

restore counters

To restore MAC and port counters, use the **restore counters** command.

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

```
restore counters channel {all | channel-id}
```

```
restore counters lacp-channel {all | channel-id}
```

Syntax Description

| | |
|---------------------|--|
| all | (Optional) Restores all ports. |
| <i>mod/ports</i> | (Optional) Number of the module and the ports on the module. |
| channel | Restores PAgP channel MAC and port counters. |
| all | Restores MAC and port counters for all PAgP channels. |
| <i>channel_id</i> | Number of a specific PAgP channel. |
| lacp-channel | Restores LACP channel MAC and port counters. |
| all | Restores MAC and port counters for all LACP channels. |
| <i>channel_id</i> | Number of a specific LACP channel. |

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.

To restore channel-based counters on a per-channel basis, use the channel ID number. Enter the **show port channel** command to find the channel ID number for PAgP channels. Enter the **show port lacp-channel** command to find the channel ID number for LACP channels.

Examples

This example shows how to restore MAC counters 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)
```

This example shows how to restore the counters for channel 769:

```
Console> (enable) restore counter channel 769  
This command will restore counter values reported by the CLI  
for PAGP channel 769 ports 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 channel traffic](#)
- [show port channel](#)
- [show port counters](#)
- [show port lacp-channel](#)

rollback

To clear changes made to the ACL edit buffer since its last save, use the **rollback** command. 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 | | Specifies QoS ACEs. |
| <i>acl_name</i> | | Name that identifies the VLAN access control list (VACL) whose ACEs are to be affected. |
| all | | Rolls back all ACLs. |
| security acl | | Specifies security ACEs. |
| adjacency | | Rolls back 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

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

session

To open a session with a module (for example, the MSM, NAM, or ATM), use the **session** command. 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 6500 Series Switches*.

For information on NAM commands, refer to the *Catalyst 6000 Family Network Analysis Module Installation and Configuration Note* and the *Catalyst 6500 Series and Cisco 7600 Series Network Analysis Module Command Reference*.

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

quit
switch console

set

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

set

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Types ROM monitor command.

Command Modes Normal.

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

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

Related Commands [varname=](#)

set accounting commands

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

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

```
set accounting commands disable
```

Syntax Description

| | |
|------------------|--|
| enable | Enables the specified accounting method for commands. |
| config | Permits accounting for configuration commands only. |
| enable | Permits accounting for enable mode commands only. |
| all | Permits accounting for all commands. |
| stop-only | (Optional) Applies the accounting method at the command end. |
| tacacs+ | Specifies TACACS+ accounting for commands. |
| disable | Disables 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

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

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

```
set accounting connect disable
```

| Syntax Description | enable | Enables the specified accounting method for connection events. |
|--------------------|-------------------|--|
| | start-stop | Applies the accounting method at the start and stop of the connection event. |
| | stop-only | Applies the accounting method at the end of the connection event. |
| | tacacs+ | Specifies TACACS+ accounting for connection events. |
| | radius | Specifies RADIUS accounting for connection events. |
| | disable | Disables 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

To enable accounting of normal login sessions on the switch, use the **set accounting exec** command.

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

```
set accounting exec disable
```

Syntax Description

| | |
|-------------------|---|
| enable | Enables the specified accounting method for normal login sessions. |
| start-stop | Specifies the accounting method applies at the start and stop of the normal login sessions. |
| stop-only | Specifies the accounting method applies at the end of the normal login sessions. |
| tacacs+ | Specifies TACACS+ accounting for normal login sessions. |
| radius | Specifies RADIUS accounting for normal login sessions. |
| disable | Disables 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

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

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

Syntax Description

| | |
|----------------------|--|
| null-username | Specifies users must have a user ID. |
| enable | Enables suppression for a specified user. |
| disable | Disables 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 username 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

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

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

```
set accounting system disable
```

| Syntax Description | enable | Enables the specified accounting method for system events. |
|--------------------|-------------------|--|
| | start-stop | Specifies the accounting method applies at the start and stop of the system event. |
| | stop-only | Specifies the accounting method applies at the end of the system event. |
| | tacacs+ | Specifies TACACS+ accounting for system events. |
| | radius | Specifies RADIUS accounting for system events. |
| | disable | Disables 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

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

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

| | | |
|---------------------------|-----------------|---|
| Syntax Description | new-info | Specifies an update when new information is available. |
| | periodic | Specifies 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 acllog ratelimit

To limit the number of packets sent to the route processor CPU for bridged ACEs, use the **set acllog ratelimit** command.

set acllog ratelimit *rate*

Syntax Description

| | |
|-------------|--|
| <i>rate</i> | Number of packets per second; valid values are 1 to 1000. See the “Usage Guidelines” section for more information. |
|-------------|--|

Defaults

ACL log rate limiting is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

After entering the **set acllog ratelimit** command or the **clear acllog** command, you must either reset the route processor or perform a shut/not shut on the route processor interfaces that have ACEs with the **log** keyword applied.

After entering the **set acllog ratelimit** command, the reset or shut/no shut action causes the bridged ACEs to be redirected to the route processor with rate limiting.

To disable ACL log rate limiting, enter the **clear acllog** command. After entering the **clear acllog** command, the reset or shut/no shut action causes the system to return to its previous behavior. The bridge action remains unchanged.

If the number of packets per second is greater than the rate that you specify, the packets that exceed the specified rate are dropped.

A *rate* value of 500 is recommended.

Examples

This example shows how to enable ACL logging and to specify a rate of 500 for rate limiting:

```
Console> (enable) set acllog ratelimit 500
```

If the ACLs-LOG were already applied, the rate limit mechanism will be effective on system restart, or after shut/no shut the interface.

```
Console> (enable)
```

Related Commands

[clear acllog](#)
[show acllog](#)

set acl mac-packet-classify

To set MAC-based ACL lookups for all packet types on a VLAN, use the **set acl mac-packet-classify** command.

```
set acl mac-packet-classify {vlans | all}
```

| Syntax Description | |
|--------------------|--|
| <i>vlan</i> s | VLAN list; valid values are 1 to 4094. |
| all | Specifies all VLANs. |

Defaults The MAC-based ACL lookups for all packet types are disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The MAC-based ACL lookup feature is available only on a system with a PFC3B or a PFC3BXL. This feature affects both security ACLs and QoS MAC ACLs.

You should only enable this feature on Layer 2 VLANs. If you want to enable this feature on Layer 3 VLANs, note the following:

- You will lose some Layer 3 features, as indicated by this message, which appears when you enable MAC-based ACLs on a Layer 3 VLAN:

```
Warning: IP RACLs, VACLs & some IP features will be ineffective on these vlans.
```

- You might see an inconsistency in the egress ACL lookup depending on whether the packet is forwarded by the software or by the hardware. We recommend that you enable this feature on all VLANs to eliminate this inconsistency.

Examples This example shows how to enable the MAC-based ACL feature on a VLAN:

```
Console> (enable) set acl mac-packet-classify 5
Enabled mac-packet-classify on vlan(s) 5.
Warning: IP RACLs, VACLs & some IP features will be ineffective on these vlans.
Console> (enable)
```

Related Commands [clear acl mac-packet-classify](#)
[show acl mac-packet-classify](#)

set alias

To define aliases (shorthand versions) of commands, use the **set alias** command.

```
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. You can set a maximum of 100 aliases on the switch. For additional information about the *parameter* value, 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

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

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

```
set arp agingtime agingtime
```

| Syntax Description | |
|--------------------|--|
| dynamic | (Optional) Specifies that entries are subject to ARP aging updates. |
| permanent | (Optional) Specifies that permanent entries are stored in NVRAM until they are removed by the clear arp or clear config command. |
| static | (Optional) Specifies 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 | Sets 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* value, 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

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

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

Defaults 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

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

```
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 | Specifies the use of the RADIUS server password to determine if you have access permission to the switch. |
| tacacs | Specifies the use of the TACACS+ server password to determine if you have access permission to the switch. |
| kerberos | Specifies the Kerberos server password to determine if you have access permission to the switch. |
| enable | Enables the specified authentication method for login. |
| console | (Optional) Specifies the authentication method for console sessions. |
| telnet | (Optional) Specifies the authentication method for Telnet sessions. |
| http | (Optional) Specifies the authentication method for HTTP sessions. |
| all | (Optional) Specifies the authentication method for all session types. |
| primary | (Optional) Specifies that the method specified is the primary authentication method for login. |
| disable | Disables the specified authentication method for login. |
| local | Specifies a local password to determine if you have access permission to the switch. |
| attempt count | Specifies the number of login attempts before initiating an error; valid values are 0, from 3 to 10, and 0 to disable. |
| lockout time | Specifies the lockout timeout; valid values are from 30 to 43200 seconds, and 0 to disable. |

Defaults 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

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

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

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

| Syntax Description | | |
|-----------------------|---|--|
| enable | Enables the specified authorization method for commands. | |
| config | Permits authorization for configuration commands only. | |
| enable | Permits authorization for enable mode commands only. | |
| all | Permits authorization for all commands. | |
| <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 | Disables authorization of command events. | |
| console | (Optional) Specifies the authorization method for console sessions. | |
| telnet | (Optional) Specifies the authorization method for Telnet sessions. | |
| both | (Optional) Specifies 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

To enable authorization of privileged mode sessions on the switch, use the **set authorization enable** command.

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

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

| Syntax Description | enable | Enables the specified authorization method. |
|--------------------|-----------------------|---|
| | <i>option</i> | Switch response to an authorization request; valid values are tacacs+ , if-authenticated , and none . See 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 | Disables the authorization method. |
| | console | (Optional) Specifies the authorization method for console sessions. |
| | telnet | (Optional) Specifies the authorization method for Telnet sessions. |
| | both | (Optional) Specifies 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

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

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

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

| Syntax Description | enable | Enables the specified authorization method. |
|--------------------|-----------------------|---|
| | <i>option</i> | Switch response to an authorization request; valid values are tacacs+ , if-authenticated , and none . See 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 | Disables authorization method. |
| | console | (Optional) Specifies the authorization method for console sessions. |
| | telnet | (Optional) Specifies the authorization method for Telnet sessions. |
| | both | (Optional) Specifies 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 mode) session events:

```
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 autoshut

To enable or disable automatic module shutdown, use the **set autoshut** command.

```
set autoshut {frequency num}
```

```
set autoshut {period minutes}
```

Syntax Description

| | |
|------------------------------|---|
| frequency <i>num</i> | Sets the number of times that the module can reset itself before shutting down; valid values are from 1 to 255 times. |
| period <i>minutes</i> | Sets the time period in which the number of resets must occur; valid values are from 0 to 255 minutes. See the “Usage Guidelines” section for more information. |

Defaults

The defaults are as follows:

- *num* is three times.
- *minutes* is two minutes.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can shut down a module manually using the **set module disable** or the **set module power down** commands.

After the module shuts down, you must reenable the module manually.

You must configure these two parameters before an automatic shutdown can occur:

- Frequency—Allows you to specify the threshold value for an automatic module shutdown. When the number of resets reaches the value that is assigned to this option, the Ethernet module can perform an automatic shutdown.
- Period—Allows you to specify the time period in which the number of resets must occur (as configured with the **frequency** keyword). The period is measured from one these conditions:
 - When the switch first comes up
 - When the supervisor engine performs a switchover
 - When the Ethernet module is powered up
 - When the autoshut counters are cleared on the module



Note If you set the **period** argument to **0**, the module shuts down when it crosses the frequency threshold, regardless of the period of time it took to reach that threshold.

When the frequency threshold is reached and occurs within the defined period, the Ethernet module automatically shuts down. The following is an example of the syslog message that displays:

```
%SYS-5-MOD_AUTOSHUT: Module 2 shutdown automatically, reset 4 times in last 5 minutes due to inband failure
```

When the frequency threshold is reached and occurs outside the defined period, the module does not automatically shut down. The following is an example of the syslog message that displays:

```
%SYS-4-MOD_AUTOSHUT_SLOW:Module 1 reset frequency exceeded threshold but over 46 mins. Hence NOT powering down module
```

The run-time variable states for Ethernet modules do not synchronize with the standby supervisor engine. The output of the **show autoshut** command on a standby supervisor engine does not track with the number of resets or the reasons for the resets. If the module is powered down by the **set autoshut** command, the output stays the same.

You do not have to enable automatic module shutdown in order to track the number of resets. Resets are tracked even if you do not enable automatic module shutdown.

The runtime counters are cleared only for these conditions:

- When you enter the **clear autoshut** command
- When the switch resets
- At module power up
- At supervisor engine switchover

Examples

This example shows how to set the threshold number of times that the specified module can reset itself:

```
Console> (enable) set autoshut frequency 4  
Console> (enable)
```

This example shows how to set the period (in minutes) over which the frequency is valid:

```
Console> (enable) set autoshut period 3  
Console> (enable)
```

Related Commands

[clear autoshut](#)
[set module autoshut](#)
[show autoshut](#)

set banner lcd

To configure the Catalyst 6500 series Switch Fabric Module (SFM) LCD user banner, use the **set banner lcd** command.

```
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 user banner cannot contain more than 801 characters, including delimiting characters and tabs. Tabs display as eight characters but use only one character of memory.

After you configure the user banner, it is sent to all Catalyst 6500 series Switch Fabric Modules in the switch.

The Switch Fabric Module front panel has a 2 line by 20 character LCD display. To see the LCD user banner, enter the SELECT button on the front panel and scroll to the USER CONFIGURATION option. Select the NEXT button to see the user banner.

To clear the LCD user banner, use the **set banner lcd cc** command.

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

```
Console> (enable) set banner lcd &HelloWorld!&
LCD banner set
Console> (enable)
```

Related Commands

- [set banner motd](#)
- [set banner telnet](#)
- [show banner](#)

set banner motd

To program an MOTD banner to appear before session login, use the **set banner motd** command.

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

Syntax Description

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

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The MOTD 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 banner lcd](#)
[set banner telnet](#)
[show banner](#)

set banner telnet

To display or suppress the “Cisco Systems Console” Telnet banner message, use the **set banner telnet** command.

set banner telnet {enable | disable}

| Syntax Description | enable | Displays the Telnet banner. |
|--------------------|---------|-------------------------------|
| | disable | Suppresses the Telnet banner. |

Defaults The “Cisco Systems Console” Telnet banner message is enabled.

Command Types Switch.

Command Modes Privileged.

Examples This example shows how to display the Telnet banner message:

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

This example shows how to suppress the Telnet banner message:

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

Related Commands [set banner lcd](#)
[set banner motd](#)
[show banner](#)

set boot auto-config

To specify one or more configuration files to use to configure the switch at bootup, use the **set boot auto-config** command. 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

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

```
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 | Sets the 16-bit configuration register value. |
| mod | (Optional) Module number of the supervisor engine containing the Flash device. |
| baud 1200 2400 4800 9600 19200 38400 | Specifies the console baud rate. |
| ignore-config | Sets the ignore-config feature. |
| enable | Enables the specified feature. |
| disable | Disables the specified feature. |
| boot | Specifies the boot image to use on the next restart. |
| rommon | Specifies booting from the ROM monitor. |
| bootflash | Specifies booting from the bootflash. |
| system | Specifies 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 with the **set boot config-register boot** command.

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

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

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

[copy](#)
[set boot auto-config](#)
[set boot system flash](#)
[set config acl nvram](#)
[show boot](#)
[show config](#)

set boot config-register auto-config

To configure auto-config file dispensation, use the **set boot config-register auto-config** command.

```
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 | Sets 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 | Sets 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 | Causes the auto-config file to overwrite the NVRAM configuration. | |
| append | Causes the auto-config file to append to the file currently in the NVRAM configuration. | |
| sync enable disable | Enables or disables 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 files 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 redundant supervisor engine. The files 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

To set the Network Analysis Module (NAM) or Intrusion Detection System (IDS) boot environment, use the **set boot device** command.

```
set boot device bootseq [,bootseq] mod [mem-test-full]
```

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. Separate multiple <i>bootseq</i> arguments with a comma. |
| <i>mod</i> | Number of the module containing the Flash device. |
| mem-test-full | (Optional) Specifies a full memory test. |

Defaults

The default is a partial memory test.

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 entering the *bootseq*, use the format *bootdevice*[:*bootdevice-qualifier*] where:

- *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 valid values for **pcmcia** 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 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

To immediately initiate synchronization of the system image between the active and redundant supervisor engine, use the **set boot sync now** command.

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 redundant supervisor engine. The files are kept consistent with what is on the active supervisor engine.

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

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

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

set boot sync timer

To specify an amount of time for the image synchronization timer, use the **set boot sync timer** command.

set boot sync timer *nsec*

| | | |
|---------------------------|-------------|--|
| Syntax Description | <i>nsec</i> | Timer amount in seconds; valid values are from 10 to 7200 seconds. |
|---------------------------|-------------|--|

| | | |
|-----------------|-----------------------------|--|
| Defaults | The default is 120 seconds. | |
|-----------------|-----------------------------|--|

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

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

| | | |
|-------------------------|---|--|
| Usage Guidelines | <p>The set boot sync timer command is used to specify an image synchronization timer amount. After the specified amount of time has passed, a process begins to synchronize the image on the redundant supervisor engine with the image on the active supervisor engine if the images are not identical.</p> | |
|-------------------------|---|--|

If you enter the **set boot sync now** command, the timer is bypassed, and the synchronization process begins immediately.

| | | |
|-----------------|---|--|
| Examples | This example shows how to set the image synchronization timer to 300 seconds: | |
|-----------------|---|--|

```
Console> (enable) set boot sync timer 300
Image auto sync timer set to 300 seconds.
Console> (enable)
```

| | | |
|-------------------------|--|--|
| Related Commands | set boot sync now show boot | |
|-------------------------|--|--|

set boot system flash

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

```
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) Places 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 problem-free 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

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, use the **set cam** command.

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

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

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

```
set cam agingtime vlan agingtime
```

| Syntax Description | | |
|----------------------|--|--|
| dynamic | | Specifies entries are subject to aging. |
| static | | Specifies entries are not subject to aging. |
| permanent | | Specifies 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 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 | | Specifies a traffic filter entry. |
| agingtime | | Sets 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 and are maintained even after a reset.

The *vlan* value 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 a port or ports are trunk ports, you must specify the VLAN.

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

You can specify 256 permanent CAM entries.

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 cam monitor

To monitor the MAC addresses that are learned and stored in the CAM table, to specify the polling interval for the CAM table, or to specify the upper and lower limits for the learning of MAC addresses, use the **set cam monitor** command.

```
set cam monitor {enable | disable} [mod/port | vlan]
```

```
set cam monitor interval time_s
```

```
set cam monitor high-threshold value [action {no-learn | shutdown | warning}]
    {mod/port | vlan}
```

```
set cam monitor low-threshold value [action {no-learn | warning}] {mod/port | vlan}
```

Syntax Description

| | |
|------------------------------------|--|
| enable | Enables CAM monitoring. |
| disable | Disables CAM monitoring. |
| <i>mod/port</i> | (Optional) Number of the module and the ports on the module. |
| <i>vlan</i> | (Optional) VLAN number; valid values are from 1 to 4094. |
| interval <i>time_s</i> | Specifies the polling interval in seconds for monitoring the CAM table; valid values are from 5 to 3600 seconds. |
| high-threshold <i>value</i> | Specifies the upper limit for MAC address learning; valid values are from 5 to 32000. |
| action | (Optional) Specifies the action to be taken when the system exceeds the threshold limits. |
| no-learn | (Optional) Specifies that the system stop learning MAC addresses when the low threshold is exceeded. |
| shutdown | (Optional) Specifies that the system shut down the port or suspend the VLAN if the low threshold is exceeded. |
| warning | (Optional) Specifies that the system display a system message when the low threshold is exceeded. |
| <i>mod/port</i> | Number of the module and the ports on the module. |
| <i>vlan</i> | VLAN number; valid values are from 1 to 4094. |
| low-threshold <i>value</i> | Specifies the lower limit for MAC address learning; valid values are from 5 to 32000. |

Defaults

CAM monitoring is enabled globally.

The polling interval is 5 seconds.

When only an interface is enabled, the low threshold is 500, and the high threshold is 32000. The violation action is a system message at the warning level (level 4).

Command Types

Switch command.

Command Modes Privileged.

Usage Guidelines The **no-learn** violation action prevents MAC address learning on an interface, but it does not delete any extra MAC addresses on the interface.

Examples This example shows how to monitor the MAC addresses that are learned on a specific port and entered into the CAM table:

```
Console> (enable) set cam monitor enable 3/1  
Successfully enabled cam monitor on 3/1  
Console> (enable)
```

This example shows how to disable monitoring of the MAC addresses that are learned on a specific port:

```
Console> (enable) set cam monitor disable 3/1  
Successfully disabled cam monitor on 3/1  
Console> (enable)
```

This example shows how to specify the polling interval for the CAM table:

```
Console> (enable) set cam monitor interval 20  
Cam monitor interval set to 20 sec  
Console> (enable)
```

This example shows how to specify the low threshold for a port and the action to be taken when this threshold is exceeded:

```
Console> (enable) set cam monitor low-threshold 500 action warning 3/1  
Successfully configured cam monitor on 3/1  
Console> (enable)
```

This example shows how to specify the high threshold for a port and the action to be taken when this threshold is exceeded:

```
Console> (enable) set cam monitor high-threshold 28000 action shutdown 3/1  
Successfully configured cam monitor on 3/1  
Console> (enable)
```

Related Commands [clear cam monitor](#)
[show cam monitor](#)

set cam notification

To set CAM notification parameters, use the **set cam notification** command.

set cam notification {enable | disable}

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

set cam notification historysize *log_size*

set cam notification interval *time*

set cam notification move {enable | disable}

set cam notification threshold {enable | disable}

set cam notification threshold limit *percentage*

set cam notification threshold interval *time*

set cam notification move counters {enable | disable}

Syntax Description

| | |
|----------------------|--|
| enable | Enables notification that a change has occurred. |
| disable | Disables notification that a change has occurred. |
| added | Specifies notification when a MAC address is learned. |
| removed | Specifies notification when a MAC address is deleted. |
| <i>mod/port</i> | Number of the module and the port. |
| historysize | Creates a notification history log. |
| <i>log_size</i> | Number of entries in the notification history log; valid sizes are between 0 and 500 entries. |
| interval | Sets the maximum wait time between notifications. |
| <i>time</i> | Time between notification; valid values are greater than or equal to 0 (specified in seconds). |
| move | Specifies MAC move notifications. |
| threshold | Sets parameters for CAM usage monitoring |
| limit | Sets CAM usage monitoring percentage. |
| <i>percentage</i> | Percentage of usage monitoring. |
| move counters | Sets the MAC move counters (MMC). |
| enable | Enables the MAC move counter. |
| disable | Disables the MAC move counter. |

Defaults

By default, notification is disabled.

By default, the interval time is set to 1 second.

By default, the history size is set to 1 entry.

By default, the MAC move counter is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

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

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

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

The severity level of the EARL facility must be set to 4 or higher. If the severity level of the EARL facility is less than 4, the following message is displayed:

```
Please change the logging level for the Earl facility, as the current logging level is set to 2 and Mac Move Counters requires a logging level of at least 4.
```

Use the **set logging level earl** command to change the severity level.

A MAC move counter is a counter that increments every time an existing MAC address moves from a given port to another port in the same VLAN.

In PVLANS, a MAC move counter is a counter that increments every time an existing MAC moves from a given port to another port in different secondary VLANs, but in the same PVLAN.

MAC move counter records a maximum of 1000 MAC moves per VLAN only. Once this maximum has been exceeded, no new moves are recorded on the VLAN. You can enter the **clear cam notification move counters** command to clear the counters.

Because of processing speed differences between CPUs and ASICs, the number of moves reported by the MAC move counter may differ from the actual number of MAC moves.

MAC move counter notification is not supported on EARL 4 and earlier versions.

Examples

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

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

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

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

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

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

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

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

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

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

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

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

This example shows how to enable MAC move notification:

```
Console> (enable) set cam notification move counters enable  
MAC move counters are enabled  
Console> (enable)
```

Related Commands

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

set cam zero-mac-filter

To discard all the ingress traffic globally with the destination MAC address 00-00-00-00-00-00, use the **set cam zero-mac-filter** command.

```
set cam zero-mac-filter { enable | disable }
```

| Syntax Description | enable | Disables EARL zero mac filter. |
|--------------------|---------|--------------------------------|
| | disable | Enables EARL zero mac filter. |

Defaults EARL zero mac filter is disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command works only with the Supervisor 720 and Supw supervisor cards. The zero mac filter and ethernet-cfm feature (except for the 6748-GE-TX, 6748-SFP, 6704-10GE, and 6724-SFP) are mutually exclusive.

Examples This example shows how to enable the EARL zero mac filter globally on the switch:

```
Console> (enable) set cam zero-mac-filter enable
Earl zero-mac-filter enabled.
Console> (enable)
```

This example shows how to disable the EARL zero mac filter globally on the switch:

```
Console> (enable) set cam zero-mac-filter disable
Earl zero-mac-filter disabled.
Console> (enable)
```

Related Commands [show cam zero-mac-filter](#)

set cdp

To enable, disable, or configure Cisco Discovery Protocol (CDP) features globally on all ports or on specified ports, use the **set cdp** command.

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 | Enables the CDP feature. |
| disable | Disables the CDP feature. |
| <i>mod/ports..</i> | Number of the module and the ports on the module. |
| interval | Specifies 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 | Specifies the global Time-To-Live (TTL) value. |
| <i>holdtime</i> | Number of seconds for the global TTL value; valid values are from 10 to 255 seconds. |
| version v1 v2 | Specifies the CDP version number. |
| format device-id | Sets the format of the device ID type-length value (TLV). |
| mac-address | Specifies that the device ID TLV carry the MAC address of the sending device in ASCII, in canonical format. |
| other | Specifies that the device's hardware serial number concatenated with the device name between parentheses. |

Defaults

The default system configuration has CDP enabled. The message interval is set to 60 seconds for every port; the default TTL value has the message interval globally set to 180 seconds. The default CDP version is version 2.

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/ports...* value 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 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 TTL 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 channelprotocol

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

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

| Syntax Description | | |
|--------------------|-------------|-----------------------|
| | pagp | Specifies PAgP. |
| | lACP | Specifies LACP. |
| | <i>mod</i> | Number of the module. |

Defaults The default for the channel protocol is PAgP.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines LACP is supported on all Ethernet interfaces.

PAgP and LACP manage channels differently. When all the ports in a channel get disabled, PAgP removes them from its internal channels list; **show** commands do not display the channel. With LACP, when all the ports in a channel get disabled, LACP does not remove the channel; **show** commands continue to display the channel even though all its ports are down. To determine if a channel is actively sending and receiving traffic with LACP, use the **show port** command to see if the link is up or down. This **set channelprotocol lACP** option changes the channel state to passive. The change of channel from **off** (before lACP) to **passive** (after lACP) is the expected behavior.

LACP does not support half-duplex links. If a port is in active/passive mode and becomes half duplex, the port is suspended (and a syslog message is generated). The port is shown as “connected” using the **show port** command and as “not connected” using the **show spantree** command. This discrepancy is because the port is physically connected but never joined spanning tree. To get the port to join spanning tree, either set the duplex to full or set the channel mode to off for that port.

For more information about PAgP and LACP, refer to the “Configuring EtherChannel” chapter of the *Catalyst 6500 Series Switch Software Configuration Guide*.

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

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

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

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

Related Commands

```
clear lacp-channel statistics
set lacp-channel system-priority
set port lacp-channel
set spantree channelcost
set spantree channelvlancost
show channelprotocol
show lacp-channel
```

set channel vlancost

To set the channel VLAN cost, use the **set channel vlancost** command.

```
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 6500 Series Switch Software Configuration Guide* for more information.



Note

With software releases 6.2(1) and earlier, the 6- and 9-slot Catalyst 6500 series 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

To copy the current committed ACL configuration from DRAM back into NVRAM, use the **set config acl nvram** command.

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

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

set config checkpoint

To create a checkpoint configuration file, use the **set config checkpoint** command.

```
set config checkpoint [name name] [device device]
```

| Syntax Description | |
|-----------------------------|--|
| name <i>name</i> | (Optional) Names the checkpoint configuration file. |
| device <i>device</i> | (Optional) Specifies device on which the checkpoint configuration file is saved. |

Defaults

The default name that the switch automatically generates is in the format CKPi_MMDDYYHHMM, where “i” represents a checkpoint number.

The file is stored on the currently specified default device.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines

A configuration checkpoint file is identified by a name that you specify when you create the file. The configuration checkpoint filename can be no more than 15 characters. If you do not specify a name, the system generates one. The system-generated name is in the format CKPi_MMDDYYHHMM, where “i” represents a checkpoint number.

The checkpoint file is stored either on the bootflash or on slotX/diskX. If you do not specify a device, the file is stored on the current default device.

The configuration checkpoint file is stored as a text file that can be read and edited. We strongly advise that you do not edit the file.

You can create a maximum of five configuration checkpoint files on a system.

The checkpoint configuration is stored in the NVRAM. The configuration is not cleared when you enter the **clear config all** command. To clear all checkpoint configuration files or a particular configuration checkpoint file, use the **clear config checkpoint** command.

This feature is supported on systems with redundant supervisor engines. The checkpoint configuration and its associated files are synchronized to the redundant supervisor engine.

Use the **set config rollback** command to roll back the current switch configuration file to a configuration checkpoint file.

Examples This example shows how to create a system-generated configuration checkpoint file:

```
Console> (enable) set config checkpoint
Configuration checkpoint CKP0_0722040712 creation successful.
Console> (enable)
```

This example shows how to specify a name and device for a configuration checkpoint file:

```
Console> (enable) set config checkpoint name SARAH_07122002 device bootflash:  
Configuration checkpoint SARAH_07122002 creation successful.  
Console> (enable)
```

Related Commands

[clear config checkpoint](#)
[set config rollback](#)
[show config checkpoints](#)

set config mode

To change the configuration mode from a binary model to a text model or to automatically save the system configuration in text mode in NVRAM, use the **set config mode** command.

set config mode binary

set config mode text { *nvr*am | *device:file-id* }

set config mode text auto-save { *enable* | *disable* }

set config mode text auto-save interval *mins*

| Syntax | Description |
|-----------------------|--|
| binary | Sets the system configuration mode to a binary model. |
| text | Sets the system configuration mode to a text model. |
| nvr am | Specifies 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. |
| auto-save | Specifies saving the text configuration in NVRAM automatically. |
| enable | Enables saving the text configuration in NVRAM automatically. |
| disable | Disables saving the text configuration in NVRAM automatically. |
| interval | Sets the time interval between occurrences of saving the text configuration in NVRAM; see the “Usage Guidelines” section for more information. |
| <i>mins</i> | (Optional) Number of minutes between occurrences of saving the text configuration in NVRAM; valid values are from 1 minute to 35000 minutes (approximately 25 days). |

Defaults

The default setting of this command is binary. The configuration is saved in NVRAM.

The number of minutes between occurrences of saving the text configuration in NVRAM is 30 minutes.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can specify the time interval between occurrences of saving the text configuration in NVRAM even if the system is in binary mode. If you do not specify the number of minutes after entering the **interval** keyword, the interval is set to the default of 30 minutes.

The text configuration is not saved automatically in NVRAM unless the auto-save feature is enabled. To enable the auto-save feature, you must first set the system configuration mode to text and configure the system to save the text configuration in NVRAM. If the system configuration mode is set to a binary model, you cannot enable the auto-save feature.

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)
```

This example shows how to enable the auto-save feature when the configuration is set to text mode and the system is configured to save the text configuration in NVRAM:

```
Console> (enable) set config mode text auto-save enable
auto-save feature has been enabled
auto-save feature has started
Please do a write mem manually if you plan to reboot the switch or any card before first
expiry of the timer
Console> (enable)
```

This example shows the message that is displayed if you attempt to enable the auto-save feature when the configuration is not set to text mode and the system is not configured to save the text configuration in NVRAM:

```
Console> (enable) set config mode text auto-save enable
auto-save cannot be enabled unless config mode is set to text and config file is stored in
nvram.
Use the 'set config mode text nvram' command to enable automatic saving of the system
configuration to nvram
Console> (enable)
```

This example shows how to set the interval between saves to 2880 minutes:

```
Console> (enable) set config mode text auto-save interval 2880
auto-save interval set to 2880 minutes
Console> (enable)
```

This example shows how to set the interval between saves to the default setting of 30 minutes:

```
Console> (enable) set config mode text auto-save interval
auto-save interval set to 30 minutes
Console> (enable)
```

Related Commands

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

set config rollback

To roll the current configuration file back to a checkpoint configuration file, use the **set config rollback** command.

set config rollback *name*

Syntax Description

| | |
|-------------|------------------------------------|
| <i>name</i> | Configuration checkpoint filename. |
|-------------|------------------------------------|

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can roll back the current switch configuration file to a previously saved configuration file in the event that the current file produces undesirable system results. You can roll back to any of the saved configuration checkpoint files in any order. Because they are generated using a complete configuration, they are independent of each other.

Use the **set config checkpoint** command to create configuration checkpoint files. Use the **show config checkpoints** command to display configuration checkpoint filenames.

Related Commands

clear config checkpoint
set config checkpoint
show config checkpoints

set cops

To configure COPS functionality, use the **set cops** command.

```
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 | Sets 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) Specifies the primary server. |
| diff-serv | (Optional) Sets the COPS server for differentiated services. |
| rsvp | (Optional) Sets the COPS server for RSVP+. |
| domain-name <i>domain_name</i> | Specifies the domain name of the switch. |
| retry-interval | Specifies 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 policy decision point (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 critical recovery delay

To configure critical recovery delay, use the **set critical-recovery-delay** command.

```
set [dot1x | mac-auth-bypass | eou | web-auth] critical-recovery-delay time
```

| Syntax Description | |
|---|--|
| dot1x | (Optional) Specifies critical recovery delay for dot1x. |
| mac-auth-bypass | (Optional) Specifies critical recovery delay for mac-auth-bypass. |
| eou | (Optional) Specifies critical recovery delay for eou. |
| web-auth | (Optional) Specifies critical recovery delay for web-auth. |
| critical-recovery-delay <i>time</i> | Specifies the time delay before critical recovery is initiated. Value can be set for 1–10000 ms. |

Defaults The default time in milliseconds is 0.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines Use this command to set critical recovery delay for each authentication feature (dot1x, mac-auth-bypass, eou, and web-auth). Critical recovery delay is disabled by default (set to 0). Set the critical recovery to 1–10000 milliseconds. When the RADIUS server is not available for authentication, the ports enabled with the critical recovery delay feature will be moved to critical state. If the RADIUS server comes back online and if the RADIUS auto-initialization feature is enabled, then the ports which were moved to a critical state are initialized. The ports are initialized after the critical recovery delay period that you configured using this command.

Examples This example shows how to configure critical recovery delay using dot1x authentication with a delay of 50 ms:

```
Console> (enable) set dot1x critical-recovery-delay 50
Dot1x critical recovery delay set to 50 milliseconds.
Console> (enable)
```