

restore counters

Use the **restore counters** command to restore MAC and port counters.

```
restore counters [all | mod/ports]
```

Syntax Description	all (Optional) Keyword to specify all ports.
	<i>mod/ports</i> (Optional) Number of the module and the ports on the module.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines If you do not specify a range of ports to be restored, then all ports on the switch are restored.

Examples This example shows how to restore MAC and port counters:

```
Console> (enable) restore counters all  
This command will restore all counter values reported by the CLI to the hardware counter values.  
Do you want to continue (y/n) [n]? y  
MAC and Port counters restored.  
Console> (enable)
```

Related Commands [clear counters](#)
[show port counters](#)

rollback

Use the **rollback** command set to clear changes made to the ACL edit buffer since its last save. The ACL is rolled back to its state at the last **commit** command.

```
rollback qos acl {acl_name | all}
```

```
rollback security acl {acl_name | all | adjacency}
```

Syntax Description

qos acl	Keyword to specify QoS ACEs.
<i>acl_name</i>	Name that identifies the VACL whose ACEs are to be affected.
all	Keyword to rollback all ACLs.
security acl	Keywords to specify security ACEs.
adjacency	Keyword to rollback all adjacency tables.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the edit buffer of a specific QoS ACL:

```
Console> (enable) rollback qos acl ip-8-1
Rollback for QoS ACL ip-8-1 is successful.
Console> (enable)
```

This example shows how to clear the edit buffer of a specific security ACL:

```
Console> (enable) rollback security acl IPACL1
IPACL1 editbuffer modifications cleared.
Console> (enable)
```

Related Commands

[show qos acl info](#)
[commit](#)

session

Use the **session** command to open a session with a module (for example, the MSM, NAM, or ATM). This command allows you to use the module-specific CLI.

session *mod*

Syntax Description

<i>mod</i>	Number of the module.
------------	-----------------------

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

After you enter this command, the system responds with the Enter Password: prompt, if one is configured on the module.

To end the session, enter the **quit** command.

Use the **session** command to toggle between router and switch sessions.

For information on ATM commands, refer to the *ATM Software Configuration Guide and Command Reference for the Catalyst 5000 Family and 6000 Family Switches*.

For information on NAM commands, refer to the *Catalyst 6000 Network Analysis Module Installation and Configuration Note*.

Examples

This example shows how to open a session with an MSM (module 4):

```
Console> session 4
Trying Router-4...
Connected to Router-4.
Escape character is '^]'.

Router>
```

Related Commands

[switch console](#)
[quit](#)

set

Use the **set** command to display all of the ROM monitor variable names with their values.

```
set
```

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Types ROM monitor command.

Command Modes Normal.

Examples This example shows how to display all of the ROM monitor variable names with their values:

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

Related Commands [varname=](#)

set accounting commands

Use the **set accounting commands** command set to enable command event accounting on the switch.

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

```
set accounting commands disable
```

Syntax Description	enable	Keyword to enable the specified accounting method for commands.
	config	Keyword to permit accounting for configuration commands only.
	enable	Keyword to permit accounting for enable mode commands only.
	all	Keyword to permit accounting for all commands.
	stop-only	(Optional) Keyword to apply the accounting method at the command end.
	tacacs+	Keyword to specify TACACS+ accounting for commands.
	disable	Keyword to disable accounting for commands.

Defaults The default is accounting is disabled.

Command Types Switch command.

Command Modes Privileged.

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

Examples This example shows how to send records at the end of the event only using a TACACS+ server:

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

Related Commands

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

set accounting connect

Use the **set accounting connect** command set to enable accounting of outbound connection events on the switch.

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

```
set accounting connect disable
```

Syntax Description

enable	Keyword to enable the specified accounting method for connection events.
start-stop	Keyword to apply the accounting method at the start and stop of the connection event.
stop-only	Keyword to apply the accounting method at the end of the connection event.
tacacs+	Keyword to specify TACACS+ accounting for connection events.
radius	Keyword to specify RADIUS accounting for connection events.
disable	Keyword to disable accounting of connection events.

Defaults

The default is accounting is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must configure the RADIUS or TACACS+ servers and shared secret keys before you enable accounting.

Examples

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

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

Related Commands

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

set accounting exec

Use the **set accounting exec** command set to enable accounting of normal login sessions on the switch.

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

```
set accounting exec disable
```

Syntax Description	enable	Keyword to enable the specified accounting method for normal login sessions.
	start-stop	Keyword to specify the accounting method applies at the start and stop of the normal login sessions.
	stop-only	Keyword to specify the accounting method applies at the end of the normal login sessions.
	tacacs+	Keyword to specify TACACS+ accounting for normal login sessions.
	radius	Keyword to specify RADIUS accounting for normal login sessions.
	disable	Keyword to disable accounting for normal login sessions.

Defaults The default is accounting is disabled.

Command Types Switch command.

Command Modes Privileged.

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

Examples This example shows how to enable accounting of normal login sessions, generating records at start and stop using a RADIUS server:

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

This example shows how to enable accounting of normal login sessions, generating records at stop using a TACACS+ server:

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

Related Commands

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

set accounting suppress

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

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

Syntax Description	Command	Description
	null-username	Keyword to specify users must have a user ID.
	enable	Keyword to enable suppression for a specified user.
	disable	Keyword to disable suppression for a specified user.

Defaults The default is accounting is disabled.

Command Types Switch command.

Command Modes Privileged.

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

Examples This example shows how to suppress accounting information for users without a username:

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

This example shows how to include users without the usernames' accounting event information:

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

Related Commands

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

set accounting system

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

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

```
set accounting system disable
```

Syntax Description	enable	Keyword to enable the specified accounting method for system events.
	start-stop	Keyword to specify the accounting method applies at the start and stop of the system event.
	stop-only	Keyword to specify the accounting method applies at the end of the system event.
	tacacs+	Keyword to specify TACACS+ accounting for system events.
	radius	Keyword to specify RADIUS accounting for system events.
	disable	Keyword to disable accounting for system events.

Defaults The default is accounting is disabled.

Command Types Switch command.

Command Modes Privileged.

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

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

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

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

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

Related Commands

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

set accounting update

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 specify an update when new information is available.
periodic	Keyword to specify an update on a periodic basis.
<i>interval</i>	(Optional) Periodic update interval time; valid values are from 1 to 71582 minutes.

Defaults The default is accounting is disabled.

Command Types Switch command.

Command Modes Privileged.

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

Examples This example shows how to 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 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.

Defaults The default is no aliases are configured.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The name **all** cannot be defined as an alias. Reserved words cannot be defined as aliases. For additional information about *parameter*, see the specific command for information about applicable parameters.

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

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

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

set arp

Use the **set arp** command set 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 that entries are subject to ARP aging updates.
permanent	(Optional) Keyword to specify that permanent entries are stored in NVRAM until they are removed by the clear arp or clear config command.
static	(Optional) Keyword to specify that entries are not subject to ARP aging updates.
<i>ip_addr</i>	IP address or IP alias to map to the specified MAC address.
<i>hw_addr</i>	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 that entries will remain in the ARP table before being deleted; valid values are from 0 to 1,000,000 seconds. Setting this value to 0 disables aging.

Defaults

The default is no ARP table entries exist; ARP aging is set to 1200 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When entering the *hw_addr*, use a 6-hexadecimal byte MAC address in canonical (00-11-22-33-44-55) or noncanonical (00:11:22:33:44:55) format.

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

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 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 <i>count</i>	Keyword and variable to specify the number of connection attempts before initiating an error; valid values are 0 , from 3 to 10 , and 0 to disable.
lockout <i>time</i>	Keyword and variable to specify the lockout timeout; valid values are from 30 to 600 seconds, and 0 to disable.

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** 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.

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 authentication](#)

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, from 3 to 10, and 0 to disable.
lockout time	Keyword and variable to specify the lockout timeout; valid values are from 30 to 600 seconds, and 0 to disable.

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.

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 attempts:

```
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 authentication](#)

set authorization commands

Use the **set authorization commands** command set 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>	<i>option</i>	Switch response to an authorization request; valid values are tacacs+ , if-authenticated , and none . See the “Usage Guidelines” section for valid value definitions.
<i>fallbackoption</i>	<i>fallbackoption</i>	Switch fallback response to an authorization request if the TACACS+ server is down or not responding; valid values are tacacs+ , deny , if-authenticated , and none . See the “Usage Guidelines” section for valid value definitions.
disable	disable	Keyword to disable authorization of command events.
console	console	(Optional) Keyword to specify the authorization method for console sessions.
telnet	telnet	(Optional) Keyword to specify the authorization method for Telnet sessions.
both	both	(Optional) Keyword to specify the authorization method for both console and Telnet sessions.

Defaults The default is authorization is disabled.

Command Types Switch command.

Command Modes Privileged.

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

- **tacacs+** specifies the TACACS+ authorization method.
- **deny** does not let you proceed.

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

Examples

This example shows how to enable authorization for all commands with the **if-authenticated** *option* and **none** *fallbackoption*:

```
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 set to enable authorization of privileged mode sessions 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 . See 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 tacacs+ , deny , if-authenticated , and none . See the “Usage Guidelines” section for valid value definitions.
	disable	Keyword to disable the authorization method.
	console	(Optional) Keyword to specify the authorization method for console sessions.
	telnet	(Optional) Keyword to specify the authorization method for Telnet sessions.
	both	(Optional) Keyword to specify the authorization method for both console and Telnet sessions.

Defaults The default is authorization is disabled.

Command Types Switch command.

Command Modes Privileged.

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

- **tacacs+** specifies the TACACS+ authorization method.
- **deny** does not let you proceed.
- **if-authenticated** allows you to proceed with your action if you have authentication.
- **none** 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, privileged login 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 set 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 . See 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 tacacs+ , deny , if-authenticated , and none . See the “Usage Guidelines” section for valid value definitions.
	disable	Keyword to disable authorization method.
	console	(Optional) Keyword to specify the authorization method for console sessions.
	telnet	(Optional) Keyword to specify the authorization method for Telnet sessions.
	both	(Optional) Keyword to specify the authorization method for both console and Telnet sessions.

Defaults The default is authorization is denied.

Command Types Switch command.

Command Modes Privileged.

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

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

Examples

This example shows how to enable authorization of configuration commands in exec, normal login 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 lcd

Use the **set banner lcd** command to configure the Catalyst 6500 series Switch Fabric Module LCD user banner.

```
set banner lcd 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

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The banner may contain no more than 800 characters, including tabs. Tabs display as eight characters but take only one character of memory.

Once you configure the user banner, it is sent down to all Catalyst 6500 series Switch Fabric Modules in the switch and displayed in the LCD.

Examples

This example shows how to set the Catalyst 6500 series Switch Fabric Module LCD user banner:

```
Console> (enable) set banner lcd &hello  
there&  
LCD banner set  
Console> (enable)
```

Related Commands

[show banner](#)

set banner motd

Use the **set banner motd** command to program an MOTD banner to appear before session login.

```
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

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The banner may contain no 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](#)
[show banner](#)

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 bootup. The list of configuration files is stored in the CONFIG_FILE environment variable.

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

Syntax Description

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

Defaults

The default CONFIG_FILE is slot0:switch.cfg.

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).

If you specify multiple configuration files, you must separate the files with a semicolon (;).

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 a single configuration file environment variable:

```
Console> (enable) set boot auto-config slot0:cfgfile2
CONFIG_FILE variable = slot0:cfgfile2
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 file environment variables:

```
Console> (enable) set boot auto-config slot0:cfgfile1;slot0:cfgfile2
CONFIG_FILE variable = slot0:cfgfile1;slot0:cfgfile2
WARNING: nvram configuration may be lost during next bootup,
        and re-configured using the file(s) specified.
Console> (enable)
```

Related Commands

set boot config-register
set boot system flash
show boot

set boot config-register

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

```
set boot config-register 0xvalue [mod]
```

```
set boot config-register baud {1200 | 2400 | 4800 | 9600 | 19200 | 38400} [mod]
```

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

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

Syntax	Description
0xvalue	Keyword to set the 16-bit configuration register value.
<i>mod</i>	(Optional) Module number of the supervisor engine containing the Flash device.
baud 1200 2400 4800 9600 19200 38400	Keywords to specify the console baud rate.
ignore-config	Keywords to set the ignore-config feature.
enable	Keyword to enable the specified feature.
disable	Keyword to disable the specified feature.
boot	Keyword to specify the boot image to use on the next restart.
rommon	Keyword to specify booting from the ROM monitor.
bootflash	Keyword to specify booting from the bootflash.
system	Keyword to specify booting from the system.

Defaults

The defaults are as follows:

- Configuration register value is 0x10F, which causes the switch to boot from what is specified by the BOOT environment variable.
- Baud rate is set to 9600.
- **ignore-config** parameter is disabled.

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.

When you enable the **ignore-config** feature, the system software ignores the configuration. 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 booting from the ROM monitor:

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

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

```
Console> (enable) set boot config-register 0x12f
Configuration register is 0x12f
break: disabled
ignore-config: disabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

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

```
Console> (enable) set boot config-register baud 4800
Configuration register is 0x90f
ignore-config: disabled
console baud: 4800
boot: image specified by the boot system commands
Console> (enable)
```

This example shows how to ignore the configuration information stored in NVRAM the next time the switch is restarted:

```
Console> (enable) set boot config-register ignore-config enable
Configuration register is 0x94f
ignore-config: enabled
console baud: 4800
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
console baud: 9600
boot: the ROM monitor
Console> (enable)
```

Related Commands

set config acl nvram
set boot auto-config
set boot system flash
show boot
copy
show config

set boot config-register auto-config

Use the **set boot config-register auto-config** command set to configure auto-config file dispensation.

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

```
set boot config-register auto-config { overwrite | append }
```

```
set boot config-register auto-config sync { enable | disable }
```

Syntax Description		
recurring	Keyword to set auto-config to recurring and specify the switch retains the contents of the CONFIG_FILE environment variable after the switch is reset or power cycled and configured.	
non-recurring	Keyword to set auto-config to nonrecurring and 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.	
<i>mod</i>	(Optional) Module number of the supervisor engine containing the Flash device.	
overwrite	Keyword to cause the auto-config file to overwrite the NVRAM configuration.	
append	Keyword to cause the auto-config file to append to the file currently in the NVRAM configuration.	
sync enable disable	Keywords to enable or disable synchronization of the auto-config file.	

Defaults

The defaults are as follows:

- **overwrite**
- **non-recurring**
- **sync is disable**

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **auto-config overwrite** command clears the NVRAM configuration before executing the Flash configuration file. The **auto-config append** command executes the Flash configuration file before clearing the NVRAM configuration.

If you delete the auto-config Flash file(s) on the supervisor engine, the files will also be deleted on the standby supervisor engine.

If you enter the **sync enable** keywords, this enables synchronization to force the configuration files to synchronize automatically to the standby supervisor engine. The file(s) are kept consistent with what is on the active supervisor engine.

If you use the **set boot auto-config bootflash:switch.cfg** with the overwrite option, you must use the **copy config bootflash:switch.cfg** command to save the switch configuration to the auto-config file.

If you use the **set boot auto-config bootflash:switchapp.cfg** with the append option, you can use the **copy acl config bootflash:switchapp.cfg** command to save the switch configuration to the auto-config file.

If the ACL configuration location is set to Flash memory, the following message is displayed after every commit operation for either security or QoS. Use the **copy** command to save your ACL configuration to Flash memory. If you reset the system and you made one or more commits but did not copy commands to one of the files specified in the CONFIG_FILE variable, the following message displays:

```
Warning: System ACL configuration has been modified but not saved to Flash.
```

The files used with the **recurring** and **non-recurring** options are those specified by the CONFIG_FILE environment variable.

Examples

This example shows how to specify the ACL configuration Flash file at system startup:

```
Console> (enable) set boot auto-config bootflash:switchapp.cfg
Console> (enable) set boot config-register auto-config recurring
Console> (enable)
```

This example shows how to ignore the configuration information stored in NVRAM the next time the switch is restarted:

```
Console> (enable) set boot config-register auto-config non-recurring
Configuration register is 0x2102
ignore-config: disabled
auto-config: non-recurring, overwrite, auto-sync disabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

This example shows how to append the auto-config file to the file currently in the NVRAM configuration:

```
Console> (enable) set boot config-register auto-config append
Configuration register is 0x2102
ignore-config: disabled
auto-config: non-recurring, append, auto-sync disabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

This example shows how to use the auto-config overwrite option to save the ACL configuration to a bootflash file:

```
Console> (enable) copy config bootflash: switch.cfg
Console> (enable) set boot auto-config bootflash:switch.cfg
Console> (enable) set boot config-register auto-config overwrite
Console> (enable)
```



Caution

The following two examples assume that you have saved the ACL configuration to the bootflash:switchapp.cfg file.

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

```
Console> (enable) set boot config-register auto-config sync enable  
Configuration register is 0x2102  
ignore-config: disabled  
auto-config: non-recurring, append, auto-sync enabled  
console baud: 9600  
boot: image specified by the boot system commands  
Console> (enable)
```

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

```
Console> (enable) set boot config-register auto-config sync disable  
Configuration register is 0x2102  
ignore-config: disabled  
auto-config: non-recurring, append, auto-sync disabled  
console baud: 9600  
boot: image specified by the boot system commands  
Console> (enable)
```

Related Commands

[set boot config-register](#)
[set boot system flash](#)
[show boot](#)

set boot device

Use the **set boot device** command to set the NAM or IDS boot environment.

```
set boot device bootseq[,bootseq] mod
```

Syntax Description		
<i>bootseq</i>	Device where the startup configuration file resides; see the “Usage Guidelines” section for format guidelines. The second <i>bootseq</i> is optional.	
<i>mod</i>	Number of the module containing the Flash device.	

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines When you enter the **set boot device** command, the existing boot string in the supervisor engine NVRAM is always overwritten.

When you enter the *bootseq*, use the following guidelines:

- *bootseq* = *bootdevice*[:*bootdevice-qualifier*]
- *bootdevice* is the device where the startup configuration file resides; valid values are **pcmcia**, **hdd**, or **network**.
- *bootdevice-qualifier* is the name of the startup configuration file; valid values for **hdd** are from 1 to 99, and for **pcmcia**, valid values are slot0 or slot1.
- The colon between *bootdevice* and *bootdevice-qualifier* is required.
- You can enter multiple *bootseqs* by separating each entry with a comma; 15 is the maximum number of boot sequences you can enter.

The supervisor engine does not validate the boot device you specify, but simply stores the boot device list in NVRAM.

This command is supported by the NAM or IDS only.

Examples This example shows how to specify the boot environment to boot to the maintenance partition of the NAM on module 2:

```
Console> (enable) set boot device hdd:2 2
Device BOOT variable = hdd:2
Warning: Device list is not verified but still set in the boot string.
Console> (enable)
```

This example shows how to specify multiple boot environments on module 5:

```
Console> (enable) set boot device hdd,hdd:5,pcmcia:slot0,network,hdd:6 5
Device BOOT variable = hdd,hdd:5,pcmcia:slot0,network,hdd:6
Warning:Device list is not verified but still set in the boot string.
Console> (enable)
```

Related Commands

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

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

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

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

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

set boot system flash

Use the **set boot system flash** command to set the BOOT environment variable that specifies a list of images the switch loads at startup.

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

Syntax Description	
<i>device</i> :	Device where the Flash resides.
<i>filename</i>	(Optional) Name of the configuration file.
prepend	(Optional) Keyword to place the device first in the list of boot devices.
<i>mod</i>	(Optional) Module number of the supervisor engine containing the Flash device.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines A colon (:) is required after the specified device.

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. Remember to clear the old entry when building a new image with a different filename in order to use the new image.

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

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

Examples This example shows how to append the filename `cat6000-sup.5-5-1.bin` on device `bootflash` to the BOOT environment variable:

```
Console> (enable) set boot system flash bootflash:cat6000-sup.5-5-1.bin
BOOT variable = bootflash:cat6000-sup.5-4-1.bin,1;bootflash:cat6000-sup.5-5-1.bin,1;
Console> (enable)
```

This example shows how to prepend `cat6000-sup.5-5-1.bin` to the beginning of the boot string:

```
Console> (enable) set boot system flash bootflash:cat6000-sup.5-5-1.bin prepend
BOOT variable = bootflash:cat6000-sup.5-5-1.bin,1;bootflash:cat6000-sup.5-4-1.bin,1;
Console> (enable)
```

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

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 and from 1025 to 4094 .	
<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) dynamic entries remain in the table before being deleted.	

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.

Setting the aging time to 0 disables aging.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

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

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

If you enter a route descriptor 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 port(s) are trunk ports, you must specify the VLAN.

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

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

**Note**

Static CAM entries that are configured on the active supervisor engine are lost after fast switchover. You must reconfigure CAM entries after fast switchover.

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 set to enable, disable, or configure CDP features globally on all ports or on specified ports.

set cdp {**enable** | **disable**} {*mod/ports...*}

set cdp interval *interval*

set cdp holdtime *holdtime*

set cdp version **v1** | **v2**

set cdp format device-id {**mac-address** | **other**}

Syntax Description		
enable	enable	Keyword to enable the CDP feature.
disable	disable	Keyword to disable the CDP feature.
<i>mod/ports..</i>		Number of the module and the ports on the module.
interval	interval	Keyword to specify the CDP message interval value.
<i>interval</i>		Number of seconds the system waits before sending a message; valid values are from 5 to 900 seconds.
holdtime	holdtime	Keyword to specify the global Time-To-Live value.
<i>holdtime</i>		Number of seconds for the global Time-To-Live value; valid values are from 10 to 255 seconds.
version v1 v2		Keywords to specify the CDP version number.
format device-id		Keywords to set the device-ID TLV format.
mac-address		Keywords to specify that the device-ID TLV carry the MAC address of the sending device in ASCII, in canonical format.
other		Keyword to specify that the device's hardware serial number concatenated with the device name between parenthesis.

Defaults

The default system configuration has CDP enabled. The message interval is set to 60 seconds for every port; the default Time-To-Live value has the message interval globally set to 180 seconds. The default CDP version is version 2. The default device-id TLV format is **other**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set cdp version** command allows you to globally set the highest version number of CDP packets to send.

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 interfaces, but the per-port **enable** (or **disable**) configuration is not changed. If you globally enable CDP, whether CDP is running on an interface or not depends on its per-port configuration.

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

The Device-Id TLV can carry two different formats of the device identifier for the sending device:

- **mac-address** format—The device-ID TLV is the MAC address of the sending device in ASCII, in canonical format.
- **other** format—The device identifier for the sending device is the device's hardware serial number concatenated with the device name between parenthesis.

Examples

This example shows how to enable the CDP message display for 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)
```

This example shows how to specify the CDP message interval value:

```
Console> (enable) set cdp interval 400  
CDP interval set to 400 seconds.  
Console> (enable)
```

This example shows how to specify the global Time-To-Live value:

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

This example shows how to set the device ID format to MAC address:

```
Console> (enable) set cdp format device-id mac-address  
Device Id format changed to MAC-address  
Console> (enable)
```

Related Commands

[show cdp](#)
[show port cdp](#)

set channel cost

Use the **set channel cost** command to set the channel path cost and adjust the port costs of the ports in the channel automatically.

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

Syntax Description	
<i>channel_id</i>	Number of the channel identification.
all	Keyword to configure all channels.
<i>cost</i>	(Optional) Port costs of the ports in the channel.

Defaults The default is the port cost is updated automatically based on the current port costs.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines When you do not enter the *cost*, the cost is updated based on the current port costs of the channeling ports. If you change the channel cost, member ports in the channel might be modified and saved to NVRAM. If this is the case, a message appears to list the ports whose port path costs were updated due to the channel cost modification.



Note

With software releases 6.2(1) and earlier, the 6- and 9-slot Catalyst 6000 family switches support a maximum of 128 EtherChannels.

With software releases 6.2(2) and later, due to the port ID handling by the spanning tree feature, the maximum supported number of EtherChannels is 126 for a 6- or 9-slot chassis and 63 for a 13-slot chassis. Note that the 13-slot chassis was first supported in software release 6.2(2).

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.
```

Related Commands [show channel](#)

set channel vlancost

Use the **set channel vlancost** command to set the channel VLAN cost.

set channel vlancost *channel_id* *cost*

Syntax Description	
<i>channel_id</i>	Number of the channel identification; valid values are from 769 to 896 .
<i>cost</i>	Port costs of the ports in the channel.

Defaults The default is the VLAN cost is updated automatically based on the current port VLAN costs of the channeling ports.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines When you do not enter the *cost*, the cost is updated based on the current port VLAN costs of the channeling ports.
You can configure only one channel at a time.



Note

The **set channel vlancost** command creates a “set spantree portvlancost” entry for each port in the channel. You must then manually reenter the **set spantree portvlancost** command for at least one port in the channel, specifying the VLAN or VLANs that you want associated with the port. When you associate the desired VLAN or VLANs with one port, all ports in the channel are automatically updated. Refer to Chapter 6, “Configuring EtherChannel,” in the *Catalyst 6000 Family Software Configuration Guide* for more information.



Note

With software releases 6.2(1) and earlier, the 6- and 9-slot Catalyst 6000 family switches support a maximum of 128 EtherChannels.

With software releases 6.2(2) and later, due to the port ID handling by the spanning tree feature, the maximum supported number of EtherChannels is 126 for a 6- or 9-slot chassis and 63 for a 13-slot chassis. Note that the 13-slot chassis was first supported in software release 6.2(2).

Examples This example shows how to set the channel 769 path cost to 10:

```
Console> (enable) set channel vlancost 769 10
Port(s) 1/1-2 vlan cost are updated to 24.
Channel 769 vlancost is set to 10.
Console> (enable)
```

After you enter this command, you must reenter the **set spantree portvlancost** command so that the desired VLAN or VLANs are associated with all the channel ports.

This example shows how to associate the channel 769 path cost to 10 for VLAN 1 through VLAN 1005:

```
Console> (enable) set spantree portvlancost 1/1 cost 24 1-1005
Port 1/1 VLANs 1025-4094 have path cost 19.
Port 1/1 VLANs 1-1005 have path cost 24.
Port 1/2 VLANs 1-1005 have path cost 24.
Console> (enable)
```

Related Commands

set spantree portvlancost
show channel

set config acl nvram

Use the **set config acl nvram** command to copy the current committed ACL configuration from DRAM back into NVRAM.

set config acl nvram

Syntax Description This command has no arguments or keywords.

Defaults The default is NVRAM.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command fails if there is not enough space in NVRAM.

This command copies the current committed configuration to NVRAM; this configuration might be different from the configuration in the auto-config file. After the ACL configuration is copied into NVRAM, you must turn off the auto-config options using the **clear boot auto-config** command.

Examples This example shows how to copy the ACL configuration to NVRAM:

```
Console> (enable) set config acl nvram
ACL configuration copied to NVRAM.
Console> (enable)
```

Related Commands

- [set boot config-register](#)
- [set boot system flash](#)
- [show boot](#)
- [copy](#)
- [clear config](#)

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.	
nvr am	Keyword to specify the saved configuration be stored in NVRAM.	
<i>device:file-id</i>	Name of the device and filename where the saved configuration will be stored.	

Defaults The default setting of this command is binary, saving the configuration to NVRAM.

Command Types Switch command.

Command Modes Privileged.

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** command set to configure COPS functionality.

set cops server *ipaddress* [*port*] [**primary**] [**diff-serv** | **rsvp**]

set cops domain-name *domain_name*

set cops retry-interval *initial incr max*

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.
diff-serv	(Optional) Keyword to set the COPS server for differentiated services.
rsvp	(Optional) Keyword to set the COPS server for RSVP+.
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.

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

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 be set globally only; 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, A-Z, 0-9, ., - and _. 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 rsvp
171.21.34.56 added to COPS server table as primary server for RSVP.
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)
```

Related Commands

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

set crypto key rsa

Use the **set crypto key rsa** command to generate and configure an RSA key pair.

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

Syntax Description	<i>nbits</i>	Size of the key; valid values are 512 to 2048 bits.
	force	(Optional) Keyword to regenerate the keys and suppress the warning prompt of overwriting existing keys.

Defaults The command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The **crypto** commands are supported on systems that run these image types only:

- supk9 image—for example, cat6000-supk9.6-1-3.bin
- supcvk9 image—for example, cat6000-supcvk9.6-1-3.bin

If you do not enter the **force** keyword, the **set crypto key** command is saved into the config file and you will have to use the **clear config all** command to clear the RSA keys.

The *nbits* value is required.

To support SSH login, you first must generate an RSA key pair.

Examples This example shows how to create an RSA key:

```
Console> (enable) set crypto key rsa 1024
Generating RSA keys.... [OK]
Console> (enable)
```

Related Commands [clear crypto key rsa](#)
[show crypto key](#)