

set

To display all of the ROM monitor command variable names, along with their values, use the **set** command.

set

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Types ROM monitor command

Command Modes Normal

Examples This example shows how to use the **set** command to display all of the monitor variable names along with their values:

```
rommon 1 > set
PS1=rommon ! >
BOOT=
?=0
rommon 2 >
```

Related Commands [varname=](#)

set accounting commands

To enable command event accounting on the switch, use the **set accounting commands** command.

```
set accounting commands enable { config | enable | all } [stop-only]{ tacacs+ }
```

```
set accounting commands disable
```

Syntax Description

enable	Enables the specified accounting method for commands.
config	Enables accounting for configuration commands only.
enable	Enables accounting for enable mode commands only.
all	Enables accounting for all commands.
stop-only	(Optional) Accounting method that applies at the conclusion of the command.
tacacs+	TACACS+ accounting for commands.
disable	Disables accounting for commands.

Defaults

Accounting is disabled.

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

You must configure the TACACS+ servers before you enable accounting.

Examples

This example shows how to enable accounting for configuration commands when sending records only upon termination of the event, using a TACACS+ server:

```
Console> (enable) set accounting commands enable config stop-only tacacs+
Accounting set to enable for commands-config events in stop-only mode.
Console> (enable)
```

This example shows how to enable accounting for all commands when sending records only upon termination of an event, using a TACACS+ server:

```
Console> (enable) set accounting commands enable all stop-only tacacs+
Accounting set to enable for commands-all events in stop-only mode.
Console> (enable) reset cancel
```

This example shows how to disable command accounting:

```
Console> (enable) set accounting commands disable
Accounting set to disable for commands-config events.
Console> (enable)
```

This example shows how to configure accounting for enable mode commands:

```
Console> (enable) set accounting commands enable enable stop-only tacacs+
Accounting set to enable for commands-enable-mode event in stop-only mode.
```

Related Commands

[set accounting connect](#)
[set accounting exec](#)
[set accounting suppress](#)
[set accounting system](#)
[set accounting update](#)
[set tacacs server](#)
[show accounting](#)

set accounting connect

To enable tracking of outbound connection events on the switch, use the **set accounting connect** command.

```
set accounting connect enable {start-stop | stop-only} {tacacs+ | radius}
```

```
set accounting connect disable
```

Syntax Description		
enable	Enables the specified accounting method for connection events.	
start-stop	Accounting method that applies at the start and stop of the connection event.	
stop-only	Accounting method that applies at the conclusion of the connection event.	
tacacs+	TACACS+ accounting for connection events.	
radius	RADIUS accounting for connection events.	
disable	Disables accounting of connection events.	

Defaults Accounting is disabled.

Command Types Switch command

Command Modes Privileged

Usage Guidelines You must configure the RADIUS or TACACS+ servers and shared keys before enabling accounting.

Examples This example shows how to enable accounting on Telnet and rlogin sessions when generating records at stop only, using a TACACS+ server:

```
Console> (enable) set accounting connect enable stop-only tacacs+
Accounting set to enable for connect events in stop-only mode.
Console> (enable)
```

This example shows how to disable accounting:

```
Console> (enable) set accounting connect disable
Accounting set to disable for connect events.
Console> (enable)
```

Related Commands

[set accounting commands](#)
[set accounting exec](#)
[set accounting suppress](#)
[set accounting system](#)
[set accounting update](#)
[set radius key](#)
[set tacacs key](#)
[set tacacs server](#)
[show accounting](#)

set accounting exec

To enable tracking of Normal mode sessions on the switch, use the **set accounting exec** command.

```
set accounting exec enable {start-stop | stop-only} {tacacs+ | radius}
```

```
set accounting exec disable
```

Syntax Description	enable	Enables the specified accounting method for Normal mode events.
	start-stop	Accounting method applied at the start and stop of the Normal mode event.
	stop-only	Accounting method applied at the conclusion of the Normal mode event.
	tacacs+	TACACS+ accounting for Normal mode events.
	radius	RADIUS accounting for Normal mode events.
	disable	Disables accounting for Normal mode events.

Defaults Accounting is disabled.

Command Types Switch command

Command Modes Privileged

Usage Guidelines You must configure the RADIUS or TACACS+ servers and shared keys before enabling accounting.

Examples This example shows how to enable accounting of Normal login mode events when generating records at start and stop, using a RADIUS server:

```
Console> (enable) set accounting exec enable start-stop radius
Accounting set to enable for exec events in start-stop mode.
Console> (enable)
```

This example shows how to enable accounting of Normal login mode events when generating records at stop only, using a RADIUS server:

```
Console> (enable) set accounting exec enable stop-only radius
Accounting set to enable for exec events in stop-only mode.
Console> (enable)
```

This example shows how to enable accounting of Normal login mode events when generating records at start and stop, using a TACACS+ server:

```
Console> (enable) set accounting exec enable start-stop tacacs+
Accounting set to enable for exec events in start-stop mode.
Console> (enable)
```

This example shows how to enable accounting of Normal login mode events when generating records at stop only, using a TACACS+ server:

```
Console> (enable) set accounting exec enable stop-only tacacs+  
Accounting set to enable for exec events in stop-only mode.  
Console> (enable)
```

This example shows how to disable accounting of Normal login mode events:

```
Console> (enable) set accounting exec disable  
Accounting set to disable for exec events in start-stop mode.  
Console> (enable)
```

Related Commands

- [set accounting commands](#)
- [set accounting connect](#)
- [set accounting suppress](#)
- [set accounting system](#)
- [set accounting update](#)
- [set radius key](#)
- [set radius server](#)
- [set tacacs key](#)
- [set tacacs server](#)
- [show accounting](#)

set accounting suppress

To enable or disable suppression of accounting information for a user who has logged in without a username, use the **set accounting suppress** command.

```
set accounting suppress null-username {enable | disable}
```

Syntax Description	Command	Description
	null-username	Unknown users.
	enable	Enables suppression for unknown users.
	disable	Disables suppression for unknown users.

Defaults Accounting is disabled.

Command Types Switch command

Command Modes Privileged

Usage Guidelines You must configure the TACACS+ servers and shared keys before enabling accounting.

Examples This example shows how to suppress accounting information for users who have logged in without a username:

```
Console> (enable) set accounting suppress null-username enable
Accounting will be suppressed for user with no username.
Console> (enable)
```

This example shows how to include accounting-event information of users who have logged in without a username:

```
Console> (enable) set accounting suppress null-username disable
Accounting will be not be suppressed for user with no username.
Console> (enable)
```

Related Commands

- [set accounting commands](#)
- [set accounting connect](#)
- [set accounting exec](#)
- [set accounting system](#)
- [set accounting update](#)
- [set tacacs key](#)
- [set tacacs server](#)
- [show accounting](#)

set accounting system

to enable accounting of system events on the switch, use the **set accounting system** command.

```
set accounting system enable {start-stop | stop-only} {tacacs+ | radius}
```

```
set accounting system disable
```

Syntax Description	enable	Enables the specified accounting method for system events.
	start-stop	Accounting method applied at the start and stop of the system event.
	stop-only	Accounting method applied at the conclusion of the system event.
	tacacs+	TACACS+ accounting for system events.
	radius	RADIUS accounting for system events.
	disable	Disables accounting for system events.

Defaults Accounting is disabled.

Command Types Switch command

Command Modes Privileged

Usage Guidelines You must configure the RADIUS or TACACS+ servers and shared keys before enabling accounting.

Examples This example shows how to enable accounting for system events when sending records only upon termination of the event, using a RADIUS server:

```
Console> (enable) set accounting system enable stop-only radius
Accounting set to enable for system events in start-stop mode.
Console> (enable)
```

This example shows how to enable accounting for system events when sending records upon the start-stop of the event, using a RADIUS server:

```
Console> (enable) set accounting system enable start-stop radius
Accounting set to enable for system events in start-stop mode.
Console> (enable)
```

This example shows how to enable accounting for system events when sending records only upon termination of the event, using a TACACS+ server:

```
Console> (enable) set accounting system enable stop-only tacacs+
Accounting set to enable for system events in start-stop mode.
Console> (enable)
```

This example shows how to enable accounting for system events when sending records upon the start-stop of the event, using a TACACS server:

```
Console> (enable) set accounting system enable start-stop tacacs+  
Accounting set to enable for system events in start-stop mode.  
Console> (enable)
```

This example shows how to disable accounting for system events:

```
Console> (enable) set accounting system disable  
Accounting set to disable for system events.  
Console> (enable)
```

Related Commands

- [set accounting commands](#)
- [set accounting connect](#)
- [set accounting exec](#)
- [set accounting suppress](#)
- [set accounting update](#)
- [set radius key](#)
- [set radius server](#)
- [set tacacs key](#)
- [set tacacs server](#)
- [show accounting](#)

set accounting update

To configure the frequency of accounting updates, use the **set accounting update** command.

```
set accounting update { new-info | periodic [interval] }
```

Syntax Description	
new-info	Update only when new information is available.
periodic	Update periodically.
<i>interval</i>	(Optional) Periodic update interval time in minutes; valid intervals are from 1 to 71582 minutes.

Defaults Accounting is disabled.

Command Types Switch command

Command Modes Privileged

Usage Guidelines You must configure the TACACS+ servers and shared keys before enabling accounting.

Examples This example shows how to send accounting updates every 200 minutes:

```
Console> (enable) set accounting update periodic 200
Accounting updates will be periodic at 200 minute intervals.
Console> (enable)
```

This example shows how to send accounting updates only when there is new information:

```
Console> (enable) set accounting update new-info
Accounting updates will be sent on new information only.
Console> (enable)
```

Related Commands

- [set accounting commands](#)
- [set accounting connect](#)
- [set accounting exec](#)
- [set accounting suppress](#)
- [set accounting system](#)
- [set radius key](#)
- [set radius server](#)
- [set tacacs key](#)
- [set tacacs server](#)
- [show accounting](#)

set alias

To define command aliases (shortened versions of command names), use the **set alias** command.

```
set alias name command [parameter]
```

Syntax Description	
<i>name</i>	Name for the alias being created.
<i>command</i>	Command for which the alias is being created.
<i>parameter</i>	(Optional) Parameter that applies to the command for which an alias is being created. See the specific command for valid parameters.

Defaults No aliases are configured.

Command Types Switch command

Command Modes Privileged

Usage Guidelines The name **all** cannot be defined as an alias. Reserved words cannot be defined as aliases.

Examples This example shows how to set arpdel as the alias for the **clear arp** command:

```
Console> (enable) set alias arpdel clear arp
Command alias added.
Console> (enable)
```

Related Commands [show alias](#)

set arp

To add IP address-to-MAC address mapping entries to the ARP table and to set the ARP aging time for the table, use the **set arp** command.

```
set arp [dynamic | permanent | static] [ip_addr | hw_addr]
```

```
set arp agingtime agingtime
```

Syntax	Description
dynamic	(Optional) Entries are subject to ARP aging updates.
permanent	(Optional) Stores permanent entries in NVRAM until they are cleared by the clear arp or clear config command.
static	(Optional) Entries are not subject to ARP aging updates.
<i>ip_addr</i>	(Optional) IP address or IP alias to map to the specified MAC address.
<i>hw_addr</i>	(Optional) MAC address to map to the specified IP address or IP alias.
agingtime	Period of time after which an ARP entry is deleted from the ARP table.
<i>agingtime</i>	Number of seconds (from 0 to 1000000) for which entries will remain in the ARP table before being deleted. Setting this value to 0 disables aging.

Defaults

The default settings are as follows:

- No ARP table entries exist
- ARP aging is 1200 seconds

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

hw_addr is 6-hexbyte MAC address expressed in canonical (00-11-22-33-44-55) or noncanonical (00:11:22:33:44:55) format.

Examples

This example shows how to configure a dynamic ARP entry mapping that will age out after the configured ARP aging time:

```
Console> (enable) set arp dynamic 198.133.219.232 00-00-0c-40-0f-bc
ARP entry added.
Console> (enable)
```

This example shows how to set the aging time for the ARP table to 1800 seconds (30 minutes):

```
Console> (enable) set arp agingtime 1800
ARP aging time set to 1800 seconds.
Console> (enable)
```

This example shows how to configure a permanent ARP entry, which will remain in the ARP cache after a system reset:

```
Console> (enable) set arp permanent 198.146.232.23 00-00-0c-30-0f-bc  
Permanent ARP entry added as 198.146.232.23 at 00-00-0c-30-0f-bc on vlan 5  
Console> (enable)
```

This example shows how to configure a static ARP entry, which will be deleted from the ARP cache after a system reset:

```
Console> (enable) set arp static 198.144.239.22 00-00-0c-50-0f-bc  
Static ARP entry added as 198.144.239.22 at 00-00-0c-50-0f-bc on vlan 5  
Console> (enable)
```

Related Commands

[clear arp](#)
[show arp](#)

set authentication enable

To configure the switch to use RADIUS, TACACS+, Kerberos, or local authentication to authenticate privileged (enable) mode access on the switch, use the **set authentication enable** command.

```
set authentication enable {radius | tacacs | kerberos} {enable} [console | telnet | http | all]
[primary]
```

```
set authentication enable {radius | tacacs | kerberos} {disable} [console | telnet | http | all]
```

```
set authentication enable local {enable | disable} [console | telnet | http | all]
```

```
set authentication enable attempt {count} [console | remote]
```

```
set authentication enable lockout {time} [console | remote]
```

Syntax Description		
radius		RADIUS authentication for privileged mode access.
tacacs		TACACS+ authentication for privileged mode access.
kerberos		Kerberos authentication for privileged mode access.
enable		Enables the specified authentication method for privileged mode access.
console	(Optional)	Applies the authentication method to console sessions.
telnet	(Optional)	Applies the authentication method to Telnet sessions.
http	(Optional)	Applies the authentication method to HTTP sessions.
all	(Optional)	Applies the authentication method to all sessions.
primary	(Optional)	Authentication method must be tried first.
disable		Disables the specified authentication method for privileged mode access.
local		Local authentication for privileged mode access.
attempt		Number of login attempts.
<i>count</i>		Number of allowed login attempts; valid configurable login attempt range is between 3 (default) to 10. Setting the maximum attempts to zero (0) disables limit checking.
remote	(Optional)	Applies the authentication method to remote logins such as Telnet, SSH, Kerberos, and HTTP.
lockout		Period of time a user is locked out of the switch after unsuccessfully attempting to log in.
<i>time</i>		Period of time a user is locked out in seconds.; valid configurable lockout range is between 30 to 7200 seconds (1/2 minute to 2 hours). Setting the time to zero (0) disables the lockout time.

Defaults

The default settings are as follows:

- Local authentication is enabled for console and Telnet sessions.
- RADIUS, TACACS+, and Kerberos are disabled for all session types.

Command Types

Switch command

Command Modes Privileged

Usage Guidelines

You can specify TACACS+ or RADIUS as the primary authentication method for login and enable access by entering the **primary** keyword. If you enter the **primary** keyword, the specified authentication method will be tried first. If you do not specify a primary authentication, authentication will be tried in the order in which you enabled the authentication methods.

You can specify that the authentication method applies to console sessions, Telnet sessions, or both, by entering the **console or telnet** keyword. If you do not specify **console** or **telnet** the authentication method applies to both console and Telnet sessions.

Examples

This example shows how to use the TACACS+ server to determine if a user has privileged access permission:

```
Console> (enable) set authentication enable tacacs enable
tacacs enable authentication set to enable for console, telnet and http session.
Console> (enable)
```

This example shows how to use the local password to determine if the user has privileged access permission:

```
Console> (enable) set authentication enable local enable
local enable authentication set to enable for console, telnet and http session.
Console> (enable)
```

This example shows how to use the RADIUS server to determine if a user has privileged access permission for all session types:

```
Console> (enable) set authentication enable radius enable
radius enable authentication set to enable for console, telnet and http session.
Console> (enable)
```

This example shows how to use the TACACS+ server to determine if a user has privileged access permission for a console session:

```
Console> (enable) set authentication enable tacacs enable console
tacacs enable authentication set to enable for console session.
Console> (enable)
```

This example shows how to set the Kerberos server to be used first:

```
Console> (enable) set authentication enable kerberos enable primary
kerberos enable authentication set to enable for console, telnet and http session
n as primary authentication method.
Console> (enable)
```

This example shows how to set the enable login attempt to 5 for both console and remote sessions:

```
Console> (enable) set authentication enable attempt 5
Enable mode authentication attempts for console and remote login set to 5.
Console> (enable)
```

This example shows how to set the enable login attempt to 7 for remote sessions:

```
Console> (enable) set authentication enable attempt 7 remote
Enable mode authentication attempts for remote login set to 7.
Console> (enable)
```

This example shows how to set the enable login attempt to 8 for console sessions:

```
Console> (enable) set authentication enable attempt 8 console  
Enable mode authentication attempts for console login set to 8.  
Console> (enable)
```

This example shows how to set the enable lockout time for both console and remote sessions to 50 seconds:

```
Console> (enable) set authentication enable lockout 50  
Enable mode lockout time for console and remote login set to 50 seconds.  
Console> (enable)
```

This example shows how to set the enable lockout time for console sessions to 5 minutes:

```
Console> (enable) set authentication enable lockout 300 console  
Enable mode lockout time for console login set to 5 minutes.  
Console> (enable)
```

This example shows how to set the enable lockout time for remote sessions to 7 minutes and 10 seconds:

```
Console> (enable) set authentication enable lockout 430 remote  
Enable mode lockout time for console and remote login set to 7 minutes and 10 seconds.  
Console> (enable)
```

Related Commands

[set authentication login](#)
[show authentication](#)

set authentication login

To configure the switch to use TACACS+, Kerberos, RADIUS, or local authentication to authenticate Normal (login) mode access on the switch, use the **set authentication login** command.

```
set authentication login attempt count [console | remote]
```

```
set authentication login lockout time [console | remote]
```

```
set authentication login {radius | tacacs | kerberos} enable [console | telnet | http | all]
    [primary]
```

```
set authentication login {radius | tacacs | kerberos} disable [console | telnet | http | all]
```

```
set authentication login local {enable | disable} [console | telnet | http | all]
```

Syntax Description

attempt <i>count</i>	Number of login attempts.
remote	(Optional) Authentication method applies to remote logins such as Telnet, SSH, kerberos, and HTTP.
lockout <i>time</i>	Period of time a user is locked out of the switch after unsuccessfully attempting to log in. The configurable range is 30 to 7200 seconds. Setting the lockout time to zero (0) disables this function.
radius	RADIUS authentication for Normal mode access.
tacacs	TACACS+ authentication for Normal mode access.
kerberos	Kerberos authentication for Normal mode access.
enable	Enables the specified authentication method for Normal mode access.
console	(Optional) Applies the authentication method to console sessions.
telnet	(Optional) Applies the authentication method to Telnet sessions.
http	(Optional) Applies the authentication method to HTTP sessions.
all	(Optional) Applies the authentication method to all sessions.
primary	(Optional) Authentication method be tried first.
disable	Disables the specified authentication method for Normal mode access.
local	Local authentication for Normal mode access.

Defaults

The defaults settings are as follows:

- Three login attempts.
- Local authentication is the primary authentication method for login.

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

This command allows you to choose the authentication method for the web interface. If you configure the authentication method for the HTTP session as RADIUS, then the username or password is validated using the RADIUS protocol, and TACACS+ and Kerberos authentication is set to disable for the HTTP sessions. By default, the HTTP login is validated using the local login password.

You can specify the authentication method for **console**, **telnet**, **http**, or **all** by entering the **console**, **telnet**, **http**, or **all** keywords. If you do not specify **console**, **telnet**, **http**, or **all**, the authentication method default is for **all** sessions.

The maximum number of login attempts from SNMP and the command-line interface (CLI) can be configured. The configurable range is from 0 to 10. To disable login attempts, set the level to 0. Failed login system logs are generated after five unsuccessful login attempts. If you are attempting access to enable mode, and the password fails more than the number of attempts allowed, the system will disable the execution of the **enable** command for the lockout time.

The lockout time is configurable from SNMP and the CLI. The configurable range is from 30 to 600 seconds (half a minute to ten minutes). For console login, the console will not allow logging in during that time. For remote logins the connection will be closed when the limit is reached, and any subsequent log in attempts from that station will be closed immediately by the switch.

When attempt limit checking is disabled, the lockout restriction is no longer applicable.

Examples

This example shows how to set the login attempt to 5 for both console and remote sessions:

```
Console> (enable) set authentication login attempt 5
Login authentication attempts for console and remote login set to 5.
Console> (enable)
```

This example shows how to set the login attempt to 7 for remote sessions:

```
Console> (enable) set authentication login attempt 7 remote
Login authentication attempts for remote login set to 7.
Console> (enable)
```

This example shows how to set the login attempt to 8 for console sessions:

```
Console> (enable) set authentication login attempt 8 console
Login authentication attempts for console login set to 8.
Console> (enable)
```

This example shows how to set the lockout time for both console and remote sessions to 50 seconds:

```
Console> (enable) set authentication login lockout 50
Login lockout time for console and remote login set to 50 seconds.
Console> (enable)
```

This example shows how to set the lockout time for console sessions to 5 minutes:

```
Console> (enable) set authentication login lockout 300 console
Login lockout time for console login set to 5 minutes.
Console> (enable)
```

This example shows how to set the lockout time for remote sessions to 7 minutes and 10 seconds:

```
Console> (enable) set authentication login lockout 430 remote
Login lockout time for console and remote login set to 7 minutes and 10 seconds.
Console> (enable)
```

This example shows how to disable TACACS+ authentication access for Telnet sessions:

```
Console> (enable) set authentication login tacacs disable telnet  
tacacs login authentication set to disable for the telnet sessions.  
Console> (enable)
```

This example shows how to disable RADIUS authentication access for console sessions:

```
Console> (enable) set authentication login radius disable console  
radius login authentication set to disable for the console sessions.  
Console> (enable)
```

This example shows how to disable Kerberos authentication access for Telnet sessions:

```
Console> (enable) set authentication login kerberos disable telnet  
kerberos login authentication set to disable for the telnet sessions.  
Console> (enable)
```

This example shows how to set TACACS+ authentication access as the primary method for HTTP sessions:

```
Console> (enable) set authentication login tacacs enable http primary  
tacacs login authentication set to enable for HTTP sessions as primary authentication  
method.  
Console> (enable)
```

Related Commands

[set authentication enable](#)
[show authentication](#)

set authorization commands

To enable authorization of command events on the switch, use the **set authorization commands** command.

```
set authorization commands enable {config | enable | all} {option} {fallbackoption} [console | telnet | both]
```

```
set authorization commands disable [console | telnet | both]
```

Syntax Description		
enable		Enables the specified authorization method for commands.
config		Enables authorization for configuration commands only.
enable		Enables authorization for enable mode commands only.
all		Enables authorization for all commands.
<i>option</i>		Switch response to an authorization request. Valid values are tacacs+ , if-authenticated , and none . See “Usage Guidelines” for more information.
<i>fallbackoption</i>		Switch fallback response to an authorization request if the TACACS+ server is down or not responding. Valid values are tacacs+ , deny , if-authenticated , and none . See “Usage Guidelines” for more information.
console	(Optional)	Applies the authorization method to console sessions.
telnet	(Optional)	Applies the authorization method to Telnet sessions.
both	(Optional)	Applies the authorization method to both console and Telnet sessions.
disable		Disables authorization for commands.

Defaults Authorization is disabled.

Command Types Switch command

Command Modes Privileged

Usage Guidelines When you define the *option* and *fallbackoption* values, the following occurs:

- **tacacs+** specifies the TACACS+ authorization method.
- **deny** does not let you proceed.
- **if-authenticated** allows you to proceed with your action if you have been authenticated.
- **none** allows you to proceed without further authorization in case the TACACS+ server does not respond.

Examples

This example shows how to enable authorization for all commands with an **if-authenticated** option and no **fallback** option, in case the TACACS+ daemon is down or does not respond:

```
Console> (enable) set authorization commands enable all if-authenticated none  
Successfully enabled commands authorization.  
Console> (enable)
```

This example shows how to disable command authorization:

```
Console> (enable) set authorization commands disable  
Successfully disabled commands authorization.  
Console> (enable)
```

This example shows how to configure authorization for enable mode commands:

```
Console> (enable) set authorization commands enable enable tacacs+ deny telnet  
Successfully enabled commands authorization.  
Console> (enable)
```

Related Commands

[set authorization enable](#)
[set authorization exec](#)
[show authorization](#)

set authorization enable

To authorize enable (privileged mode) session events on the switch, use the **set authorization enable** command.

```
set authorization enable enable {option} {fallbackoption} [console | telnet | both]
```

```
set authorization enable disable [console | telnet | both]
```

Syntax Description	enable	Enables the specified authorization method.
	<i>option</i>	Switch response to an authorization request. Valid values are tacacs+ , if-authenticated , and none . See “Usage Guidelines” for more information.
	<i>fallbackoption</i>	Switch fallback response to an authorization request if the TACACS+ server is down or not responding. Valid values are tacacs+ , deny , if-authenticated , and none . See “Usage Guidelines” for more information.
	console	(Optional) Applies the authorization method to console sessions.
	telnet	(Optional) Applies the authorization method to Telnet sessions.
	both	(Optional) Applies the authorization method to both console and Telnet sessions.
	disable	Disables the specified authorization method.

Defaults Authorization is disabled.

Command Types Switch command

Command Modes Privileged

Usage Guidelines The **tacacs+** value allows you to proceed with your action if you have authorization. The **deny** value does not let you proceed if the TACACS+ server does not respond. The **if-authenticated** value allows you to proceed with your action if you have been authenticated. The **none** value allows you to proceed without further authorization in case the TACACS+ server does not respond.

Examples This example shows how to enable authorization of configuration commands in enable mode sessions:

```
Console> (enable) set authorization enable enable if-authenticated
Successfully enabled enable authorization.
Console> (enable)
```

This example shows how to disable enable mode authorization:

```
Console> (enable) set authorization enable disable
Successfully disabled enable authorization.
Console> (enable)
```

■ `set authorization enable`

Related Commands [set authorization commands](#)
 [set authorization exec](#)
 [show authorization](#)

set authorization exec

To enable authorization of exec (Normal mode) session events on the switch, use the **set authorization exec** command.

```
set authorization exec enable {option} {fallbackoption} [console | telnet | both]
```

```
set authorization exec disable [console | telnet | both]
```

Syntax Description		
enable		Enables the specified authorization method.
<i>option</i>		Switch response to an authorization request; valid values are tacacs+ , if-authenticated , and none . See “Usage Guidelines” for more information.
<i>fallbackoption</i>		Switch fallback response to an authorization request if the TACACS+ server is down or not responding; valid values are tacacs+ , deny , if-authenticated , and none . See “Usage Guidelines” for more information.
console		(Optional) Applies the authorization method to console sessions.
telnet		(Optional) Applies the authorization method to Telnet sessions.
both		(Optional) Applies the authorization method to console and Telnet sessions.
disable		Disables the specified authorization method.

Defaults Authorization is disabled.

Command Types Switch command

Command Modes Privileged

Usage Guidelines

The **tacacs+** value allows you to proceed with your action if you have authorization.

The **deny** value does not let you proceed if the TACACS+ server does not respond.

The **if-authenticated** value allows you to proceed with your action if you have been authenticated.

The **none** value allows you to proceed without further authorization in case the TACACS+ server does not respond.

Examples This example shows how to enable authorization of configuration commands in exec mode sessions:

```
Console> (enable) set authorization exec enable if-authenticated
Successfully enabled exec authorization.
Console> (enable)
```

This example shows how to disable exec mode authorization:

```
Console> (enable) set authorization exec disable
Successfully disabled exec authorization.
Console> (enable)
```

■ set authorization exec

Related Commands [set authorization commands](#)
[set authorization enable](#)
[show authorization](#)

set banner motd

To create a login banner that is displayed when users access the switch, use the **set banner motd** command.

```
set banner motd c [text] c
```

Syntax Description	
<i>c</i>	Delimiting character used to begin and end the message.
<i>text</i>	(Optional) Message of the day.

Defaults The MOTD banner is not displayed.

Command Types Switch command

Command Modes Privileged

Usage Guidelines The banner cannot contain more than 3070 characters, including tabs. Tabs display as eight characters but use only one character of space in memory.

You can use either the **clear banner motd** command or the **set banner motd** command to clear the message-of-the-day banner.

Examples This example shows how to set the message of the day using the pound sign (#) as the delimiting character:

```
Console> (enable) set banner motd #
** System upgrade: starting: 6:00am Tuesday.
** Please log out before leaving on Monday. #
MOTD banner set.
Console> (enable)
```

This example shows how to clear the message of the day using the **set banner motd** command:

```
Console> (enable) set banner motd ##
MOTD banner cleared.
Console> (enable)
```

Related Commands [clear banner motd](#)

set banner telnet

To create a login banner that is displayed when users access the switch using Telnet, use the **set banner telnet** command.

```
set banner telnet {enable | disable}
```

Syntax Description	enable	Displays the default console banner.
	disable	Suppresses the default console banner.

Defaults The default console banner is displayed.

Command Types Switch command

Command Modes Privileged

Examples This example shows how to enable the default console banner:

```
Console> (enable) set banner telnet enable
Cisco Systems Console banner will be printed at telnet.
Console> (enable>
```

This example shows how to disable the default console banner:

```
Console> (enable) set banner telnet disable
Cisco Systems Console banner will not be printed at telnet.
Console> (enable>
```

set boot auto-config

To specify one or more configuration files to use to configure the switch at startup and to set the recurrence option. A list of configuration files is stored in the CONFIG_FILE environment variable, use the **set boot auto-config** command.

```
set boot auto-config device:filename [;device:filename...] [mod]
```

Syntax Description	
<i>device:</i>	Device where the startup configuration file resides.
<i>filename</i>	Name of the startup configuration file.
<i>mod</i>	(Optional) Module number of the supervisor engine containing the Flash device.

Defaults

The default settings are as follows:

- The **set boot auto-config** command is non-recurring.
- The CONFIG_FILE environment variable is not defined.

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

The **set boot auto-config** command always overwrites the existing CONFIG_FILE environment variable (you cannot prepend or append a file to the variable).

Multiple configuration files can be specified in the Catalyst 4000 family switches, but they must be separated by a semicolon (;).

To set the recurrence on the Catalyst 4000 family switches, use the **set boot config-register auto-config** command.

Examples

This example shows how to specify the configuration file environment variable:

```
Console> (enable) set boot auto-config slot0:cfg1
CONFIG_FILE variable = slot0:cfg1
WARNING: nvram configuration may be lost during next bootup,
        and re-configured using the file(s) specified.
Console> (enable)
```

Related Commands

[set boot system flash](#)

set boot config-register

To set the boot configuration register value, use the **set boot config-register** command.

```
set boot config-register value [mod]
```

```
set boot config-register boot {rommon | bootflash | system} [mod]
```

```
set boot config-register baud {1200 | 2400 | 4800 | 9600} [mod]
```

```
set boot config-register ignore-config {enable | disable} [mod]
```

```
set boot config-register auto-config {recurring | non-recurring} [mod]
```

Syntax Description

value	16-bit configuration register value. This value is a hexadecimal value and the valid range is 0x0 to 0xFFFF.
<i>mod</i>	(Optional) Module number of the supervisor engine on which to set the configuration register value.
boot	Boot method to use the next time the switch is reset or the power is cycled.
rommon	Causes the switch to remain in ROM monitor mode the next time the switch is reset or the power is cycled.
bootflash	Causes the switch to boot using the first valid system image in bootflash the next time the switch is reset or the power is cycled.
system	Causes the switch to boot using the system images specified in the BOOT environment variable the next time the switch is reset or the power is cycled.
baud	Sets the console baud rate.
1200 2400 4800 9600	Baud rate for the ROM monitor console port.
ignore-config	Switch should ignore the configuration in NVRAM the next time the switch is restarted.
enable	Causes the switch to ignore the configuration in NVRAM the next time the switch is restarted.
disable	Prevents the switch from ignoring the configuration in NVRAM the next time the switch is restarted.
auto-config	Sets the switch to use the configuration in NVRAM the next time the switch is restarted.
recurring	Retains the contents of the CONFIG_FILE environment variable after the switch is reset or power cycled and configured using the files specified by the CONFIG_FILE environment variable.
non-recurring	Clears the contents of the CONFIG_FILE environment variable after the switch is reset or power cycled and before the switch is configured using the files specified by the CONFIG_FILE environment variable.

Defaults

The default settings are as follows:

- The default configuration register value is 0x10F, which specifies the following settings:
 - Boot method is “system” (the switch boots using the system images specified in the BOOT environment variable).
 - ROM monitor console port baud rate set to 9600.
 - The ignore-config parameter disabled.
 - The auto-config parameter set to non recurring.

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

We recommend that you use only the **rommon** and **system** keywords with the **set boot config-register boot** command.

Each time you enter one of the **set boot config-register** commands, the system displays all current configuration register information (the equivalent of entering the **show boot** command).

The baud rate specified in the configuration register is used by the ROM monitor only and is different from the baud rate specified by the **set system baud** command.

The auto-config_file variable is slot0:switch.cfg for **non-recurring** and bootflash:switch.cfg for the Catalyst 4000 family switches.



Caution

Enabling the **ignore-config** parameter is the same as entering the **clear config all** command; that is, it clears the entire configuration stored in NVRAM the next time the switch is restarted.



Caution

When you use the **set boot config-register 0xvalue** command we recommend that you confirm and verify the 0xvalue. If you enter an incorrect 0xvalue the switch might either boot incorrectly or lose the configuration in NVRAM.

Examples

This example shows how to specify the default 16-bit configuration register value:

```
Console> (enable) set boot config-register 0x10f
Configuration register is 0x10f
ignore-config: disabled
auto-config: non-recurring
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

This example shows how to specify rommon as the boot image to use on the next restart:

```
Console> (enable) set boot config-register boot rommon
Configuration register is 0x100
ignore-config: disabled
auto-config: non-recurring
console baud: 9600
boot: the ROM monitor
Console> (enable)
```

This example shows how to change the ROM monitor console port baud rate to 4800:

```
Console> (enable) set boot config-register baud 4800
Configuration register is 0x900
ignore-config: disabled
auto-config: non-recurring
console baud: 4800
boot: the ROM monitor
Console> (enable)
```

This example shows how to cause the switch to ignore the configuration in NVRAM the next time the switch is reset or power cycled:

```
Console> (enable) set boot config-register ignore-config enable
Configuration register is 0x940
ignore-config: enabled
auto-config: non-recurring
console baud: 4800
boot: the ROM monitor
Console> (enable)
```

This example shows how to set the auto-configuration to recurring:

```
Console> (enable) set boot config-register auto-config recurring
Configuration register is 0x960
ignore-config: enabled
auto-config: recurring
console baud: 4800
boot: the ROM monitor
Console> (enable)
```

Related Commands

[clear boot—switch](#)
[show boot—switch](#)

set boot sync now

To initiate synchronization of the auto-config file, use the **set boot sync now** command.

```
set boot sync now
```

Syntax Description This command has no arguments or keywords.

Defaults Synchronization is disabled.

Command Types Switch command

Command Modes Privileged

Usage Guidelines The **set boot sync now** command is similar to the [set boot config-register](#) command. The **set boot sync now** command initiates synchronization to force the configuration files to synchronize automatically to the standby supervisor engine. The files are kept consistent with what is on the active supervisor engine.

Examples This example shows how to initiate synchronization of the auto-config file:

```
Console> (enable) set boot sync now
Console> (enable)
```

Related Commands [set boot auto-config](#)
[show boot—switch](#)

set boot system flash

To set the BOOT environment variable, which specifies a list of software images that the switch attempts to load at startup, use the **set boot system flash** command.

set boot system flash *device:filename* [**prepend**] [*mod*]

Syntax Description	<i>device:</i>	Flash device where the software image is stored (the colon [:] is required).
	<i>filename</i>	Name of the software image file on the Flash device.
	prepend	(Optional) Places the software image file at the beginning of the list of images used to boot the switch.
	<i>mod</i>	(Optional) Module number of the supervisor engine on which to modify the BOOT environment variable.

Defaults This command has no default settings.

Command Types Switch command

Command Modes Privileged

Usage Guidelines You can enter several **boot system** commands to provide a fail-safe method for booting the switch. The system stores and executes the **boot system** commands in the order in which you enter them.

When you copy a new software image to a Flash device and want to switch to boot that image the next time the switch is reset, clear the BOOT environment variable using the **clear boot system all** command or use the **prepend** keyword to place the new software image file first in the list of images to attempt to boot.

If the file does not exist (for example, if you entered the wrong filename), then the filename is appended to the bootstring, and a message displays, “Warning: File not found but still added in the bootstring.”

If the file does exist, but is not a supervisor engine software image, the file is not added to the bootstring, and a message displays, “Warning: file found but it is not a valid boot image.”

Examples This example shows how to append a software image file to the BOOT environment variable:

```
Console> (enable) set boot system flash bootflash:cat4000-sup3.5-1-1.bin
BOOT variable =
bootflash:cat4000-sup3.5-2-1.bin,1;bootflash:cat4000-sup3.5-1-1.bin,1;
Console> (enable)
```

This example shows how to prepend a software image file to the BOOT environment variable:

```
Console> (enable) set boot system flash slot0:cat4000-sup3.5-2-1.bin prepend
BOOT variable =
slot0:cat4000-sup3.5-2-1.bin,1;bootflash:cat4000-sup3.4-5-2.bin,1;
Console> (enable)
```

Related Commands [clear boot—switch](#)
 [show boot—switch](#)

set cam

To add entries into the CAM table, use the **set cam** command.

```
set cam {dynamic | static | permanent} {unicast_mac | route_descr} {mod/port} [vlan]
```

```
set cam {static | permanent} {multicast_mac} {mod/ports...} [vlan]
```

```
set cam {static | permanent} filter {unicast_mac} [vlan]
```

Syntax Description

dynamic	Entries are subject to aging.
static	Entries are not subject to aging. Static (nonpermanent) entries will remain in the table until the system is reset.
permanent	Permanent entries are stored in NVRAM until they are cleared by the clear cam or clear config command.
<i>unicast_mac</i>	MAC address of the destination host used for a unicast.
<i>route_descr</i>	Route descriptor of the “next hop” relative to this switch. This variable is entered as two hexadecimal bytes in the following format: 004F. Do not use a hyphen (-) to separate the bytes.
<i>mod/port</i>	Number of the module and the port.
<i>vlan</i>	(Optional) Number of the VLAN. This number is optional unless you are setting CAM entries to dynamic, static, or permanent for a trunk port.
<i>multicast_mac</i>	MAC address of the destination host used for a multicast.
<i>mod/ports...</i>	Number of the module and the ports.
filter	Traffic filter entry.

Defaults

The default settings are as follows:

- The default configuration has a local MAC address.
- The spanning tree address is 01-80-c2-00-00-00.
- CDP multicast address is for destination port 1/3 (the supervisor engine).
- The Aging time for all configured VLANs is 300 seconds.

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

The *vlan* variable is required when you configure the traffic filter entry.

If the given MAC address is a multicast address (the least significant bit of the most significant byte is set to 1) or broadcast address (ff-ff-ff-ff-ff-ff) and you specify multiple ports, the ports must all be in the same VLAN. If the given address is a unicast address and you specify multiple ports, the ports must be in different VLANs.

The MSM does not support the **set cam** command.

If you enter a route descriptor and do not specify a VLAN parameter, the default is the VLAN already associated with the port. If you enter a route descriptor, you can use only a single port number (for the associated port).

The MAC address and VLAN for a host can be stored in the NVRAM. It is maintained even after a reset.

The *vlan* number is optional unless you are setting CAM entries to dynamic, static, or permanent for a trunk port, or if you are using the **agingtime** keyword.

If port(s) are trunk ports, you must specify the VLAN.

Static (nonpermanent) entries remain in the table until you reset the active supervisor engine.

Enter the *route_descr* variable as two hexadecimal bytes in the following format: 004F. Do not use a hyphen (-) to separate the bytes.

Examples

This example shows how to add a static unicast entry to the cam table for module 2, port 9:

```
Console> (enable) set cam static 00-00-0c-a0-03-fa 2/9  
Static unicast entry added to CAM table.  
Console> (enable)
```

This example shows how to add a permanent multicast entry to the cam table for a group of ports:

```
Console> (enable) set cam permanent 01-40-0b-a0-03-fa 1/1,2/1,2/3,2/8-12  
Permanent multicast entry added to CAM table.  
Console> (enable)
```

This example shows how to add a static traffic filter entry to the cam table:

```
Console> (enable) set cam static filter 00-02-03-04-05-06 1  
Filter entry added to CAM table.  
Console> (enable)
```

This example shows how to add a filter for a specific MAC address:

```
Console> (enable) set cam static filter 00-02-03-04-05-06 1  
Filter entry added to CAM table.  
Console> (enable)
```

Related Commands

[clear cam](#)
[set cam agingtime](#)
[set cam notification](#)
[show cam](#)
[show cam notification](#)

set cam agingtime

To set the aging time for the CAM table, use the **set cam agingtime** command.

```
set cam agingtime [vlan] agingtime
```

Syntax Description	
<i>vlan</i>	(Optional) Number of the VLAN. This number is optional unless you are setting CAM entries to dynamic, static, or permanent for a trunk port, or if you are using the <i>agingtime</i> variable.
<i>agingtime</i>	Number of seconds that dynamic entries remain in the table before being deleted; valid ranges are from 15 to 1,000,000 seconds. Setting aging time to zero (0) disables aging.

Defaults This command has no default settings.

Command Types Switch command

Command Modes Privileged

Usage Guidelines Setting the aging time to 0 disables aging. The minimum configurable non-zero aging time is 15 seconds. You cannot configure an aging of from 1 to 14 seconds.

Examples This example shows how to set the CAM table aging time for VLAN 1 to 300 seconds:

```
Console> (enable) set cam agingtime 1 300
Vlan 1 CAM aging time set to 300 seconds.
Console> (enable)
```

Related Commands

- [clear cam](#)
- [set cam](#)
- [set cam notification](#)
- [show cam](#)
- [show cam notification](#)

set cam notification

To enable notification when a MAC address change occurs to the CAM table and to set the time between notifications, use the **set cam notification** command.

```
set cam notification {enable | disable}
```

```
set cam notification {added | removed} {enable | disable} {mod/port}
```

```
set cam notification historysize log_size
```

```
set cam notification interval time
```

Syntax	Description
enable	Enables notification that a change has occurred.
disable	Disables notification that a change has occurred.
added	Notifies when a MAC address is learned.
removed	Notifies when a MAC address is deleted.
<i>mod/port</i>	Number of the module and the port.
historysize	Creates a notification history log.
<i>log_size</i>	Number of entries in the notification history log; valid sizes are between 0 and 500 entries.
interval	Sets the maximum wait time between notifications.
<i>time</i>	Time between notification; valid values are from 0 to 4,294,967,295 (specified in seconds).

Defaults

The default settings are as follows:

- Notification is disabled.
- Interval time is set to 1 second.
- History size is set to 1 entry.

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

You can globally disable notifications using the **set cam notification disable** command, but the other notification configuration settings will remain configured. The notification configuration settings can be reset using the **clear config** command. The **clear cam notification** command can be used to clear the history log or reset notification counters.

If you set the interval time to 0, the switch will send notifications immediately. There is an impact on the performance of the switch when you set the interval time to zero (0).

You can configure the switch to generate MAC notification SNMP traps using the **set snmp enable macnotification** command. MAC notification SNMP traps are generated even when the history log size is set to zero (0).

Examples

This example shows how to enable notification when a MAC address change occurs to the CAM table:

```
Console> (enable) set cam notification enable
MAC address change detection globally enabled
Be sure to specify which ports are to detect MAC address changes
with the 'set cam notification [added|removed] enable <m/p>' command.
SNMP traps will be sent if 'set snmp trap enable macnotification' has been set.
Console> (enable)
```

This example shows how to enable notification when a new MAC address is added to ports 1-4 on module 3 in the CAM table:

```
Console> (enable) set cam notification added enable 3/1-4
MAC address change notifications for added addresses are
enabled on port(s) 3/1-4
Console> (enable)
```

This example shows how to enable notification when a new MAC address is added to the CAM table on ports 1-4 on module 2:

```
Console> (enable) set cam notification added enable 2/1-4
MAC address change notifications for added addresses are
enabled on port(s) 2/1-4
Console> (enable)
```

This example shows how to enable notification when a MAC address is deleted from the CAM table of ports 3-6 on module 3:

```
Console> (enable) set cam notification removed enable 3/3-6
MAC address change notifications for removed addresses are
enabled on port(s) 3/3-6
```

This example shows how to set the history log size to 300 entries:

```
Console> (enable) set cam notification historysize 300
MAC address change history log size set to 300 entries
Console> (enable)
```

This example shows how to set the interval time to 10 seconds between notifications:

```
Console> (enable) set cam notification interval 10
MAC address change notification interval set to 10 seconds
Console> (enable)
```

Related Commands

- [clear cam](#)
- [set cam](#)
- [set cam agingtime](#)
- [set snmp trap](#)
- [show cam](#)
- [show cam notification](#)

set cdp

To enable or disable the Cisco Discovery Protocol (CDP) globally or on specified ports, and to configure the CDP hold time, use the **set cdp** command.

```
set cdp { enable | disable } [mod/ports...]
```

Syntax Description

enable	Enables the CDP feature.
disable	Disables the CDP feature.
<i>mod/ports...</i>	(Optional) Number of the module and ports.

Defaults

The default settings are as follows:

- CDP enabled in system configuration.
- Message interval set to 60 seconds for every port.

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

If you enter the global **set cdp enable** or **disable** command, CDP is globally configured. If CDP is globally disabled, CDP is automatically disabled on all ports, but the per-port **enable** (or **disable**) configuration is not changed. If CDP is globally enabled, whether CDP is running on a port depends on its per-port configuration.

If you configure CDP on a per-port basis, the *mod/ports...* can be entered as a single module and port or a range of ports; for example, 2/1-12,3/5-12.

Examples

This example shows how to enable the CDP globally:

```
Console> (enable) set cdp enable
CDP enabled globally
Console> (enable)
```

This example shows how to enable the CDP on port 1 on module 2:

```
Console> (enable) set cdp enable 2/1
CDP enabled on port 2/1.
Console> (enable)
```

This example shows how to disable CDP globally:

```
Console> (enable) set cdp disable
CDP disabled globally
Console> (enable)
```

This example shows how to disable the CDP message display for port 1 on module 2:

```
Console> (enable) set cdp disable 2/1  
CDP disabled on port 2/1.  
Console> (enable)
```

Related Commands [show cdp](#)

set cdp holdtime

To configure the Cisco Discovery Protocol (CDP) holding time, use the **set cdp holdtime** command.

set cdp holdtime *holdtime*

Syntax Description	<i>holdtime</i>	Number of seconds for the global CDP holding time value; valid values are from 10 to 255 seconds.
---------------------------	-----------------	---

Defaults	CDP <i>holdtime</i> interval is 180 seconds.
-----------------	--

Command Types	Switch command
----------------------	----------------

Command Modes	Privileged
----------------------	------------

Examples	This example shows how to set the global CDP holding time value to 200 seconds:
-----------------	---

```
Console> (enable) set cdp 200  
CDP holdtime set to 200 seconds.  
Console> (enable)
```

Related Commands	show cdp
-------------------------	--------------------------

set cdp interval

To globally set the message interval for the Cisco Discovery Protocol (CDP), use the **set cdp interval** command.

set cdp interval *interval*

Syntax Description	<i>interval</i>	Number of seconds the system waits between CDP message transmissions; valid values are from 5 to 900 seconds
--------------------	-----------------	--

Defaults	Message <i>interval</i> is 60 seconds.
----------	--

Command Types	Switch command
---------------	----------------

Command Modes	Privileged
---------------	------------

Examples	This example shows how to set the CDP message interval to 100 seconds:
----------	--

```
Console> (enable) set cdp interval 100
CDP message interval set to 100 seconds for all ports.
Console> (enable)
```

Related Commands	set cdp show cdp
------------------	---

set cdp version

To set the version of the Cisco Discovery Protocol (CDP) to run on the switch, use the **set cdp version** command.

```
set cdp version {v1 | v2}
```

Syntax Description	v1 v2 Version of CDP.
---------------------------	--------------------------------

Defaults	The CDP version is v2.
-----------------	------------------------

Command Types	Switch command
----------------------	----------------

Command Modes	Privileged
----------------------	------------

Examples	This example shows how to set the CDP to version 1:
-----------------	---

```
Console> (enable) set cdp version v1
CDP version set to v1
Console> (enable)
```

Related Commands	set cdp show cdp
-------------------------	---

set cgmp

To enable or disable Cisco Group Management Protocol (CGMP) on the switch, use the **set cgmp** command.

set cgmp {enable | disable}

Syntax Description	enable	Disables CGMP on the switch.
	disable	Enables CGMP on the switch.

Defaults Disabled

Command Types Switch command

Command Modes Privileged

Usage Guidelines CGMP requires that you connect the switch to a router running CGMP.

Examples This example shows how to enable CGMP on a device:

```
Console> (enable) set cgmp enable
CMGP support for IP multicast enabled.
Console> (enable)
```

This example shows how to disable CGMP on a device:

```
Console> (enable) set cgmp disable
CMGP support for IP multicast disabled.
Console> (enable)
```

This example shows what happens if you try to enable CGMP if IGMP snooping is already enabled:

```
Console> (enable) set cgmp enable
Disable IGMP Snooping feature to enable CGMP.
Console> (enable)
```

Related Commands

- [clear multicast router](#)
- [set cgmp fastleave](#)
- [set cgmp leave](#)
- [set multicast router](#)
- [show cgmp leave](#)
- [show cgmp statistics](#)
- [show multicast group](#)
- [show multicast group count](#)

set cgmp fastleave

To enable or disable Cisco Group Management Protocol (CGMP) fast-leave processing, use the **set cgmp fastleave** command.

```
set cgmp fastleave {enable | disable}
```

Syntax Description	enable	Disables CGMP fast-leave processing.
	disable	Enables CGMP fast-leave processing.

Defaults Disabled

Command Types Switch command

Command Modes Privileged

Examples This example shows how to enable CGMP fast-leave processing:

```
Console> (enable) set cgmp fastleave enable
CMGP fastleave processing enabled.
Console> (enable)
```

This example shows how to disable CGMP fast-leave processing:

```
Console> (enable) set cgmp fastleave disable
CMGP fastleave processing disabled.
Console> (enable)
```

Related Commands

- [clear multicast router](#)
- [set cgmp](#)
- [set cgmp leave](#)
- [set multicast router](#)
- [show cgmp leave](#)
- [show cgmp statistics](#)
- [show multicast group](#)
- [show multicast group count](#)

set cgmp leave

To enable or disable Cisco Group Management Protocol (CGMP) leave processing, use the **set cgmp leave** command.

```
set cgmp fastleave { enable | disable }
```

Syntax Description	enable	Disables CGMP leave processing.
	disable	Enables CGMP leave processing.

Defaults Disabled

Command Types Switch command

Command Modes Privileged

Examples This example shows how to enable CGMP leave processing:

```
Console> (enable) set cgmp leave enable
CMGP leave processing enabled.
Console> (enable)
```

This example shows how to disable CGMP leave processing:

```
Console> (enable) set cgmp leave disable
CMGP leave processing disabled.
Console> (enable)
```

Related Commands

- [clear multicast router](#)
- [set cgmp](#)
- [set cgmp fastleave](#)
- [set multicast router](#)
- [show cgmp leave](#)
- [show cgmp statistics](#)
- [show multicast group](#)
- [show multicast group count](#)

set channel cost

To set the spanning tree port cost for an EtherChannel port bundle, use the **set channel cost** command.

```
set channel cost {channel_id | all} [cost]
```

Syntax Description	
<i>channel_id</i>	EtherChannel ID of the channel to modify.
all	EtherChannel port bundles on the switch.
<i>cost</i>	(Optional) Spanning tree port cost to apply to the EtherChannel.

Defaults Spanning tree port cost is calculated automatically (based on the current port costs of the ports in the EtherChannel).

Command Types Switch command

Command Modes Privileged

Usage Guidelines To determine the *channel_id* of an EtherChannel port bundle, use the **show channel** command. If you do not specify the *cost*, the spanning tree port cost is updated based on the current port costs of the channeling ports. If you change the channel port cost, the port costs of member ports in the channel are modified to reflect the new cost. A message listing the ports for which the port costs were changed is displayed.

Examples This example shows how to set the channel 768 path cost to 23:

```
Console> (enable) set channel cost 768 23
Port(s) 1/1-2,7/3,7/5 port path cost are updated to 60.
Channel 768 cost is set to 23.
Warning:channel cost may not be applicable if channel is broken.
Console> (enable)
```

This example shows how to set all channel path costs to 15:

```
Console> (enable) set channel cost all 15
Port(s) 4/1-4 port path cost are updated to 39.
Channel 768 cost is set to 15.
Warning:channel cost may not be applicable if channel is broken.
Console> (enable)
```

■ set channel cost

Related Commands

set channel vlancost
set port channel
show channel
show channel group
show port channel
set spantree portcost

set channelprotocol

To set the protocol that manages channeling on a module, use the **set channel protocol** command.

```
set channelprotocol { pagp | lacp } mod
```

Syntax Description		
	pagp	PAGP.
	lacp	LACP.
	<i>mod</i>	Module number.

Defaults PAGP

Command Types Switch command

Command Modes Privileged

Examples This example shows how to set PAGP for module 3:

```
Console> (enable) set channelprotocol pagp 3
Channeling protocol set to PAGP for module(s) 3.
Console> (enable)
```

This example shows how to set LACP for modules 2, 4, 5, and 6:

```
Console> (enable) set channelprotocol lacp 2,4-6
Channeling protocol set to LACP for module(s) 2,4,5,6.
Console> (enable)
```

Related Commands

- [clear lacp-channel statistics](#)
- [set lacp-channel system-priority](#)
- [set port lacp-channel](#)
- [set spantree channelcost](#)
- [set spantree channelvlancost](#)
- [set port lacp-channel](#)
- [show lacp-channel](#)

set channel vlancost

To set the spanning tree port-VLAN cost for an EtherChannel port bundle, use the **set channel vlancost** command.

```
set channel vlancost channel_id [cost]
```

Syntax Description	
<i>channel_id</i>	EtherChannel ID of the channel to modify.
<i>cost</i>	(Optional) Spanning tree port-VLAN cost to apply to the EtherChannel.

Defaults Spanning tree port-VLAN cost is calculated automatically (based on the current port-VLAN costs of the ports in the EtherChannel).

Command Types Switch command

Command Modes Privileged

Usage Guidelines You can configure the port-VLAN cost of only one EtherChannel at a time. To determine the *channel_id* of an EtherChannel port bundle, use the **show channel** command. If you do not specify the *cost*, the spanning tree port-VLAN cost is updated based on the current port-VLAN costs of the channeling ports. If you change the channel port-VLAN cost, the port-VLAN costs of member ports in the channel are modified to reflect the new cost. A message listing the ports for which the port costs were changed is displayed.

Examples This example shows how to set the channel 768 port-VLAN cost to 10:

```
Console> (enable) set channel vlancost 768 10
Port(s) 1/1-2 vlan cost are updated to 24.
Channel 768 vlancost is set to 10.
Console> (enable)
```

Related Commands

- [set channel cost](#)
- [set port channel](#)
- [show channel](#)
- [show channel group](#)
- [show port channel](#)
- [set spantree portvlancost](#)

set config mode

To change the configuration mode from binary to text format, use the **set config mode** command.

```
set config mode binary
```

```
set config mode text { nvram | device:file-id }
```

Syntax Description	binary	Sets the system configuration mode to binary format.
	text	Sets the system configuration mode to text format.
	nvr am	Stores the saved configuration in NVRAM.
	<i>device:file-id</i>	Name of the device and filename where the saved configuration will be stored.

Defaults Mode is binary (saves the configuration to NVRAM when the **write memory** command is used).

Command Types Switch command

Command Modes Privileged

Usage Guidelines When you configure the system to use text file configuration mode the system stores its configuration as a text file in nonvolatile storage, either in NVRAM or FLASH memory. The text file consists of commands entered by you to configure various features. For example, if you disable a port the command to disable that port will be in the text configuration file.

The text file only contains commands you have used to configure your switch. Because the text configuration file in most cases requires less space NVRAM is a good place for the file to be stored. If the text file exceeds NVRAM space, it can also be stored to FLASH memory.

User settings are not immediately saved to NVRAM. To save user settings you must enter the **write memory** command to store the configuration in nonvolatile storage.

Examples This example shows how to set the configuration mode to binary:

```
Console> (enable) set config mode binary
System configuration copied to NVRAM. Configuration mode set to binary.
Console> (enable)
```

This example shows how to set the configuration mode to text and designate the location and filename for saving the text configuration file:

```
Console> (enable) set config mode text bootflash:switch.cfg  
Binary system configuration has been deleted from NVRAM. Configuration mode set to text.  
Use the write memory command to save configuration changes. System configuration file set  
to: bootflash:switch.cfg  
The file specified will be used for configuration during the next bootup.  
Console> (enable)
```

Related Commands

[show config mode](#)
[write](#)

set crypto key rsa

To generate and configure an RSA key pair, use the **set crypto key rsa** command.

```
set crypto key rsa nbits [force]
```

Syntax Description	<p><i>nbits</i> Size of the key; valid values are from 512 to 2048 bits.</p> <p>force (Optional) Regenerates the keys and suppress the warning prompt of overwriting existing keys.</p>
Defaults	Key size is 1024 bits.
Command Types	Switch command
Command Modes	Privileged
Usage Guidelines	<p>If you do not enter the force keyword, the set crypto key command is saved into the configuration file, and you will have to use the clear config all command to clear the RSA keys.</p> <p>To support SSH login, you first must generate an RSA key pair.</p>
Examples	<p>This example shows how to create an RSA key pair with a size of 1004 bits:</p> <pre>Console> (enable) set crypto key rsa 1004 Generating RSA keys.... [OK] Console> (enable)</pre>
Related Commands	<p>clear crypto key rsa</p> <p>show crypto key</p>

set dot1q-all-tagged

To enable tagging of packets on native VLANs, use the **set dot1q-all-tagged** command.

set dot1q-all-tagged enable | disable [all]

Syntax Description	enable	Enables dot1q tagged mode.
	disable	Disables dot1q tagged mode.
	all	(Optional) Dot1q tagging for all ports.

Defaults This command has no default settings.

Command Types Switch command

Command Modes Privileged

Usage Guidelines When you enable dot1q all tagged mode, all data packets are sent out tagged and all received untagged data packets are dropped on all 802.1Q trunks.

You cannot enable the dot1q tunneling feature on a port until dot1q tagged mode is enabled.

You cannot disable dot1q tagged mode on the switch until dot1q tunneling is disabled on all the ports on the switch.

The optional **all** keyword is not supported.



Note

PBF does not work with 802.1Q tunnel traffic. PBF is supported on Layer 3 IP unicast traffic, but it is not applicable to Layer 2 traffic. At the intermediate (PBF) switch, all 802.1Q tunnel traffic appears as Layer 2 traffic.

Examples This example shows how to enable dot1q tagging:

```
Console> (enable) set dot1q-all-tagged enable
Dot1q tagging is enabled
Console> (enable)
```

This example shows how to enable dot1q tagging on all ports:

```
Console> (enable) set dot1q-all-tagged enable all
Dot1q tagging is enabled
Console> (enable)
```

This example shows how to disable dot1q tagging:

```
Console> (enable) set dot1q-all-tagged disable  
Dot1q tagging is disabled  
Console> (enable)
```

Related Commands [show dot1q-all-tagged](#)

set dot1x

To configure dot1x on a system, use the **set dot1x** command set.

set dot1x system-auth-control {enable | disable}

set dot1x {quiet-period | tx-period | re-authperiod} *seconds*

set dot1x {supptimeout | server-timeout} *seconds*

set dot1x max-req *count*

set dot1x dhcp-relay-agent {enable | disable} *vlangs*

Syntax Description

system-auth-control	Authentication for the system.
enable	Enables the specified dot1x function.
disable	Disables the specified dot1x function.
quiet-period <i>seconds</i>	Idle time between authentication attempts; valid values are from 0 to 65535 seconds.
tx-period <i>seconds</i>	Time for the retransmission of EAP-Request/Identity frame; valid values are from 0 to 65535 seconds. See “Usage Guidelines” for more information.
re-authperiod <i>seconds</i>	Time constant for the retransmission reauthentication time; valid values are from 1 to 65535 seconds.
supp-timeout <i>seconds</i>	Time constant for the retransmission of EAP-Request packets; valid values are from 0 to 65535 seconds. See “Usage Guidelines” for more information.
server-timeout <i>seconds</i>	Time constant for the retransmission of packets by the backend authenticator to the authentication server; valid values are from 1 to 65535 seconds. See “Usage Guidelines” for more information.
max-req <i>count</i>	Maximum number of times that the state machine retransmits an EAP-Request frame to the supplicant before it times out the authentication session; valid values are from 1 to 10.
dhcp-relay-agent	802.1X authentication for the DHCP Relay Agent.
<i>vlangs</i>	Number of the VLAN; valid values are from 1 to 1000 and 1025 to 4094. See “Usage Guidelines” for more information.

Defaults

The default settings are as follows:

- **system-auth-control** is enabled
- **quiet-period** is 60 seconds
- **tx-period** is 30 seconds
- **re-authperiod** is 3,600 seconds
- **supp-timeout** is 30 seconds
- **server-timeout** is 30 seconds
- **max-req** count is 2

Command Types Switch command

Command Modes Privileged

Usage Guidelines When you set the **system-auth-control**, the following applies:

- The **enable** keyword allows you to control the authorization status for each port per the port-control parameter that you set using the **set port dot1x** command.
- The **disable** keyword allows you to make all ports behave as though the port-control parameter is set to **force-authorized**.

If you do not enable reauthentication, reauthentication does not automatically occur after authentication has occurred.

When the supplicant does not notify the authenticator that it received the EAP-request/identity packet, the authenticator waits a period of time (set by entering the **tx-period seconds** parameter), and then retransmits the packet.

When the supplicant does not notify the backend authenticator that it received the EAP-request packet, the backend authenticator waits a period of time (set by entering the **supp-timeout seconds** parameter), and then retransmits the packet.

When the authentication server does not notify the backend authenticator that it received specific packets, the backend authenticator waits a period of time (set by entering the **server-timeout seconds** parameter), and then retransmits the packets.

When you enter the **set dot1x dhcp-relay-agent** command, you can enter more than one VLAN.

Examples This example shows how to set the system authentication control:

```
Console> (enable) set dot1x system-auth-control enable
dot1x authorization enabled.
Console> (enable)
```

This example shows how to set the idle time between authentication attempts:

```
Console> (enable) set dot1x quiet-period 45
dot1x quiet-period set to 45 seconds.
Console> (enable)
```

This example shows how to set the retransmission time:

```
Console> (enable) set dot1x tx-period 15
dot1x tx-period set to 15 seconds.
Console> (enable)
```

This example shows you how to specify the reauthentication time:

```
Console> (enable) set dot1x re-authperiod 7200
dot1x re-authperiod set to 7200 seconds
Console> (enable)
```

This example shows you how to specify the retransmission of EAP-Request packets by the authenticator to the supplicant:

```
Console> (enable) set dot1x supp-timeout 15
dot1x supp-timeout set to 15 seconds.
```

```
Console> (enable)
```

This example shows how to specify the retransmission of packets by the backend authenticator to the authentication server:

```
Console> (enable) set dot1x server-timeout 15  
dot1x server-timeout set to 15 seconds.  
Console> (enable)
```

This example shows how to specify the maximum number of packet retransmissions:

```
Console> (enable) set dot1x max-req 5  
dot1x max-req set to 5.  
Console> (enable)
```

This example shows how to enable authentication for the DHCP Relay Agent on VLANs 1 through 5 and 24:

```
Console> (enable) set dot1x dhcp-relay-agent enable 1-5,24  
dot1x dhcp-relay-agent enabled for vlans 1-5, 24.  
Console> (enable)
```

This example shows how to disable authentication for the DHCP Relay Agent on VLAN 1:

```
Console> (enable) set dot1x dhcp-relay-agent disable 1  
dot1x dhcp-relay-agent disable for vlan 1  
Console> (enable)
```

Related Commands

[clear dot1x config](#)
[clear dot1x guest-vlan](#)
[set port dot1x](#)
[show dot1x](#)
[show port dot1x](#)