC address learned at the switch does not change.

Source-based distribution prevents the switch from misordering frame transmissions. If not configured to preserve the order, the partner can distribute traffic arbitrarily, and unicast traffic is transmitted on the link where the source address was last seen. This provides the maximum possible load balancing configuration.

A special case of source-based distribution is the hot-standby operation, which distributes all Fast EtherChannel traffic on one link. A partner that is capable of distributing different source addresses on different links results in a good load balancing configuration while still preserving the order of frames. Otherwise, traffic could be restricted to a single link. To configure the switch to preserve frame ordering, use the **port-channel preserve-order** command.

By default, frame ordering is not preserved. However, the chances for frame misordering is highly unlikely, even in this mode. This default setting maximizes load balancing on the switch.

When the Fast EtherChannel feature is configured with PAgP disabled, the switch cannot negotiate with its partner about its learning capability. Whether the switch preserves frame ordering or not depends on whether the Fast EtherChannel *partner* performs source-based distribution.

Packet Forwarding Behavior

This section describes the concepts involved with the packet forwarding behavior of a Catalyst 1900 or Catalyst 2820 switch configured to use the Fast EtherChannel feature.

- **Active port** — The Fast EtherChannel port member that has either the highest numerical value of hot-standby port priority or the lowest ifIndex value, if all member ports have the same port priority value.

The active port selection depends on the port-channel mode of the port. If the port-channel mode is on, the active port will be the link with the highest priority value. If the mode is Desirable or Auto, the active port is selected based on the priority of the links on the switch that has the higher Ethernet address. When two ports on the switch with the higher Ethernet address have the same priority, the port with the lower ifIndex is selected.

- **Flooded traffic**—Traffic that includes unknown unicast, unregistered multicast, and broadcast packets.
- **Known unicast traffic**—Traffic that has a known destination address on the switch.

Packet Forwarding for Flooded Traffic

For flooded traffic, the switch always transmits packets on the active link.

Packet Forwarding for Known Unicast Traffic

EtherChannel-capable devices forward known unicast traffic in one of these ways:

- **Forwards traffic on the physical port where the address is learned.**

In order to preserve frame ordering, an address should be learned on one port and remain on that port. This prevents packets with the same destination address from being forwarded by alternating between the two links. This is done by having the partner perform source-based distribution. This method is used by the Catalyst 1900 and Catalyst 2820 switches.

- **Forwards packets on either port, irrespective of the physical port where the address is learned.** The Catalyst 5000 switch can do this type of forwarding.

Adding Addresses

This section discusses adding static and multicast addresses to the switch. Addresses can be entered before or after a port-channel is formed. Use the **show interfaces port-channel** command to see whether the port-channel is enabled.

If you add an address when the port-channel is down, the address is added only to the physical link specified. If you add an address when the port-channel is up, the address can be added to the physical link or to the port-channel. If the address is added to the port-channel, the address is located as if it was added to the physical port associated with the active link.

Irrespective of where the address is added, when the port-channel is formed, packets destined for an address are forwarded on the physical port of the active port-channel link.

Deleting Static Addresses

If you delete an address when the port-channel is up, the address is deleted from the physical member ports and the port-channel link.

Fast EtherChannel Configuration Guidelines

Certain port configurations are not supported by the Fast EtherChannel feature. It cannot be enabled if either of the two Fast Ethernet ports is configured as follows:

- Port security is enabled.
- The port is a monitor port.
- The port is a dynamic VLAN port.
- Port Fast is enabled.
- The port is a network port.
- Bridge groups are enabled.

The trunk status of both Fast Ethernet ports must be identical (trunking or nontrunking) in order for the ports to aggregate.

Note The DISL state must be the same for both Fast Ethernet ports. Once the port-channel is formed, a change to the DISL state of one port is propagated to both ports in the port-channel.

To avoid network loops and other problems, Fast EtherChannel links do not form if they are not properly configured.

The following information applies to the interaction of Fast EtherChannel and other features of the Catalyst 1900 and Catalyst 2820 switches:

- When the Fast EtherChannel link is running, the CGMP Configuration Menu address options are applied to the link address that was first added. Packets can be forwarded to either member port.
- When the Fast EtherChannel link is running, the address shown in the Port Addressing Menu is for the physical port where the address was added. Packets for these addresses can be forwarded to either member port.
- When the Fast EtherChannel link is running, the address shown in the Multicast Registration Menu is for the link whose address was first added. Traffic can be for either member port.

Configuring the Fast EtherChannel Feature

To configure the Fast EtherChannel feature, follow these steps:

- Step 1** Make sure that the ports you want to channel are configured according to the configuration guidelines.
- Step 2** Make sure you have cabled a loop-free topology for all channeled VLANs.
- Step 3** Create a Fast EtherChannel link by using the following command in global configuration mode:

```
switch(config)# port-channel mode {on | desirable | auto}
```

- Step 4** If you want to change the template port for port channel parameters, use the following command in global configuration mode:

```
switch(config)# port-channel template-port template_port
```

- Step 5** If you use PAgP, configure the PAgP port priority to select the active link using the following command in interface configuration mode:

```
switch(config-if)# pagp-port-priority priority
```

Verifying Fast EtherChannel

To verify that the Fast EtherChannel feature is configured correctly, use the **show interfaces** command. The following display is an example from the **show interfaces** command when the port-channel is down:

```
PortChannel is down
Port-channel mode: on, preserve-order: Disabled
Port parameters template port: A
Port Member Priority Cap. Partner Partner Partner
                          Device-id Port-id Priority Cap.
-----
A   No      128    1    00-00-00-00-00-00          0      0
B   No      128    1    00-00-00-00-00-00          0      0
```

The following display is an example of the **show interfaces** command when the port-channel is up:

```
PortChannel is Enabled
802.1d STP State: Forwarding Forward Transitions: 1
Port-channel mode: on, preserve-order: Disabled
Port parameters template port: A
Active port: A
Port Member Priority Cap. Partner Partner Partner
                          Device-id Port-id Priority Cap.
-----
A   Yes     128    1    00-00-00-00-00-00          0      0
B   Yes     128    1    00-00-00-00-00-00          0      0
```

Fast EtherChannel Example

This example shows how to enable the Fast EtherChannel feature in desirable mode, specifies port 27 or port B as the template port for member-port configuration, and configures the hot-standby port priority of Fast Ethernet port B to 100.

```
switch(config)# port-channel mode desirable  
switch(config)# port-channel template port fastethernet 0/27  
switch(config)# interface fastethernet 0/27  
switch(config-if)# pagp-port-priority 100
```

Supported CLI Commands

The following CLI commands for Fast EtherChannel support are fully documented in the *Catalyst 1900 Series and Catalyst 2820 Series Command Reference* (online only):

- port-channel mode**
- port-channel preserve-order**
- port-channel template-port**
- pagp-port-priority**
- show interfaces**

Web Console Support for Fast EtherChannel Configuration

To configure the Fast EtherChannel feature from the switch web console, click **PORT** on the menu bar. The Port Management Page is displayed. (See Figure 3-1.)

Figure 3-1 Port Management Menu

Member Switch Host Name: DS2820-1 Command Switch IP: 10.1.126.45

Port Management

Fast EtherChannel Management

Module Management

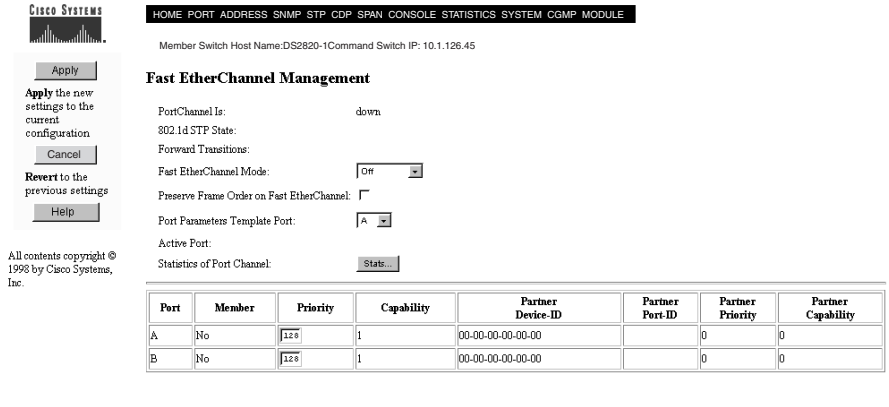
10 Base-T Ports Table:

Module	Port	Status: Requested Actual	Duplex Mode: Requested Actual	Flood Unknown MACs	Port Name/ Description	Statistics
Ethernet 0/1		<input checked="" type="checkbox"/> Enable enabled	[Half duplex] half duplex	<input checked="" type="checkbox"/> unicast <input checked="" type="checkbox"/> multicast		Stats...
Ethernet 0/2		<input checked="" type="checkbox"/> Enable suspended-linkbeat	[Half duplex] half duplex	<input checked="" type="checkbox"/> unicast <input checked="" type="checkbox"/> multicast		Stats...
Ethernet 0/3		<input checked="" type="checkbox"/> Enable suspended-linkbeat	[Half duplex] half duplex	<input checked="" type="checkbox"/> unicast <input checked="" type="checkbox"/> multicast		Stats...
Ethernet 0/4		<input checked="" type="checkbox"/> Enable suspended-linkbeat	[Half duplex] half duplex	<input checked="" type="checkbox"/> unicast <input checked="" type="checkbox"/> multicast		Stats...
Ethernet 0/5		<input checked="" type="checkbox"/> Enable suspended-linkbeat	[Half duplex] half duplex	<input checked="" type="checkbox"/> unicast <input checked="" type="checkbox"/> multicast		Stats...
Ethernet 0/6		<input checked="" type="checkbox"/> Enable suspended-linkbeat	[Half duplex] half duplex	<input checked="" type="checkbox"/> unicast <input checked="" type="checkbox"/> multicast		Stats...
Ethernet 0/7		<input checked="" type="checkbox"/> Enable	[Half duplex] half duplex	<input checked="" type="checkbox"/> unicast <input checked="" type="checkbox"/> multicast		Stats...

All contents copyright © 1998 by Cisco Systems, Inc.

Click Fast EtherChannel Management to display the Fast EtherChannel Page. (See Figure 3-2.)

Figure 3-2 Fast EtherChannel Submenu



Select information in the fields for Fast EtherChannel Mode, Preserve Order of Frames on Fast EtherChannel, and Port Parameters Template Port. Enter a number in the Port Priority field.

Trunking with the Fast EtherChannel Feature

When using a Fast EtherChannel link as a trunk, configure the same trunk mode on all ports in a channel and on both ends of the link. Configuring ports in a channel in different trunk modes can prevent a port-channel from forming.

Spanning-Tree Protocol UplinkFast

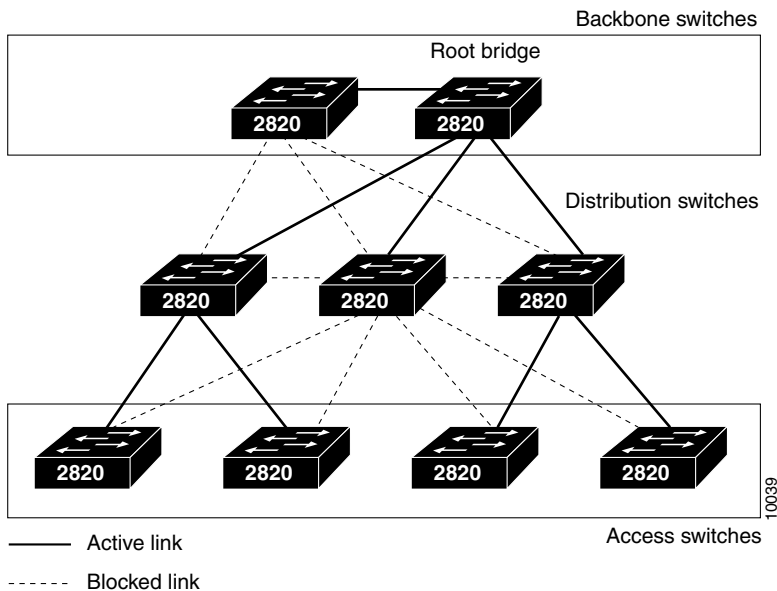
UplinkFast is an enhancement to the STP that provides fast convergence whenever STP picks a new root port. STP will select a new root port automatically when a link or switch fails or when STP parameters change. VLANs must be enabled to configure Uplink Fast features.

Note The Spanning-Tree Protocol UplinkFast feature is most useful in access or edge switches. This feature might not be useful for backbone applications.

How UplinkFast Works

Switches are normally connected hierarchically, as shown in Figure 3-3. (In simpler networks, the upper two levels of the hierarchy might be collapsed into a single backbone layer.) Figure 3-3 shows the network topology after STP has blocked the redundant links to avoid loops. Every access switch and distribution switch in Figure 3-3 has at least one redundant uplink. The switch begins using the alternate paths as soon as STP selects a new root port. The root port transitions to the forwarding state immediately without going through the listening and learning states, as they would with normal STP procedures.

Figure 3-3 Hierarchical Switch Topology



Note UplinkFast is not available if you have configured bridge groups. For more information on bridge groups, see the “Bridge Groups” section on page 3-15.

Station-Learning Frame Generation Rate

When the UplinkFast feature is enabled and the root port fails, station-learning multicast frames are sent out from the new root port. Each frame has a source address equal to an address on a designated port. The designated port must now be reached from the backbone by way of the new root port. We recommend that you limit the generation rate for these frames so that the network is not flooded with these packets.

The rate of station-learning frame generation is expressed as frames per 100 ms. If zero is entered, station-learning frames are not generated. If station-learning frames are not generated, the STP topology converges more slowly after a loss of connectivity.

Note 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. When UplinkFast is disabled, the bridge priorities of all VLANs and path costs of all ports are set to default values.

Configuring UplinkFast

To configure UplinkFast using the menu-based console, do the following:

Step	Action
1 Access the Network Management Configuration Menu.	Enter [N] Network Management at the selection prompt in the Main Menu.
2 Access the Bridge Configuration screen.	Select [B] Bridge Configuration .
3 Select the Uplink Fast feature.	Select [U] Uplink Fast .
4 Enable or disable the Uplink Fast feature.	Enter [E]nable or [D]isable , and press Return .
5 Select the station-learning frame generation rate option.	Select [R] Station-learning Frame Generation Rate .
6 Specify the desired station-learning frame generation rate.	Enter the desired rate, and press Return .

You can configure two Uplink Fast parameters (Enable Uplink Fast and Uplink Fast Learning Rate) from the web console. Click **STP** from the menu bar to display the Spanning-Tree Management Page. The Uplink Fast parameters are in the Spanning Tree Configurations section.

Figure 3-4 Uplink Fast Configuration Options

The screenshot shows the Spanning-Tree Management page for a Cisco switch. The page includes a navigation menu at the top with options like HOME, PORT, ADDRESS, SNMP, STP, CDP, SPAN, CONSOLE, STATISTICS, SYSTEM, CGMP, and MODULE. The main content area is titled "Spanning-Tree Management" and contains several sections:

- Spanning Tree Operating Parameters:**
 - Bridge ID: 8000 00E0 1E87 2140
 - Number of Member Ports: 27
 - Max Age: 20 seconds
 - Hello Time: 2 seconds
 - Topology Changes: 0
 - Designated Root: 8000 00E0 1E7E BE80
 - Root Port: 1
 - Root Path Cost: 100
 - Forward Delay: 15 seconds
 - Last TopChange: 0400100m00s
- Spanning Tree Configurations:**
 - Enable Uplink Fast:
 - Uplink Fast Learning Rate: 15 frames/100ms
 - Bridge Priority: 2768
 - Max Age: 20 seconds
 - Hello Time: 2 seconds
 - Forward Delay: 15 seconds
- Port Parameters:** A table showing the status of various ports.

On the left side of the interface, there are buttons for "Apply", "Cancel", "Revert to the previous settings", and "Help". Below these buttons, it says "Apply the new settings to the current configuration" and "Revert to the previous settings". At the bottom left, there is a copyright notice: "All contents copyright © 1998 by Cisco Systems, Inc."

Module	Port	State	Forward Transitions	Path Cost	Priority	Port Fast Mode
	Ethernet 0/1	Forwarding	1	100	128	<input checked="" type="checkbox"/> Enable
	Ethernet 0/2	Blocking	0	100	128	<input checked="" type="checkbox"/> Enable
	Ethernet 0/3	Blocking	0	100	128	<input checked="" type="checkbox"/> Enable
	Ethernet 0/4	Blocking	0	100	128	<input checked="" type="checkbox"/> Enable
	Ethernet 0/5	Blocking	0	100	128	<input checked="" type="checkbox"/> Enable
	Ethernet 0/6	Blocking	0	100	128	<input checked="" type="checkbox"/> Enable
	Ethernet 0/7	Blocking	0	100	128	<input checked="" type="checkbox"/> Enable

Bridge Groups

A bridge group is a group of ports that form a single broadcast domain that is local to the switch. Bridge groups are a feature of the Catalyst 1900 and Catalyst 2820 series standard software. The complete instructions to configure bridge groups are in the *Catalyst 1900 Series Installation and Configuration Guide* and the *Catalyst 2820 Series Installation and Configuration Guide*.

Bridge groups interact with the Enterprise Edition software in the following ways:

- When configuring the switch, you can use either bridge groups or VLANs. You cannot use both.
- By default, bridge groups are disabled, and VLANs are enabled.
- If you enable bridge groups, the following features are disabled on the switch:
 - All VLAN features
 - Uplink Fast feature
 - DISL
 - Fast EtherChannel features
- When you change from VLANs to bridge groups and vice versa, all options that you have configured are reset to their default settings. You will need to reconfigure any options that you need for VLANs or bridge groups.

To switch between VLANs and bridge groups, use the **[T] Reset to enable VLANs** option in the System Menu.

TACACS+

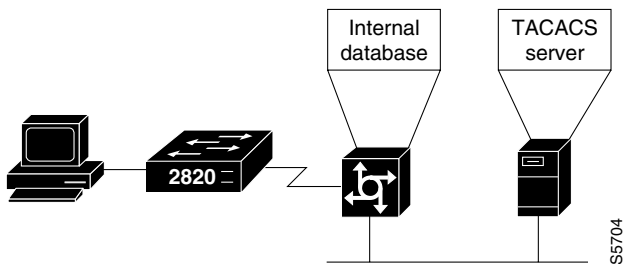
The TACACS+ protocol exchanges network access server (NAS) information between a network device and a centralized database. TACACS+ is a Cisco proprietary enhancement of TACACS, an access-control protocol referenced by RFC 1492.

TACACS+ uses a server to provide authentication, authorization, and accounting (AAA). These services are independent of one another. A given TACACS+ configuration can use any or all of the three services.

Note The TACACS+ feature for the Catalyst 1900 and Catalyst 2820 switches supports only the authentication feature.

The switch authentication access can use locally configured passwords or can use the other services available on the TACACS+ server or on the network, as shown in Figure 3-5.

Figure 3-5 TACACS+ Protocol Authentication



You can enable or disable TACACS+ at your discretion. If TACACS+ is not enabled, the current switch login interface is enabled by default.

You can use the TACACS+ feature for these authentication tasks:

- Enable or disable TACACS+ authentication to determine if a user has permission to access the switch.

- Enable or disable TACACS+ authentication to determine if a user has permission to enter privileged mode
- Define the action to be performed when the TACACS+ servers cannot be reached.
- Define the addresses for up to three TACACS+ servers.
- Set the number of login attempts allowed.
- Set the timeout interval for server response.
- Enable or disable the directed-request option.

If directed-request is enabled when you enter your assigned ID (password), you can specify the TACACS+ server to be used for password authentication. This example authenticates the *user* at the TACACS+ server named *host*:

```
user@host
```

Note that *host* must be one of the configured TACACS+ servers.

- Specify a key that is used to encrypt the protocol packets.

How TACACS+ Authentication Works

Authentication controls access to network devices by determining the identity of a user or an entity. TACACS+ works with a fixed password that is assigned to you by the TACACS+ security administrator at your site (that is, passwords are not dynamically assigned by the TACACS+ server). Your identity is authenticated each time you log into a switch using your assigned password.

When you send a request for privileged or restricted service, TACACS+ prompts you for the information necessary to access the privileged service.

By default, if the TACACS+ server cannot be contacted, access to the console is denied. This can be overridden with the **last-resort** command. The default setting of the **last-resort** command denies access if TACACS+ authentication cannot be performed.

If the TACACS+ **last-resort** command is configured to require a password and the TACACS+ server is down or unreachable, then the password authentication rules are the same as when TACACS+ is disabled—that is, the encrypted (secret) password takes precedence over the unencrypted password. Disabling TACACS+ authentication automatically reenables local authentication.

Note HTTP web connections are always authenticated using the local password.

A TACACS+ key can be configured on the switch so that you can encrypt the packets transmitted to the server. The key must be the same as the one configured on the server daemon. If a TACACS+ key is not configured, the packets are not encrypted.

Up to three TACACS+ servers can be configured. The servers are tried in the order in which they are configured



Caution Make sure that TACACS+ is enabled and configured correctly before disabling local login or enabling authentication. If TACACS+ is enabled but not configured correctly, or if the TACACS+ server is not on, you might not be able to log into the switch. If this occurs, you will need to access the boot code and reset the console, but not the system, to default values.

For more information on accessing the boot code, see the *Catalyst 1900 Series Installation and Configuration Guide*, or the *Catalyst 2820 Series Installation and Configuration Guide*.

Configuring TACACS+

You must configure a TACACS+ server before enabling TACACS+ on the Catalyst 1900 or Catalyst 2820 switch.

To configure TACACS+, perform these steps in privileged mode from the CLI:

Task	Command
Step 1 Enable TACACS+ authentication for login.	login tacacs
Step 2 Enable TACACS+ authentication for enable.	enable use-tacacs
Step 3 Configure the action to be taken when TACACS+ servers cannot be reached.	tacacs-server last-resort [password succeed]
Step 4 Configure the key used to encrypt packets.	tacacs-server key <i>key</i>
Step 5 Configure the IP address of the TACACS+ server.	tacacs-server host <i>hostaddress</i>
Step 6 Configure the number of login attempts allowed to the TACACS+ server (optional).	tacacs-server attempts <i>integer</i>
Step 7 Set the timeout interval in which the server must respond (optional).	tacacs-server timeout <i>seconds</i>

Supported CLI Commands

The following TACACS+ commands are fully documented in the *Catalyst 1900 Series and Catalyst 2820 Series Command Reference* (online only):

enable use-tacacs
login tacacs
show tacacs
tacacs-server attempts
tacacs-server directed-request

tacacs-server host
tacacs-server key
tacacs-server last-resort
tacacs-server timeout

TACACS+ Example

The following example enables TACACS+ login authentication, configures a TACACS+ server at address 192.20.22.7, sets the server key to “I am cool,” sets the maximum allowable login attempts to 3, and sets the server timeout to 5 seconds.

```
switch(config)# login tacacs
switch(config)# tacacs-server host 192.20.22.7
switch(config)# tacacs-server key "I am cool"
switch(config)# tacacs-server attempts 3
switch(config)# tacacs-server timeout 5
```

TACACS+ Verification

To verify the TACACS+ configuration settings, use the **show tacacs** command. After entering the command, you see this display:

```
switch# show tacacs

Enable use-tacacs:Enabled
Login tacacs:Enabled
Tacacs-server last-resort:password
Tacacs-server hosts:192.20.27.7
Tacacs-server key:I am cool
Tacacs-server login attempts:3
Tacacs-server timeout:5 seconds
Tacacs-server directed-request:Disabled
```

Note The **tacacs-server key** setting displays only in privileged Exec mode.

Configuration File Upload and Download

With the Configuration File Upload/Download feature, you can upload the current non-default switch configuration to an ASCII file on a TFTP server or download a saved configuration file from a TFTP server. You can also configure the switch to automatically retrieve the configuration file from a TFTP server when the switch powers on.

Note The Configuration File Upload/Download feature works best for a switch operating the default configuration.

The configuration file is downloaded to switch volatile memory, where it is read and executed line by line after the switch boots. After the entire file is read, the configuration file is removed from switch memory, and the temporary storage area is freed.

The switch does not maintain a copy of the file, nor does it store any comments that are in the file. If you enter the **show running-config** command to view the current configuration, no comments, other than the default comments, are listed.

In addition, because the switch executes the commands, but does not save the original file, output from the **show running-config** command might list the commands in a different order from which they appeared in the original file. The same is true when uploading the current configuration to a TFTP server.

The configuration download stops if the total size of the CLI command file exceeds 15 KB.

Automatic Configuration File Retrieval

A Catalyst 1900 or Catalyst 2820 switch can automatically retrieve the configuration file from the TFTP server when it powers on. You can either specify the address of the TFTP server or have the switch send a broadcast to the IP address 255.255.255.255. Once this feature is configured, the switch requests to download one of the following filenames, in this order:

- *hostname-config*
- *hostname.cfg*

- switch-config
- ciscosw.cfg

You can also use DHCP to trigger an automatic download of the configuration file, as described in the “DHCP Auto Configuration” section.

Configuration File Upload/Download Commands

To configure the switch to download the configuration immediately from a TFTP server, use the following command in privileged mode:

```
switch# copy tftp://host/src_file nvram
```

To configure the switch to upload the current configuration to a TFTP server, use the following command in privileged mode:

```
switch# copy nvram tftp://host/dst_file
```

To configure the IP address of a TFTP server so that the configuration is downloaded when the switch powers on, use the following command in global configuration mode:

```
switch(config)# tftp server host
```

To configure the switch to automatically retrieve the configuration file from a TFTP server, use the following command in global configuration mode:

```
switch(config)# service config
```

Verifying Current Configuration

To display the current configuration of the switch, use the following command:

```
switch# show running-config
```

Supported CLI Commands

The following commands are fully documented in the *Catalyst 1900 Series and Catalyst 2820 Series Command Reference* (online only):

```
copy tftp
copy nvram tftp
service config
show running-config
tftp accept
tftp server
```

Configuration File Examples

The following example configures the switch to download a configuration file named `corporate.cfg` from the TFTP server `192.20.22.7`:

```
switch# copy tftp://192.20.22.7/corporate.cfg nvram
```

The following example configures the switch to upload its configuration to a file named `normal.cfg` on the TFTP server named `tahoe`:

```
switch# copy nvram tftp://tahoe/normal.cfg
```

The following example sets the TFTP server address to `192.20.22.7` and configures the switch to automatically retrieve the configuration upon cold-start:

```
switch(config)# tftp server 192.20.22.7
switch(config)# service config
```

DHCP Auto Configuration

DHCP can be used to enable automatic configuration download, whether or not the **service config** command has been configured on the switch. Using DHCP, the switch gets its address from a DHCP server on the network. To use DHCP, you must do the following:

- Configure the Tag Length Value (TLV) in the DHCP server database for vendor-specific information. Enter the information in the encapsulated vendor-specific option field as follows:
 - code = 133
 - len = 16
 - data = “spaceship-auto=1” (to *enable* DHCP auto configuration)

OR

— data = “spaceship-auto=0” (to *disable* DHCP auto configuration)

- Disable switch auto configuration with the following command:

```
# switch (config)# no service config
```