CHAPTER 6

Administer the Switch Module

This chapter describes how to perform one-time operations to administer the CGR 2010 ESM, as well as how to monitor the switch module's temperature and configure the temperature yellow threshold. This chapter contains the following topics:

- Managing the System Time and Date, page 6-1
- Configuring a System Name and Prompt, page 6-15
- Creating a Banner, page 6-18
- Monitoring Temperature and Configuring the Yellow Threshold, page 6-21
- Managing the MAC Address Table, page 6-22
- Managing the ARP Table, page 6-34

Managing the System Time and Date

You can manage the system time and date on your switch module using automatic configuration, such as the Network Time Protocol (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, Release 12.2*.

These sections contain the following configuration information:

- Understanding the System Clock, page 6-1
- Understanding the Network Time Protocol, page 6-2
- Configuring the Network Time Protocol, page 6-3
- Configuring Time and Date Manually, page 6-12

Understanding the System Clock

The heart 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:

- Network Time Protocol
- 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 Universal Time Coordinated (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. For configuration information, see the "Configuring Time and Date Manually" section on page 6-12.

Understanding the Network Time Protocol

The Network Time Protocol (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.

Figure 6-1 shows a typical network example using NTP. Switch A is the NTP master, with Switches 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 module, Switch B and Switch F.

Figure 6-1   *Typical NTP Network Configuration*
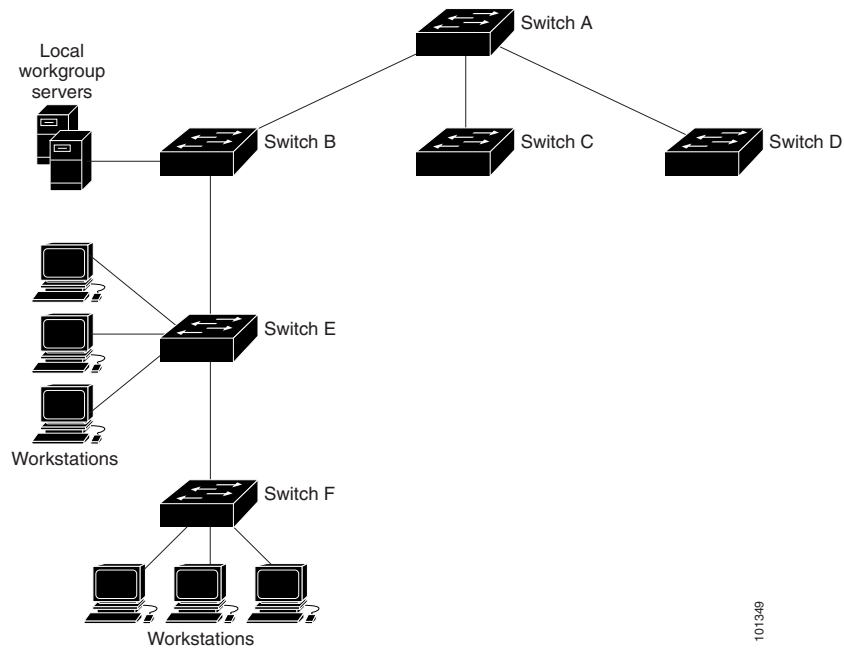
If the network is isolated from the Internet, Cisco's implementation of NTP allows a device to act as if it is synchronized through NTP, when in fact it has learned the time by using other means. Other devices then synchronize to that device through NTP.

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.

Configuring the Network Time Protocol

The switch module does not have a hardware-supported clock and cannot function as an NTP master clock to which peers synchronize themselves when an external NTP source is not available. The switch module also has no hardware support for a calendar. As a result, the **ntp update-calendar** and the **ntp master** global configuration commands are not available.

These sections contain this configuration information:

Default NTP Configuration

Table 6-1 shows the default NTP configuration.

Table 6-1   Default NTP Configuration

Feature	Default Setting
NTP authentication	Disabled - no authentication key is specified
NTP peer or server associations	None configured
NTP broadcast service	Disabled; no interface sends or receives NTP broadcast packets
NTP access restrictions	No access control is specified
NTP packet source IP address	The source address is set by the outgoing interface

NTP is enabled on all interfaces by default. All interfaces receive NTP packets.

Configuring NTP Authentication

This procedure must be coordinated with the administrator of the NTP server; the information you configure in this procedure must be matched by the servers used by the switch module to synchronize its time to the NTP server.

Beginning in privileged EXEC mode, follow these steps to authenticate the associations (communications between devices running NTP that provide for accurate timekeeping) with other devices for security purposes:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable the NTP authentication feature, which is disabled by default.	**ntp authenticate**
Step 3	Define the authentication keys. By default, none are defined. • For *number*, specify a key number. The range is 1 to 4294967295. • **md5** specifies that message authentication support is provided by using the message digest algorithm 5 (MD5). • For *value*, enter an arbitrary string of up to eight characters for the key. the switch module does not synchronize to a device unless both have one of these authentication keys, and the key number is specified by the **ntp trusted-key** *key-number* command.	**ntp authentication-key** *number* **md5** *value*

Step		Command
Step 4	Specify one or more key numbers (defined in Step 3) that a peer NTP device must provide in its NTP packets for this switch module to synchronize to it. By default, no trusted keys are defined. For *key-number*, specify the key defined in Step 3. This command provides protection against accidentally synchronizing the switch module to a device that is not trusted.	**ntp trusted-key** *key-number*
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries.	**show running-config**
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To disable NTP authentication, use the **no ntp authenticate** global configuration command. To remove an authentication key, use the **no ntp authentication-key** *number* global configuration command. To disable authentication of the identity of a device, use the **no ntp trusted-key** *key-number* global configuration command.

This example shows how to configure the switch module to synchronize only to devices providing authentication key 42 in the device's NTP packets:

```
Switch(config)# ntp authenticate
Switch(config)# ntp authentication-key 42 md5 aNiceKey
Switch(config)# ntp trusted-key 42
```

Configuring NTP Associations

An NTP association can be a peer association (this switch module can either synchronize to the other device or allow the other device to synchronize to it), or it can be a server association (meaning that only this switch module synchronizes to the other device, and not the other way around).

Beginning in privileged EXEC mode, follow these steps to form an NTP association with another device:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Configure the switch module system clock to synchronize a peer or to be synchronized by a peer (peer association). or Configure the switch module system clock to be synchronized by a time server (server association). No peer or server associations are defined by default. • For *ip-address* in a peer association, specify either the IP address of the peer providing, or being provided, the clock synchronization. For a server association, specify the IP address of the time server providing the clock synchronization. • (Optional) For *number*, specify the NTP version number. The range is 1 to 3. By default, Version 3 is selected. • (Optional) For *keyid*, enter the authentication key defined with the **ntp authentication-key** global configuration command. • (Optional) For *interface*, specify the interface from which to pick the IP source address. By default, the source IP address is taken from the outgoing interface. • (Optional) Enter the **prefer** keyword to make this peer or server the preferred one that provides synchronization. This keyword reduces switch moduleing back and forth between peers and servers.	**ntp peer** *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**] or **ntp server** *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries.	**show running-config**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

You need to configure only one end of an association; the other device can automatically establish the association. If you are using the default NTP version (Version 3) and NTP synchronization does not occur, try using NTP Version 2. Many NTP servers on the Internet run Version 2.

To remove a peer or server association, use the **no ntp peer** *ip-address* or the **no ntp server** *ip-address* global configuration command.

This example shows how to configure the switch module to synchronize its system clock with the clock of the peer at IP address 172.16.22.44 using NTP Version 2:

```
Switch(config)# ntp server 172.16.22.44 version 2
```

Configuring NTP Broadcast Service

The communications between devices running NTP (known as *associations*) are usually statically configured; each device is given the IP addresses 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, the information flow is one-way only.

the switch module can send or receive NTP broadcast packets on an interface-by-interface basis if there is an NTP broadcast server, such as a router, broadcasting time information on the network. the switch module can send NTP broadcast packets to a peer so that the peer can synchronize to it. the switch module can also receive NTP broadcast packets to synchronize its own clock. This section provides procedures for both sending and receiving NTP broadcast packets.

Beginning in privileged EXEC mode, follow these steps to configure the switch module to send NTP broadcast packets to peers so that they can synchronize their clock to the switch module:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the interface to send NTP broadcast packets, and enter interface configuration mode.	**interface** *interface-id*
Step 3	Enable the port, if necessary. By default, user network interfaces (UNIs) and enhanced network interfaces (ENIs) are disabled, and network node interfaces (NNIs) are enabled.	**no shutdown**
Step 4	Enable the interface to send NTP broadcast packets to a peer. By default, this feature is disabled on all interfaces. • (Optional) For *number*, specify the NTP version number. The range is 1 to 3. If you do not specify a version, Version 3 is used. • (Optional) For *keyid*, specify the authentication key to use when sending packets to the peer. • (Optional) For *destination-address*, specify the IP address of the peer that is synchronizing its clock to this switch module.	**ntp broadcast** [**version** *number*] [**key** *keyid*] [*destination-address*]
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries.	**show running-config**

	Step	Command
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**
Step 8	Configure the connected peers to receive NTP broadcast packets as described in the next procedure.	

To disable the interface from sending NTP broadcast packets, use the **no ntp broadcast** interface configuration command.

This example shows how to configure a port to send NTP Version 2 packets:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ntp broadcast version 2
```

Beginning in privileged EXEC mode, follow these steps to configure the switch module to receive NTP broadcast packets from connected peers:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the interface to receive NTP broadcast packets, and enter interface configuration mode.	**interface** *interface-id*
Step 3	Enable the port, if necessary. By default, UNIs and enhanced network interfaces (ENIs) are disabled, and NNIs are enabled.	**no shutdown**
Step 4	Enable the interface to receive NTP broadcast packets. By default, no interfaces receive NTP broadcast packets.	**ntp broadcast client**
Step 5	Return to global configuration mode.	**exit**
Step 6	(Optional) Change the estimated round-trip delay between the switch module and the NTP broadcast server. The default is 3000 microseconds; the range is 1 to 999999.	**ntp broadcastdelay** *microseconds*
Step 7	Return to privileged EXEC mode.	**end**
Step 8	Verify your entries.	**show running-config**
Step 9	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To disable an interface from receiving NTP broadcast packets, use the **no ntp broadcast client** interface configuration command. To change the estimated round-trip delay to the default, use the **no ntp broadcastdelay** global configuration command.

This example shows how to configure a port to receive NTP broadcast packets:

```
Switch(config)# interface gigabitethernet0/1
```

```
Switch(config-if)# ntp broadcast client
```

Configuring NTP Access Restrictions

You can control NTP access on two levels as described in these sections:

Creating an Access Group and Assigning a Basic IP Access List

Beginning in privileged EXEC mode, follow these steps to control access to NTP services by using access lists:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Create an access group, and apply a basic IP access list. The keywords have these meanings: • **query-only**—Allows only NTP control queries. • **serve-only**—Allows only time requests. • **serve**—Allows time requests and NTP control queries, but does not allow the switch module to synchronize to the remote device. • **peer**—Allows time requests and NTP control queries and allows the switch module to synchronize to the remote device. For *access-list-number*, enter a standard IP access list number from 1 to 99.	**ntp access-group** {**query-only** | **serve-only** | **serve** | **peer**} *access-list-number*
Step 3	Create the access list. • For *access-list-number*, enter the number specified in Step 2. • Enter the **permit** keyword to permit access if the conditions are matched. • For *source*, enter the IP address of the device that is permitted access to the switch module. • (Optional) For *source-wildcard*, enter the wildcard bits to be applied to the source. **Note** When creating an access list, remember that, by default, the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.	**access-list** *access-list-number* **permit** *source* [*source-wildcard*]
Step 4	Return to privileged EXEC mode.	**end**

	Step	Command
Step 5	Verify your entries.	**show running-config**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

The access group keywords are scanned in this order, from least restrictive to most restrictive:

- **peer**—Allows time requests and NTP control queries and allows the switch module to synchronize itself to a device whose address passes the access list criteria.
- **serve**—Allows time requests and NTP control queries, but does not allow the switch module to synchronize itself to a device whose address passes the access list criteria.
- **serve-only**—Allows only time requests from a device whose address passes the access list criteria.
- **query-only**—Allows only NTP control queries from a device whose address passes the access list criteria.

If the source IP address matches the access lists for more than one access type, the first type is granted. If no access groups are specified, all access types are granted to all devices. If any access groups are specified, only the specified access types are granted.

To remove access control to the switch module NTP services, use the **no ntp access-group** {**query-only** | **serve-only** | **serve** | **peer**} global configuration command.

This example shows how to configure the switch module to allow itself to synchronize to a peer from access list 99. However, the switch module restricts access to allow only time requests from access list 42:

```
Switch# configure terminal
Switch(config)# ntp access-group peer 99
Switch(config)# ntp access-group serve-only 42
Switch(config)# access-list 99 permit 172.20.130.5
Switch(config)# access list 42 permit 172.20.130.6
```

Disabling NTP Services on a Specific Interface

NTP services are enabled on all interfaces by default.

Beginning in privileged EXEC mode, follow these steps to disable NTP packets from being received on an interface:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and specify the interface to disable.	**interface** *interface-id*
Step 3	Enable the port, if necessary. By default, UNIs and enhanced network interfaces (ENIs) are disabled, and NNIs are enabled.	**no shutdown**
Step 4	Disable NTP packets from being received on the interface. By default, all interfaces receive NTP packets.	**ntp disable**
Step 5	Return to privileged EXEC mode.	**end**

Step		Command
Step 6	Verify your entries.	**show running-config**
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To re-enable receipt of NTP packets on an interface, use the **no ntp disable** interface configuration command.

Configuring the Source IP Address for NTP Packets

When the switch module sends an NTP packet, the source IP address is normally set to the address of the interface through which the NTP packet is sent. Use the **ntp source** global configuration command when you want to use a particular source IP address for all NTP packets. The address is taken from the specified interface. This command is useful if the address on an interface cannot be used as the destination for reply packets.

Beginning in privileged EXEC mode, follow these steps to configure a specific interface from which the IP source address is to be taken:

Step		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the interface type and number from which the IP source address is taken. By default, the source address is set by the outgoing interface.	**ntp source** *type number*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries.	**show running-config**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

The specified interface is used for the source address for all packets sent to all destinations. If a source address is to be used for a specific association, use the **source** keyword in the **ntp peer** or **ntp server** global configuration command as described in the "Configuring NTP Associations" section on page 6-5.

Displaying the NTP Configuration

You can use two privileged EXEC commands to display NTP information:

- **show ntp associations** [**detail**]
- **show ntp status**

For detailed information about the fields in these displays, see the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*.

Configuring Time and Date Manually

If no other source of time is available, you can manually configure the time and date after the system is restarted. The time remains accurate until the next system restart. We recommend that you use manual configuration only as a last resort. If you have an outside source to which the switch module can synchronize, you do not need to manually set the system clock.

These sections contain this configuration information:

- Setting the System Clock, page 6-12
- Displaying the Time and Date Configuration, page 6-12
- Configuring the Time Zone, page 6-13
- Configuring Summer Time (Daylight Saving Time), page 6-14

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.

Beginning in privileged EXEC mode, follow these steps to set the system clock:

	Step	Command
Step 1	Manually set the system clock using one of these formats. - For *hh*:*mm*:*ss*, specify the time in hours (24-hour format), minutes, and seconds. The time specified is relative to the configured time zone. - For *day*, specify the day by date in the month. - For *month*, specify the month by name. - For *year*, specify the year (no abbreviation).	**clock set** *hh*:*mm*:*ss day month year* or **clock set** *hh*:*mm*:*ss month day year*

This example shows how to manually set the system clock to 1:30 P.M. on September 30, 2010:

```
Switch# clock set 13:30:00 30 September 2010
```

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

Beginning in privileged EXEC mode, follow these steps to manually configure the time zone:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Set the time zone. The switch module keeps internal time in universal time coordinated (UTC), so this command is used only for display purposes and when the time is manually set: • For *zone*, enter the name of the time zone to be displayed when standard time is in effect. The default is UTC. • For *hours-offset*, enter the hours offset from UTC. • (Optional) For *minutes-offset*, enter the minutes offset from UTC.	**clock timezone** *zone hours-offset* [*minutes-offset*]
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries.	**show running-config**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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.

Configuring Summer Time (Daylight Saving Time)

Beginning in privileged EXEC mode, follow these steps to configure summer time (daylight saving time) in areas where it starts and ends on a particular day of the week each year:

	Steps	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Configure summer time to start and end on the specified days every year.	**clock summer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]
	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.	
	• For *zone*, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect	
	• (Optional) For *week*, specify the week of the month (1 to 5 or **last**)	
	• (Optional) For *day*, specify the day of the week (Sunday, Monday...)	
	• (Optional) For *month*, specify the month (January, February...)	
	• (Optional) For *hh*:*mm*, specify the time (24-hour format) in hours and minutes	
	• (Optional) For *offset*, specify the number of minutes to add during summer time; default is 60	
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries.	**show running-config**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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.

This example shows how to specify that summer time starts on the first Sunday in June at 02:00 and ends on the last Sunday in September at 02:00:

```
Switch(config)# clock summer-time PDT recurring 1 Sunday June 2:00 last Sunday September
2:00
```

Beginning in privileged EXEC mode, 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):

Steps		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Configure summer time to start on the first date and end on the second date.	**clock summer-time** *zone* **date** [*month date year* *hh***:***mm month date year hh***:***mm* [*offset*]]
	Summer time is disabled by default.	or
	• For *zone*, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect	**clock summer-time** *zone* **date** [*date month year* *hh***:***mm date month year hh***:***mm* [*offset*]]
	• (Optional) For *week*, specify the week of the month (1 to 5 or **last**)	
	• (Optional) For *day*, specify the day of the week (Sunday, Monday...)	
	• (Optional) For *month*, specify the month (January, February...)	
	• (Optional) For *hh***:***mm*, specify the time (24-hour format) in hours and minutes	
	• (Optional) For *offset*, specify the number of minutes to add during summer time; default is 60	
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries.	**show running-config**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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.

This example shows how to set summer time to start on June 20, 2010, at 02:00, and end on September 23, 2010, at 02:00:

```
Switch(config)# clock summer-time pdt date 20 June 2010 2:00 23 September 2010 2:00
```

Configuring a System Name and Prompt

You configure the system name on the switch module 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.

For complete syntax and usage information for the commands used in this section, see the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* and the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*.

These sections contain this configuration information:

Default System Name and Prompt Configuration

The default switch module system name and prompt is *Switch*.

Configuring a System Name

Beginning in privileged EXEC mode, follow these steps to manually configure a system name:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Manually configure a system name. The default setting is *switch*. 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.	**hostname** *name*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries.	**show running-config**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-confi**g

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.

Understanding 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 module, 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.

These sections contain this configuration information:

- Default DNS Configuration, page 6-17
- Setting Up DNS, page 6-17
- Displaying the DNS Configuration, page 6-18

Default DNS Configuration

Table 6-2 shows the default DNS configuration.

Table 6-2   Default DNS Configuration

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

Setting Up DNS

Beginning in privileged EXEC mode, follow these steps to set up your switch module to use the DNS:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Define a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name. At boot time, no domain name is configured; however, if the switch module 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).	**ip domain-name** *name*

Step		Command
Step 3	Specify the address of one or more name servers to use for name and address resolution.	**ip name-server** *server-address1* [*server-address2 ... server-address6*]
	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 module sends DNS queries to the primary server first. If that query fails, the backup servers are queried.	
Step 4	(Optional) Enable DNS-based hostname-to-address translation on your switch module. This feature is enabled by default.	**ip domain-lookup**
	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).	
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries.	**show running-config**
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

If you use the switch module 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.

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 module, use the **no ip domain-lookup** global configuration command.

Displaying the DNS Configuration

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

Creating a Banner

You can configure a message-of-the-day (MOTD) and a login banner. The MOTD banner displays 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 also displays 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 12.2.*

These sections contain this configuration information:

Default Banner Configuration

The message of the day and login banners are not configured by default.

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 module.

Beginning in privileged EXEC mode, follow these steps to configure a message of the day login banner:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the message of the day. For *c*, enter 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. For *message*, enter a banner message up to 255 characters. You cannot use the delimiting character in the message.	**banner motd** *c message c*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries.	**show running-config**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To delete the message of the day banner, use the **no banner motd** global configuration command.

This example shows how to configure a message of the day banner for the switch module 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 172.2.5.4
Trying 172.2.5.4...
Connected to 172.2.5.4.
Escape character is '^]'.

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

User Access Verification

Password:
```

Configuring a Login Banner

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

Beginning in privileged EXEC mode, follow these steps to configure a login banner:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the login message.	**banner login** *c message c*
	For *c*, enter 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.	
	For *message*, enter a login message up to 255 characters. You cannot use the delimiting character in the message.	
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries.	**show running-config**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

This example shows how to configure a login banner for the switch module 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)#
```

Monitoring Temperature and Configuring the Yellow Threshold

The CGR 2010 ESM includes sensors that measure and monitor the status and internal temperature of critical components. Internal component temperatures are measured for the central processor, internal components, and interface cards.

The measured temperature is compared to predetermined threshold limits and, if the temperature does not fall within the limits, the information is recorded and a warning sent to the system administrator by means of Simple Network Management Protocol (SNMP) traps until the temperature falls back to its normal range.

- Use the **show env temperature status** privileged EXEC command to display the current temperature value, state, and thresholds of the switch module's CPU and Ethernet board (see Table 6-3 below). The temperature value is the temperature in the switch module (not the external temperature). If the temperature exceeds the threshold, a warning message is sent.

- You can configure the yellow threshold level (in Celsius) by using the **system env temperature threshold yellow** *value* global configuration command to set the difference between the yellow and red thresholds. You cannot configure the green or red thresholds (see "Configuring the Yellow Threshold" below for details).

Temperature Show Commands

The switch module monitors the temperature conditions to determine the health of the power supplies. The temperature value is the temperature in the switch module (not the external temperature).

Table 6-3 describes the **Show** commands that monitor the switch module's temperature:

Table 6-3   Temperature Show Commands

Command	Function
Switch# **show env** *all	temperature status*	• *all*: Displays all environmental monitor parameters and enhanced to show the history data. • *temperature status*: Shows temperature status and threshold levels of the switch module's CPU and Ethernet board.

Configuring the Yellow Threshold

You cannot configure the green and red thresholds but you can configure the yellow threshold.

Use the **system env temperature threshold yellow** *value* global configuration command to specify the difference between the yellow and red threshold values and to configure the yellow threshold (in Celsius). The range is 20 to 25. The default value is 20.

For example, if the red threshold is 60º C and you want to configure the yellow threshold as 51º C (a 9º difference), set the 9º difference between the red and yellow thresholds by using the **system env temperature threshold yellow 9** command.

Use the **no** form of this command to return to the default value.

The default yellow thresholds differ for the switch module's Copper and SFP models (see Table 6-4).

Table 6-4   Default Yellow and Red Thresholds for Copper and SFP Models

Model	Default Yellow Threshold	Default Red Threshold
GRWIC-D-ES-2S-8PC (Copper model)	85ºC	105º C
GRWIC-D-ES-6S (SFP model)	90º C	105º C

Managing the MAC Address Table

The MAC address table contains address information that the switch module 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 module 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 module 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.

These sections contain this configuration information:

Building the Address Table

With multiple MAC addresses supported on all ports, you can connect any port on the switch module to individual workstations, repeaters, switches, routers, or other network devices. The switch module 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 stations are added or removed from the network, the switch module 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 module maintains an address table for each VLAN, and STP can accelerate the aging interval on a per-VLAN basis.

The switch module sends packets between any combination of ports, based on the destination address of the received packet. Using the MAC address table, the switch module 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 module 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 1, 9, and 10 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.

For more information about private VLANs, see Chapter 12, "Private VLAN Configuration."

Customers in a service provider network can tunnel a large number of MAC addresses through the network and fill up the available MAC address table space. You can control MAC address learning on a VLAN and manage the MAC address table space that is available on the switch module by controlling which VLANs, and 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 module system configuration. Disabling MAC address learning on a VLAN could cause flooding in the network. See the "Disabling MAC Address Learning on a VLAN" section on page 6-32 for more information.

Default MAC Address Table Configuration

Table 6-5 shows the default MAC address table configuration.

Table 6-5   Default MAC Address Table Configuration

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

Changing the Address Aging Time

Dynamic addresses are source MAC addresses that the switch module learns and then ages when they are not in use. You can change the aging time setting for all VLANs or for a specified VLAN.

Setting too short an aging time can cause addresses to be prematurely removed from the table. Then when the switch module receives a packet for an unknown destination, it floods the packet to all ports in the same VLAN as the receiving port. This unnecessary flooding can impact performance. Setting too long an aging time can cause the address table to be filled with unused addresses, which prevents new addresses from being learned. Flooding results, which can impact switch module performance.

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.	**mac address-table aging-time** [**0** | *10-1000000*] [**vlan** *vlan-id*]
	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.	
	For *vlan-id*, valid IDs are 1 to 4094. Do not enter leading zeros.	
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries.	**show mac address-table aging-time**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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 module 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.

Beginning in privileged EXEC mode, follow these steps to configure the switch module to send MAC address change notification traps to an NMS host:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the recipient of the trap message. • For *host-addr*, specify the name or address of the NMS. • Specify **traps** (the default) to send SNMP traps to the host. Specify **informs** to send SNMP informs to the host. • Specify the SNMP version to support. Version 1, the default, is not available with informs. • For *community-string,* specify 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. • For *notification-type*, use the **mac-notification** keyword.	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string* *notification-type*
Step 3	Enable the switch module to send MAC address change notification traps to the NMS.	**snmp-server enable traps mac-notification change**
Step 4	Enable the MAC address change notification feature.	**mac address-table notification change**

	Step	Command
Step 5	Enter the trap interval time and the history table size. • (Optional) For **interval** *value,* specify 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) For **history-size** *value*, specify the maximum number of entries in the MAC notification history table. The range is 0 to 500; the default is 1.	**mac address-table notification change** [**interval** *value*] [**history-size** *value*]
Step 6	Enter interface configuration mode, and specify the Layer 2 interface on which to enable the SNMP MAC address notification trap.	**interface** *interface-id*
Step 7	Enable the MAC address change notification trap on the interface. • Enable the trap when a MAC address is **added** on this interface. • Enable the trap when a MAC address is **removed** from this interface.	**snmp trap mac-notification change** {**added** | **removed**}
Step 8	Return to privileged EXEC mode.	**end**
Step 9	Verify your entries.	**show mac address-table notification change interface** **show running-config**
Step 10	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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.

This example shows how to specify 172.20.10.10 as the NMS, enable the switch module to send 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 gigabitethernet0/2
Switch(config-if)# snmp trap mac-notification change added
```

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.

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.

Beginning in privileged EXEC mode, follow these steps to configure the switch module to send MAC address-move notification traps to an NMS host:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the recipient of the trap message. • For *host-addr*, specify the name or address of the NMS. • Specify **traps** (the default) to send SNMP traps to the host. Specify **informs** to send SNMP informs to the host. • Specify the SNMP version to support. Version 1, the default, is not available with informs. • For *community-string,* specify 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. • For *notification-type*, use the **mac-notification** keyword.	**snmp-server host** *host-addr* {**traps**	**informs**} {**version** {**1**	**2c**	**3**}} *community-string notification-type*
Step 3	Enable the switch module to send MAC address move notification traps to the NMS.	**snmp-server enable traps mac-notification move**
Step 4	Enable the MAC address move notification feature.	**mac address-table notification mac-move**
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries.	**show mac address-table notification mac-move** **show running-config**
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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.

This example shows how to specify 172.20.10.10 as the NMS, enable the switch module to send MAC address move notification traps to the NMS, enable the MAC address move notification feature, and enable traps when a MAC address moves from one port to another.

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
```

```
Switch(config)# snmp-server enable traps mac-notification move
Switch(config)# mac address-table notification mac-move
```

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.

Beginning in privileged EXEC mode, follow these steps to configure the switch module to send MAC address table threshold notification traps to an NMS host:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the recipient of the trap message. • For *host-addr*, specify the name or address of the NMS. • Specify **traps** (the default) to send SNMP traps to the host. Specify **informs** to send SNMP informs to the host. • Specify the SNMP version to support. Version 1, the default, is not available with informs. • For *community-string,* specify 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. • For *notification-type*, use the **mac-notification** keyword.	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*
Step 3	Enable the switch module to send MAC threshold notification traps to the NMS.	**snmp-server enable traps mac-notification threshold**
Step 4	Enable the MAC address threshold notification feature.	**mac address-table notification threshold**

Step		Command
Step 5	Enter the threshold value for the MAC address threshold usage monitoring. • (Optional) For limit percentage, specify the percentage of the MAC address table use; valid values are from 1 to 100 percent. The default is 50 percent. • (Optional) For interval time, specify the time between notifications; valid values are greater than or equal to 120 seconds. The default is 120 seconds.	**mac address-table notification threshold** [**limit** *percentage*]	[**interval** *time*]
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Verify your entries.	**show mac address-table notification threshold** **show running-config**
Step 8	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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.

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
```

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

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 module 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 module 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 Chapter 12, "Private VLAN Configuration."

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Add a static address to the MAC address table. • For *mac-addr*, specify 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. • For *vlan-id*, specify the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094; do not enter leading zeros. • For *interface-id*, specify 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.	**mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries.	**show mac address-table static**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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.

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
gigabitethernet0/1
```

Configuring Unicast MAC Address Filtering

When unicast MAC address filtering is enabled, the switch module 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 module 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 module 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 module adds the MAC address as a static address.

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

Beginning in privileged EXEC mode, follow these steps to configure the switch module to drop a source or destination unicast static address:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable unicast MAC address filtering and configure the switch module to drop a packet with the specified source or destination unicast static address. • For *mac-addr*, specify a source or destination unicast MAC address. Packets with this MAC address are dropped. • For *vlan-id*, specify the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094.	**mac address-table static** *mac-addr* **vlan** *vlan-id* **drop**
Step 3	Return to privileged EXEC mode.	**end**

	Step	Command
Step 4	Verify your entries.	**show mac address-table static**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

This example shows how to enable unicast MAC address filtering and to configure the switch module to 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
```

Disabling MAC Address Learning on a VLAN

By default, MAC address learning is enabled on all VLANs on the switch module. You can control MAC address learning on a VLAN to manage the available MAC address table space by controlling which VLANs, and 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 module 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 module virtual interface (SVI). The switch module then floods all IP packets in the Layer 2 domain.

- You can disable MAC address learning on a single VLAN ID from 1 to 4094 (for example, **no mac address-table learning vlan 223**) or a range of VLAN IDs, separated by a hyphen or comma (for example, **no mac address-table learning vlan 1-10, 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 module is flooded in that VLAN domain.

- You cannot disable MAC address learning on a VLAN that is used internally by the switch module. If the VLAN ID that you enter is an internal VLAN, the switch module 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.

Beginning in privileged EXEC mode, follow these steps to disable MAC address learning on a VLAN

:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	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 1 to 4094. It cannot be an internal VLAN.	**no mac address-table learning vlan** *vlan-id*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify the configuration.	**show mac address-table learning** [**vlan** *vlan-id*]
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To reenable MAC address learning on a VLAN, use the **default mac address-table learning vlan** *vlan-id* global configuration command. You can also reenable MAC address learning on a VLAN by entering the **mac address-table learning vlan** *vlan-id* global configuration command. The first (**default**) command returns to a default condition and 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.

This example shows how to disable MAC address learning on VLAN 200:

```
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.

Displaying MAC Address Table Entries

You can display the MAC address table by using one or more of the privileged EXEC commands described in Table 6-6:

Table 6-6   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.

Table 6-6   Commands for Displaying the MAC Address Table (continued)

Command	Description
show mac address-table interface	Displays the MAC address table information for the specified interface.
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.

Managing the ARP Table

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 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 Chapter 2, "Command Line Interface" and the Cisco IOS Release 12.2 documentation on Cisco.com.