

set spantree priority

To set the bridge priority for a VLAN or an instance when PVST+ or MISTP is running, use the **set spantree priority** command.

set spantree priority *bridge_priority* *vlan*s

set spantree priority *bridge_priority* **mistp-instance** *instances*

set spantree priority *bridge_priority* **mst** *instances*

Syntax Description		
	<i>bridge_priority</i>	Number representing the priority of the bridge; see the “Usage Guidelines” section for valid values.
	<i>vlan</i> s	Number of the VLAN; valid values are from 1 to 4094.
	mistp-instance <i>instances</i>	Specifies the instance numbers; valid values are from 1 to 16.
	mst <i>instances</i>	Specifies the MST instance numbers; valid values are from 1 to 15.

Defaults The default is the bridge priority is set to 32768.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines If MISTP or the MAC reduction feature is enabled, valid *bridge_priority* values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440, with 0 indicating high priority and 61440, low priority.

If MISTP or the MAC reduction feature is disabled, valid *bridge_priority* values are from 0 to 65535.

If you enable MISTP, you cannot set the VLAN bridge priority.

If you enable PVST+, you cannot set the instance priority.

If you try to set instance priority with PVST+ enabled, this message is displayed:

```
This command is only valid when STP is in MISTP or MISTP-PVST+ mode.
```

Examples This example shows how to set the bridge priority of instance 3:

```
Console> (enable) set spantree priority 14 mistp-instance 3
Instance 3 bridge priority set to 14.
Instance 3 does not exist.
Your configuration has been saved to NVRAM only.
Console> (enable)
```

This example shows how to set the bridge priority for MST instance 0:

```
Console> (enable) set spantree priority 28672 mst 0  
MST Spantree 0 bridge priority set to 28672.  
Console> (enable)
```

This example shows how to set the bridge priority for multiple MST instances:

```
Console> (enable) set spantree priority 28672 mst 0-4  
MST Spantrees 0-4 bridge priority set to 28672.  
Console> (enable)
```

Related Commands [show spantree](#)

set spantree root

To set the primary or secondary root for specific VLANs, all VLANs of the switch, or an instance, use the **set spantree root** command.

```
set spantree root [secondary] [vlans] [dia network_diameter] [hello hello_time]
```

```
set spantree root [secondary] mistp-instance instance [dia network_diameter]  
[hello hello_time]
```

```
set spantree root [secondary] mst instance [dia network_diameter] [hello hello_time]
```

Syntax Description	
secondary	(Optional) Designates this switch as a secondary root, should the primary root fail.
<i>vlan</i> s	(Optional) Number of the VLAN; valid values are from 1 to 4094.
dia <i>network_diameter</i>	(Optional) Specifies the maximum number of bridges between any two points of end stations; valid values are from 1 through 7.
hello <i>hello_time</i>	(Optional) Specifies in seconds, the duration between the generation of configuration messages by the root switch.
mistp-instance <i>instance</i>	Specifies the instance number; valid values are from 0 to 4094.
mst <i>instance</i>	Specifies an MST instance; valid values are from 0 to 4094.

Defaults

If you do not specify the **secondary** keyword, the default is to make the switch the primary root.

The default value of the network diameter is 7.

If you do not specify the *hello_time* value, the current value of *hello_time* is calculated from the network diameter.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a VLAN number, VLAN 1 is assumed.

This command is run on backbone or distribution switches.

You can run the secondary root many times to create backup switches in case of a root failure.

The **set spantree root secondary** bridge priority value is 16384, except when MAC reduction or MISTP are enabled, then the value is 28672.

The **set spantree root** bridge priority value is 16384, except when MAC reduction or MISTP are enabled, then the value is 24576.

This command increases path costs to a value greater than 3000.

If you enable MISTP, you cannot set the VLAN root. If you enable PVST+, you cannot set the instance root.

Examples

This example shows how to set the primary root for a range of VLANs:

```
Console> (enable) set spantree root 1-10 dia 4  
VLANs 1-10 bridge priority set to 8192  
VLANs 1-10 bridge max aging time set to 14 seconds.  
VLANs 1-10 bridge hello time set to 2 seconds.  
VLANs 1-10 bridge forward delay set to 9 seconds.  
Switch is now the root switch for active VLANs 1-6.  
Console> (enable)
```

This example shows how to set the primary root for an instance:

```
Console> (enable) set spantree root mistp-instance 2-4 dia 4  
Instances 2-4 bridge priority set to 8192  
VLIstances 2-4 bridge max aging time set to 14 seconds.  
Instances 2-4 bridge hello time set to 2 seconds.  
Instances 2-4 bridge forward delay set to 9 seconds.  
Switch is now the root switch for active Instances 1-6.  
Console> (enable)
```

This example shows how to set the primary root for MST instance 5:

```
Console> (enable) set spantree root mst 5  
Instance 5 bridge priority set to 24576.  
Instance 5 bridge max aging time set to 16.  
Instance 5 bridge hello time set to 2.  
Instance 5 bridge forward delay set to 15.  
Switch is now the root switch for active Instance 5.  
Console> (enable)
```

This example shows how to set the secondary root for MST instance 0:

```
Console> (enable) set spantree root secondary mst 0  
Instance 0 bridge priority set to 28672.  
Instance 0 bridge max aging time set to 20.  
Instance 0 bridge hello time set to 2.  
Instance 0 bridge forward delay set to 15.  
Console> (enable)
```

This example shows how to set the maximum number of bridges and the hello time of the root for MST instance 0:

```
Console> (enable) set spantree root mst 0 dia 7 hello 2  
Instance 0 bridge priority set to 24576.  
Instance 0 bridge max aging time set to 20.  
Instance 0 bridge hello time set to 2.  
Instance 0 bridge forward delay set to 15.  
Switch is now the root switch for active Instance 0.  
Console> (enable)
```

These examples show that setting the bridge priority to 8192 was not sufficient to make this switch the root. The priority was further reduced to 7192 (100 less than the current root switch) to make this switch the root switch. However, reducing it to this value did not make it the root switch for active VLANs 16 and 17.

```
Console> (enable) set spantree root 11-20.  
VLANs 11-20 bridge priority set to 7192  
VLANs 11-10 bridge max aging time set to 20 seconds.  
VLANs 1-10 bridge hello time set to 2 seconds.
```

set spantree root

```
VLANs 1-10 bridge forward delay set to 13 seconds.  
Switch is now the root switch for active VLANs 11-15,18-20.  
Switch could not become root switch for active VLAN 16-17.  
Console> (enable)
```

```
Console> (enable) set spantree root secondary 22,24 dia 5 hello 1  
VLANs 22,24 bridge priority set to 16384.  
VLANs 22,24 bridge max aging time set to 10 seconds.  
VLANs 22,24 bridge hello time set to 1 second.  
VLANs 22,24 bridge forward delay set to 7 seconds.  
Console> (enable)
```

Related Commands [show spantree](#)

set spantree uplinkfast

To enable fast switchover to alternate ports when the root port fails, use the **set spantree uplinkfast** command. This command applies to a switch, not to a WAN.

```
set spantree uplinkfast {enable | disable} [rate station_update_rate] [all-protocols {off | on}]
```

Syntax Description		
enable		Enables fast switchover.
disable		Disables fast switchover.
rate <i>station_update_rate</i>		(Optional) Specifies the number of multicast packets transmitted per 100 ms when an alternate port is chosen after the root port goes down.
all-protocols		(Optional) Specifies whether or not to generate multicast packets for all protocols (IP, IPX, AppleTalk, and Layer 2 packets).
off		(Optional) Turns off the all-protocols feature.
on		(Optional) Turns on the all-protocols feature.

Defaults

The default *station_update_rate* is 15 packets per 100 milliseconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not available in MST mode.

The **set spantree uplinkfast enable** command has the following results:

- Changes the bridge priority to 49152 for all VLANs (allowed VLANs).
- Increases the path cost and portvlancost of all ports to a value greater than 3000.
- On detecting the failure of a root port, an instant cutover occurs to an alternate port selected by Spanning Tree Protocol.

If you run the **set spantree uplinkfast enable** command on a switch that has this feature already enabled, only the station update rate is updated. The rest of the parameters are not modified.

If you run the **set spantree uplinkfast disable** command on a switch, the UplinkFast feature is disabled but the switch priority and port cost values are not reset to the default settings. To reset the values to the default settings, enter the **clear spantree uplinkfast** command.

The default *station_update_rate* value is 15 packets per 100 milliseconds, which is equivalent to a 1-percent load on a 10-megabit per second Ethernet network. If you specify this value as 0, the generation of these packets is turned off.

You do not have to turn on the all-protocols feature on Catalyst 6500 series switches that have both the UplinkFast and protocol filtering features enabled. Use the all-protocols feature only on Catalyst 6500 series switches that have UplinkFast enabled but do not have protocol filtering; upstream switches in the network use protocol filtering. You must enter the **all-protocols** option to inform the UplinkFast task whether or not to generate multicast packets for all protocols.

Examples

This example shows how to enable spantree UplinkFast and specify the number of multicast packets transmitted to 40 packets per 100 milliseconds:

```
Console> (enable) set spantree uplinkfast enable rate 40
VLANs 1-4094 bridge priority set to 49152.
The port cost and portvlancost of all ports set to above 3000.
Station update rate set to 40 packets/100ms.
uplinkfast all-protocols field set to off.
uplinkfast enabled for bridge.
Console> (enable)
```

This example shows how to disable spantree UplinkFast:

```
Console> (enable) set spantree uplinkfast disable
Uplinkfast disabled for switch.
Use clear spantree uplinkfast to return stp parameters to default.
Console> (enable) clear spantree uplink
This command will cause all portcosts, portvlancosts, and the
bridge priority on all vlans to be set to default.
Do you want to continue (y/n) [n]? y
VLANs 1-1005 bridge priority set to 32768.
The port cost of all bridge ports set to default value.
The portvlancost of all bridge ports set to default value.
uplinkfast disabled for bridge.
Console> (enable)
```

This example shows how to turn on the all-protocols feature:

```
Console> (enable) set spantree uplinkfast enable all-protocols on
uplinkfast update packets enabled for all protocols.
uplinkfast enabled for bridge.
Console> (enable)
```

This example shows how to turn off the all-protocols feature:

```
Console> (enable) set spantree uplinkfast enable all-protocols off
uplinkfast all-protocols field set to off.
uplinkfast already enabled for bridge.
Console> (enable)
```

This example shows the output when instances have been configured:

```
Console> (enable) set spantree uplinkfast enable
Instances 1-15 bridge priority set to 49152.
The port cost and portinstancecost of all ports set to above 3000.
Station update rate set to 15 mpackets/100ms.
uplinkfast all-protocols field set to off.
uplinkfast already enabled for bridge.
Console> (enable)
```

Related Commands

[clear spantree uplinkfast](#)
[show spantree uplinkfast](#)

set ssh mode

To set the Secure Shell (SSH) version, use the **set ssh mode** command.

```
set ssh mode {v1 | v2}
```

Syntax Description	v1	SSH version 1.
	v2	SSH version 2.

Defaults If you do not specify either the **v1** or the **v2** keyword, SSH operates in compatibility mode. See the “Usage Guidelines” for more information about compatibility mode.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The current implementation of Secure Shell encryption supports SSH version 1 and version 2. SSH version 1 supports the DES and 3DES encryption methods, and SSH version 2 supports the 3 DES and AES encryption methods.

Secure shell encryption can be used with RADIUS and TACACS+ authentication. To configure authentication with Secure Shell encryption, use the **telnet** keyword in the **set authentication** commands.

If you enter the **set ssh mode v1** command, the server accepts only SSH version 1 connections. If you enter the **set ssh mode v2** command, the server accepts only SSH version 2 connections.

In compatibility mode, both SSH version 1 connections and version 2 connections are supported. You can return to compatibility mode after operating in version 1 or version 2 mode by entering the **clear ssh mode** command.

Examples This example shows how to configure SSH to accept only version 1 connections:

```
Console> (enable) set ssh mode v1
SSH protocol mode set to SSHv1 Only.
Console> (enable)
```

This example shows how to configure SSH to accept only version 2 connections:

```
Console> (enable) set ssh mode v2
SSH protocol mode set to SSHv2 Only.
Console> (enable)
```

Related Commands

[clear ssh mode](#)
[set authentication enable](#)
[set authentication login](#)
[show ssh](#)

set summertime

To specify whether the system should set the clock ahead one hour during daylight saving time, use the **set summertime** command.

```
set summertime {enable | disable} [zone]
```

```
set summertime recurring [{week} {day} {month} {hh:mm} {week | day | month | hh:mm} [offset]]
```

```
set summertime date {month} {date} {year} {hh:mm} {month | date | year | hh:mm} [offset]
```

Syntax Description

enable	Causes the system to set the clock ahead one hour during daylight saving time.
disable	Prevents the system from setting the clock ahead one hour during daylight saving time.
<i>zone</i>	(Optional) Time zone used by the set summertime command.
recurring	Specifies the summertime dates that recur every year.
<i>week</i>	(Optional) Week of the month (first, second, third, fourth, last, 1...5).
<i>day</i>	(Optional) Day of the week (Sunday, Monday, Tuesday , and so forth).
<i>month</i>	Month of the year (January, February, March , and so forth).
<i>hh:mm</i>	Hours and minutes.
<i>offset</i>	(Optional) Amount of offset in minutes (from 1 to 1440 minutes).
<i>date</i>	Day of the month (from 1 to 31).
<i>year</i>	Number of the year (from 1993 to 2035).

Defaults

By default, the **set summertime** command is disabled. Once enabled, the default for *offset* is 60 minutes, following U.S. standards.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

After you enter the **clear config** command, the dates and times are set to default.

Unless you configure it otherwise, this command advances the clock one hour at 2:00 a.m. on the first Sunday in April and moves back the clock one hour at 2:00 a.m. on the last Sunday in October.

Examples

This example shows how to cause the system to set the clock ahead one hour during daylight saving time:

```
Console> (enable) set summertime enable PDT
Summertime is enabled and set to "PDT".
Console> (enable)
```

This example shows how to prevent the system from setting the clock ahead one hour during daylight saving time:

```
Console> (enable) set summertime disable
Summertime disabled.
Console> (enable)
```

This example shows how to set daylight saving time to the zonename AUS and repeat every year, starting from the third Monday of February at noon and ending at the second Saturday of August at 3:00 p.m. with an offset of 30 minutes:

```
Console> (enable) set summertime AUS recurring 3 Mon Feb 12:00 2 Saturday Aug 15:00 30
Summer time is disabled and set to 'AUS' with offset 30 minutes.
  start: 12:00:00 Sun Feb 13 2000
  end:   14:00:00 Sat Aug 26 2000
  Recurring, starting at 12:00:00 on Sunday of the third week of February and ending
  on Saturday of the fourth week of August.
Console> (enable)
```

This example shows how to set the daylight saving time to start on January 29, 1999 at 2:00 a.m. and end on August 19, 2004 at 3:00 p.m. with an offset of 30 minutes:

```
Console> (enable) set summertime date jan 29 1999 02:00 aug 19 2004 15:00 30
Summertime is disabled and set to ''
Start : Fri Jan 29 1999, 02:00:00
End   : Thu Aug 19 2004, 15:00:00
Offset: 30 minutes
Recurring: no
Console> (enable)
```

This example shows how to set recurring to reset default to US summertime:

```
Console> (enable) set summertime recurring 3 mon feb 4 thurs oct 8:00 500
Command authorization none.
Summertime is enabled and set to ''
Start : Mon Feb 21 2000, 03:00:00
End   : Fri Oct 20 2000, 08:00:00
Offset: 500 minutes (8 hours 20 minutes)
Recurring: yes, starting at 03:00am of third Monday of February and ending on 08:00am of
fourth Thursday of October.
Console> (enable)
```

Related Commands [show summertime](#)

set system baud

To set the console port baud rate, use the **set system baud** command.

```
set system baud rate
```

Syntax Description	<i>rate</i> Baud rate; valid rates are 600, 1200, 2400, 4800, 9600, 19200, and 38400 .
---------------------------	---

Defaults	The default is 9600 baud.
-----------------	---------------------------

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

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

Examples	This example shows how to set the system baud rate to 19200: <pre>Console> (enable) set system baud 19200 System console port baud rate set to 19200. Console> (enable)</pre>
-----------------	---

Related Commands	show system
-------------------------	-----------------------------

set system contact

To identify a contact person for the system, use the **set system contact** command.

```
set system contact [contact_string]
```

Syntax Description

contact_string (Optional) Text string that contains the name of the person to contact for system administration. If you do not specify a contact string, the system contact string is cleared.

Defaults

The default is no system contact is configured.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the system contact string:

```
Console> (enable) set system contact Xena ext.24  
System contact set.  
Console> (enable)
```

Related Commands

[show system](#)

set system core-dump

To enable or disable the core dump feature, use the **set system core-dump** command.

```
set system core-dump { enable | disable }
```

Syntax Description	enable	Disables the core dump feature.
	disable	Enables the core dump feature.

Defaults The default is disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The core dump feature generates a report of images when your system fails due to a software error. The core image is stored in the file system. From this file, you can examine an error condition of a process when it is terminated due to an exception.

The size of the file system depends on the memory card size. The core dump file generated is proportional to the size of the system DRAM. Make sure that you have enough memory available to store the core dump file.

In order to maintain the core dump image, the yield CPU is disabled during the core dump process. You should have a redundant supervisor engine installed to take over normal operations. If the switch has a redundant supervisor engine setup, the redundant supervisor engine takes over automatically before the core dump occurs. The previously active supervisor engine resets itself after the core dump completes.

Examples This example shows how to enable the core dump feature:

```
Console> (enable) set system core-dump enable
(1) In the event of a system crash, this feature will
    cause a core file to be written out.
(2) Core file generation may take up to 20 minutes.
(3) Selected core file is slot0:crash.hz
(4) Please make sure the above device has been installed,
    and ready to use
Core-dump enabled
Console> (enable)
```

This example shows how to disable the core dump feature:

```
Console> (enable) set system core-dump disable
Core-dump disabled
Console> (enable)
```

set system core-file

To specify the core image filename, use the **set system core-file** command.

```
set system core-file {device:[filename]}
```

Syntax Description	device	Device where the core image file resides; valid values are bootflash and slot0 .
	filename	(Optional) Name of the core image file.

Defaults The default *filename* is “crashinfo.”

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines A device name check is performed when you enter the **set system core-file** command. If a valid device name is not found, an error message displays.

When a core dump occurs, the actual file written out will append the date to the filename in this format: `_{yymmdd}-{hhmmss}`.

Examples This example shows how to use the default core image filename:

```
Console> (enable) set system core-file bootflash:
Attach default filename crashinfo to the device
System core-file set.
Console> (enable)
```

This example shows how to set the core image filename:

```
Console> (enable) set system core-file slot0:abc
System core-file set.
Console> (enable)
```

Related Commands [set system core-dump](#)

set system countrycode

To specify the country where the system is physically located, use the **set system countrycode** command.

set system countrycode *code*

Syntax Description	<i>code</i> Country code; see the “Usage Guidelines” section for format information.
Defaults	The default is US (United States).
Command Types	Switch command.
Command Modes	Privileged.
Usage Guidelines	The country code is a two-letter country code taken from ISO-3166 (for example, VA=Holy See [Vatican City State], VU=Vanuatu, and TF=French Southern Territories).
Examples	This example shows how to set the system country code: <pre>Console> (enable) set system countrycode US Country code is set to US. Console> (enable)</pre>

set system crashinfo

To permit the system to write a crash information file, use the **set system crashinfo** command.

```
set system crashinfo {enable | disable}
```

```
set system crashinfo-file device:filename
```

Syntax Description

enable	Permits the system to write a crash information file.
disable	Prevents the system from writing a crash information file.
crashinfo-file	Sets the crash information file name.
<i>device:filename</i>	Device and crash information file name.

Defaults

The crash information feature is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The crash information file contains extended system information that is captured quickly when the system reloads because of an error condition. Like the crash-dump file, the crash-info file is stored in the file system. The information in the crash information file should be used in addition to the core dump information and does not replace that information. By examining both the crash-info file and core dump file, Cisco TAC can better analyze an error condition.

To clear a system crash information file, enter the **set system crashinfo-file** command with no arguments.

Examples

This example shows how to permit the system to write a crash information file:

```
Console> (enable) set system crashinfo enable
Crashinfo enabled
Console> (enable)
```

This example shows how to specify the device where the crash information file is saved and the name of the file:

```
Console> (enable) set system crashinfo-file slot0:crashinfo
System crashinfo-file set.
Console> (enable)
```

This example shows how to clear a crash information file:

```
Console> (enable) set system crashinfo-file
System crashinfo-file cleared.
Console> (enable)
```

Related Commands [show system](#)

set system crossbar-fallback

To select the action taken when the Switch Fabric Module fails, use the **set system crossbar-fallback** command.

```
set system crossbar-fallback { bus-mode | none }
```

Syntax Description

bus-mode	Fails to the system bus.
none	Does not fail over to the system bus.

Defaults

The default is **bus-mode**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can either have the Switch Fabric Module fail over to the bus or have the switch not fail over at all (in which case, the switch should be down).

This command is supported on systems configured with a Switch Fabric Module and the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Examples

This example shows how to set the Switch Fabric Module to fail over to the system bus:

```
Console> (enable) set system crossbar-fallback bus-mode
System crossbar-fallback set to bus-mode.
Console> (enable)
```

This example shows how to set the Switch Fabric Module to not fail over:

```
Console> (enable) set system crossbar-fallback none
System crossbar-fallback set to none.
Console> (enable)
```

Related Commands

[show fabric channel](#)

set system highavailability

To enable or disable high system availability for the switch, use the **set system highavailability** command.

```
set system highavailability {enable | disable}
```

Syntax Description

enable	Activates system high availability.
disable	Deactivates system high availability.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

High availability provides Layer 2 and Layer 3 protocol redundancy.

If you enable high availability while the redundant supervisor engine is running, the switch checks the version compatibility between the two supervisor engines. If the versions are compatible, database synchronization occurs. When you disable high availability, database synchronization does not occur and protocols restart on the redundant supervisor engine after switchover.

If you disable high availability from the enabled state, synchronization from the active supervisor engine is stopped. On the redundant supervisor engine, current synchronization data is discarded. If you enable high availability from the disabled state, synchronization from the active supervisor engine to the redundant supervisor engine starts (if you have a redundant supervisor engine and its image version is compatible with the active supervisor engine).

Examples

This example shows how to enable high availability:

```
Console> (enable) set system highavailability enable  
System high availability enabled.  
Console> (enable)
```

This example shows how to disable high availability:

```
Console> (enable) set system highavailability disable  
System high availability disabled.  
Console> (enable)
```

Related Commands

[set system highavailability versioning](#)
[show system highavailability](#)

set system highavailability versioning

To enable and disable support for supervisor engine image versioning, use the **set system highavailability versioning** command.

```
set system highavailability versioning {enable | disable}
```

Syntax Description

enable	Activates system high-availability versioning.
disable	Deactivates system high-availability versioning.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The high-availability versioning feature allows the Catalyst 6500 series switch to run different images on the active and redundant supervisor engines. When you enable image versioning, Flash image synchronization (from active to the redundant supervisor engines) does not occur, allowing active and redundant supervisor engines to run different images.



Caution

When you disable image versioning, the active and redundant supervisor engines must run the same image version.

If you disable the image versioning option from the enabled state, no additional action is necessary on the redundant supervisor engine. (The redundant supervisor engine should be running the same image as the active supervisor engine.) If you want to load a different image, you have to restart the redundant supervisor engine.

If you enable the image versioning option from the disabled state and you have a redundant supervisor engine and active supervisor engine running a different image than that of the active supervisor engine, Flash synchronization will copy the active supervisor engine image to the redundant supervisor engine image and then restart it.

If you enable the image versioning option on the active supervisor engine and the redundant supervisor engine is running a different image, the NVRAM synchronization cannot occur because the NVRAM versions are not compatible. If this is the case, after switchover, the old NVRAM configuration on the supervisor engine is used.

Examples

This example shows how to enable high-availability versioning:

```
Console> (enable) set system highavailability versioning enable  
Image versioning enabled.  
Console> (enable)
```

This example shows how to disable high-availability versioning:

```
Console> (enable) set system highavailability versioning disable  
Image versioning disabled.  
Console> (enable)
```

Related Commands

[set system highavailability](#)
[show system highavailability](#)

set system info-log

To log the output of specified show commands to a server for troubleshooting and debugging, use the **set system info-log** command.

set system info-log {*enable* | *disable*}

set system info-log command {*ccommand_stringc*} [*position*]

set system info-log interval *mins*

set system info-log {*tftp* | *ftp* | *rcp username*} *host filename*

Syntax Description		
enable disable		Activates or deactivates system information logging.
command		Logs the specified show command to the server.
c		Delimiting character used to begin and end the show command.
<i>command_string</i>		Show command whose output is logged; valid values are show commands.
<i>position</i>		(Optional) Position of the show command in the system information logging index; valid values are from 1 to 15.
interval		Specifies the amount of time between system information logging events.
<i>mins</i>		Minutes between system information logging events; valid values are from 1 to 35000 minutes (approximately 25 days).
tftp		Copies system information logging output to a TFTP server.
ftp		Copies system information logging output to an FTP server.
rcp		Copies system information logging output to an RCP server.
<i>username</i>		RCP username.
<i>host</i>		IP address or IP alias of the host.
<i>filename</i>		Name of the file.

Defaults

System information logging is disabled.

The interval between system information logging events is 1440 minutes.

System information logging output is copied to a TFTP server, and the filename is sysinfo.

If you do not provide an absolute path for the file, the TFTP directory is tftpboot. For RCP, the directory is the user's home directory.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enter the **show** command whose output is to be logged, you must type a delimiting character with no spaces on either side of the command. You can add only one show command at a time.

You can enter a maximum of 15 show commands for system information logging.

Examples

This example shows how to activate the system information logging feature:

```
Console> (enable) set system info-log enable  
Successfully enabled system information logging.  
Console> (enable)
```

This example shows how to include the output of the **show version** command in the log:

```
Console> (enable) set system info-log command "show version"  
System command was successfully added to the list.  
Console> (enable)
```

This example shows how to list the **show module** command as the third command in the system information logging index:

```
Console> (enable) set system info-log command >show module> 3  
System command was successfully added to the list.  
Console> (enable)
```

This example shows how to save system information logging with a specific filename to a specific TFTP server:

```
Console> (enable) set system info-log tftp 10.5.2.10 sysinfo  
Successfully set the system information logging file to tftp:sysinfo  
Console> (enable)
```

This example shows how to save system information logging with a specific filename to an RCP server:

```
Console> (enable) set system info-log rcp shravan 10.5.2.10 sysinfo  
Successfully set the system information logging file to rcp:sysinfo  
Console> (enable)
```

Related Commands

[clear config](#)
[clear system info-log command](#)
[show system info-log](#)

set system location

To identify the location of the system, use the **set system location** command.

```
set system location [location_string]
```

Syntax Description

location_string (Optional) Text string that indicates where the system is located.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a location string, the system location is cleared.

Examples

This example shows how to set the system location string:

```
Console> (enable) set system location Closet 230 4/F  
System location set.  
Console> (enable)
```

Related Commands

[show system](#)

set system modem

To enable or disable modem control lines on the console port, use the **set system modem** command.

```
set system modem {enable | disable}
```

Syntax Description

enable	Activates modem control lines on the console port.
disable	Deactivates modem control lines on the console port.

Defaults

The default is modem control lines are disabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to disable modem control lines on the console port:

```
Console> (enable) set system modem disable  
Modem control lines disabled on console port.  
Console> (enable)
```

Related Commands

[show system](#)

set system name

To configure a name for the system, use the **set system name** command.

```
set system name [name_string]
```

Syntax Description

name_string (Optional) Text string that identifies the system.

Defaults

The default is no system name is configured.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use the **set system name** command to assign a name to the switch, the switch name is used as the prompt string. However, if you specify a different prompt string using the **set prompt** command, that string is used for the prompt.

If you do not specify a system name, the system name is cleared and a DNS lookup is initiated for a system name. If a name is found, that is the name used; if no name is found, no name is designated.

The system name can be 255 characters long, and the prompt can be 20 characters long. The system name is truncated appropriately when used as a prompt; a greater-than symbol (>) is appended to the truncated system name. If the system name was found from a DNS lookup, it is truncated to remove the domain name.

If the prompt is obtained using the system name, it is updated whenever the system name changes. You can overwrite this prompt any time by setting the prompt manually. Any change in the prompt is reflected in all current open sessions.

If you do not specify a name, the system name is cleared.

Examples

This example shows how to set the system name to Information Systems:

```
Console> (enable) set system name Information Systems  
System name set.  
Console> (enable)
```

Related Commands

[set prompt](#)
[show system](#)

set system profile

To configure a system profile file, use the **set system profile** command.

```
set system profile device:filename
```

```
set system profile {enable | disable} mod_list
```

Syntax Description		
<i>device:filename</i>		Name of the device and the profile filename separated by a colon.
enable		Enables profile file loading on a per-module basis.
disable		Disables profile file loading on a per-module basis.
<i>mod_list</i>		Numbers of the modules on which profile file loading is enabled or disabled; valid values are from 1 to 9, 15, and 16.

Defaults

The default value for the PROFILE_FILE variable is null.

The system profile feature is enabled on each module.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A profile file allows you to have a customized configuration as the designated configuration on the switch. The profile file allows you to load a configuration on the switch either as the default configuration or as a custom configuration that would enable or disable certain features. With the profile files, you can eliminate the features or processes that might pose security risks (for example, disabling CDP or turning off auto-trunking on a port) to your switch.

A profile file that has most of the security risks disabled is also known as a “lockdown” profile. A lockdown profile changes the functionality of the switch from enabling access to preventing access by default. When a lockdown profile is applied, you must manually enable the features that were disabled by the profile file. For a sample lockdown profile, see to the “Working with Configuration Files” chapter of the *Catalyst 6500 Series Software Configuration Guide*.

Follow these guidelines when working with profile files:

- A profile file can be either from internal bootflash or from PCMCIA slots but not from a TFTP server.
- A profile file must be a Catalyst operating system configuration file type that starts with “begin.”
- Keywords that are supported in release 8.4 are ALL_MODULES, ALL_PORTS, ALL_MODULE_PORTS, and ALL_VLANS.
- The ALL_MODULES, ALL_PORTS, and ALL_VLANS keywords can be anywhere in the profile file.

- The ALL_MODULE_PORTS keyword must be within a module section that is explicitly defined, as all module sections are explicitly defined in Catalyst operating system configuration files. If the ALL_MODULE_PORTS keyword is not in a module section, the keyword statement is ignored.
- A profile name in PROFILE_FILE must be fully qualified. You must specify a device name.
- A profile file configuration must be loaded after a text configuration and before an auto-config configuration.

The **set system profile {enable | disable} mod_list** command allows you to enable or disable profile file loading for a specified module.

For more information about system profile files, see to the “Working with Configuration Files” chapter of the *Catalyst 6500 Series Software Configuration Guide*.

Examples

This example shows how to set the name of the device and the profile filename:

```
Console> (enable) set system profile bootflash:test.cfg  
System is set to be configured with profile file bootflash:test.cfg.  
Console> (enable)
```

This example shows how to disable system profile loading on a specified module:

```
Console> (enable) set system profile disable 2  
System profile loading is disabled for module 2.  
Console> (enable)
```

Related Commands

[clear config](#)
[clear system profile](#)
[show system profile](#)

set system supervisor-update

To configure the Erasable Programmable Logic Device (EPLD) upgrade process, use the **set system supervisor-update** command.

```
set system supervisor-update {automatic | disable | force}
```

Syntax Description

automatic	Upgrades an earlier supervisor engine EPLD image at bootup.
force	Upgrades supervisor engine EPLD image regardless of the version label.
disable	Disables automatic updates of supervisor engine EPLD image at bootup.

Defaults

The supervisor engine EPLD upgrade is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you specify the **automatic** keyword, the system checks the version level of the bundled EPLD image and performs the upgrade if the bundled EPLD image version is greater than the existing version.

If you specify the **force** keyword, the system upgrades the existing EPLD image with the bundled EPLD image regardless of the version level. After a forced upgrade, the configuration reverts back to the automatic default setting.

If you specify the **disable** keyword, the automatic EPLD upgrade process is disabled.



Note

Supervisor engine EPLD upgrades are supported only on Supervisor Engine 2. Non-supervisor engine module (switching modules and service modules) EPLD upgrades are supported using Supervisor Engine 1 or Supervisor Engine 2.

The EPLD image for Supervisor Engine 2 is included in the Catalyst supervisor engine software image. The EPLD image for non-supervisor engine modules is provided in a separate downloadable image.

Examples

This example shows how to specify the automatic option for EPLD upgrades:

```
Console> (enable) set system supervisor-update automatic
Down-rev supervisor EPLD's will be re-programmed next reset.
Console> (enable)
```

This example shows how to specify the force option for EPLD upgrades:

```
Console> (enable) set system supervisor-update force
Supervisor EPLD's will synchronize to the image bundle during the next reset.
Console> (enable)
```

This example shows how to disable EPLD upgrades:

```
Console> (enable) set system supervisor-update disable  
Supervisor EPLD update during reset is disabled.  
Console> (enable)
```

Related Commands

[download](#)
[show system supervisor-update](#)
[show version](#)

set system switchmode allow

To configure the switching mode for the system, use the **set system switchmode allow** command.

```
set system switchmode allow {truncated | bus-only}
```

Syntax Description	truncated	Specifies truncated mode; see the “Usage Guidelines” section for additional information.
	bus-only	Forces the system to be in flow-through mode.

Defaults The default is truncated.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines When you install a Switch Fabric Module in a Catalyst 6500 series switch, the traffic is forwarded to and from modules in one of the following modes:

- Flow-through mode—In this mode, data passes between the local bus and the supervisor engine bus. This mode is used for traffic to or from nonfabric-enabled modules.
- Truncated mode—In this mode, only the truncated data (the first 64 bytes of the frame) is sent over the switch fabric channel if both the destination and the source modules are fabric-enabled modules. If either the source or destination is not a fabric-enabled module, the data goes through the switch fabric channel and the data bus. The Switch Fabric Module does not get involved when traffic is forwarded between nonfabric-enabled modules.
- Compact mode—In this mode, a compact version of the DBus header is forwarded over the switch fabric channel, delivering the best possible switching rate. Nonfabric-enabled modules do not support the compact mode and will generate CRC errors if they receive frames in compact mode. This mode is only used if nonfabric-enabled modules are not installed in the chassis.

If you enter the **truncated** keyword and your system does not contain nonfabric-enabled modules, the system is placed in compact mode.

If two or more fabric-enabled modules are installed in your system with a nonfabric-enabled module, forwarding between these modules occurs in truncated mode.

If there is a combination of a Supervisor Engine 720 with switch fabric capability and nonfabric-enabled modules in the chassis, the **bus-only** keyword is not permitted. The system stays in truncated mode.

Examples This example shows how to set the switching mode to truncated:

```
Console> (enable) set system switchmode allow truncated
System switchmode allow set to truncated.
Console> (enable)
```

This example shows how to set the switching mode to bus-only:

```
Console> (enable) set system switchmode allow bus-only  
System switchmode allow set to bus-only.  
Console> (enable)
```

Related Commands

[show system switchmode](#)

set system syslog-dump

To write system messages in the syslog buffer to a flash file before the system fails, use the **set system syslog-dump** command.

```
set system syslog-dump {enable | disable}
```

Syntax Description	enable	Disables the syslog dump feature.
	disable	Disables the syslog dump feature.

Defaults The syslog dump feature is disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines If the system fails, a file containing the system messages in the syslog buffer (as displayed when entering the **show logging buffer** command) is produced.

Enter the **set system syslog-file** command to specify the flash device and syslog filename for the syslog dump when the system fails.

Examples This example shows how to enable the syslog dump feature:

```
Console> (enable) set system syslog-dump enable
(1) In the event of a system crash, this feature will
    cause a syslog file to be written out.
(2) Selected syslog file is slot0:sysloginfo
(3) Please make sure the above device has been installed,
    and ready to use.
Syslog-dump enabled
Console> (enable)
```

This example shows how to disable the syslog dump feature:

```
Console> (enable) set system syslog-dump disable
Syslog-dump disabled
Console> (enable)
```

Related Commands [set system syslog-file](#)
[show system](#)

set system syslog-file

To specify the flash device and filename for the syslog dump when the system fails, use the **set system syslog-file** command.

```
set system syslog-file [device:[filename]]
```

Syntax Description

device: (Optional) Name of the flash device.

filename (Optional) Name of the file for the syslog dump.

Defaults

The flash device is slot0.

The filename is sysloginfo.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Enter the **set system syslog-dump** command to enable or disable the syslog dump feature. You can change the flash device and the filename when the syslog dump feature is enabled or disabled.

If you only specify the flash device, the filename is automatically set to sysloginfo. If you do not specify the device or the filename, the previous filename for the syslog dump is cleared, and the default flash device and filename (slot0:sysloginfo) are used.

Examples

This example shows how to set the flash device for the syslog dump feature:

```
Console> (enable) set system syslog-file bootflash:
Default filename sysloginfo added to the device bootflash:
System syslog-file set.
Console> (enable)
```

This example shows how to set the flash device and the filename:

```
Console> (enable) set system syslog-file bootflash:sysmsgsl
System syslog-file set.
Console> (enable)
```

This example shows how to restore the flash device and the filename to the default settings:

```
Console> (enable) set system syslog-file
System syslog-file set to the default file.
Console> (enable)
```

Related Commands

[set system syslog-dump](#)
[show system](#)

set tacacs attempts

To configure the maximum number of login attempts allowed to the TACACS+ server, use the **set tacacs attempts** command.

set tacacs attempts *count*

Syntax Description	<i>count</i> Number of login attempts allowed; valid values are from 1 to 10.
---------------------------	---

Defaults	The default is three attempts.
-----------------	--------------------------------

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

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

Examples	This example shows how to configure the TACACS+ server to allow a maximum of six login attempts:
-----------------	--

```
Console> (enable) set tacacs attempts 6  
Tacacs number of attempts set to 6.  
Console> (enable)
```

Related Commands	show tacacs
-------------------------	-----------------------------

set tacacs directedrequest

To enable or disable the TACACS+ directed-request option, use the **set tacacs directedrequest** command. When enabled, you can direct a request to any of the configured TACACS+ servers and only the username is sent to the specified server.

set tacacs directedrequest {enable | disable}

Syntax Description	enable	Sends the portion of the address before the @ sign (the username) to the host specified after the @ sign.
	disable	Sends the entire address string to the default TACACS+ server.

Defaults The default is the TACACS+ directed-request option is disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines When you enable TACACS+ directed-request, you must specify a configured TACACS+ server after the @ sign. If the specified host name does not match the IP address of a configured TACACS+ server, the request is rejected. When TACACS+ directed-request is disabled, the Catalyst 6500 series switch queries the list of servers beginning with the first server in the list and then sends the entire string, accepting the first response from the server. This command is useful for sites that have developed their own TACACS+ server software to parse the entire address string and make decisions based on the contents of the string.

Examples This example shows how to enable the **tacacs directedrequest** option:

```
Console> (enable) set tacacs directedrequest enable
Tacacs direct request has been enabled.
Console> (enable)
```

Related Commands [show tacacs](#)

set tacacs key

To set the key for TACACS+ authentication and encryption, use the **set tacacs key** command.

```
set tacacs key key
```

Syntax Description	<i>key</i> Printable ASCII characters used for authentication and encryption.
Defaults	The default value of <i>key</i> is null.
Command Types	Switch command.
Command Modes	Privileged.
Usage Guidelines	<p>The key must be the same key used on the TACACS+ server. All leading spaces are ignored. Spaces within the key and at the end of the key are included. Double quotation marks are not required, even if there are spaces between words in the key, unless the quotation marks themselves are part of the key. The key can consist of any printable ASCII characters except the tab character.</p> <p>The key length must be less than 100 characters long.</p>
Examples	<p>This example shows how to set the authentication and encryption key:</p> <pre>Console> (enable) set tacacs key Who Goes There The tacacs key has been set to Who Goes There. Console> (enable)</pre>
Related Commands	clear spantree uplinkfast show tacacs

set tacacs server

To define a TACACS+ server, use the **set tacacs server** command.

```
set tacacs server ip_addr [primary]
```

Syntax Description	<i>ip_addr</i>	IP address of the server on which the TACACS+ server resides.
	primary	(Optional) Designates the specified server as the primary TACACS+ server.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines You can configure a maximum of three servers. The primary server, if configured, is contacted first. If no primary server is configured, the first server configured becomes the primary server.

Examples This example shows how to configure the server on which the TACACS+ server resides and to designate it as the primary server:

```
Console> (enable) set tacacs server 170.1.2.20 primary
170.1.2.20 added to TACACS server table as primary server.
Console> (enable)
```

Related Commands [clear tacacs server](#)
[show tacacs](#)

set tacacs timeout

To set the response timeout interval for the TACACS+ server daemon, use the **set tacacs timeout** command. The TACACS+ server must respond to a TACACS+ authentication request before this interval expires or the next configured server is queried.

set tacacs timeout *seconds*

Syntax Description	<i>seconds</i> Timeout response interval in seconds; valid values are from 1 to 255.
Defaults	The default is 5 seconds.
Command Types	Switch command.
Command Modes	Privileged.
Examples	This example shows how to set the response timeout interval for the TACACS+ server to 8 seconds: <pre>Console> (enable) set tacacs timeout 8 Tacacs timeout set to 8 seconds. Console> (enable)</pre>
Related Commands	show tacacs

set test diagfail-action

To set the action that the supervisor engine takes when a diagnostics test fails, use the **set test diagfail-action** command.

```
set test diagfail-action { offline | ignore }
```

Syntax Description

offline	Sets the supervisor engine to stay offline after a diagnostics test failure.
ignore	Sets the supervisor engine to ignore the diagnostics test failure and to boot up.

Defaults

The supervisor engine stays offline.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Enter the **show test diagfail-action** command to display the action that the supervisor engine takes after a test failure.

Examples

This example shows how to set the supervisor engine to stay offline:

```
Console> (enable) set test diagfail-action offline
Diagnostic failure action for SUP set to offline.
Console> (enable)
```

This example shows how to set the supervisor engine to ignore the diagnostics test failure and to boot up:

```
Console> (enable) set test diagfail-action ignore
Diagnostic failure action for SUP set to ignore.
Console> (enable)
```

Related Commands

[show test](#)

set test diaglevel

To set the diagnostic level, use the **set test diaglevel** command.

```
set test diaglevel { complete | minimal | bypass }
```

Syntax Description	complete	minimal	bypass
	Specifies complete diagnostics.	Specifies minimal diagnostics.	Specifies bypass diagnostics.

Defaults The default is **minimal**. See the “Usage Guidelines” section for more information about the three diagnostic levels.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines Setting the diagnostic level determines the level of testing that occurs when the system or module is reset. The three levels are as follows:

- **complete**—This level runs all tests.
- **minimal**—This level runs only EARL tests for the supervisor engine and loopback tests for all ports in the system.
- **bypass**—This level skips all tests.



Note

Although the default is **minimal**, we recommend that you set the diagnostic level at **complete**. We strongly recommend that you do not set the diagnostic level to **bypass**.

Examples This example shows how to set the diagnostic level to complete:

```
Console> (enable) set test diaglevel complete
Diagnostic level set to complete.
Console> (enable)
```

This example shows how to set the diagnostic level to bypass:

```
Console> (enable) set test diaglevel bypass
Diagnostic level set to bypass.
Console> (enable)
```

Related Commands [show test](#)

set time

To change the time of day on the system clock, use the **set time** command.

```
set time [day_of_week] [mm/dd/yy] [hh:mm:ss]
```

Syntax Description

day_of_week (Optional) Day of the week.

mm/dd/yyyy (Optional) Month, day, and year.

hh:mm:ss (Optional) Current time in 24-hour format.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the system clock to Sunday, October 31, 2004, 7:50 a.m:

```
Console> (enable) set time sun 10/31/2004 7:50
Sun Oct 31 2004, 07:50:00
Console> (enable)
```

Related Commands

[show time](#)

set timezone

To set the time zone for the system, use the **set timezone** command.

```
set timezone [zone_name] [hours [minutes]]
```

Syntax Description	<i>zone_name</i> (Optional) Name of the time zone to be displayed.
	<i>hours</i> (Optional) Number of hours offset from UTC.
	<i>minutes</i> (Optional) Number of minutes offset from UTC. If the specified <i>hours</i> value is a negative number, then the <i>minutes</i> value is assumed to be negative as well.

Defaults The default is the time zone is set to UTC.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The **set timezone** command is effective only when Network Time Protocol (NTP) is running. If you set the time explicitly and NTP is disengaged, the **set timezone** command has no effect. If you have enabled NTP and have not entered the **set timezone** command, the Catalyst 6500 series switch displays UTC by default.

Examples This example shows how to set the time zone to pacific standard time with an offset of minus 8 hours from UTC:

```
Console> (enable) set timezone PST -8  
Timezone set to "PST", offset from UTC is -8 hours.  
Console> (enable)
```

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

set traffic monitor

To configure the threshold at which a high-traffic log will be generated, use the **set traffic monitor** command.

set traffic monitor *threshold*

Syntax Description	<i>threshold</i> 1 to 100 percent.
---------------------------	------------------------------------

Defaults	The threshold is set to 100 percent; no high-traffic log is created.
-----------------	--

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

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

Usage Guidelines	If backplane traffic exceeds the threshold configured by the set traffic monitor command, a high-traffic log is created. If the threshold is set to 100 percent, no high-traffic system warning is generated.
-------------------------	--

Examples	This example shows how to set the high-traffic threshold to 80 percent:
-----------------	---

```
Console> (enable) set traffic monitor 80  
Traffic monitoring threshold set to 80%.  
Console> (enable)
```

Related Commands	show traffic
-------------------------	------------------------------

set transceiver-monitoring

To enable or disable transceiver monitoring, use the **set transceiver-monitoring** command.

```
set transceiver-monitoring {enable | disable | {interval interval}}
```

Syntax Description		
	enable	Enables transceiver monitoring.
	disable	Disables transceiver monitoring.
	interval <i>interval</i>	Sets the transceiver monitoring interval; valid values are from 1 to 15 minutes.

Defaults

The defaults are as follows:

- Transceiver monitoring is enabled.
- *interval* is 10 minutes.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The DOM feature measures the transceiver characteristics such as temperature, voltage, laser bias current, receive optical power, and laser transmit power, and allows software to monitor them against alarm and threshold values.

Examples

This example shows how to enable transceiver monitoring:

```
Console> (enable) set transceiver-monitoring enable  
Transceiver monitoring is successfully enabled  
Console> (enable)
```

This example shows how to disable transceiver monitoring:

```
Console> (enable) set transceiver-monitoring disable  
Transceiver monitoring is successfully disabled  
Console> (enable)
```

This example shows how to set the transceiver monitoring interval to 12 minutes:

```
Console> (enable) set transceiver-monitoring interval 12  
Transceiver monitoring interval is set to 12 minutes  
Console> (enable)
```

Related Commands

[show port transceiver](#)

set trunk

To configure trunk ports and to add VLANs to the allowed VLAN list for existing trunks, use the **set trunk** command.

```
set trunk mod/ports {on | off | desirable | auto | nonegotiate} [vlans | none]
[isl | dot1q | dot10 | lane | negotiate]
```

```
set trunk all off
```

Syntax Description

<i>mod/port</i>	Number of the module and the port or ports on the module.
on	Forces the port to become a trunk port and persuade the neighboring port to become a trunk port. The port becomes a trunk port even if the neighboring port does not agree to become a trunk.
off	Forces the port to become a nontrunk port and persuade the neighboring port to become a nontrunk port. The port becomes a nontrunk port even if the neighboring port does not agree to become a nontrunk port.
desirable	Causes the port to negotiate actively with the neighboring port to become a trunk link.
auto	Causes the port to become a trunk port if the neighboring port tries to negotiate a trunk link.
nonegotiate	Forces the port to become a trunk port but prevents it from sending DTP frames to its neighbor.
<i>vlans</i>	(Optional) VLANs to add to the list of allowed VLANs on the trunk; valid values are from 1 to 4094.
none	(Optional) Clears all VLANs from the trunk. See the “Usage Guidelines” section for more information.
isl	(Optional) Specifies an ISL trunk on a Fast or Gigabit Ethernet port.
dot1q	(Optional) Specifies an IEEE 802.1Q trunk on a Fast or Gigabit Ethernet port.
dot10	(Optional) Specifies an IEEE 802.10 trunk on a FDDI or CDDI port.
lane	(Optional) Specifies an ATM LANE trunk on an ATM port.
negotiate	(Optional) Specifies that the port become an ISL (preferred) or 802.1Q trunk, depending on the configuration and capabilities of the neighboring port.
all off	Turns off trunking on all ports.

Defaults

The default port mode is **auto**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

The following usage guidelines apply when using the **set trunk** command:

- If a trunk-type keyword (**isl**, **dot1q**, **negotiate**) is not specified when configuring an EtherChannel trunk, the current trunk type is not affected.
- To return a trunk to its default trunk type and mode, enter the **clear trunk mod/port** command.
- Trunking capabilities are hardware-dependent. Refer to the *Catalyst 6500 Series Module Installation Guide* to determine the trunking capabilities of your hardware, or enter the **show port capabilities** command.
- Catalyst 6500 series switches use DTP to negotiate trunk links automatically on EtherChannel ports. Whether or not a port will negotiate to become a trunk port depends on both the mode and the trunk type specified for that port. Refer to the *Catalyst 6500 Series Switch Software Configuration Guide* for detailed information on how trunk ports are negotiated.
- DTP is a point-to-point protocol. However, some internetworking devices might improperly forward DTP frames. You can avoid this problem by ensuring that trunking is turned **off** on ports connected to non-Catalyst 6500 series switch devices if you do not intend to trunk across those links. When enabling trunking on a link to a Cisco router, enter the **noneg** keyword to cause the port to become a trunk but not generate DTP frames.
- To remove VLANs from the allowed list for a trunk, enter the **clear trunk mod/port vlans** command. When you first configure a port as a trunk, the **set trunk** command always adds *all* VLANs to the allowed VLAN list for the trunk, even if you specify a VLAN range. (The specified VLAN range is ignored.)
- To remove VLANs from the allowed list, enter the **clear trunk mod/port vlans** command. To later add VLANs that were removed, enter the **set trunk mod/port vlans** command.
- You cannot change the allowed VLAN range on the MSM port. The MSM port can be configured only as an IEEE 802.1Q-type trunk.
- For trunking to be negotiated on EtherChannel ports, the ports must be in the same VTP domain. However, you can use the **on** or **noneg** mode to force a port to become a trunk, even if it is in a different domain.
- When you configure a trunk, all VLANs are active on the trunk by default. If you do not want any active VLANs on the trunk, enter the **none** keyword. The **none** keyword clears all VLANs from the trunk.

Examples

This example shows how to set port 2 on module 1 as a trunk port:

```
Console> (enable) set trunk 1/2 on
Port(s) 1/2 trunk mode set to on.
Console> (enable)
```

This example shows how to add VLANs 5 through 50 to the allowed VLAN list for a trunk port (VLANs were previously removed from the allowed list with the **clear trunk** command):

```
Console> (enable) set trunk 1/1 5-50
Adding vlans 5-50 to allowed list.
Port(s) 1/1 allowed vlans modified to 1,5-50,101-1005.
Console> (enable)
```

This example shows how to set port 5 on module 4 as an 802.1Q trunk port in **desirable** mode:

```
Console> (enable) set trunk 4/5 desirable dot1q
Port(s) 4/5 trunk mode set to desirable.
Port(s) 4/5 trunk type set to dot1q.
Console> (enable)
```

This example shows how to configure a trunk without any VLANs:

```
Console> (enable) set trunk 7/1 on none dot1q  
Removing Vlan(s) 1-4094 from allowed list.  
Port 7/1 allowed vlans modified to none.  
Port(s) 7/1 trunk mode set to on.  
Port(s) 7/1 trunk type set to dot1q.  
Console> (enable)
```

This example shows how to configure trunk mode to off and trunk port to negotiate:

```
Console> (enable) set trunk 2/5 off negotiate  
Port(s) 2/5 trunk mode set to off.  
Port(s) 2/5 trunk type set to negotiate.  
Console> (enable)
```

Related Commands

clear trunk
set vtp
show port dot1q-ethertype
show trunk
show vtp statistics