

set accounting update

Use the **set accounting update** command to configure the frequency of accounting updates.

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

Syntax Description		
	new-info	Keyword to update when new information is available.
	periodic	Keyword to update on a periodic basis.
	<i>interval</i>	(Optional) Periodic update interval time; valid intervals are from 1 to 71582 minutes.

Defaults Accounting is disabled by default.

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 tacacs server](#)
- [show accounting](#)

set alias

Use the **set alias** command to define command aliases (shorthand versions of commands).

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

Syntax Description	
<i>name</i>	Name of alias being created.
<i>command</i>	Command for which the alias is being created.
<i>parameter</i>	(Optional) Parameters to apply to the command for which an alias is being created. See the specific command for information about parameters that apply.

Defaults No aliases 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

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

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

```
set arp agingtime agingtime
```

Syntax Description

dynamic	(Optional) Keyword to specify entries are subject to ARP aging updates.
permanent	(Optional) Keyword to specify permanent entries are stored in NVRAM until they are removed by the clear arp or clear config command.
static	(Optional) Keyword to specify 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 <i>agingtime</i>	Keyword and variable to set the period of time (in seconds) after which an ARP entry is removed from the ARP table; valid values are from 0 to 1,000,000 seconds. Setting to 0 disables aging.

Defaults

No ARP table entries exist; ARP aging is set to 1200 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The *hw_addr* value is 6-hexbyte MAC address 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:

```
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 removed 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 alias](#)

set authentication enable

Use the **set authentication enable** command set to enable authentication using the TACACS+, RADIUS, or Kerberos server to determine if you have privileged access permission.

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

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

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

```
set authentication enable attempt count [console | telnet]
```

```
set authentication enable lockout time [console | telnet]
```

Syntax	Description
radius	Keyword to specify RADIUS authentication for login.
tacacs	Keyword to specify TACACS+ authentication for login.
kerberos	Keyword to specify Kerberos authentication for login.
enable	Keyword to enable the specified authentication method for login.
console	(Optional) Keyword to specify the authentication method for console sessions.
telnet	(Optional) Keyword to specify the authentication method for Telnet sessions.
http	(Optional) Keyword to specify the specified authentication method for HTTP sessions.
all	(Optional) Keyword to apply the authentication method to all session types.
primary	(Optional) Keyword to specify the specified authentication method be tried first.
disable	Keyword to disable the specified authentication method for login.
local	Keyword to specify local authentication for login.
attempt count	Keyword and variable to specify the number of connection attempts before initiating an error; valid values are 0 and from 3 to 10 .
lockout time	Keyword and variable to specify the lockout timeout; valid values are from 30 to 600 seconds.

Defaults

The default is local authentication is enabled for console and Telnet sessions. RADIUS, TACACS+, and Kerberos are disabled for all session types. If authentication is enabled, the default **attempt count** value is 3.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Use authentication configuration for both console and Telnet connection attempts unless you use the **console** or **telnet** keywords to specify the authentication methods for each connection type individually. If you enter a 0 for the *count* or *time* values, you disable the specified action.

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 all session types:

```
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 as
primary authentication method.
Console> (enable)
```

This example shows how to limit enable mode login attempts:

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

This example shows how to set the enable mode lockout time for both console and Telnet connections:

```
Console> (enable) set authentication enable lockout 50
Enable mode lockout time for console and telnet logins set to 50.
Console> (enable)
```

Related Commands

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

set authentication login

Use the **set authentication login** command set to enable TACACS+, RADIUS, or Kerberos as the authentication method for login.

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

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

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

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

Syntax Description	
radius	Keyword to specify the use of the RADIUS server password to determine if you have access permission to the switch.
tacacs	Keyword to specify the use of the TACACS+ server password to determine if you have access permission to the switch.
kerberos	Keyword to specify the Kerberos server password to determine if you have access permission to the switch.
enable	Keyword to enable the specified authentication method for login.
console	(Optional) Keyword to specify the authentication method for console sessions.
telnet	(Optional) Keyword to specify the authentication method for Telnet sessions.
http	(Optional) Keyword to specify the authentication method for HTTP sessions.
all	(Optional) Keyword to specify the authentication method for all session types.
primary	(Optional) Keyword to specify that the method specified is the primary authentication method for login.
disable	Keyword to disable the specified authentication method for login.
local	Keyword to specify a local password to determine if you have access permission to the switch.
attempt count	Keyword and variable to specify the number of login attempts before initiating an error; valid values are 0 and from 3 to 10 .
lockout time	Keyword and variable to specify the lockout timeout; valid values are from 30 to 600 seconds.

Defaults

The default is 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.

If you enter a 0 for the *count* or *timevalue*, you disable the specified action.

Examples 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)
```

This example shows how to limit login attempt:

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

This example shows how to set the lockout time for both console and Telnet connections:

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

Related Commands [set authentication enable](#)
[show arp](#)

set authorization commands

Use the **set authorization commands** command to enable authorization of command events on the switch.

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

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

Syntax Description		
enable	enable	Keyword to enable the specified authorization method for commands.
config	config	Keyword to permit authorization for configuration commands only.
enable	enable	Keyword to permit authorization for enable mode commands only.
all	all	Keyword to permit authorization for all commands.
<i>option</i>	option	Switch response to an authorization request; valid values are tacacs+ , if-authenticated , and none . Refer to the “Usage Guidelines” section for valid value definitions.
<i>fallbackoption</i>	fallbackoption	Switch fallback response to an authorization request if the TACACS+ server is down or not responding; valid values are deny , if-authenticated , and none . Refer to the “Usage Guidelines” section for valid value definitions.
disable	disable	Keyword to disable authorization for commands.
console	console	(Optional) Keyword to specify the authorization method applies to console sessions.
telnet	telnet	(Optional) Keyword to specify the authorization method applies to Telnet sessions.
both	both	(Optional) Keyword to specify the authorization method applies to both console and Telnet sessions.

Defaults Authorization is disabled by default.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The **tacacs+** keyword allows you to proceed with your action if you have authorization. The **if-authenticated** keyword allows you to proceed with your action if you have been authenticated. The **none** keyword allows you to proceed without further authorization if the TACACS+ server does not respond. The **deny** keyword does not allow you to proceed if 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)
```

Related Commands

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

set authorization enable

Use the **set authorization enable** command to enable authorization of enable (privileged mode) session events on the switch.

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

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

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

Defaults Authorization is disabled by default.

Command Types Switch command.

Command Modes Privileged.

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

Related Commands

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

set authorization exec

Use the **set authorization exec** command to enable authorization of exec (normal login mode) session events on the switch.

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

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

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

Defaults Authorization is disabled by default.

Command Types Switch command.

Command Modes Privileged.

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

Related Commands

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

set banner motd

Use the **set banner motd** command to create a login banner to display when users access the switch.

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

Syntax Description	<table border="1"> <tr> <td><i>c</i></td> <td>Delimiting character used to begin and end the message.</td> </tr> <tr> <td><i>text</i></td> <td>(Optional) Message of the day.</td> </tr> </table>	<i>c</i>	Delimiting character used to begin and end the message.	<i>text</i>	(Optional) Message of the day.
<i>c</i>	Delimiting character used to begin and end the message.				
<i>text</i>	(Optional) Message of the day.				
Defaults	No MOTD banner is defined.				
Command Types	Switch command.				
Command Modes	Privileged.				
Usage Guidelines	<p>The banner cannot contain more than 3,070 characters, including tabs. Tabs display as eight characters but take only one character of memory.</p> <p>You can use either the clear banner motd command or the set banner motd cc command to clear the message-of-the-day banner.</p>				
Examples	<p>This example shows how to set the message of the day using the pound sign (#) as the delimiting character:</p> <pre>Console> (enable) set banner motd # ** System upgrade at 6:00am Tuesday. ** Please log out before leaving on Monday. # MOTD banner set. Console> (enable)</pre> <p>This example shows how to clear the message of the day:</p> <pre>Console> (enable) set banner motd ## MOTD banner cleared. Console> (enable)</pre>				
Related Commands	clear banner motd				

set boot auto-config

Use the **set boot auto-config** command 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.

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

```
set boot auto-config {cfg1 | cfg2 | cfg1;cfg2}
```

```
set boot auto-config {recurring | non-recurring}
```

Syntax Description

<i>device:</i>	Device where the startup configuration file resides.
<i>filename</i>	Names of the startup configuration file.
<i>mod</i>	(Optional) Module number of the supervisor engine containing the Flash device.
cfg1	Keyword to specify the first startup configuration file on the Supervisor Engine II G and III G. Use a semicolon-separated list to specify multiple cfg files.
cfg2	Keyword to specify the second startup configuration file on the Supervisor Engine II G and III G.
recurring	Keyword to retain <code>config_file</code> environment variable settings. Available only on the Supervisor Engine II G and III G.
non-recurring	Keyword to clear <code>config_file</code> environment variable settings before the startup configuration file runs. Available only on the Supervisor Engine II G and III G.

Defaults

The default setting of this command is non-recurring and the `config_file` 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 settings (you cannot prepend or append a file to the variable contents).

In the Supervisor Engine III, multiple configuration files may be specified. Separate the files using a semicolon (;).

In the Supervisor Engine II G and III G, two configuration files may be specified. Separate the files using a semicolon (;).

You can set **recurring**, **non-recurring**, **cfg1**, and **cfg2** keywords in Supervisor Engines II G and III G only.

Use a semicolon-separated list to specify multiple **cfg** files.

To set the recurrence on other supervisor engines and 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)
```

This example shows how to specify the configuration file environment variable on Supervisor Engines II G and III G:

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

This example shows how to specify multiple configuration files on Supervisor Engines II G and III G:

```
Console> (enable) set boot auto-config cfg1;cfg2
CONFIG_FILE variable = cfg1;cfg2
WARNING: nvram configuration may be lost during next bootup,
        and re-configured using the file(s) specified.
Console> (enable)
```

This example shows how to set the auto-configuration to **recurring** on Supervisor Engines II G and III G:

```
Console> (enable) set boot auto-config recurring
auto-config: recurring
Console> (enable)
```

Related Commands

[set boot system flash](#)

set boot config-register

Use the **set boot config-register** command to set the boot configuration register value.

set boot config-register *0xvalue* [*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		
0xvalue		Keyword to set the 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		Keyword to specify the boot method to use the next time the switch is reset or power cycled.
rommon		Keyword to cause the switch to remain in ROM monitor mode the next time the switch is reset or power cycled.
bootflash		Keyword to cause the switch to boot using the first valid system image in bootflash the next time the switch is reset or power cycled.
system		Keyword to cause the switch to boot using the system images specified in the BOOT environment variable the next time the switch is reset or power cycled.
baud		Keyword to set the console baud rate.
1200 2400 4800 9600		Keywords to specify the ROM monitor console port baud rate.
ignore-config		Keyword to specify whether the switch should ignore the configuration in NVRAM the next time the switch is restarted.
enable		Keyword to cause the switch to ignore the configuration in NVRAM the next time the switch is restarted.
disable		Keyword to prevent the switch from ignoring the configuration in NVRAM the next time the switch is restarted.
auto-config recurring		Keyword to cause the switch to retain 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.
auto-config non-recurring		Keyword to cause the switch to clear 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 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 is set to 9600.
- The **ignore-config** parameter is disabled.
- The **auto-config** parameter is set to non-recurring.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

We recommend that you use only the **rommon** and **system** options to 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**.

**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.

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](#)
[show boot](#)

set boot sync now

Use the **set boot sync now** command to immediately initiate synchronization of the system image between the active and standby supervisor engine.

set boot sync now

Syntax Description This command has no arguments or keywords.

Defaults The default is synchronization is disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The **set boot sync now** command initiates synchronization to force the configuration files to synchronize automatically to the standby supervisor engine. The configuration files remain consistent with the files on the active supervisor engine.

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

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

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

set boot system flash

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

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) Keyword to place the software image file first in the list of images to attempt to boot.
	<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 reliable 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:cat5000-sup3.6-1-1.bin
BOOT variable =
bootflash:cat5000-sup3.5-2-1.bin,1;bootflash:cat5000-sup3.6-1-1.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:cat5000-sup3.6-1-1.bin prepend  
BOOT variable =  
slot0:cat5000-sup3.6-1-1.bin,1;bootflash:cat5000-sup3.4-5-2.bin,1;  
Console> (enable)
```

Related Commands

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

set bridge apart

Use the **set bridge apart** command to enable or disable APaRT on FDDI.

```
set bridge apart {enable | disable}
```

Syntax Description	enable	disable
	Keyword to activate APaRT on FDDI.	Keyword to deactivate APaRT on FDDI.

Defaults The default is APaRT enabled.

Command Types Switch command.

Command Modes Privileged.

Examples This example shows how to disable APaRT:

```
Console> (enable) set bridge apart disable
APaRT disabled
Console> (enable)
```

Related Commands [set bridge fddicheck](#)

set bridge fddicheck

Use the **set bridge fddicheck** command to enable or disable the relearning of MAC addresses (as FDDI MAC addresses) that were already learned from an Ethernet interface (as Ethernet MAC addresses).

```
set bridge fddicheck {enable | disable}
```

Syntax Description

enable	Keyword to permit FDDI to relearn MAC addresses learned from an Ethernet interface.
disable	Keyword to prevent FDDI from relearning MAC addresses learned from an Ethernet interface.

Defaults

The default configuration has **fddicheck** disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When **fddicheck** is enabled, a MAC address seen on the FDDI ring is not learned (stored in FDDI CAM) as an FDDI MAC address if the MAC address was previously learned from an Ethernet interface (as an Ethernet MAC address).

With **fddicheck** enabled, MAC addresses previously learned from an Ethernet interface will not be relearned on the FDDI interface until the CAM is cleared.

This command requires information from the FDDI CAM. If you disable APaRT, **fddicheck** is also automatically disabled. To enable **fddicheck**, first enable APaRT.

Examples

This example shows how to enable **fddicheck** on the switch:

```
Console> (enable) set bridge fddicheck enable
FDDICHECK enabled
Console> (enable)
```

Related Commands

[show bridge](#)

set bridge ipx 8022toether

Use the **set bridge ipx 8022toether** command to set the default method for translating IPX packets from FDDI 802.2 to Ethernet.

```
set bridge ipx 8022toether { 8023 | snap | eii | 8023raw }
```

Syntax Description	8023	Keyword to specify Ethernet 802.3 as the default translation method.
	snap	Keyword to specify Ethernet SNAP as the default translation method.
	eii	Keyword to specify Ethernet II as the default translation method.
	8023raw	Keyword to specify Ethernet 802.3 RAW as the default translation method.

Defaults The default translation method for FDDI 802.2 to Ethernet networks is 8023 (Ethernet 802.3).

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The default translation method specified is used only until the real protocol types are learned.

Examples This example shows how to set the default protocol to SNAP for translating IPX packets between FDDI 802.2 and Ethernet networks:

```
Console> (enable) set bridge ipx 8022toether snap
8022 to ETHER translation set.
Console> (enable)
```

Related Commands [show bridge](#)

set bridge ipx 8023rawtofdi

Use the **set bridge ipx 8023rawtofdi** command to set the default method for translating IPX packets from Ethernet 802.3 to FDDI.

```
set bridge ipx 8023rawtofdi {8022 | snap | fddiraw}
```

Syntax Description	8022	Keyword to specify FDDI 802.2 as the default translation method.
	snap	Keyword to specify FDDI SNAP as the default translation method.
	fddiraw	Keyword to specify FDDI RAW as the default translation method.

Defaults The default translation method for Ethernet 802.3 to FDDI networks is SNAP (FDDI SNAP).

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The default translation method specified is used only until the real protocol types are learned.

Examples This example shows how to set the default translation method to FDDI SNAP for translating IPX packets between Ethernet 802.3 and FDDI networks:

```
Console> (enable) set bridge ipx 8023rawtofdi snap
8023RAW to FDDI translation set.
Console> (enable)
```

Related Commands [show bridge](#)

set bridge ipx snaptoether

Use the **set bridge ipx snaptoether** command to set the default method for translating IPX FDDI SNAP frames to Ethernet frames.

set bridge ipx snaptoether { 8023 | snap | eii | 8023raw }

Syntax Description	8023	Keyword to specify Ethernet 802.3 as the default frame type.
	snap	Keyword to specify Ethernet SNAP as the default frame type.
	eii	Keyword to specify Ethernet II as the default frame type.
	8023raw	Keyword to specify Ethernet 802.3 RAW as the default frame type.

Defaults The default translation method for translating IPX FDDI SNAP frames to Ethernet frames is 8023raw (Ethernet 802.3 RAW).

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The default translation specified is used for all broadcast IPX SNAP frames and for any unlearned Ethernet MAC addresses.

Examples This example shows how to set the default method for translating IPX FDDI SNAP frames to Ethernet frames to SNAP:

```
Console> (enable) set bridge ipx snaptoether snap
Bridge snaptoether default IPX translation set.
Console> (enable)
```

Related Commands [show bridge](#)

set cam

Use the **set cam** command set to add entries into the CAM table, set the aging time for the CAM table, and configure traffic filtering from and to a specific host.

```
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
```

```
set cam agingtime vlan agingtime
```

Syntax Description		
dynamic	Keyword to specify entries are subject to aging.	
static	Keyword to specify entries are not subject to aging.	
permanent	Keyword to specify permanent entries are stored in NVRAM until they are removed 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; valid values are from 0 to 0xffff.	
<i>mod/port</i>	Number of the module and the port on the module.	
<i>vlan</i>	(Optional) Number of the VLAN; valid values are from 1 to 1005 .	
<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 on the module.	
filter	Keyword to specify a traffic filter entry.	
agingtime	Keyword to set the period of time after which an entry is removed from the table.	
<i>agingtime</i>	Number of seconds (0 to 1,000,000) that dynamic entries remain in the table before being deleted. Setting the aging time to 0 disables aging.	

Defaults

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

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

Usage Guidelines

Static (nonpermanent) entries remain in the CAM table until the system is reset.

Entering 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 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 multiple ports are specified, the ports must all be in the same VLAN. If the given address is a unicast address and multiple ports are specified, the ports must be in different VLANs.

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

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

If you enter a route descriptor with no VLAN parameter specified, the default is the VLAN already associated with the port. If you enter a route descriptor, you may only use a single port number (of 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 the ports are trunk ports, you must specify the VLAN.

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

Examples

This example shows how to set the CAM table aging time to 300 seconds:

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

This example shows how to add a unicast entry to the 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 table for module 1, port 1, and module 2, ports 1, 3, and 8 through 12:

```
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 traffic filter entry to the table:

```
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](#)
[show cam](#)

set cdp

Use the **set cdp** command to enable or disable CDP globally or on specified ports, and to configure the CDP hold time.

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

Syntax Description

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

Defaults

The default system configuration has CDP enabled; the message interval is 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 or not depends on its per-port configuration.

If you configure CDP on a per-port basis, the *mod/ports...* value 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 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 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

Use the **set cdp holdtime** command to configure the CDP hold time.

set cdp holdtime *holdtime*

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

Defaults	The default CDP hold time value has the message interval globally set to 180 seconds.
-----------------	---

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

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

Usage Guidelines	This command is not supported on Catalyst 5000 family switches with supervisor engine software release 4.2(2) and earlier and 3.2(4) and earlier.
-------------------------	---

Examples	This example shows how to specify the global CDP hold time value:
-----------------	---

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

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

set cdp interval

Use the **set cdp interval** command to globally set the message interval for CDP.

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	The default is set to 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

Use the **set cdp version** command to set the version of CDP to run on the switch.

```
set cdp version v1 | v2
```

Syntax Description	v1 v2	Keywords to specify the version of CDP.
---------------------------	---------	---

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

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

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

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

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

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

set cgmp

Use the **set cgmp** command to enable or disable CGMP on the switch.

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

Syntax Description	enable	Keyword to enable CGMP on the switch.
	disable	Keyword to disable CGMP on the switch.

Defaults The default is CGMP is 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 multicast router](#)
- [show multicast group](#)
- [show multicast group count](#)

set cgmp leave

Use the **set cgmp leave** command to enable or disable CGMP leave processing.

set cgmp leave {enable | disable}

Syntax Description	enable	Keyword to enable CGMP leave processing.
	disable	Keyword to disable CGMP leave processing.

Defaults The default is CGMP leave processing is 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 support for leave processing enabled.
Console> (enable)
```

This example shows how to disable CGMP leave processing:

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

Related Commands

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

set channel cost

Use the **set channel cost** command to set the spanning tree port cost for an EtherChannel port bundle.

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

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

Defaults The default is the 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 appears listing the ports whose port costs were changed.

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)
```

Related Commands

- [set channel vlancost](#)
- [set port channel](#)
- [show channel](#)
- [show channel group](#)
- [show port channel](#)

set channel vlancost

Use the **set channel vlancost** command to set the spanning tree port-VLAN cost for an EtherChannel port bundle.

```
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 The default is the 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 appears listing the ports whose port-VLAN costs were changed.

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 config mode

Use the **set config mode** command to change the configuration mode from a binary model to a text model.

```
set config mode binary
```

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

Syntax Description		
binary	Keyword to set the system configuration mode to a binary model.	
text	Keyword to set the system configuration mode to a text model.	
nvram	Keyword to store the saved configuration in NVRAM.	
<i>device:file-id</i>	Name of the device and filename where the saved configuration will be stored.	

Defaults The default is binary, which 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 you enter to disable that port will be saved in the text configuration file.

The text file contains only commands you have used to configure your switch. Because the text configuration file usually requires less space, NVRAM is a suitable location for the file to be stored. If the text file exceeds NVRAM space, it also can 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 cops

Use the **set cops** commands to configure COPS functionality.

```
set cops server ipaddress [port] [primary]
```

```
set cops domain-name domain_name
```

```
set cops retry-interval initial incr max
```

```
set cops roles {role_name}
```

Syntax	Description
server	Keyword to set the name of the COPS server.
<i>ipaddress</i>	IP address or IP alias of the server.
<i>port</i>	(Optional) Number of the TCP port the switch connects to on the server.
primary	(Optional) Keyword to specify the primary server.
domain-name <i>domain_name</i>	Keyword and variable to specify the domain name of the switch.
retry-interval	Keyword to specify the retry interval in seconds.
<i>initial</i>	Initial timeout value; valid values are from 0 to 65535 seconds.
<i>incr</i>	Incremental value; valid values are from 0 to 65535 seconds.
<i>max</i>	Maximum timeout value; valid values are from 0 to 65535 seconds.
roles <i>role_name</i>	Keyword and variable to specify physical characteristic (such as backbone, branch office, etc.).

Defaults

The defaults are as follows:

- The retry interval default values are initial = 30 seconds, incr = 30 seconds, max = 5 minutes.
- The default domain name is a string of length zero.
- No PDP servers are configured.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A switch may have multiple roles, and you can configure up to 64 roles per switch.

You can configure the names or addresses of up to two PDP servers. One must be the primary, and the optional second server is a secondary, or backup, PDP server.

The COPS domain name can only be set globally; there is no option to set it for each COPS client.

Names such as the server, domain name, and roles can contain a maximum of 31 characters; longer names are truncated to 31 characters. Valid letters are a-z and A-Z. Valid numbers are 0-9. Valid symbols are period (.), dash (-) and underscore (_). Names cannot start with an underscore (_). The names are not case sensitive for matching, but are case sensitive for display.

When specifying the **retry-interval**, the total of the initial timeout value and the incremental value (increment on each subsequent failure) may not exceed the maximum timeout value.

Examples

This example shows how to configure a server as a primary server:

```
Console> (enable) set cops server 171.21.34.56 primary
171.21.34.56 added to COPS server table as primary server.
Console> (enable)
```

This example shows how to configure a server as a primary RSVP+ server:

```
Console> (enable) set cops server 171.21.34.56 primary
171.21.34.56 added to COPS server table as primary server.
Console> (enable)
```

This example shows how to configure a server as a secondary (or backup) server:

```
Console> (enable) set cops server my_server2
my_server2 added to the COPS server table as backup server.
Console> (enable)
```

This example shows how to set the domain name:

```
Console> (enable) set cops domain-name my_domain
Domain name set to my_domain.
Console> (enable)
```

This example shows how to set the retry interval:

```
Console> (enable) set cops retry-interval 15 1 30
Connection retry intervals set.
Console> (enable)
```

This example shows the display output if the total of the initial timeout value and the incremental value you entered exceeds the maximum timeout value:

```
Console> (enable) set cops retry-interval 15 1 10
The initial timeout plus the increment value may not exceed the max value.
Console> (enable)
```

This example shows how to set the switch with the role backbone:

```
Console> (enable) set cops roles backbone
Role added successfully.
Console> (enable)
```

Related Commands

[clear cops](#)
[show cops](#)

set default portstatus

Use the **set default portstatus** command to set the default port status.

```
set default portstatus {enable | disable}
```

Syntax Description	enable	Keyword to activate default port status.
	disable	Keyword to deactivate default port status.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The **set default portstatus** command is supported by systems with chassis idprom. When you enter **clear config all**, or during configuration loss, all ports collapse into VLAN 1, which might cause a security and network instability problem. To prevent a security breach, enter the **set default portstatus** command. All ports enter into disable status, and the traffic flowing through the ports during a configuration loss situation is blocked. You can then manually configure ports to the enable status.

After you enter the **set default portstatus** command, you must reset the system for the new configuration to take effect.

This command is not saved in the configuration file.

After you have set the default port status, the setup is not cleared when you enter the **clear config all** command.

Examples This example shows how to disable the default port status:

```
Console> (enable) set default portstatus disable
Default port status set to disable.
Console> (enable)
```

Related Commands [show default](#)

set dot1x

Use the **set dot1x** command to configure dot1x on a system.

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

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

```
set dot1x {supp-timeout | server-timeout} seconds
```

```
set dot1x max-req count
```

Syntax Description

system-auth-control	Keyword to specify authentication for the system.
enable	Keyword to enable authentication for the system.
disable	Keyword to disable authentication for the system.
quiet-period <i>seconds</i>	Keyword to specify the idle time between authentication attempts; valid values are from 0 to 65535 seconds.
tx-period <i>seconds</i>	Keyword to specify the time for the retransmission of EAP-Request/Identity frame; valid values are from 0 to 65535 seconds. See the “Usage Guidelines” section for additional information.
re-authperiod <i>seconds</i>	Keyword and variable to specify the time constant for the retransmission reauthentication time; valid values are from 1 to 65535 seconds.
supp-timeout <i>seconds</i>	Keyword and variable to specify the time constant for the retransmission of EAP-Request packets; valid values are from 0 to 65535 seconds. See the “Usage Guidelines” section for additional information.
server-timeout <i>seconds</i>	Keyword and variable to specify the time constant for the retransmission of packets by the backend authenticator to the authentication server; valid values are from 0 to 65535 seconds. See the “Usage Guidelines” section for additional information.
max-req <i>count</i>	Keyword and variable to specify the 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 .

Defaults

The default settings are:

- **system-auth-control** is enabled
- **quiet-period** is 60 seconds
- **tx-period** is 30 seconds
- **re-authperiod** is 3600 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 authentication value, the following applies:

- The **enable** keyword allows you to control each port's authorization status per the port-control parameter 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**.

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.

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)
```

Related Commands

[clear dot1x config](#)
[set port dot1x](#)
[show dot1x](#)
[show port dot1x](#)