



Administering the System

- [Finding Feature Information](#), on page 1
- [Information About Administering the Switch](#), on page 1
- [Configuration Examples for Switch Administration](#), on page 34

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Information About Administering the Switch

System Time and Date Management

You can manage the system time and date on your switch using automatic configuration methods (RTC and NTP), or manual configuration methods.



Note For complete syntax and usage information for the commands used in this section, see the *Cisco IOS Configuration Fundamentals Command Reference* on Cisco.com.

Related Topics

[Configuring the Time Zone](#), on page 5

System Clock

The basis of the time service is the system clock. This clock runs from the moment the system starts up and keeps track of the date and time.

The system clock can then be set from these sources:

- NTP
- Manual configuration

The system clock can provide time to these services:

- User **show** commands
- Logging and debugging messages

The system clock keeps track of time internally based on Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT). You can configure information about the local time zone and summer time (daylight saving time) so that the time appears correctly for the local time zone.

The system clock keeps track of whether the time is *authoritative* or not (that is, whether it has been set by a time source considered to be authoritative). If it is not authoritative, the time is available only for display purposes and is not redistributed.

Related Topics

[Setting the System Clock](#), on page 4

[Example: Setting the System Clock](#), on page 34

Network Time Protocol

The NTP is designed to time-synchronize a network of devices. NTP runs over User Datagram Protocol (UDP), which runs over IP. NTP is documented in RFC 1305.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

NTP uses the concept of a *stratum* to describe how many NTP hops away a device is from an authoritative time source. A stratum 1 time server has a radio or atomic clock directly attached, a stratum 2 time server receives its time through NTP from a stratum 1 time server, and so on. A device running NTP automatically chooses as its time source the device with the lowest stratum number with which it communicates through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP avoids synchronizing to a device whose time might not be accurate by never synchronizing to a device that is not synchronized. NTP also compares the time reported by several devices and does not synchronize to a device whose time is significantly different than the others, even if its stratum is lower.

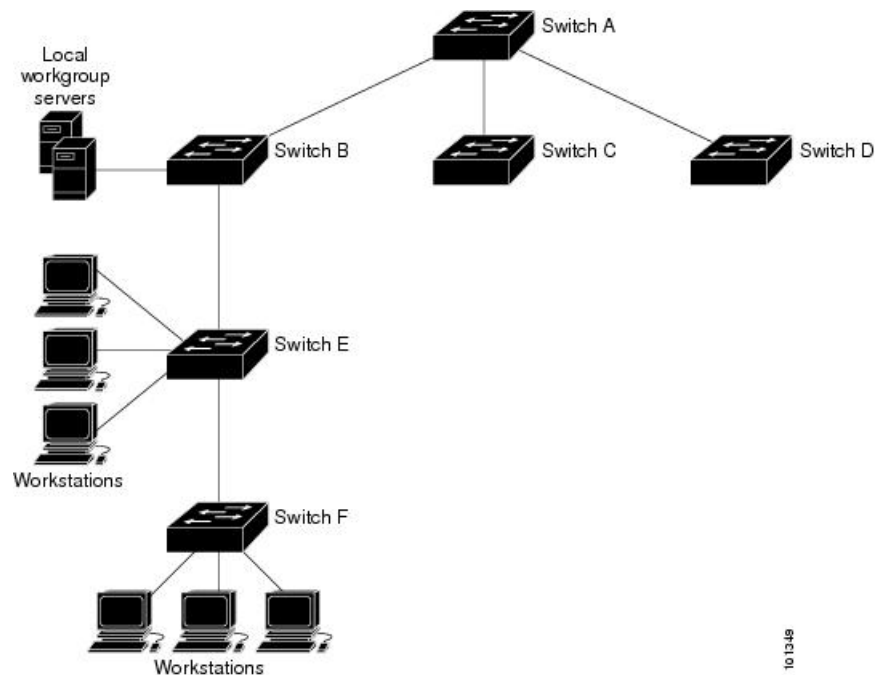
The communications between devices running NTP (known as associations) are usually statically configured; each device is given the IP address of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, in that case, information flow is one-way only.

The time kept on a device is a critical resource; you should use the security features of NTP to avoid the accidental or malicious setting of an incorrect time. Two mechanisms are available: an access list-based restriction scheme and an encrypted authentication mechanism.

Cisco's implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. We recommend that the time service for your network be derived from the public NTP servers available on the IP Internet.

The Figure shows a typical network example using NTP. Switch A is the NTP master, with the **Switch B, C, and D** configured in NTP server mode, in server association with Switch A. Switch E is configured as an NTP peer to the upstream and downstream Switch, Switch B and Switch F, respectively.

Figure 1: Typical NTP Network Configuration



If the network is isolated from the Internet, Cisco's implementation of NTP allows a device to act as if it is synchronized through NTP, when in fact it has learned the time by using other means. Other devices then synchronize to that device through NTP.

When multiple sources of time are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

Several manufacturers include NTP software for their host systems, and a publicly available version for systems running UNIX and its various derivatives is also available. This software allows host systems to be time-synchronized as well.

NTP Version 4

NTP version 4 is implemented on the switch. NTPv4 is an extension of NTP version 3. NTPv4 supports both IPv4 and IPv6 and is backward-compatible with NTPv3.

NTPv4 provides these capabilities:

- Support for IPv6.

- Improved security compared to NTPv3. The NTPv4 protocol provides a security framework based on public key cryptography and standard X509 certificates.
- Automatic calculation of the time-distribution hierarchy for a network. Using specific multicast groups, NTPv4 automatically configures the hierarchy of the servers to achieve the best time accuracy for the lowest bandwidth cost. This feature leverages site-local IPv6 multicast addresses.



Note You can disable NTP packets from being received on routed ports and VLAN interfaces. You cannot disable NTP packets from being received on access ports. For details, see the *Disabling NTPv4 Services on a Specific Interface* section of the *Implementing NTPv4 in IPv6* chapter of the *Cisco IOS IPv6 Configuration Guide, Release 12.4T*.

For details about configuring NTPv4, see the *Implementing NTPv4 in IPv6* chapter of the *Cisco IOS IPv6 Configuration Guide, Release 12.4T*.

Configuring the Time and Date Manually

System time remains accurate through restarts and reboot, however, you can manually configure the time and date after the system is restarted.

We recommend that you use manual configuration only when necessary. If you have an outside source to which the switch can synchronize, you do not need to manually set the system clock.



Note You must reconfigure this setting if you have manually configured the system clock before the fails and a different stack member assumes the role of .

Setting the System Clock

If you have an outside source on the network that provides time services, such as an NTP server, you do not need to manually set the system clock.

Follow these steps to set the system clock:

SUMMARY STEPS

1. **enable**
2. Use one of the following:
 - **clock set** *hh:mm:ss day month year*
 - **clock set** *hh:mm:ss month day year*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example:	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
	Switch> enable	
Step 2	Use one of the following: <ul style="list-style-type: none"> • clock set <i>hh:mm:ss day month year</i> • clock set <i>hh:mm:ss month day year</i> Example: Switch# clock set 13:32:00 23 March 2013	Manually set the system clock using one of these formats: <ul style="list-style-type: none"> • <i>hh:mm:ss</i>—Specifies the time in hours (24-hour format), minutes, and seconds. The time specified is relative to the configured time zone. • <i>day</i>—Specifies the day by date in the month. • <i>month</i>—Specifies the month by name. • <i>year</i>—Specifies the year (no abbreviation).

Related Topics

[System Clock](#), on page 2

[Example: Setting the System Clock](#), on page 34

Displaying the Time and Date Configuration

To display the time and date configuration, use the **show clock[detail]** privileged EXEC command.

The system clock keeps an *authoritative* flag that shows whether the time is authoritative (believed to be accurate). If the system clock has been set by a timing source such as NTP, the flag is set. If the time is not authoritative, it is used only for display purposes. Until the clock is authoritative and the *authoritative* flag is set, the flag prevents peers from synchronizing to the clock when the peers' time is invalid.

The symbol that precedes the **show clock** display has this meaning:

- *—Time is not authoritative.
- (blank)—Time is authoritative.
- .—Time is authoritative, but NTP is not synchronized.

Configuring the Time Zone

Follow these steps to manually configure the time zone:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **clock timezone** *zone hours-offset [minutes-offset]*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Switch> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Switch# configure terminal	Enters the global configuration mode.
Step 3	clock timezone zone hours-offset [minutes-offset] Example: Switch(config)# clock timezone AST -3 30	Sets the time zone. Internal time is kept in Coordinated Universal Time (UTC), so this command is used only for display purposes and when the time is manually set. <ul style="list-style-type: none"> • <i>zone</i>—Enters the name of the time zone to be displayed when standard time is in effect. The default is UTC. • <i>hours-offset</i>—Enters the hours offset from UTC. • (Optional) <i>minutes-offset</i>—Enters the minutes offset from UTC. This available where the local time zone is a percentage of an hour different from UTC.
Step 4	end Example: Switch(config)# end	Returns to privileged EXEC mode.
Step 5	show running-config Example: Switch# show running-config	Verifies your entries.
Step 6	copy running-config startup-config Example: Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

What to do next

The *minutes-offset* variable in the **clock timezone** global configuration command is available for those cases where a local time zone is a percentage of an hour different from UTC. For example, the time zone for some

sections of Atlantic Canada (AST) is UTC-3.5, where the 3 means 3 hours and .5 means 50 percent. In this case, the necessary command is **clock timezone AST -3 30**.

To set the time to UTC, use the **no clock timezone** global configuration command.

Related Topics

[System Time and Date Management](#), on page 1

Configuring Summer Time (Daylight Saving Time)

The first part of the **clock summer-time** global configuration command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.

To configure summer time (daylight saving time) in areas where it starts and ends on a particular day of the week each year, perform this task:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **clock summer-time zone date date month year hh:mm date month year hh:mm [offset]**
4. **clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]]**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Switch> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: <pre>Switch# configure terminal</pre>	Enters the global configuration mode.
Step 3	clock summer-time zone date date month year hh:mm date month year hh:mm [offset] Example: <pre>Switch(config)# clock summer-time PDT date 10 March 2013 2:00 3 November 2013 2:00</pre>	Configures summer time to start and end on specified days every year.

	Command or Action	Purpose
Step 4	<p>clock summer-time zone recurring [<i>week day month hh:mm week day month hh:mm</i> [<i>offset</i>]]</p> <p>Example:</p> <pre>Switch(config)# clock summer-time PDT recurring 10 March 2013 2:00 3 November 2013 2:00</pre>	<p>Configures summer time to start and end on the specified days every year. All times are relative to the local time zone. The start time is relative to standard time.</p> <p>The end time is relative to summer time. Summer time is disabled by default. If you specify clock summer-time zone recurring without parameters, the summer time rules default to the United States rules.</p> <p>If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.</p> <ul style="list-style-type: none"> • <i>zone</i>—Specifies the name of the time zone (for example, PDT) to be displayed when summer time is in effect. • (Optional) <i>week</i>— Specifies the week of the month (1 to 4, first, or last). • (Optional) <i>day</i>—Specifies the day of the week (Sunday, Monday...). • (Optional) <i>month</i>—Specifies the month (January, February...). • (Optional) <i>hh:mm</i>—Specifies the time (24-hour format) in hours and minutes. • (Optional) <i>offset</i>—Specifies the number of minutes to add during summer time. The default is 60.
Step 5	<p>end</p> <p>Example:</p> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
Step 6	<p>show running-config</p> <p>Example:</p> <pre>Switch# show running-config</pre>	Verifies your entries.
Step 7	<p>copy running-config startup-config</p> <p>Example:</p> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Related Topics

[Examples: Configuring Summer Time](#), on page 34

The first part of the **clock summer-time** global configuration command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere. To disable summer time, use the **no clock summer-time** global configuration command.

Follow these steps if summer time in your area does not follow a recurring pattern (configure the exact date and time of the next summer time events):

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **clock summer-time zone date** [*month date year hh:mm month date year hh:mm [offset]*] **or** **clock summer-time zone date** [*date month year hh:mm date month year hh:mm [offset]*]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Switch> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: <pre>Switch# configure terminal</pre>	Enters the global configuration mode.
Step 3	clock summer-time zone date [<i>month date year hh:mm month date year hh:mm [offset]</i>] or clock summer-time zone date [<i>date month year hh:mm date month year hh:mm [offset]</i>]	Configures summer time to start on the first date and end on the second date. Summer time is disabled by default. <ul style="list-style-type: none"> • For <i>zone</i>, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect. • (Optional) For <i>week</i>, specify the week of the month (1 to 5 or last). • (Optional) For <i>day</i>, specify the day of the week (Sunday, Monday...). • (Optional) For <i>month</i>, specify the month (January, February...).

	Command or Action	Purpose
		<ul style="list-style-type: none"> • (Optional) For <i>hh:mm</i>, specify the time (24-hour format) in hours and minutes. • (Optional) For <i>offset</i>, specify the number of minutes to add during summer time. The default is 60.
Step 4	end Example: <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
Step 5	show running-config Example: <pre>Switch# show running-config</pre>	Verifies your entries.
Step 6	copy running-config startup-config Example: <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

System Name and Prompt

You configure the system name on the Switch to identify it. By default, the system name and prompt are Switch.

If you have not configured a system prompt, the first 20 characters of the system name are used as the system prompt. A greater-than symbol [`>`] is appended. The prompt is updated whenever the system name changes.

If you are accessing a stack member through the `,` you must use the **session** *stack-member-number* privileged EXEC command. The stack member number range is from 1 through 9. When you use this command, the stack member number is appended to the system prompt. For example, Switch-2# is the prompt in privileged EXEC mode for stack member 2, and the system prompt for the switch stack is Switch.

For complete syntax and usage information for the commands used in this section, see the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.4* and the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*.

Default System Name and Prompt Configuration

The default Switch system name and prompt is Switch.

Configuring a System Name

Follow these steps to manually configure a system name:

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `hostname name`
4. `end`
5. `show running-config`
6. `copy running-config startup-config`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Switch> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: <pre>Switch# configure terminal</pre>	Enters the global configuration mode.
Step 3	hostname name Example: <pre>Switch(config)# hostname remote-users</pre>	<p>Configures a system name. When you set the system name, it is also used as the system prompt.</p> <p>The default setting is Switch.</p> <p>The name must follow the rules for ARPANET hostnames. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names can be up to 63 characters.</p>
Step 4	end Example: <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
Step 5	show running-config Example: <pre>Switch# show running-config</pre>	Verifies your entries.
Step 6	copy running-config startup-config Example: <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

What to do next

When you set the system name, it is also used as the system prompt.

To return to the default hostname, use the **no hostname** global configuration command.

DNS

The DNS protocol controls the Domain Name System (DNS), a distributed database with which you can map hostnames to IP addresses. When you configure DNS on your switch, you can substitute the hostname for the IP address with all IP commands, such as **ping**, **telnet**, **connect**, and related Telnet support operations.

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, for example, the File Transfer Protocol (FTP) system is identified as *ftp.cisco.com*.

To keep track of domain names, IP has defined the concept of a domain name server, which holds a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the hostnames, specify the name server that is present on your network, and enable the DNS.

Default DNS Settings

Table 1: Default DNS Settings

Feature	Default Setting
DNS enable state	Enabled.
DNS default domain name	None configured.
DNS servers	No name server addresses are configured.

Related Topics

[Setting Up DNS](#), on page 12

Setting Up DNS

If you use the switch IP address as its hostname, the IP address is used and no DNS query occurs. If you configure a hostname that contains no periods (.), a period followed by the default domain name is appended to the hostname before the DNS query is made to map the name to an IP address. The default domain name is the value set by the **ip domain-name** global configuration command. If there is a period (.) in the hostname, the Cisco IOS software looks up the IP address without appending any default domain name to the hostname.

Follow these steps to set up your switch to use the DNS:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip domain-name** *name*
4. **ip name-server** *server-address1* [*server-address2* ... *server-address6*]
5. **ip domain-lookup** [**nsap** | **source-interface** *interface*]
6. **end**

7. `show running-config`
8. `copy running-config startup-config`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Switch> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Switch# configure terminal</pre>	Enters the global configuration mode.
Step 3	<p>ip domain-name <i>name</i></p> <p>Example:</p> <pre>Switch(config)# ip domain-name Cisco.com</pre>	<p>Defines a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name).</p> <p>Do not include the initial period that separates an unqualified name from the domain name.</p> <p>At boot time, no domain name is configured; however, if the switch configuration comes from a BOOTP or Dynamic Host Configuration Protocol (DHCP) server, then the default domain name might be set by the BOOTP or DHCP server (if the servers were configured with this information).</p>
Step 4	<p>ip name-server <i>server-address1</i> [<i>server-address2</i> ... <i>server-address6</i>]</p> <p>Example:</p> <pre>Switch(config)# ip name-server 192.168.1.100 192.168.1.200 192.168.1.300</pre>	<p>Specifies the address of one or more name servers to use for name and address resolution.</p> <p>You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The switch sends DNS queries to the primary server first. If that query fails, the backup servers are queried.</p>
Step 5	<p>ip domain-lookup [<i>nsap</i> <i>source-interface interface</i>]</p> <p>Example:</p> <pre>Switch(config)# ip domain-lookup</pre>	<p>(Optional) Enables DNS-based hostname-to-address translation on your switch. This feature is enabled by default.</p> <p>If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS).</p>
Step 6	<p>end</p> <p>Example:</p>	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Switch(config)# end	
Step 7	show running-config Example: Switch# show running-config	Verifies your entries.
Step 8	copy running-config startup-config Example: Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

What to do next

To remove a domain name, use the **no ip domain-name** *name* global configuration command. To remove a name server address, use the **no ip name-server** *server-address* global configuration command. To disable DNS on the switch, use the **no ip domain-lookup** global configuration command.

Related Topics

[Default DNS Settings](#), on page 12

Displaying the DNS Configuration

To display the DNS configuration information, use the **show running-config** privileged EXEC command.

Login Banners

You can configure a message-of-the-day (MOTD) and a login banner. The MOTD banner is displayed on all connected terminals at login and is useful for sending messages that affect all network users (such as impending system shutdowns).

The login banner is also displayed on all connected terminals. It appears after the MOTD banner and before the login prompts.



Note For complete syntax and usage information for the commands used in this section, see the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.4*.

Default Banner Configuration

The MOTD and login banners are not configured.

Related Topics

[Configuring a Login Banner](#), on page 16

[Example: Configuring a Login Banner](#), on page 35

Configuring a Message-of-the-Day Login Banner

You can create a single or multiline message banner that appears on the screen when someone logs in to the switch.

Follow these steps to configure a MOTD login banner:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **banner motd *c message c***
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Switch> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: <pre>Switch# configure terminal</pre>	Enters the global configuration mode.
Step 3	banner motd <i>c message c</i> Example: <pre>Switch(config)# banner motd # This is a secure site. Only authorized users are allowed. For access, contact technical support. #</pre>	Specifies the message of the day. <i>c</i> —Enters the delimiting character of your choice, for example, a pound sign (#), and press the Return key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded. <i>message</i> —Enters a banner message up to 255 characters. You cannot use the delimiting character in the message.
Step 4	end Example: <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
Step 5	show running-config Example:	Verifies your entries.

	Command or Action	Purpose
	Switch# <code>show running-config</code>	
Step 6	copy running-config startup-config Example: Switch# <code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

What to do next

To delete the MOTD banner, use the **no banner motd** global configuration command.

Related Topics

[Example: Configuring a MOTD Banner](#), on page 34

Configuring a Login Banner

You can configure a login banner to be displayed on all connected terminals. This banner appears after the MOTD banner and before the login prompt.

Follow these steps to configure a login banner:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **banner login *c message c***
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Switch> <code>enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Switch# <code>configure terminal</code>	Enters the global configuration mode.
Step 3	banner login <i>c message c</i>	Specifies the login message.

	Command or Action	Purpose
	<p>Example:</p> <pre>Switch(config)# banner login \$ Access for authorized users only. Please enter your username and password. \$</pre>	<p><i>c</i>— Enters the delimiting character of your choice, for example, a pound sign (#), and press the Return key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded.</p> <p><i>message</i>—Enters a login message up to 255 characters. You cannot use the delimiting character in the message.</p>
Step 4	<p>end</p> <p>Example:</p> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
Step 5	<p>show running-config</p> <p>Example:</p> <pre>Switch# show running-config</pre>	Verifies your entries.
Step 6	<p>copy running-config startup-config</p> <p>Example:</p> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

What to do next

To delete the login banner, use the **no banner login** global configuration command.

Related Topics

[Default Banner Configuration](#), on page 14

[Example: Configuring a Login Banner](#), on page 35

Managing the MAC Address Table

MAC Address Table

The MAC address table contains address information that the switch uses to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports. The address table includes these types of addresses:

- Dynamic address—A source MAC address that the switch learns and then ages when it is not in use.
- Static address—A manually entered unicast address that does not age and that is not lost when the switch resets.

The address table lists the destination MAC address, the associated VLAN ID, and port number associated with the address and the type (static or dynamic).



Note For complete syntax and usage information for the commands used in this section, see the command reference for this release.

MAC Address Table Creation

With multiple MAC addresses supported on all ports, you can connect any port on the switch to other network devices. The switch provides dynamic addressing by learning the source address of packets it receives on each port and adding the address and its associated port number to the address table. As devices are added or removed from the network, the switch updates the address table, adding new dynamic addresses and aging out those that are not in use.

The aging interval is globally configured. However, the switch maintains an address table for each VLAN, and STP can accelerate the aging interval on a per-VLAN basis.

The switch sends packets between any combination of ports, based on the destination address of the received packet. Using the MAC address table, the switch forwards the packet only to the port associated with the destination address. If the destination address is on the port that sent the packet, the packet is filtered and not forwarded. The switch always uses the store-and-forward method: complete packets are stored and checked for errors before transmission.

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. Unicast addresses, for example, could be forwarded to port 1 in VLAN 1 and ports 9, 10, and 1 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.

When private VLANs are configured, address learning depends on the type of MAC address:

- Dynamic MAC addresses learned in one VLAN of a private VLAN are replicated in the associated VLANs. For example, a MAC address learned in a private-VLAN secondary VLAN is replicated in the primary VLAN.
- Static MAC addresses configured in a primary or secondary VLAN are not replicated in the associated VLANs. When you configure a static MAC address in a private VLAN primary or secondary VLAN, you should also configure the same static MAC address in all associated VLANs.

MAC Addresses and Switch Stacks

The MAC address tables on all stack members are synchronized. At any given time, each stack member has the same copy of the address tables for each VLAN. When an address ages out, the address is removed from the address tables on all stack members. When a Switch joins a switch stack, that Switch receives the addresses for each VLAN learned on the other stack members. When a stack member leaves the switch stack, the remaining stack members age out or remove all addresses learned by the former stack member.

Default MAC Address Table Settings

The following table shows the default settings for the MAC address table.

Table 2: Default Settings for the MAC Address

Feature	Default Setting
Aging time	300 seconds
Dynamic addresses	Automatically learned
Static addresses	None configured

Changing the Address Aging Time

Follow these steps to configure the dynamic address table aging time:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mac address-table aging-time [0 | 10-1000000] [routed-mac | vlan *vlan-id*]**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Switch> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: <pre>Switch# configure terminal</pre>	Enters the global configuration mode.
Step 3	mac address-table aging-time [0 10-1000000] [routed-mac vlan <i>vlan-id</i>] Example: <pre>Switch(config)# mac address-table aging-time 500 vlan 2</pre>	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. The range is 10 to 1000000 seconds. The default is 300. You can also enter 0, which disables aging. Static address entries are never aged or removed from the table. <i>vlan-id</i> —Valid IDs are 1 to 4094.

	Command or Action	Purpose
Step 4	end Example: Switch(config)# end	Returns to privileged EXEC mode.
Step 5	show running-config Example: Switch# show running-config	Verifies your entries.
Step 6	copy running-config startup-config Example: Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

What to do next

To return to the default value, use the **no mac address-table aging-time** global configuration command.

Removing Dynamic Address Entries

To remove all dynamic entries, use the **clear mac address-table dynamic** command in privileged EXEC mode. You can also remove a specific MAC address (**clear mac address-table dynamic address *mac-address***), remove all addresses on the specified physical port or port channel (**clear mac address-table dynamic interface *interface-id***), or remove all addresses on a specified VLAN (**clear mac address-table dynamic vlan *vlan-id***).

To verify that dynamic entries have been removed, use the **show mac address-table dynamic** privileged EXEC command.

Configuring MAC Address Change Notification Traps

MAC address change notification tracks users on a network by storing the MAC address change activity. When the switch learns or removes a MAC address, an SNMP notification trap can be sent to the NMS. If you have many users coming and going from the network, you can set a trap-interval time to bundle the notification traps to reduce network traffic. The MAC notification history table stores MAC address activity for each port for which the trap is set. MAC address change notifications are generated for dynamic and secure MAC addresses. Notifications are not generated for self addresses, multicast addresses, or other static addresses.

Follow these steps to configure the switch to send MAC address change notification traps to an NMS host:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host *host-addr* *community-string* *notification-type* { informs | traps } {version {1 | 2c | 3}} {vrf *vrf instance name*}**

4. **snmp-server enable traps mac-notification change**
5. **mac address-table notification change**
6. **mac address-table notification change [interval *value*] [history-size *value*]**
7. **interface *interface-id***
8. **snmp trap mac-notification change {added | removed}**
9. **end**
10. **show running-config**
11. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Switch> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: <pre>Switch# configure terminal</pre>	Enters the global configuration mode.
Step 3	snmp-server host <i>host-addr</i> <i>community-string</i> <i>notification-type</i> { informs traps } {version {1 2c 3}} {vrf <i>vrf instance name</i>} Example: <pre>Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification</pre>	Specifies the recipient of the trap message. <ul style="list-style-type: none"> • <i>host-addr</i>—Specifies the name or address of the NMS. • traps (the default)—Sends SNMP traps to the host. • informs—Sends SNMP informs to the host. • version—Specifies the SNMP version to support. Version 1, the default, is not available with informs. • <i>community-string</i>—Specifies the string to send with the notification operation. Though you can set this string by using the snmp-server host command, we recommend that you define this string by using the snmp-server community command before using the snmp-server host command. • <i>notification-type</i>—Uses the mac-notification keyword. • vrf <i>vrf instance name</i>—Specifies the VPN routing/forwarding instance for this host.
Step 4	snmp-server enable traps mac-notification change Example:	Enables the switch to send MAC address change notification traps to the NMS.

	Command or Action	Purpose
	<pre>Switch(config)# snmp-server enable traps mac-notification change</pre>	
Step 5	<p>mac address-table notification change</p> <p>Example:</p> <pre>Switch(config)# mac address-table notification change</pre>	Enables the MAC address change notification feature.
Step 6	<p>mac address-table notification change [interval value] [history-size value]</p> <p>Example:</p> <pre>Switch(config)# mac address-table notification change interval 123 Switch(config)# mac address-table notification change history-size 100</pre>	<p>Enters the trap interval time and the history table size.</p> <ul style="list-style-type: none"> • (Optional) interval value—Specifies the notification trap interval in seconds between each set of traps that are generated to the NMS. The range is 0 to 2147483647 seconds; the default is 1 second. • (Optional) history-size value—Specifies the maximum number of entries in the MAC notification history table. The range is 0 to 500; the default is 1.
Step 7	<p>interface interface-id</p> <p>Example:</p> <pre>Switch(config)# interface gigabitethernet1/0/2</pre>	Enters interface configuration mode, and specifies the Layer 2 interface on which to enable the SNMP MAC address notification trap.
Step 8	<p>snmp trap mac-notification change {added removed}</p> <p>Example:</p> <pre>Switch(config-if)# snmp trap mac-notification change added</pre>	<p>Enables the MAC address change notification trap on the interface.</p> <ul style="list-style-type: none"> • Enables the trap when a MAC address is added on this interface. • Enables the trap when a MAC address is removed from this interface.
Step 9	<p>end</p> <p>Example:</p> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
Step 10	<p>show running-config</p> <p>Example:</p> <pre>Switch# show running-config</pre>	Verifies your entries.
Step 11	<p>copy running-config startup-config</p> <p>Example:</p>	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	Switch# <code>copy running-config startup-config</code>	

What to do next

To disable MAC address-change notification traps, use the **no snmp-server enable traps mac-notification change** global configuration command. To disable the MAC address-change notification traps on a specific interface, use the **no snmp trap mac-notification change {added|removed}** interface configuration command. To disable the MAC address-change notification feature, use the **no mac address-table notification change** global configuration command.

You can verify your settings by entering the **show mac address-table notification change interface** and the **show mac address-table notification change** privileged EXEC commands.

Related Topics

[Example: Configuring MAC Address Change Notification Traps](#), on page 35

Configuring MAC Address Move Notification Traps

When you configure MAC-move notification, an SNMP notification is generated and sent to the network management system whenever a MAC address moves from one port to another within the same VLAN.

Follow these steps to configure the switch to send MAC address-move notification traps to an NMS host:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host *host-addr* {traps | informs} {version {1 | 2c | 3}} *community-string notification-type***
4. **snmp-server enable traps mac-notification move**
5. **mac address-table notification mac-move**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Switch> <code>enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Switch# <code>configure terminal</code>	Enters the global configuration mode.

	Command or Action	Purpose
Step 3	<p>snmp-server host <i>host-addr</i> {traps informs} {version {1 2c 3}} <i>community-string notification-type</i></p> <p>Example:</p> <pre>Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification</pre>	<p>Specifies the recipient of the trap message.</p> <ul style="list-style-type: none"> • <i>host-addr</i>—Specifies the name or address of the NMS. • traps (the default)—Sends SNMP traps to the host. • informs—Sends SNMP informs to the host. • version—Specifies the SNMP version to support. Version 1, the default, is not available with informs. • <i>community-string</i>—Specifies the string to send with the notification operation. Though you can set this string by using the snmp-server host command, we recommend that you define this string by using the snmp-server community command before using the snmp-server host command. • <i>notification-type</i>—Uses the mac-notification keyword.
Step 4	<p>snmp-server enable traps mac-notification move</p> <p>Example:</p> <pre>Switch(config)# snmp-server enable traps mac-notification move</pre>	Enables the switch to send MAC address move notification traps to the NMS.
Step 5	<p>mac address-table notification mac-move</p> <p>Example:</p> <pre>Switch(config)# mac address-table notification mac-move</pre>	Enables the MAC address move notification feature.
Step 6	<p>end</p> <p>Example:</p> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
Step 7	<p>show running-config</p> <p>Example:</p> <pre>Switch# show running-config</pre>	Verifies your entries.
Step 8	<p>copy running-config startup-config</p> <p>Example:</p> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

What to do next

To disable MAC address-move notification traps, use the **no snmp-server enable traps mac-notification move** global configuration command. To disable the MAC address-move notification feature, use the **no mac address-table notification mac-move** global configuration command.

You can verify your settings by entering the **show mac address-table notification mac-move** privileged EXEC commands.

Configuring MAC Threshold Notification Traps

When you configure MAC threshold notification, an SNMP notification is generated and sent to the network management system when a MAC address table threshold limit is reached or exceeded.

Follow these steps to configure the switch to send MAC address table threshold notification traps to an NMS host:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host *host-addr* {traps | informs} {version {1 | 2c | 3}} *community-string notification-type***
4. **snmp-server enable traps mac-notification threshold**
5. **mac address-table notification threshold**
6. **mac address-table notification threshold [*limit percentage*] | [*interval time*]**
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Switch> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: <pre>Switch# configure terminal</pre>	Enters the global configuration mode.
Step 3	snmp-server host <i>host-addr</i> {traps informs} {version {1 2c 3}} <i>community-string notification-type</i> Example: <pre>Switch(config)# snmp-server host 172.20.10.10 traps private</pre>	Specifies the recipient of the trap message. <ul style="list-style-type: none"> • <i>host-addr</i>—Specifies the name or address of the NMS. • traps (the default)—Sends SNMP traps to the host. • informs—Sends SNMP informs to the host.

	Command or Action	Purpose
	<code>mac-notification</code>	<ul style="list-style-type: none"> • version—Specifies the SNMP version to support. Version 1, the default, is not available with informs. • <i>community-string</i>—Specifies the string to send with the notification operation. You can set this string by using the snmp-server host command, but we recommend that you define this string by using the snmp-server community command before using the snmp-server host command. • <i>notification-type</i>—Uses the mac-notification keyword.
Step 4	snmp-server enable traps mac-notification threshold Example: <pre>Switch(config)# snmp-server enable traps mac-notification threshold</pre>	Enables MAC threshold notification traps to the NMS.
Step 5	mac address-table notification threshold Example: <pre>Switch(config)# mac address-table notification threshold</pre>	Enables the MAC address threshold notification feature.
Step 6	mac address-table notification threshold [limit percentage] [interval time] Example: <pre>Switch(config)# mac address-table notification threshold interval 123 Switch(config)# mac address-table notification threshold limit 78</pre>	<p>Enters the threshold value for the MAC address threshold usage monitoring.</p> <ul style="list-style-type: none"> • (Optional) limit percentage—Specifies the percentage of the MAC address table use; valid values are from 1 to 100 percent. The default is 50 percent. • (Optional) interval time—Specifies the time between notifications; valid values are greater than or equal to 120 seconds. The default is 120 seconds.
Step 7	end Example: <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
Step 8	show running-config Example: <pre>Switch# show running-config</pre>	Verifies your entries.

	Command or Action	Purpose
Step 9	copy running-config startup-config Example: <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

What to do next

To disable MAC address-threshold notification traps, use the **no snmp-server enable traps mac-notification threshold** global configuration command. To disable the MAC address-threshold notification feature, use the **no mac address-table notification threshold** global configuration command.

You can verify your settings by entering the **show mac address-table notification threshold** privileged EXEC commands.

Related Topics

[Example: Configuring MAC Threshold Notification Traps](#), on page 36

Adding and Removing Static Address Entries

A static address has these 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 add and remove static addresses and define the forwarding behavior for them. The forwarding behavior defines 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 specify. You can specify a different list of destination ports for each source port.

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.

You add a static address to the address table by specifying the destination MAC unicast address and the VLAN from which it is received. Packets received with this destination address are forwarded to the interface specified with the *interface-id* option.

When you configure a static MAC address in a private-VLAN primary or secondary VLAN, you should also configure the same static MAC address in all associated VLANs. Static MAC addresses configured in a private-VLAN primary or secondary VLAN are not replicated in the associated VLAN. For more information about private VLANs, see *Configuring Private VLANs*.

Follow these steps to add a static address:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mac address-table static mac-addr vlan vlan-id interface interface-id**
4. **end**

5. `show mac address-table static`
6. `show running-config`
7. `copy running-config startup-config`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Switch> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: <pre>Switch# configure terminal</pre>	Enters the global configuration mode.
Step 3	mac address-table static <i>mac-addr</i> vlan <i>vlan-id</i> interface <i>interface-id</i> Example: <pre>Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet 1/0/1</pre>	<p>Adds a static address to the MAC address table.</p> <ul style="list-style-type: none"> • <i>mac-addr</i>—Specifies the destination MAC unicast address to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface. • <i>vlan-id</i>—Specifies the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094. • <i>interface-id</i>—Specifies the interface to which the received packet is forwarded. Valid interfaces include physical ports or port channels. For static multicast addresses, you can enter multiple interface IDs. For static unicast addresses, you can enter only one interface at a time, but you can enter the command multiple times with the same MAC address and VLAN ID.
Step 4	end Example: <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.
Step 5	show mac address-table static	Verify your entries.
Step 6	show running-config Example: <pre>Switch# show running-config</pre>	Verifies your entries.

	Command or Action	Purpose
Step 7	copy running-config startup-config Example: <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

What to do next

To remove static entries from the address table, use the **no mac address-table static mac-addr vlan vlan-id [interface interface-id]** global configuration command.

Related Topics

[Example: Adding the Static Address to the MAC Address Table](#), on page 36

Configuring Unicast MAC Address Filtering Guidelines

When unicast MAC address filtering is enabled, the Switch drops packets with specific source or destination MAC addresses. This feature is disabled by default and only supports unicast static addresses.

Follow these guidelines when using this feature:

- Multicast MAC addresses, broadcast MAC addresses, and router MAC addresses are not supported. If you specify one of these addresses when entering the **mac address-table static mac-addr vlan vlan-id drop** global configuration command, one of these messages appears:
 - Only unicast addresses can be configured to be dropped
 - CPU destined address cannot be configured as drop address
- Packets that are forwarded to the CPU are also not supported.
- If you add a unicast MAC address as a static address and configure unicast MAC address filtering, the Switch either adds the MAC address as a static address or drops packets with that MAC address, depending on which command was entered last. The second command that you entered overrides the first command.

For example, if you enter the **mac address-table static mac-addr vlan vlan-id interface interface-id** global configuration command followed by the **mac address-table static mac-addr vlan vlan-id drop** command, the switch drops packets with the specified MAC address as a source or destination.

If you enter the **mac address-table static mac-addr vlan vlan-id drop** global configuration command followed by the **mac address-table static mac-addr vlan vlan-id interface interface-id** command, the switch adds the MAC address as a static address.

You enable unicast MAC address filtering and configure the switch to drop packets with a specific address by specifying the source or destination unicast MAC address and the VLAN from which it is received.

Configuring Unicast MAC Address Filtering

Follow these steps to configure the Switch to drop a source or destination unicast static address:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mac address-table static mac-addr vlan vlan-id drop**

4. `end`
5. `show mac address-table static`
6. `show running-config`
7. `copy running-config startup-config`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example:</p> <pre>Switch> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<p><code>configure terminal</code></p> <p>Example:</p> <pre>Switch# configure terminal</pre>	Enters the global configuration mode.
Step 3	<p><code>mac address-table static mac-addr vlan vlan-id drop</code></p> <p>Example:</p> <pre>Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop</pre>	<p>Enables unicast MAC address filtering and configure the switch to drop a packet with the specified source or destination unicast static address.</p> <ul style="list-style-type: none"> • <i>mac-addr</i>—Specifies a source or destination unicast MAC address (48-bit). Packets with this MAC address are dropped. • <i>vlan-id</i>—Specifies the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094.
Step 4	<p><code>end</code></p> <p>Example:</p> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
Step 5	<p><code>show mac address-table static</code></p>	Verify your entries.
Step 6	<p><code>show running-config</code></p> <p>Example:</p> <pre>Switch# show running-config</pre>	Verifies your entries.
Step 7	<p><code>copy running-config startup-config</code></p> <p>Example:</p> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

What to do next

To disable unicast MAC address filtering, use the **no mac address-table static *mac-addr* vlan *vlan-id*** global configuration command.

Related Topics

[Example: Configuring Unicast MAC Address Filtering](#), on page 36

Disabling MAC Address Learning on a VLAN Guidelines

By default, MAC address learning is enabled on all VLANs on the Switch. You can control MAC address learning on a VLAN to manage the available MAC address table space by controlling which VLANs, and therefore which ports, can learn MAC addresses. Before you disable MAC address learning, be sure that you are familiar with the network topology and the switch system configuration. Disabling MAC address learning on a VLAN could cause flooding in the network.

Follow these guidelines when disabling MAC address learning on a VLAN:

- Use caution before disabling MAC address learning on a VLAN with a configured Switch virtual interface (SVI). The Switch then floods all IP packets in the Layer 2 domain.
- You can disable MAC address learning on a single VLAN ID (for example, **no mac address-table learning vlan 223**) or on a range of VLAN IDs (for example, **no mac address-table learning vlan 1-20, 15.**)
- We recommend that you disable MAC address learning only in VLANs with two ports. If you disable MAC address learning on a VLAN with more than two ports, every packet entering the Switch is flooded in that VLAN domain.
- You cannot disable MAC address learning on a VLAN that is used internally by the Switch. If the VLAN ID that you enter is an internal VLAN, the Switch generates an error message and rejects the command. To view internal VLANs in use, enter the **show vlan internal usage** privileged EXEC command.
- If you disable MAC address learning on a VLAN configured as a private-VLAN primary VLAN, MAC addresses are still learned on the secondary VLAN that belongs to the private VLAN and are then replicated on the primary VLAN. If you disable MAC address learning on the secondary VLAN, but not the primary VLAN of a private VLAN, MAC address learning occurs on the primary VLAN and is replicated on the secondary VLAN.
- You cannot disable MAC address learning on an RSPAN VLAN. The configuration is not allowed.
- If you disable MAC address learning on a VLAN that includes a secure port, MAC address learning is not disabled on that port. If you disable port security, the configured MAC address learning state is enabled.

Related Topics

[Disabling MAC Address Learning on a VLAN](#), on page 31

Disabling MAC Address Learning on a VLAN

Follow these steps to disable MAC address learning on a VLAN:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **configure terminal**
4. **no mac address-table learning vlan *vlan-id***
5. **end**

6. `show mac address-table learning[vlanvlan-id]`
7. `show running-config`
8. `copy running-config startup-config`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Switch> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: <pre>Switch# configure terminal</pre>	Enters the global configuration mode.
Step 3	configure terminal	Enter global configuration mode.
Step 4	no mac address-table learning vlan <i>vlan-id</i>	Disable MAC address learning on the specified VLAN or VLANs. You can specify a single VLAN ID or a range of VLAN IDs separated by a hyphen or comma. Valid VLAN IDs are 1 to 4094.
Step 5	end Example: <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
Step 6	show mac address-table learning[vlanvlan-id]	
Step 7	show running-config Example: <pre>Switch# show running-config</pre>	Verifies your entries.
Step 8	copy running-config startup-config Example: <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

What to do next

To reenble MAC address learning on a VLAN, use the **default mac address-table learning vlanvlan-id** global configuration command. You can also reenble MAC address learning on a VLAN by entering the the

mac address-table learning vlan *vlan-id* global configuration command. The first(**default**) command returns to a default condition and therefore does not appear in the output from the **show running-config** command. The second command causes the configuration to appear in the **show running-config** privileged EXEC command display.

```
Switch(config)# no mac address-table learning vlan 200
```

You can display the MAC address learning status of all VLANs or a specified VLAN by entering the **show mac-address-table learning [vlan *vlan-id*]** privileged EXEC command.

Related Topics

[Disabling MAC Address Learning on a VLAN Guidelines](#), on page 31

Displaying Address Table Entries

You can display the MAC address table by using one or more of the privileged EXEC commands described in this table:

Table 3: Commands for Displaying the MAC Address Table

Command	Description
show ip igmp snooping groups	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays only dynamic MAC address table entries.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table learning	Displays MAC address learning status of all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC notification parameters and history table.
show mac address-table static	Displays only static MAC address table entries.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

ARP Table Management

To communicate with a device (over Ethernet, for example), the software first must learn the 48-bit MAC address or the local data link address of that device. The process of learning 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. Using an IP address, ARP finds the associated MAC address. When a MAC

address is found, 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, see the Cisco IOS Release 12.4 documentation on *Cisco.com*.

Configuration Examples for Switch Administration

Example: Setting the System Clock

This example shows how to manually set the system clock:

```
Switch# clock set 13:32:00 23 July 2013
```

Related Topics

[Setting the System Clock](#), on page 4

[System Clock](#), on page 2

Examples: Configuring Summer Time

This example (for daylight savings time) shows how to specify that summer time starts on March 10 at 02:00 and ends on November 3 at 02:00:

```
Switch(config)# clock summer-time PDT recurring PST date  
10 March 2013 2:00 3 November 2013 2:00
```

This example shows how to set summer time start and end dates:

```
Switch(config)#clock summer-time PST date  
20 March 2013 2:00 20 November 2013 2:00
```

Related Topics

[Configuring Summer Time \(Daylight Saving Time\)](#), on page 7

Example: Configuring a MOTD Banner

This example shows how to configure a MOTD banner by using the pound sign (#) symbol as the beginning and ending delimiter:

```
Switch(config)# banner motd #
```

```
This is a secure site. Only authorized users are allowed.  
For access, contact technical support.
```

```
#  
Switch(config)#
```

This example shows the banner that appears from the previous configuration:

```
Unix> telnet 192.0.2.15  
Trying 192.0.2.15...  
Connected to 192.0.2.15.  
Escape character is '^]'.  
This is a secure site. Only authorized users are allowed.  
For access, contact technical support.  
User Access Verification  
Password:
```

Related Topics

[Configuring a Message-of-the-Day Login Banner](#), on page 15

Example: Configuring a Login Banner

This example shows how to configure a login banner by using the dollar sign (\$) symbol as the beginning and ending delimiter:

```
Switch(config)# banner login $  
Access for authorized users only. Please enter your username and password.  
$  
Switch(config)#
```

Related Topics

[Configuring a Login Banner](#), on page 16

[Default Banner Configuration](#), on page 14

Example: Configuring MAC Address Change Notification Traps

This example shows how to specify 172.20.10.10 as the NMS, enable MAC address notification traps to the NMS, enable the MAC address-change notification feature, set the interval time to 123 seconds, set the history-size to 100 entries, and enable traps whenever a MAC address is added on the specified port:

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification  
Switch(config)# snmp-server enable traps mac-notification change  
Switch(config)# mac address-table notification change  
Switch(config)# mac address-table notification change interval 123  
Switch(config)# mac address-table notification change history-size 100  
Switch(config)# interface gigabitethernet1/2/1
```

```
Switch(config-if) # snmp trap mac-notification change added
```

Related Topics

[Configuring MAC Address Change Notification Traps](#), on page 20

Example: Configuring MAC Threshold Notification Traps

This example shows how to specify 172.20.10.10 as the NMS, enable the MAC address threshold notification feature, set the interval time to 123 seconds, and set the limit to 78 per cent:

```
Switch(config) # snmp-server host 172.20.10.10 traps private mac-notification
Switch(config) # snmp-server enable traps mac-notification threshold
Switch(config) # mac address-table notification threshold
Switch(config) # mac address-table notification threshold interval 123
Switch(config) # mac address-table notification threshold limit 78
```

Related Topics

[Configuring MAC Threshold Notification Traps](#), on page 25

Example: Adding the Static Address to the MAC Address Table

This example shows how to add the static address c2f3.220a.12f4 to the MAC address table. When a packet is received in VLAN 4 with this MAC address as its destination address, the packet is forwarded to the specified port:

```
Switch(config) # mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet1/1/1
```

Related Topics

[Adding and Removing Static Address Entries](#), on page 27

Example: Configuring Unicast MAC Address Filtering

This example shows how to enable unicast MAC address filtering and how to configure drop packets that have a source or destination address of c2f3.220a.12f4. When a packet is received in VLAN 4 with this MAC address as its source or destination, the packet is dropped:

```
Switch(config) # mac address-table static c2f3.220a.12f4 vlan 4 drop
```

Related Topics

[Configuring Unicast MAC Address Filtering](#), on page 29

Additional References for Switch Administration

Related Documents

Related Topic	Document Title
System management commands	
Network management configuration	
Layer 2 configuration	
VLAN configuration	

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

