

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 that specifies update when new information is available.
	periodic	Keyword that specifies to update on a periodic basis.
	<i>interval</i>	(Optional) Periodic update interval time; valid intervals are 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 radius key**
- set radius server**
- set tacacs key**
- 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>	Alias being created.
<i>command</i>	Command for which the alias is being created.
<i>parameter</i>	(Optional) Parameters that 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 that specifies that entries are subject to ARP aging updates.
permanent	(Optional) Keyword that specifies that permanent entries are stored in NVRAM until they are removed by the clear arp or clear config command.
static	(Optional) Keyword that specifies that 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	Keyword to set the period of time after which an ARP entry is removed from the ARP table.
<i>agingtime</i>	Number of seconds (from 0 to 1,000,000) that entries will remain in the ARP table before being deleted. Setting this value 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 *hw_addr* is 6-hexbyte MAC address in canonical (00-11-22-33-44-55) or non-canonical (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 arp

set authentication enable

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

```
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]
```

Syntax Description

radius	Keyword that specifies RADIUS authentication for privileged mode access.
tacacs	Keyword that specifies TACACS+ authentication for privileged mode access.
kerberos	Keyword that specifies Kerberos authentication for privileged mode access.
enable	Keyword that specifies to enable the specified authentication method for privileged mode access.
console	(Optional) Keyword that specifies the authentication method applies to console sessions.
telnet	(Optional) Keyword that specifies the authentication method applies to Telnet sessions.
http	(Optional) Keyword that specifies the authentication method applies to http sessions.
all	(Optional) Keyword that specifies the authentication method applies to all sessions.
primary	(Optional) Keyword that specifies the specified authentication method be tried first.
disable	Keyword that specifies to disable the specified authentication method for privileged mode access.
local	Keyword that specifies local authentication for privileged mode access.

Defaults

The default is 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 them.

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

Related Commands

set authentication login
show authentication

set authentication login

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

```
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

radius	Keyword that specifies RADIUS authentication for normal mode access.
tacacs	Keyword that specifies TACACS+ authentication for normal mode access.
kerberos	Keyword that specifies Kerberos authentication for normal mode access.
enable	Keyword that specifies to enable the specified authentication method for normal mode access.
console	(Optional) Keyword that specifies the authentication method applies to console sessions.
telnet	(Optional) Keyword that specifies the authentication method applies to Telnet sessions.
http	(Optional) Keyword that specifies the authentication method applies to HTTP sessions.
all	(Optional) Keyword that specifies the authentication method applies to all sessions.
primary	(Optional) Keyword that specifies the specified authentication method be tried first.
disable	Keyword that specifies to disable the specified authentication method for normal mode access.
local	Keyword that specifies local authentication for normal mode access.

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 that 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.

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)
```

Related Commands

set authentication enable
show authentication

set authorization commands

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

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

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

Syntax Description		
enable	enable	Keyword that enables the specified authorization method for commands.
config	config	Keyword that permits authorization for configuration commands only.
all	all	Keyword that permits 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 on page 2-151 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 tacacs+ , deny , if-authenticated , and none . Refer to the “Usage Guidelines” section on page 2-151 for valid value definitions.
console	console	(Optional) Keyword that specifies the authorization method applies to console sessions.
telnet	telnet	(Optional) Keyword that specifies the authorization method applies to Telnet sessions.
both	both	(Optional) Keyword that specifies the authorization method applies to both console and Telnet sessions.
disable	disable	Keyword that specifies to disable authorization for commands.

Defaults Authorization is disabled by default.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The **tacacs+** values 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 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	enable	Keyword that specifies to enable the specified authorization method.
<i>option</i>	option	Switch response to an authorization request; valid values are tacacs+ , if-authenticated , and none . Refer to the “Usage Guidelines” section on page 2-153 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 tacacs+ , deny , if-authenticated , and none . Refer to the “Usage Guidelines” section on page 2-153 for valid value definitions.
console	console	(Optional) Keyword that specifies the authorization method applies to console sessions.
telnet	telnet	(Optional) Keyword that specifies the authorization method applies to Telnet sessions.
both	both	(Optional) Keyword that specifies the authorization method applies to both console and Telnet sessions.
disable	disable	Keyword that specifies to disable authorization method.

Defaults Authorization is disabled by default.

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 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 that specifies 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 on page 2-155 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 tacacs+ , deny , if-authenticated , and none . Refer to the “Usage Guidelines” section on page 2-155 for valid value definitions.
console		(Optional) Keyword that specifies the authorization method applies to console sessions.
telnet		(Optional) Keyword that specifies the authorization method applies to Telnet sessions.
both		(Optional) Keyword that specifies the authorization method applies to both console and Telnet sessions.
disable		Keyword that specifies to disable authorization method.

Defaults Authorization is disabled by default.

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 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

<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

The banner cannot contain more than 3,070 characters, including tabs. Tabs display as eight characters but take only one character of memory.

You can use either the **clear banner motd** command or the **set banner motd cc** 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 at 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:

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

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_num]
```

```
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_num</i>	(Optional) Module number of the supervisor engine containing the Flash device.	
cfg1	Keyword that specifies 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 that specifies the second startup configuration file on the Supervisor Engine II G and III G. Use a semicolon-separated list to specify multiple cfg files.	
recurring	Keyword that specifies to retain <code>config_file</code> variable settings. Available only on the Supervisor Engine II G and III G.	
non-recurring	Keyword that specifies to clear <code>config_file</code> 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 Catalyst 5000 family Supervisor Engine III or III F, and Catalyst 4000 family, 2926G series, and 2948G switches, multiple configuration files may be specified, but they must be separated by a semicolon (;).

In the Catalyst 5000 family 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.

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_num]
```

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

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

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

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

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.
mod_num		(Optional) Module number of the supervisor engine on which to set the configuration register value.
boot		Keyword that specifies the boot method to use the next time the switch is reset or power cycled.
rommon		Keyword that causes the switch to remain in ROM monitor mode the next time the switch is reset or power cycled.
bootflash		Keyword that causes the switch to boot using the first valid system image in bootflash the next time the switch is reset or power cycled.
system		Keyword that causes 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 that specifies to set the console baud rate.
1200 2400 4800 9600		Keywords that specifies the ROM monitor console port baud rate.
ignore-config		Keyword that specifies whether the switch should ignore the configuration in NVRAM the next time the switch is restarted.
enable		Keyword that causes the switch to ignore the configuration in NVRAM the next time the switch is restarted.
disable		Keyword that prevents the switch from ignoring the configuration in NVRAM the next time the switch is restarted.
recurring		Keyword that causes 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.
non-recurring		Keyword that causes 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** 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.

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 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_num]
```

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 that specifies to place the software image file first in the list of images to attempt to boot.
<i>mod_num</i>	(Optional) Module number of the supervisor engine on which to modify the BOOT environment variable.

Defaults This command has no default setting.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command is not supported on the Catalyst 5000 Supervisor Engine II. The *mod_num* option is not supported on the Catalyst 2926G series switch.

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 sys flash bootflash:cat5000-sup3.5-1-1.bin
BOOT variable =
bootflash:cat5000-sup3.5-2-1.bin,1;bootflash:cat5000-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:cat5000-sup3.5-2-1.bin prepend
BOOT variable =
slot0:cat5000-sup3.5-2-1.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	Keyword that specifies to activate APaRT on FDDI.
	disable	Keyword that specifies to deactivate APaRT on FDDI.

Defaults The default configuration has APaRT enabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command is supported by the Catalyst 5000 family switches.

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	disable
	Keyword that specifies to permit FDDI to relearn MAC addresses learned from an Ethernet interface.	Keyword that specifies 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 This command is supported by the Catalyst 5000 family switches.

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

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

Syntax Description	8023	Keyword that specifies Ethernet 802.3 as the default translation method.
	snap	Keyword that specifies Ethernet SNAP as the default translation method.
	eii	Keyword that specifies Ethernet II as the default translation method.
	8023raw	Keyword that specifies 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 This command is supported by the Catalyst 5000 family switches.

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

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

Syntax Description	8022	Keyword that specifies FDDI 802.2 as the default translation method.
	snap	Keyword that specifies FDDI SNAP as the default translation method.
	fddiraw	Keyword that specifies 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 This command is supported by the Catalyst 5000 family switches.

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

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

Syntax Description	<table border="1"> <tbody> <tr> <td>8023</td> <td>Keyword that specifies Ethernet 802.3 as the default frame type.</td> </tr> <tr> <td>snap</td> <td>Keyword that specifies Ethernet SNAP as the default frame type.</td> </tr> <tr> <td>eii</td> <td>Keyword that specifies Ethernet II as the default frame type.</td> </tr> <tr> <td>8023raw</td> <td>Keyword that specifies Ethernet 802.3 RAW as the default frame type.</td> </tr> </tbody> </table>	8023	Keyword that specifies Ethernet 802.3 as the default frame type.	snap	Keyword that specifies Ethernet SNAP as the default frame type.	eii	Keyword that specifies Ethernet II as the default frame type.	8023raw	Keyword that specifies Ethernet 802.3 RAW as the default frame type.
8023	Keyword that specifies Ethernet 802.3 as the default frame type.								
snap	Keyword that specifies Ethernet SNAP as the default frame type.								
eii	Keyword that specifies Ethernet II as the default frame type.								
8023raw	Keyword that specifies 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	This command is supported by the Catalyst 5000 family switches.								
Examples	<p>This example shows how to set the default method for translating IPX FDDI SNAP frames to Ethernet frames to SNAP:</p> <pre>Console> (enable) set bridge ipx snaptoether snap Bridge snaptoether default IPX translation set. Console> (enable)</pre>								
Related Commands	show bridge								

set cam

Use the **set cam** command to add entries into the CAM table and to set the aging time for the CAM table.

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

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

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

```
set cam agingtime vlan agingtime
```

Syntax Description

dynamic	Keyword that specifies that entries are subject to aging.
static	Keyword that specifies that entries are not subject to aging. Static (nonpermanent) entries will remain in the table until the system is reset.
permanent	Keyword that specifies that 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>mod/port</i>	Number of the module and the port.
<i>vlan</i>	(Optional) Number of the VLAN.
<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 “-” to separate the bytes.
<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.
agingtime	Keyword that specifies to set the period of time after which an entry is removed from the table.
<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 agingtime keyword.
<i>agingtime</i>	Number of seconds (0 to 1,000,000 for the Catalyst 5000 family and 2926G series switches; 0 and 15 to 1,000,000 for the Catalyst 4000 family and 2948G switches) that dynamic entries remain in the table before being deleted. Setting aging time to 0 disables aging.

Defaults

The default aging time for all configured VLANs is 300 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set cam {dynamic | static | permanent} {route_descr} {mod/port} [vlan]** command is not supported by the Catalyst 4000 family, 2948G, and 2980G switches.

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 **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 minimum configurable non-zero age time for the Catalyst 4000 family, 2948G, and 2980G switches is 15 seconds. You cannot configure an aging time between 1 and 15 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)
```

This example shows how to add a static 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 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)
```

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 that specifies to enable the CDP feature.
disable	Keyword that specifies 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...* 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	holdtime	Keyword that specifies the global CDP hold time value.
	<i>holdtime</i>	Number of seconds for the global CDP hold time value; valid values are 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 The **holdtime** argument is not supported on Catalyst 5000 family and 2926G series switches with supervisor engine software release 4.2(2) and earlier and 3.2(4) and earlier, and Catalyst 4000 family, 2948G, and 2980G switches.

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 (5 to 900) the system waits between CDP message transmissions.
---------------------------	-----------------	--

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 that 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: <pre>Console> (enable) set cdp version v1 CDP version set to v1 Console> (enable)</pre>
Related Commands	<pre>set cdp show cdp</pre>

set cgmp

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

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

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

Defaults By default, 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 that specifies to enable CGMP leave processing.
	disable	Keyword that specifies to disable CGMP leave processing.

Defaults By default, 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 that specifies 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 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 that specifies 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 that specifies the primary server.
domain-name <i>domain_name</i>	Keyword and variable that specifies the domain name of the switch.
retry-interval	Keyword that specifies the retry interval in seconds.
<i>initial</i>	Initial timeout value; valid values are 0 to 65535 seconds.
<i>incr</i>	Incremental value; valid values are 0 to 65535 seconds.
<i>max</i>	Maximum timeout value; valid values are 0 to 65535 seconds.
roles	Keyword that specifies a user designated characteristic.
<i>role_name</i>	Keyword that specifies a user-designated physical characteristic (such as backbone, branchoffice, etc.). A switch may have multiple roles, and up to 64 roles may be configured per switch.

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

This command is supported by the Catalyst 5000 family switches.

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	disable
	Keyword that specifies to activate default port status.	Keyword that specifies to deactivate default port status.

Defaults This command has no default setting.

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 hole, 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**