

set qos mac-cos

Use the **set qos mac-cos** command to map a CoS value to a MAC address and VLAN pair.

```
set qos mac-cos dest_mac vlan cos
```

Syntax Description	
<i>dest_mac</i>	MAC address of the destination host.
<i>vlan</i>	Number of the VLAN; valid values are from 1 to 1001 .
<i>cos</i>	CoS value; valid values are from 0 to 7 , with the higher numbers representing higher priority.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command is supported only on Supervisor Engine II G or III G, or Supervisor Engine III.

The **set qos mac-cos** command creates a permanent CAM entry that remains in the CAM table until the active supervisor is reset.

The port associated with the MAC address is learned when the first packet with this source MAC address is received. These entries are not aged out.

If you enter the **show cam** command, entries made with the **set qos mac-cos** command are displayed as dynamic. Entries made using the **set qos mac-cos** command do not age out.

Examples This example shows how to map a CoS value to a MAC address and VLAN:

```
Console> (enable) set qos mac-cos 0f-ab-12-12-00-13 2 3
CoS 3 is assigned to 0f-ab-12-12-00-13 vlan 2.
Console> (enable)
```

Related Commands

- [clear qos mac-cos](#)
- [show qos mac-cos](#)

set qos map

Use the **set qos map** command to associate CoS values to a transmit queue and drop threshold.

```
set qos map port_type q# threshold# cos coslist
```

Syntax Description	<i>port_type</i> 1q4t is the only valid port type.
	<i>q#</i> Transmit queue number.
	<i>threshold#</i> Drop threshold number. The higher the threshold number, the lower the chance traffic will be dropped.
	cos coslist Keyword and variable to specify the CoS values; valid values are from 0 to 7 , with the higher numbers indicating higher priority.

Defaults

The default mappings are:

- CoS value-to-drop threshold mapping
 - Drop threshold 1: CoS 0–1
 - Drop threshold 2: CoS 2–3
 - Drop threshold 3: CoS 4–5
 - Drop threshold 4: CoS 6–7
- CoS value-to-transmit queue mapping
 - Transmit queue 1: CoS 0–7

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is supported on switches configured with Supervisor Engine II G or III G or Supervisor Engine III.

Only port type 1q4t is supported, which consists of one transmit queue and four drop thresholds.

Examples

This example shows how to assign the CoS values 1 and 2 to the first transmit queue and the first drop threshold for that queue on a 1q4t port (Catalyst 5000 family switches):

```
Console> (enable) set qos map 1q4t tx 1 1 cos 1-2
Qos tx priority queue and threshold mapped to cos successfully.
Console> (enable)
```

This example shows how to assign the CoS values 4 through 7 to the first transmit queue and the second drop threshold for that queue on a 1q4t port (Catalyst 5000 family switches):

```
Console> (enable) set qos map 1q4t tx 1 2 cos 4-7  
Qos tx priority queue and threshold mapped to cos successfully.  
Console> (enable)
```

Related Commands

[clear qos map](#)
[show qos info](#)

set qos policy-source

Use the **set qos policy-source** command to set the QoS policy source.

set qos policy-source local | cops

Syntax Description	local	Keyword to set the policy source to local NVRAM configuration.
	cops	Keyword to set the policy source to COPS configuration.

Defaults The default is all ports are set to local.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines When you set the policy source to local, the QoS policy is taken from local configuration stored in NVRAM. If you set the policy source to local after it was set to COPS, the QoS policy reverts back to the local configuration stored in NVRAM.

When you set the policy source to COPS, all configuration that is global to the device, such as the DSCP to marked-down DSCP, is taken from policy downloaded to the PEP by the PDP. Configuration of each physical port, however, is taken from COPS only if the policy source for that port has been set to COPS.

Examples This example shows how to set the policy source to COPS:

```
Console> (enable) set qos policy-source cops
QoS policy source for the switch set to COPS.
Console> (enable)
```

This example shows how to set the policy source to local NVRAM:

```
Console> (enable) set qos policy-source local
QoS policy source for the switch set to local.
Console> (enable)
```

This example shows the output if you attempt to set the policy source to COPS and none are available:

```
Console> (enable) set qos policy-source cops
QoS policy source for the switch set to COPS.
Warning: No COPS servers configured. Use the 'set cops server' command
to configure COPS servers.
Console> (enable)
```

Related Commands

- [clear qos config](#)
- [show qos info](#)
- [show qos policy-source](#)

set qos router-mac

Use the **set qos router-mac** command to specify router MAC addresses for ACE-based classification.

```
set qos router-mac mac_address vlan
```

Syntax Description	
<i>mac_address</i>	MAC address contained in the packets to be filtered. You can enter this address in canonical format (00-11-33-44-55) or noncanonical format (00:11:22:33:44:55).
<i>vlan</i>	Number of the VLAN; valid values are from 1 to 1005 .

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command is supported only on Supervisor Engine II G or III G, or Supervisor Engine III. This command is not supported by the MLS-RP.

Use this command to specify the MAC address of a router for which to perform ACE-based classification. For IPv4 traffic destined for a router, QoS can classify packets that match an ACE by setting the IP precedence bits (in the IP TOS header) and CoS value in the frame header.

If you are using MLS, QoS can perform ACE-based classification only for traffic that is switched using MLS. ACE-based classification is performed at the switch egress port as the flow is being multilayer switched. QoS cannot perform ACE-based classification on traffic that the MLS-RP routes off the switch. QoS learns the address of the MLS-RP automatically when MLS is configured on the switch.

Examples This example shows how to set the router MAC address on a specific VLAN:

```
Console> (enable) set qos router-mac 00-40-0b-30-03-48 2
Router MAC/Vlan is set for QoS.
Console> (enable)
```

Related Commands [clear qos router-mac](#)
[show qos mac-cos](#)

set qos wred-threshold

Use the **set qos wred-threshold** command to specify the transmit queue drop thresholds on all ports in the switch.

```
set qos wred-threshold port_type [rx | tx] queue {q# thr1 thr2 thr3 thr4}
```

Syntax Description	
<i>port_type</i>	Only valid value for <i>port_type</i> is 1q4t .
rx	(Optional) Keyword to specify input queuing. This keyword is not supported.
tx	(Optional) Keyword to specify output queuing.
queue	Keyword to specify the queue value.
<i>q#</i>	Number of queue. The only valid value is 1 .
<i>thr#</i>	Value of threshold; valid values are from 1 to 100 percent.

Defaults The defaults are output queuing and the threshold values are 30%, 50%, 80%, and 100%.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command is supported only on Supervisor Engine II G or III G, or Supervisor Engine III.

The number preceding the t letter in the *port_type* (1q4t) determines the number of threshold values the hardware supports. For example, with 1q4t, the number of thresholds specified is four.

The number preceding the q letter in the *port_type* determines the number of the queues that the hardware supports. For example, with 1q4t, the number of queues specified is one.

The transmit drop threshold percentages specified select a buffer usage level where each threshold applies.

The percentages to buffer usage level are as follows:

- 1% is a threshold when 2,044 bytes of the transmit queue buffer have been used
- 2% and 3% = 4,092 bytes have been used
- 4% through 7% = 8,188 bytes have been used
- 8% through 14% = 16,380 bytes have been used
- 15% through 28% = 32,767 bytes have been used
- 29% through 57% = 65,532 bytes have been used
- 58% through 100% = 131,068 bytes have been used

Due to the granularity of programming the hardware, the values set in hardware will be close approximations of the values provided.

Examples

This example shows how to configure the transmit queue drop thresholds:

```
Console> (enable) set qos wred-threshold 1q4t tx queue 1 30 50 80 100  
Transmit drop thresholds for queue 1 set at 30% 50% 80% 100%  
Console> (enable)
```

Related Commands

[show qos info](#)

set radius deadline

Use the **set radius deadline** command to set the time to skip RADIUS servers that do not reply.

set radius deadline *minutes*

Syntax Description	<i>minutes</i> The length of time a RADIUS server does not respond to an authentication request; valid values are from 0 to 1440 minutes.
---------------------------	---

Defaults	The default is 0 minutes.
-----------------	---------------------------

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

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

Usage Guidelines	If only one RADIUS server is configured or if all the configured servers are marked dead, deadline will be ignored because there are no alternate servers available. By default, the deadline will be 0 minutes, that is, the RADIUS servers will not be marked dead if they do not respond.
-------------------------	--

Examples	This example shows how to set the RADIUS deadline to 10 minutes:
-----------------	--

```
Console> (enable) set radius deadline 10  
Radius deadline set to 10 minutes.  
Console> (enable)
```

Related Commands	show radius
-------------------------	-----------------------------

set radius key

Use the **set radius key** command to set the encryption and authentication for all communication between the RADIUS client and the server.

```
set radius key key
```

Syntax Description	<i>key</i> Key to authenticate the transactions between the RADIUS client and the server.
---------------------------	---

Defaults	The default of the key is set to NULL.
-----------------	--

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

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

Usage Guidelines	The key you set must be the same one as configured in the RADIUS server. All leading spaces are ignored, spaces within and at the end of the key are not ignored. Double quotes are not required even if there are spaces in the key, unless the quotes themselves are part of the key. The length of the key is limited to 65 characters. It can include any printable ASCII character except tabs.
-------------------------	--

Examples	This example shows how to set the RADIUS encryption and authentication key to Make my day:
-----------------	--

```
Console> (enable) set radius key Make my day
Radius key set to Make my day.
Console> (enable)
```

Related Commands	show radius
-------------------------	-----------------------------

set radius retransmit

Use the **set radius retransmit** command to specify the number of times the RADIUS servers are tried before giving up on the server.

set radius retransmit *count*

Syntax Description	<i>count</i>	Number of times the RADIUS servers are tried before giving up on the server; valid values are from 1 to 100 .
---------------------------	--------------	---

Defaults	The default is two times (three attempts).
-----------------	--

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

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

Examples	This example shows how to set the retransmit attempts to 3:
-----------------	---

```
Console> (enable) set radius retransmit 3  
Radius retransmit count set to 3.  
Console> (enable)
```

Related Commands	show radius
-------------------------	-----------------------------

set radius server

Use the **set radius server** command to set up the RADIUS server.

```
set radius server ipaddr [auth-port port] [acct-port port][primary]
```

Syntax Description	
<i>ipaddr</i>	Number of the IP address or IP alias in dot notation a.b.c.d.
auth-port <i>port</i>	(Optional) Keyword and variable to specify a destination UDP port for RADIUS authentication messages.
acct-port <i>port</i>	(Optional) Keyword and variable to specify a destination UDP port for RADIUS accounting messages.
primary	(Optional) Keyword to specify that this server be contacted first.

Defaults The default **auth-port** is 1812. The default **acct-port** is 1813.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines You can add up to three RADIUS servers.
The RADIUS server will not be used for authentication if the port number is set to 0.

Examples This example shows how to add a primary server using an IP alias:

```
Console> (enable) set radius server tampa.users.com
tampa.users.com added to RADIUS server table as primary server.
Console> (enable)
```

Related Commands [show radius](#)

set radius timeout

Use the **set radius timeout** command to set the time between retransmissions to the RADIUS server.

set radius timeout *seconds*

Syntax Description	<i>seconds</i> Number of seconds to wait for a reply; valid values are from 1 to 1000 seconds.
Defaults	The default timeout is 5 seconds.
Command Types	Switch command.
Command Modes	Privileged.
Examples	This example shows how to set the time between retransmissions to 7 seconds: <pre>Console> (enable) set radius timeout 7 Radius timeout set to 7 seconds. Console> (enable)</pre>
Related Commands	show radius

set rcp username

Use the **set rcp username** command to specify your username for rcp file transfers.

```
set rcp username username
```

Syntax Description	<i>username</i> Username up to 14 characters long.
---------------------------	--

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

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

Usage Guidelines	Username must be different from “root” and not a null string. The only case where rcp username is not used is for the VMPS database. For the VMPS database, an rcp VMPS username is used.
-------------------------	---

Examples	This example shows how to set the username for rcp:
-----------------	---

```
Console> (enable) set rcp username jdoe
Console> (enable)
```

Related Commands	set vmps downloadmethod
-------------------------	---

set rgmp

Use the **set rgmp** command to enable or disable the RGMP feature on the switch.

```
set rgmp {enable | disable}
```

Syntax Description

enable Keyword to enable RGMP on the switch.

disable Keyword to disable RGMP on the switch.

Defaults

The default is RGMP is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

RGMP is a global command. You cannot enable or disable RGMP on a per-VLAN basis.

The RGMP feature is operational only if IGMP snooping is enabled on the switch (see the [set igmp](#) command).

Examples

This example shows how to enable RGMP on the switch:

```
Console> (enable) set rgmp enable
RGMP is enabled.
Console> (enable)
```

This example shows how to disable RGMP on the switch:

```
Console> (enable) set rgmp disable
RGMP is disabled.
Console> (enable)
```

Related Commands

[clear rgmp statistics](#)
[set igmp](#)
[set igmp fastleave](#)
[show rgmp group](#)
[show rgmp statistics](#)

set rsmautostate

Use the **set rsmautostate** command to enable and disable line protocol state determination of the RSMs due to port state changes.

```
set rsmautostate {enable | disable}
```

Syntax Description	enable	disable
	Keyword to activate line protocol state determination.	Keyword to deactivate line protocol state determination.

Defaults The default configuration has line protocol state determination disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines When you enable **rsmautostate**, VLAN interfaces on the RSM are active only when there is at least one other active interface within the Catalyst 5000 family switches. This interface could be a physical end-user port, a trunk connection for which the VLAN is active, or another RSM with an equivalent VLAN interface.

This command is useful for discontinuing the advertisement of routing paths when access to them is severed (either through fault or administrative disabling).

If you disable **rsmautostate**, you might have to use the **shutdown/no shutdown** Cisco IOS command to disable and then restart the VLAN interface to bring the RSM back up.

Examples This example shows how to enable the line protocol state determination of the RSM:

```
Console> (enable) set rsmautostate enable
Console> (enable)
```

This example shows how to disable the line protocol state determination of the RSM:

```
Console> (enable) set rsmautostate disable
Console> (enable)
```

Related Commands [show rsmautostate](#)

set snmp access

Use the **set snmp access** command to define the access rights of an SNMP group with a specific security model in different security levels.

```
set snmp access [-hex] {groupname} {security-model {v1 | v2c}} [read [-hex] {readview}]
[write [-hex] {writeview}] [notify [-hex] {notifyview}] [volatile | nonvolatile]
```

```
set snmp access [-hex] {groupname} {security-model v3 {noauthentication | authentication
| privacy}} [read [-hex] {readview}] [write [-hex] {writeview}] [notify [-hex]
{notifyview}] [volatile | nonvolatile]
```

Syntax Description

-hex	(Optional) Keyword to display the <i>groupname</i> , <i>readview</i> , <i>writeview</i> , and <i>notifyview</i> as a hexadecimal format.
<i>groupname</i>	Name of the SNMP group.
security-model v1 v2c	Keywords to specify security-model v1 or v2c.
read readview	(Optional) Keyword and variable to specify the name of the view that allows you to see the MIB objects
write writeview	(Optional) Keyword and variable to specify the name of the view that allows you to configure the contents of the agent.
notify notifyview	(Optional) Keyword and variable to specify the name of the view that allows you to send a trap about MIB objects.
v3	Keyword to specify security model v3.
noauthentication	Keyword to specify the security model is not set to use the authentication protocol.
authentication	Keyword to specify the type of authentication protocol.
privacy	Keyword to specify the messages sent on behalf of the user are protected from disclosure.
volatile	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify that the storage type is defined as persistent memory and the content remains after the device is power cycled.

Defaults

The defaults are as follows:

- storage type is nonvolatile.
- **read readview** is Internet OID space.
- **write writeview** is NULL OID.
- **notify notifyview** is NULL OID.

Command Types

Switch command.

Command Modes Privileged.

Usage Guidelines If you use special characters for *groupname*, *readview*, *writeview*, and *notifyview* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

readview is assumed to be every object belonging to the Internet (1.3.6.1) OID space; you can use the **read** option to override this state.

For *writeview*, you must also configure write access.

For *notifyview*, if a view is specified, any notifications in that view are sent to all users associated with the group (an SNMP server host configuration must exist for the user).

Examples This example shows how to set the SNMP access rights for a group:

```
Console> (enable) set snmp access cisco-group security-model v3 authentication
SNMP access group was set to cisco-group version v3 level authentication, readview
internet, nonvolatile.
Console> (enable)
```

Related Commands [clear snmp access](#)
[show snmp](#)

set snmp community

Use the **set snmp community** command to set SNMP communities and associated access types.

```
set snmp community {read-only | read-write | read-write-all} [community_string]
```

Syntax Description		
read-only	Keyword to assign read-only access to the specified SNMP community.	
read-write	Keyword to assign read-write access to the specified SNMP community.	
read-write-all	Keyword to assign read-write-all access to the specified SNMP community.	
<i>community_string</i>	(Optional) Name of the SNMP community.	

Defaults

The default configuration has the following communities and access types defined:

- public—read-only
- private—read-write
- secret—read-write-all

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

There are three configurable SNMP communities, one for each access type. If you do not specify the community string, the community string configured for that access type is cleared.

Examples

This example shows how to set read-write access to the SNMP community called yappledapple:

```
Console> (enable) set snmp community read-write yappledapple
SNMP read-write community string set.
Console> (enable)
```

This example shows how to clear the community string defined for read-only access:

```
Console> (enable) set snmp community read-only
SNMP read-only community string cleared.
Console> (enable)
```

Related Commands

[clear snmp community](#)
[show snmp](#)

set snmp extendedrmon

Use the **set snmp extendedrmon** command to enable or disable the Network Analysis Module.

```
set snmp extendedrmon {enable | disable}
```

Syntax Description	enable	disable
	Keyword to enable the Network Analysis Module.	Keyword to disable the Network Analysis Module.

Defaults The default is enabled.

Command Types Switch command.

Command Modes Privileged.

Examples This example shows how to enable the Network Analysis Module:

```
Console> (enable) set snmp extendedrmon enable
Snmpr extended RMON module enabled
Console> (enable)
```

This example shows how to disable the Network Analysis Module:

```
Console> (enable) set snmp extendedrmon disable
Snmpr extended RMON module disabled
Console> (enable)
```

Related Commands [show snmp](#)

set snmp extendedrmon netflow

Use the **set snmp extendedrmon netflow** command to enable or disable the Network Analysis Module to receive the NDE stream from an NFFC or NFFC II and present the resulting statistics on reserved ifIndex.3000.

```
set snmp extendedrmon netflow {enable password | disable}
```

Syntax Description	enable	enable <i>password</i> disable
	enable	Keyword to allow the Network Analysis Module to receive the NDE stream from an NFFC or NFFC II installed in the Catalyst 5000 family switches.
	<i>password</i>	NetFlow Monitor registration password.
	disable	Keyword to prevent the Network Analysis Module from receiving the NDE stream.

Defaults The default is SNMP-extended RMON NetFlow disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines To enable the NetFlow Monitor option, you must purchase a NetFlow Monitor option license from your Cisco sales representative.

The option license has a registration key and URL on it. Access the URL and enter the registration key and the MAC address of the Network Analysis Module to generate the password for your Network Analysis Module.

Examples This example shows how to enable SNMP-extended RMON NetFlow support:

```
Console> (enable) set snmp extendedrmon netflow enable <password>
Snm extended RMON netflow enabled
Console> (enable)
```

This example shows how to disable SNMP-extended RMON NetFlow support:

```
Console> (enable) set snmp extendedrmon netflow disable
Snm extended RMON netflow disabled
Console> (enable)
```

Related Commands [show snmp](#)

set snmp extendedrmon vlanagent

Use the **set snmp extendedrmon vlanagent** command to enable or disable the VLANagent option. If the VLANagent option is enabled, the NAM aggregates statistics by VLAN as well as by port.

set snmp extendedrmon vlanagent { enable | disable }

Syntax Description	enable	disable
	Keyword to activate SNMP-extended RMON VLANagent support.	Keyword to deactivate SNMP-extended RMON VLANagent support.

Defaults The default is SNMP-extended RMON VLANagent disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The VLANagent creates an increased memory load on the NAM and might not be suitable for use on a heavily loaded switch or when the switch is configured to analyze a high volume of network traffic.

Examples This example shows how to enable extended RMON VLANagent support:

```
Console> (enable) set snmp extendedrmon vlanagent enable
Snm extended RMON vlanagent enabled
Console> (enable)
```

This example shows how to disable extended RMON VLANagent support:

```
Console> (enable) set snmp extendedrmon vlanagent disable
Snm extended RMON vlanagent disabled
Console> (enable)
```

Related Commands [show snmp](#)

set snmp extendedrmon vlanmode

Use the **set snmp extendedrmon vlanmode** command to enable or disable the VLAN monitor option. If the VLAN monitor option is enabled, the Network Analysis Module aggregates statistics by VLAN, instead of by source MAC address.

```
set snmp extendedrmon vlanmode {enable | disable}
```

Syntax Description	enable	disable
	Keyword that activates SNMP-extended RMON VLAN mode support.	Keyword that deactivates SNMP-extended RMON VLAN mode support.

Defaults The default is SNMP-extended RMON VLAN mode disabled.

Command Types Switch command.

Command Modes Privileged.

Examples This example shows how to enable extended-RMON VLAN mode support:

```
Console> (enable) set snmp extendedrmon vlanmode enable
Snm extended RMON vlanmode enabled
Console> (enable)
```

This example shows how to disable extended-RMON VLAN mode support:

```
Console> (enable) set snmp extendedrmon vlanmode disable
Snm extended RMON vlanmode disabled
Console> (enable)
```

Related Commands [show snmp](#)

set snmp group

Use the **set snmp group** command to establish the relationship between an SNMP group and a user with a specific security model.

```
set snmp group [-hex] {groupname} user [-hex] {username} {security-model {v1 | v2c | v3}} [volatile | nonvolatile]
```

Syntax Description		
-hex	(Optional) Keyword to display the <i>groupname</i> and <i>username</i> as a hexadecimal format.	
<i>groupname</i>	Name of the SNMP group that defines an access control; the maximum length is 32 bytes.	
user	Keyword to specify the SNMP group user name.	
<i>username</i>	Name of the SNMP user that belongs to the SNMP group; the maximum length is 32 bytes.	
security-model v1 v2c v3	Keywords to specify security-model v1, v2c, or v3.	
volatile	(Optional) Keyword to define the storage type as temporary memory and the content is deleted if the device is turned off.	
nonvolatile	(Optional) Keyword to define the storage type as persistent memory and the content remains after the device is turned off and on again.	

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines If you use special characters for *groupname* or *username* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples This example shows how to set the SNMP group:

```
Console> (enable) set snmp group cisco-group user joe security-model v3
SNMP group was set to cisco-group user joe and version v3,nonvolatile.
Console> (enable)
```

Related Commands [clear snmp group](#)
[show snmp group](#)

set snmp notify

Use the **set snmp notify** command to set the *notifyname* entry in the *snmpNotifyTable* and the *notifytag* entry in the *snmpTargetAddrTable*.

```
set snmp notify [-hex] {notifyname} tag [-hex] {notifytag} [trap | inform] [volatile | nonvolatile]
```

Syntax Description		
-hex	(Optional) Keyword to display <i>notifyname</i> and <i>notifytag</i> as a hexadecimal format.	
<i>notifyname</i>	Keyword to specify a unique identifier to index the <i>snmpNotifyTable</i> .	
tag	Keyword to specify the tag name in the taglist.	
<i>notifytag</i>	Keyword to specify selected entries in the <i>snmpTargetAddrTable</i> .	
trap	(Optional) Keyword to specify all messages that contain snmpv2-Trap PDUs.	
inform	(Optional) Keyword to specify all messages that contain InfoRequest PDUs.	
volatile	(Optional) Keyword to define the storage type as temporary memory and the content is deleted if the device is turned off.	
nonvolatile	(Optional) Keyword to define the storage type as persistent memory and the content remains after the device is power cycled.	

Defaults The default storage type is volatile and the default notify type is trap.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines If you use special characters for the *notifyname* and *notifytag* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples This example shows how to set the SNMP notify for a specific notifyname:

```
Console> (enable) set snmp notify hello tag world inform
SNMP notify name was set to hello with tag world notifyType inform, and storageType
nonvolatile.
Console> (enable)
```

Related Commands [clear snmp notify](#)
[show snmp notify](#)

set snmp rmon

Use the **set snmp rmon** command to enable or disable SNMP RMON support.

```
set snmp rmon {enable | disable}
```

Syntax Description	enable	disable
	Keyword to activate SNMP RMON support.	Keyword to deactivate SNMP RMON support.

Defaults The default for RMON support is disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines RMON statistics are collected on a segment basis instead of a repeater-port basis for the Catalyst 5000 family switching Ethernet modules (WS-X5020 and WS-X5223).

The RMON feature deinstalls the domains for all of the interfaces on an Ethernet module that has been removed from the system.

RMON is supported on Ethernet, Fast Ethernet, Gigabit Ethernet, and Token Ring switch ports.

When RMON is enabled, the supported RMON groups for Ethernet ports are Statistics, History, Alarms, and Events, as specified in RFC 1757. When RMON is enabled, the supported RMON groups for Token Ring ports are Mac-Layer Statistics, Promiscuous Statistics, Mac-Layer History, Promiscuous History, Ring Station Order Table, Alarms, and Events, as specified in RFC 1513 and RFC 1757.



Note

You need a separate software license to use this command. Contact Cisco [Technical Assistance Center](#) for additional information.

Examples This example shows how to enable RMON support:

```
Console> (enable) set snmp rmon enable
SNMP RMON support enabled.
Console> (enable)
```

This example shows how to disable RMON support:

```
Console> (enable) set snmp rmon disable
SNMP RMON support disabled.
Console> (enable)
```

Related Commands [show snmp](#)

set snmp rmonmemory

Use the **set snmp rmonmemory** command to set the memory usage limit in a percentage value format.

```
set snmp rmonmemory percentage
```

Syntax Description	<i>percentage</i> Memory usage limit: valid values are 0 to 100 percent. See the “Usage Guidelines” section for additional information.
---------------------------	---

Defaults	The default is 85 percent.
-----------------	----------------------------

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

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

Usage Guidelines	When you set the percentage value to 85, the RMON is not using 85 percent of memory; this value does not allow you to create new RMON entries or restore entries from the NVRAM if the memory usage exceeds 85 percent.
-------------------------	---

If you expect the device to run other sessions such as Telnet, you need to set a lower value to the memory limit. Otherwise, the new Telnet sessions may fail because there is not enough available memory.

Examples	This example shows how to set the memory usage limit:
-----------------	---

```
Console> (enable) set snmp rmonmemory 90  
Console> (enable)
```

Related Commands	show snmp rmonmemory
-------------------------	--------------------------------------

set snmp targetaddr

Use the **set snmp targetaddr** command to configure the SNMP target address entries in the snmpTargetAddressTable.

```
set snmp targetaddr [-hex] {addrname} param [-hex] {paramsname} {ipaddr} [udpport
  {port}] [timeout {value}] [retries {value}] [volatile | nonvolatile] [taglist {[hex] tag}]
  [[hex] tag tagvalue]
```

Syntax Description		
-hex	(Optional) Keyword to display the <i>addrname</i> , <i>paramsname</i> , <i>tag</i> , and <i>tagvalue</i> as a hexadecimal format.	
<i>addrname</i>	Arbitrary but unique name of the target agent; the maximum length is 32 bytes.	
param	Keyword to specify an entry in the snmpTargetParamsTable, which provides parameters to be used when generating a message to the target; the maximum length is 32 bytes.	
<i>paramsname</i>	Entry in the snmpTargetParamsTable; the maximum length is 32 bytes.	
<i>ipaddr</i>	IP address of the target.	
udpport <i>port</i>	(Optional) Keyword and variable to specify which UDP port of the target host to use.	
timeout <i>value</i>	(Optional) Keyword and variable to specify the number of timeouts.	
retries <i>value</i>	(Optional) Keyword and variable to specify the number of retries.	
volatile	(Optional) Keyword to define the storage type as temporary memory and the content is deleted if the device is turned off.	
nonvolatile	(Optional) Keyword to define the storage type as persistent memory and the content remains after the device is power cycled.	
taglist <i>tag</i>	(Optional) Keyword and variable to specify a tag name in the taglist.	
tag <i>tagvalue</i>	(Optional) Keyword and variable to specify the tag name.	

Defaults

The defaults are as follows:

- storage type is nonvolatile.
- **udpport** is 162.
- **timeout** is 1500.
- **retries** is 3.
- **taglist** is NULL.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for the *addrname*, *paramsname*, *tag*, and *tagvalue* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

The maximum *tagvalue* and *taglist* length is 255 bytes.

Examples

This example shows how to set the target address in the snmpTargetAddressTable:

```
Console> (enable) set snmp targetaddr foo param bar 10.1.2.4 udp 160 timeout 10 retries 3
taglist tag1 tag2 tag3
SNMP targetaddr name was set to foo with param bar ipAddr 10.1.2.4, udpport 160, timeout
10, retries 3, storageType nonvolatile with taglist tag1 tag2 tag3.
Console> (enable)
```

Related Commands

[clear snmp targetaddr](#)
[show snmp targetaddr](#)

set snmp targetparams

Use the **set snmp targetparams** command set to configure the SNMP parameters used in the snmpTargetParamsTable when generating a message to a target.

```
set snmp targetparams [-hex] {paramsname} user [-hex] {username} {security-model
{v1 | v2c}} {message-processing {v1 | v2c | v3}} [volatile | nonvolatile]
```

```
set snmp targetparams [-hex] {paramsname} user [-hex] {username} {security-model v3}
{message-processing v3 {noauthentication | authentication | privacy}} [volatile |
nonvolatile]
```

Syntax Description		
-hex	(Optional) Keyword to display the <i>paramsname</i> and <i>username</i> as a hexadecimal format.	
<i>paramsname</i>	A unique identifier used to index the snmpTargetParamsTable; the maximum length is 32 bytes.	
user	Keyword to specify the SNMP group user name.	
<i>username</i>	Name of the SNMP user that belongs to the SNMP group; the maximum length is 32 bytes.	
security-model v1 v2c	Keywords to specify security-model v1 or v2c.	
message-processing v1 v2c v3	Keywords to specify the version number used by the message processing model.	
security-model v3	Keywords to specify security-model v3.	
message-processing v3	Keywords to specify version 3 is used by the message-processing model.	
noauthentication	Keyword to specify security model is not set to use authentication protocol.	
authentication	Keyword to specify the type of authentication protocol.	
privacy	Keyword to specify the messages sent on behalf of the user are protected from disclosure.	
volatile	(Optional) Keyword to define the storage type as temporary memory and the content is deleted if the device is turned off.	
nonvolatile	(Optional) Keyword to define the storage type as persistent memory and the content remains after the device is power cycled.	

Defaults The default storage type is volatile.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines

If you use special characters for the *paramsname* and *username* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples

This example shows how to set target parameters in the snmpTargetParamsTable:

```
Console> (enable) set snmp targetparams bar user joe security-model v3 message-processing
v3 authentication
SNMP target params was set to bar v3 authentication, message-processing v3, user joe
nonvolatile.
Console> (enable)
```

Related Commands

[clear snmp targetparams](#)
[show snmp targetparams](#)

set snmp trap

Use the **set snmp trap** command set to enable or disable the different SNMP traps on the system or to add an entry into the SNMP authentication trap receiver table.

```
set snmp trap {enable | disable} [all | module | chassis | bridge | repeater | auth | vtp |
  ippermit | vmpls | config | entity | stpx | syslog]
```

```
set snmp trap rcvr_addr rcvr_community
```

Syntax Description

enable	Keyword to activate SNMP traps.
disable	Keyword to deactivate SNMP traps.
all	(Optional) Keyword to specify all trap types.
module	(Optional) Keyword to specify the moduleUp and moduleDown traps from the CISCO-STACK-MIB.
chassis	(Optional) Keyword to specify the ciscoSyslogMIB trap from the CISCO-SYSLOG-MIB.
bridge	(Optional) Keyword to specify the newRoot and topologyChange traps from RFC 1493 (the BRIDGE-MIB).
repeater	(Optional) Keyword to specify the rptrHealth, rptrGroupChange, and rptrResetEvent traps from RFC 1516 (the SNMP-REPEATER-MIB).
auth	(Optional) Keyword to specify the authenticationFailure trap from RFC 1157.
vtp	(Optional) Keyword to specify the VTP from the CISCO-VTP-MIB.
ippermit	(Optional) Keyword to specify the IP Permit Denied access from the CISCO-STACK-MIB.
vmpls	(Optional) Keyword to specify the vmVmplsChange trap from the CISCO-VLAN-MEMBERSHIP-MIB.
config	(Optional) Keyword to specify the sysConfigChange trap from the CISCO-STACK-MIB.
entity	(Optional) Keyword to specify the entityMIB trap from the ENTITY-MIB.
stpx	(Optional) Keyword to specify the STPX trap.
syslog	(Optional) Keyword to specify the system log.
<i>rcvr_addr</i>	IP address or IP alias of the system to receive SNMP traps.
<i>rcvr_community</i>	Community string to use when sending authentication traps.

Defaults

The default configuration has SNMP traps disabled.

Command Types

Switch command.

Command Modes Privileged.

Usage Guidelines An IP permit trap is sent when unauthorized access based on the IP permit list is attempted. Use the **show snmp** command to verify that the appropriate traps were configured.

Examples This example shows how to enable SNMP chassis traps:

```
Console> (enable) set snmp trap enable chassis
SNMP chassis alarm traps enabled.
Console> (enable)
```

This example shows how to enable all traps:

```
Console> (enable) set snmp trap enable
All SNMP traps enabled.
Console> (enable)
```

This example shows how to disable SNMP chassis traps:

```
Console> (enable) set snmp trap disable chassis
SNMP chassis alarm traps disabled.
Console> (enable)
```

This example shows how to add an entry in the SNMP trap receiver table:

```
Console> (enable) set snmp trap 192.122.173.42 public
SNMP trap receiver added.
Console> (enable)
```

Related Commands

- [clear ip permit](#)
- [clear port filter](#)
- [set ip permit](#)
- [show ip permit](#)
- [show port counters](#)
- [show snmp](#)
- [test snmp trap](#)

set snmp user

Use the **set snmp user** command to configure a new SNMP user.

```
set snmp user [-hex] {username} {remote {engineid}} [authentication {md5 | sha |
authpassword}] [privacy {privpassword}] [volatile | nonvolatile]
```

Syntax Description		
-hex	(Optional) Keyword to display <i>username</i> as a hexadecimal format.	
<i>username</i>	Name of the SNMP user.	
remote <i>engineid</i>	Keyword and variable to specify the remote SNMP engine ID.	
authentication	(Optional) Keyword to specify the authentication protocol.	
md5	Keyword to specify HMAC-MD5-96 authentication protocol.	
sha	Keyword to specify HMAC-SHA-96 authentication protocol.	
authpassword	Password for authentication.	
privacy <i>privpassword</i>	(Optional) Keyword and variable to enable the host to encrypt the contents of the message sent to or from the agent; the maximum length is 32 bytes, password for privacy.	
volatile	(Optional) Keyword to define the storage type as temporary memory and the content is deleted if the device is turned off.	
nonvolatile	(Optional) Keyword to define the storage type as persistent memory and the content remains after the device is power cycled.	

Defaults The default storage type is volatile.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines If you use special characters for *username* (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

The **authpassword** and *privpassword* values must be hexadecimal characters without delimiters in between.

If the **authentication** keyword is not specified, the security level default will be no authentication. If the **privacy** keyword is not specified, the default will be no privacy.

Examples

This example shows how to set a specific user name:

```
Console> (enable) set snmp user joe  
Snmp user was set to joe authProt no-auth privProt no-priv with engineid 00:00.  
Console> (enable)
```

This example shows how to set a specific user name, authentication, and authpassword:

```
Console> (enable) set snmp user John authentication md5 arizona2  
Snmp user was set to John authProt md5 authPasswd arizona2. privProt no-priv wi.  
Console> (enable)
```

Related Commands

[clear snmp user](#)
[show snmp user](#)

set snmp view

Use the **set snmp view** command to configure the SNMP MIB view.

```
set snmp view [-hex] {viewname} {subtree} [mask] [included | excluded] [volatile | nonvolatile]
```

Syntax Description	
-hex	(Optional) Keyword to display the <i>viewname</i> as a hexadecimal format.
<i>viewname</i>	Name of a MIB view.
<i>subtree</i>	The MIB subtree.
mask	(Optional) Keyword to specify that the bit mask is used with the subtree. A bit mask can be all ones, all zeros or any combination; the maximum length is 3 bytes.
included excluded	(Optional) Keywords to specify that the MIB subtree is included or excluded.
volatile	(Optional) Keyword to define the storage type as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to define the storage type as persistent memory and the content remains after the device is turned off and on again.

Defaults

The defaults are as follows:

- Storage type is volatile.
- Bit mask is NULL.
- MIB subtree is included.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *viewname* (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

A MOB subtree with a mask defines a view subtree. The MIB subtree can be in OID format or a text name mapped to a valid OID.

Examples

This example shows how to assign a subtree to the view public:

```
Console> (enable) set snmp view public 1.3.6.1 included
Snmp view name was set to public with subtree 1.3.6.1 included, nonvolatile.
Control> (enable)
```

This example shows the response when the subtree is incorrect:

```
Console> (enable) set snmp view stats statistics excluded
Statistics is not a valid subtree OID
Control> (enable)
```

Related Commands

[clear snmp view](#)
[show snmp view](#)

set span

Use the **set span** command to enable or disable SPAN and to set up the switch port and VLAN analyzer for multiple SPAN sessions.

```
set span disable [dest_mod/dest_port | all]
```

```
set span {src_mod/src_ports... | src_vlan... | sc0} {dest_mod/dest_port} [rx | tx | both]  
[inpkts {enable | disable}] [learning {enable | disable}] [multicast {enable | disable}]  
[create]
```

Syntax Description

disable	Keyword to disable SPAN.
<i>dest_mod</i>	(Optional) Monitoring module (SPAN destination).
<i>dest_port</i>	(Optional) Monitoring port (SPAN destination).
all	(Optional) Keyword to disable the spanning for all VLANs.
<i>src_mod</i>	Monitored module (SPAN source).
<i>src_ports...</i>	Monitored ports (SPAN source).
<i>src_vlan...</i>	Monitored VLAN (SPAN source).
sc0	Keyword to specify the in-band interface.
rx	(Optional) Keyword to specify that information received at the source is monitored.
tx	(Optional) Keyword to specify that information transmitted from the source is monitored.
both	(Optional) Keyword to specify that information both transmitted from the source and received at the source is monitored.
inpkts enable	(Optional) Keywords to enable the receiving of normal inbound traffic on the SPAN destination port.
inpkts disable	(Optional) Keywords to disable the receiving of normal inbound traffic on the SPAN destination port.
learning enable	(Optional) Keywords to learn the packet's source address.
learning disable	(Optional) Keywords to not learn the packet's source address.
multicast enable	(Optional) Keywords to enable the receiving multicast packets on the SPAN destination port.
multicast disable	(Optional) Keywords to disable the receiving multicast packets on the SPAN destination port.
create	(Optional) Keyword to create a new SPAN session.

Defaults

The default has no SPAN set up.

learning is enabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines When configuring the SPAN session, follow these guidelines:

- You can configure multiple SPAN sessions to run at the same time. One ingress SPAN session (RX or Both direction) and four egress SPAN sessions (TX direction only) can be configured.
- For monitoring inbound traffic, only one ingress session (or both direction) SPAN is allowed regardless of the port-based SPAN. An egress SPAN can coexist with other SPAN sessions.

When configuring the source or destination ports, follow these guidelines:

- A trunk port can be configured as a source or destination port. If the destination port is a trunk port, the outgoing packets through the SPAN port will carry ISL or 802.1Q VLAN headers.
- Source and destination ports cannot be the same port.
- A FDDI port can be a source or destination port.
- The Token Ring port can be a source or destination port. When monitoring the Tx direction on a Token Ring module, only one source port is allowed.
- You can configure a disabled port to be a source or destination port, but the SPAN function will not work until you enable SPAN on both ports.
- You can configure additional SPAN ports which monitor VLANs only. These ports support a source of one or more VLANs and require the destination port to be a trunk-capable port. This port will filter all traffic except traffic from the configured VLAN for that port.
- You can specify an RSM port as the SPAN source port. However, you cannot specify an RSM port as the SPAN destination port. The source and destination ports have to be within the module.
- If you are configuring SPAN on the Catalyst 5000 family Gigabit EtherChannel switching module, the source and destination ports must be on the same module. This restriction does not apply to the three-port Gigabit Ethernet module (WS-X5403).

If SPAN is enabled:

- And you change the VLAN configuration of the SPAN port (destination), you must disable SPAN before the new configuration will be in effect.
- And you disable a source or destination port, the SPAN function will not work until you enable SPAN on both ports.
- For monitoring a particular VLAN, the number of ports being monitored changes when you move a switched port into or out of the specified monitored VLAN.
- And no parameters were ever set, the first configured SPAN is used as a reference.

When entering keywords, use these guidelines:

- Use the **inpkts** keyword with the **enable** option to allow the SPAN destination port to receive normal incoming traffic in addition to the traffic mirrored from the SPAN source. Use the **disable** option to prevent the SPAN destination port from receiving normal incoming traffic.
- The keyword **learning** is dependent on the **inpkts** option. If the **inpkts** option is disabled, learning will not take effect. The **inpkts** option must be set to **enable** to use **learning**.

- When the keyword **learning** is enabled, the `dont_learn` control bit is disabled, allowing the system to learn a packet's source address. When **learning** is disabled, the packet is forwarded to its destination as usual.
- If you are configuring the Gigabit EtherChannel switching module VLAN, only the **both** argument is allowed, you cannot specify **tx** or **rx**.
- The Token Ring module does not support the **inpkts** option.

A Token Ring port can only monitor another Token Ring port.

If you are running a supervisor engine software release prior to release 4.5(1), we recommend that you configure only a single source port to be monitored. With the supervisor engine software release 4.5(1) and later, a single source port will be the standard Token Ring SPAN configuration.

You cannot monitor a VLAN to which none of the ports belong.

Use either a dedicated RMON probe (such as the NAM) or a network analyzer to monitor ports.

Examples

This example shows how to configure SPAN so that both the transmit traffic and receive traffic on the source port (1/1) is mirrored to the destination port (2/1), and how to verify SPAN configuration:

```
Console> (enable) set span 1/1 2/1
Enabled monitoring of Port 1/1 transmit/receive traffic by Port 2/1
Console> (enable) show span
Status           : enabled
Admin Source     : Port 1/1
Oper Source      : Port 1/1
Destination      : Port 2/1
Direction        : transmit/receive
Incoming Packets: disabled
Console> (enable)
```

This example shows how to set VLAN 522 as the SPAN source and port 2/1 as the SPAN destination:

```
Console> (enable) set span 522 2/1
Enabled monitoring of VLAN 522 transmit/receive traffic by Port 2/1
Console> (enable) show span
Status           : enabled
Admin Source     : VLAN 522
Oper Source      : Port 3/1-2
Destination      : Port 2/1
Direction        : transmit/receive
Incoming Packets: disabled
Console> (enable)
```

This example shows how to enable **learning** on the SPAN source and port 1/1:

```
Console> (enable) set span 522 1/1 learning enable
Overwrote Port 1/1 to monitor transmit/receive traffic of VLAN 522
Incoming Packets disabled. Learning enabled. Multicast enabled.
Console> (enable)
```

This example shows how to disable **learning** on the SPAN source and port 1/1:

```
Console> (enable) set span 522 1/1 learning disable
Overwrote Port 1/1 to monitor transmit/receive traffic of VLAN 522
Incoming Packets disabled. Learning disabled. Multicast enabled.
Console> (enable)
```

This example shows how to disable SPAN:

```
Console> (enable) set span disable  
This command WILL disable your span session(s).  
Do you want to continue (y/n) [n]?y  
Disabled all sessions  
Console> (enable)
```

Related Commands

[clear config](#)
[show span](#)

set spantree backbonefast

Use the **set spantree backbonefast** command to enable or disable the spanning tree BackboneFast convergence feature.

set spantree backbonefast {enable | disable}

Syntax Description	enable	disable
	Keyword to enable BackboneFast convergence.	Keyword to disable BackboneFast convergence.

Defaults The default configuration has BackboneFast convergence disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines BackboneFast convergence is not supported on Token Ring VLANs.
For BackboneFast convergence to work, you must enable it on all switches in the network.

Examples This example shows how to enable BackboneFast convergence:

```
Console> (enable) set spantree backbonefast enable
Backbonefast enabled for all VLANs.
Console> (enable)
```

Related Commands [show spantree](#)

set spantree bpdu-skewing

Use the **set spantree bpdu-skewing** command to enable or disable collection of the spanning tree BPDU skewing detection statistics.

set spantree bpdu-skewing {enable | disable}

Syntax Description

enable	Keyword to enable BPDU skewing detection statistics collection.
disable	Keyword to disable BPDU skewing detection statistics collection.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can use this command to help troubleshooting slow network convergence due to skewing. Skewing occurs when spanning tree timers lapse and expected BPDUs are not received and spanning tree detects topology changes. The difference between the expected result and the BPDUs actually received is a “skew.” The skew causes BPDUs to be reflooded onto the network to keep the spanning tree topology database up-to-date.

Examples

This example shows how to enable the BPDU skew detection feature:

```
Console> (enable) set spantree bpdu-skewing enable  
Spantree bpdu-skewing enabled on this switch.  
Console> (enable)
```

This example shows how to disable the BPDU skew detection feature:

```
Console> (enable) set spantree bpdu-skewing disable  
Spantree bpdu-skewing disabled on this switch.  
Console> (enable)
```

Related Commands

[show spantree bpdu-skewing](#)

set spantree disable

Use the **set spantree disable** command to disable the spanning tree algorithm for all VLANs.

set spantree disable all

Syntax Description	all Keyword to disable the spanning tree algorithm for all VLANs.
---------------------------	--

Defaults	The default configuration has all spanning trees enabled.
-----------------	---

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

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

Usage Guidelines	The all option is supported only on systems configured with a Supervisor Engine III. You cannot enable or disable spanning tree on a per-VLAN basis.
-------------------------	---

Examples	This example shows how to disable the spanning tree algorithm:
-----------------	--

```
Console> (enable) set spantree disable all
VLAN 1 bridge spanning tree disabled.
Console> (enable)
```

Related Commands	set spantree enable show spantree
-------------------------	--

set spantree enable

Use the **set spantree enable** command to enable the spanning tree algorithm for a VLAN or all VLANs.

set spantree enable all

Syntax Description

all	Keyword to enable the spanning tree algorithm for all VLANs.
------------	--

Defaults

The default configuration has all spanning trees enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **all** option is supported only on systems configured with a Supervisor Engine II. You cannot enable or disable spanning tree on a per VLAN basis.

Examples

This example shows how to activate the spanning tree algorithm 1:

```
Console> (enable) set spantree enable all
VLAN 1 bridge spanning tree enabled.
Console> (enable)
```

Related Commands

[set spantree disable](#)
[show spantree](#)

set spantree fwddelay

Use the **set spantree fwddelay** command to set the bridge forward delay for a VLAN.

```
set spantree fwddelay delay [vlan]
```

Syntax Description		
<i>delay</i>	Number of seconds for the bridge forward delay; valid values are from 4 to 30 seconds.	
<i>vlan</i>	(Optional) Number of the VLAN; if a VLAN number is not specified, VLAN 1 is assumed; valid values are from 1 to 1005 .	

Defaults The default configuration has the bridge forward delay set to 15 seconds for all VLANs.

Command Types Switch command.

Command Modes Privileged.

Examples This example shows how to set the bridge forward delay for VLAN 100 to 16 seconds:

```
Console> (enable) set spantree fwddelay 16 100
Spantree 100 forward delay set to 16 seconds.
Console> (enable)
```

Related Commands [show spantree](#)

set spantree guard

Use the **set spantree guard** command to enable or disable the spanning tree root guard or loop guard feature on a per-port basis.

```
set spantree guard { none | root | loop } mod/port
```

Syntax Description	none	Keyword to disable the spanning tree guard feature.
	root	Keyword to enable the root guard feature.
	loop	Keyword to enable the loop guard feature.
	<i>mod/port</i>	Number of the module and ports on the module.

Defaults The default is root guard and loop guard are disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines

If you enable loop guard on a channel and the first link becomes unidirectional, loop guard will block the entire channel until the affected port is removed from the channel.

You may want to prevent switches from becoming the root switch. The root guard feature forces a port to become a designated port so that no switch on the other end of the link can become a root switch.

When you enable root guard, it is automatically applied to all of the active instances or VLANs to which that port belongs. When you disable root guard, it is disabled for the specified port(s). If a port goes into the root-inconsistent state, it automatically goes into the listening state.

Use care when enabling loop guard. Loop guard is useful only in those topologies where there are blocked ports. Topologies where there are no blocked ports are loop free by definition and do not need this feature to be enabled.

Loop guard should be enabled only on root and alternate root ports.

Loop guard should be used mainly on access switches.

When you enable loop guard, it is automatically applied to all of the active instances or VLANs to which that port belongs. When you disable loop guard, it is disabled for the specified port(s). Disabling loop guard moves all loop-inconsistent ports to the listening state.

You cannot enable loop guard on portfast-enabled or dynamic VLAN ports.

You cannot enable portfast on loop guard-enabled ports.

You cannot enable loop guard if root guard is enabled.

Examples

This example shows how to enable root guard:

```
Console> (enable) set spantree guard root 5/1
Rootguard on port 5/1 is enabled.
Warning!! Enabling rootguard may result in a topology change.
Console> (enable)
```

This example shows how to enable the loop guard feature:

```
Console> (enable) set spantree guard loop 5/1
Rootguard is enabled on port 5/1, enabling loopguard will disable rootguard on
this port.
Do you want to continue (y/n) [n]? y
Loopguard on port 5/1 is enabled.
Console> (enable)
```

Related Commands

[show spantree guard](#)

set spantree hello

Use the **set spantree hello** command to set the bridge hello time for a VLAN.

```
set spantree hello interval [vlan]
```

Syntax Description	<i>interval</i>	Number of seconds the system waits before sending a bridge hello message (a multicast message indicating that the system is active); valid values are from 1 to 10 .
	<i>vlan</i>	(Optional) Number of the VLAN; if a VLAN number is not specified, VLAN 1 is assumed; valid values are from 1 to 1005 .

Defaults The default configuration has the bridge hello time set to two seconds for all VLANs.

Command Types Switch command.

Command Modes Privileged.

Examples This example shows how to set the spantree hello time for VLAN 100 to three seconds:

```
Console> (enable) set spantree hello 3 100  
Spantree 100 hello time set to 3 seconds.  
Console> (enable)
```

Related Commands [show spantree](#)

set spantree macreduction

Use the **set spantree macreduction** command to enable or disable the spanning tree MAC address reduction feature.

set spantree macreduction enable | disable

Syntax Description	enable	disable
	Keyword to enable MAC address reduction.	Keyword to disable MAC address reduction.

Defaults The default is MAC address reduction is disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The MAC address reduction feature is used to enable extended-range VLAN identification. You cannot disable this feature if extended range VLANs exist.

Examples This example shows how to disable the MAC address reduction feature:

```
Console> (enable) set spantree macreduction disable
MAC address reduction disabled
Console> (enable)
```

Related Commands [show spantree](#)

set spantree maxage

Use the **set spantree maxage** command to set the bridge maximum aging time for a VLAN.

```
set spantree maxage agingtime [vlan]
```

Syntax Description	<i>agingtime</i>	Maximum number of seconds that the system retains the information received from other bridges through Spanning Tree Protocol; valid values are from 6 to 40 seconds.
	<i>vlan</i>	(Optional) Number of the VLAN; if a VLAN number is not specified, VLAN 1 is assumed; valid values are from 1 to 1005 .

Defaults The default configuration is 20 seconds for all VLANs.

Command Types Switch command.

Command Modes Privileged.

Examples This example shows how to set the maximum aging time for VLAN 1000 to 25 seconds:

```
Console> (enable) set spantree maxage 25 1000  
Spantree 1000 max aging time set to 25 seconds.  
Console> (enable)
```

Related Commands [show spantree](#)

set spantree multicast-address

Use the **set spantree multicast-address** command to specify the bridge functional address instead of the IEEE Spanning Tree Protocol address when you configure a TrBRF to use the IEEE Spanning Tree Protocol.

```
set spantree multicast-address trbrf_num {ieee | ibm}
```

Syntax Description	<table border="1"> <tbody> <tr> <td><i>trbrf_num</i></td> <td>Number of the TrBRF for which you are setting the address.</td> </tr> <tr> <td>ieee</td> <td>Keyword to specify use of the IEEE Spanning Tree Protocol address.</td> </tr> <tr> <td>ibm</td> <td>Keyword to specify use of the IBM Spanning Tree Protocol address.</td> </tr> </tbody> </table>	<i>trbrf_num</i>	Number of the TrBRF for which you are setting the address.	ieee	Keyword to specify use of the IEEE Spanning Tree Protocol address.	ibm	Keyword to specify use of the IBM Spanning Tree Protocol address.
<i>trbrf_num</i>	Number of the TrBRF for which you are setting the address.						
ieee	Keyword to specify use of the IEEE Spanning Tree Protocol address.						
ibm	Keyword to specify use of the IBM Spanning Tree Protocol address.						
Defaults	The default configuration is IEEE.						
Command Types	Switch command.						
Command Modes	Privileged.						
Usage Guidelines	This command applies only to Token Ring modules and only to a TrBRF that runs IEEE Spanning Tree Protocol.						
Examples	<p>The following example shows how to specify the bridge functional address to be used:</p> <pre>Console> (enable) set spantree multicast-address 1 ibm</pre>						
Related Commands	show spantree						

set spantree portcost

Use the **set spantree portcost** command to set the path cost for a port or TrCRF.

```
set spantree portcost {mod/port | trcrf} cost
```

Syntax Description		
<i>mod/port</i>		Number of the module and the port on the module.
<i>trcrf</i>		Number of the TrCRF for which you are setting the path cost.
<i>cost</i>		Number of the path cost; valid values are from 1 to v, with zero (0) the low cost and 65535 the high cost.

Defaults

The default configuration is as follows:

10-Gbps module port cost = 2

1-Gbp module port cost = 4

622-Mbps module port cost = 6

155-Mbps module port cost = 14

100-Mbps module port cost = 19

45-Mbps module port cost = 39

16-Mbp module port cost = 80

10-Mbps module port cost = 100

4-Mbps module port cost = 250

10/100-Mbps module port cost = See “Usage Guidelines”

4/16-Mbps module port cost = See “Usage Guidelines”

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The Spanning Tree Protocol uses port path costs to determine which port to select as a forwarding port. You should assign lower numbers to ports attached to faster media (such as full duplex) and higher numbers to ports attached to slower media.

For 10/100 and 4/16 modules, the default port cost is set automatically depending on the current speed of the port. For example, if a 10/100 port is working at 10 Mbps, the port cost is 100. If the port speed changes to 100 Mbps, the port cost adjusts automatically to 19.

Examples

The following example shows how to set the port cost for port 12 on module 2 to 19:

```
Console> (enable) set spantree portcost 2/12 19  
Spantree port 2/12 path cost set to 19.  
Console> (enable)
```

Related Commands

[show spantree](#)

set spantree portfast

Use the **set spantree portfast** command to allow a port that is connected to a single workstation or PC to start faster when it is connected.

```
set spantree portfast mod/port {enable | disable}
```

Syntax Description	<i>mod/port</i>	Number of the module and the port on the module.
	enable	Keyword to enable the spanning tree port fast-start feature on the port.
	disable	Keyword to disable the spanning tree port fast-start feature on the port.

Defaults The default configuration has the port fast-start feature disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines When a port configured with the **spantree portfast enable** command is connected, the port immediately enters the spanning tree forwarding state instead of going through the normal spanning tree states such as listening and learning. Use this command on ports that are connected to a single workstation or PC only; do not use it on ports that are connected to networking devices such as hubs, routers, switches, bridges, or concentrators.

Examples This example shows how to enable the spanning tree port fast-start feature on port 2 on module 1:

```
Console> (enable) set spantree portfast 1/2 enable
```

```
Warning: Spantree port fast start should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc. to a fast start port can cause temporary spanning tree loops. Use with caution.
```

```
Spantree port 1/2 fast start enabled.
```

```
Console> (enable)
```

Related Commands [show spantree](#)

set spantree portfast bpdu-filter

Use the **set spantree portfast bpdu-filter** command to enable or disable BPDU packet filtering on the switch.

set spantree portfast bpdu-filter {enable | disable}

Syntax Description

enable	Keyword to enable BPDU packet filtering.
disable	Keyword to disable BPDU packet filtering.

Defaults

The default is BPDU packet filtering is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

BPDU packet filtering turns off BPDU transmission on portfast-enabled ports and non-trunking ports.

Examples

This example shows how to enable the BPDU packet filtering:

```
Console> (enable) set spantree portfast bpdu-filter enable
Spantree portfast bpdu-filter enabled on this switch.
Console> (enable)
```

This example shows how to disable the BPDU packet filtering:

```
Console> (enable) set spantree portfast bpdu-filter disable
Spantree portfast bpdu-filter disabled on this switch.
Console> (enable)
```

Related Commands

[show spantree](#)

set spantree portfast bpdu-guard

Use the **set spantree portfast bpdu-guard** command to enable and disable BPDU Guard on the switch. You can prevent loops by moving a non-trunking port configured for PortFast into an ErrDisable state when a BPDU is received on that port.

```
set spantree portfast bpdu-guard {enable | disable}
```

Syntax Description	enable	Keyword to enable the spanning tree PortFast BPDU-Guard.
	disable	Keyword to disable the spanning tree PortFast BPDU-Guard.

Defaults The default configuration has PortFast BPDU-Guard disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines When you enable PortFast BPU-Guard, a non-trunking PortFast-enabled port is moved into an ErrDisable state when a BPDU is received on that port. When PortFast BPDU Guard is disabled, a PortFast-enabled non-trunking port will stay up when it receives BPDUs, which may cause spanning tree loops.

Examples This example shows how to enable the spanning tree PortFast BPDU-Guard:

```
Console> (enable) set spantree portfast bpdu-guard enable  
Spantree portfast bpdu-guard enabled on this switch.  
Console> (enable)
```

This example shows how to disable the spanning tree PortFast BPDU-Guard:

```
Console> (enable) set spantree portfast bpdu-guard disable  
Spantree portfast bpdu-guard disabled on this switch.  
Console> (enable)
```

Related Commands [show spantree summary](#)

set spantree portpri

Use the **set spantree portpri** command to set the bridge priority for a spanning tree port.

```
set spantree portpri {mod/port | trcrf} [priority | trcrf_priority]
```

Syntax Description	
<i>mod/port</i>	Number of the module and the port on the module.
trcrf	Keyword to specify the number of the TrCRF for which you are setting the bridge priority.
<i>priority</i>	(Optional) Number that represents the cost of a link in a spanning tree bridge; valid values are from 0 (high) to 63 (low).
<i>trcrf_priority</i>	(Optional) Number that represents the cost of the TrCRF; valid values are from 0 (high) to 7 (low).

Defaults The default configuration has all ports with bridge priority set to 32.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The specified bridge priority on an ATM port applies to all emulated LANs on that port.

Examples This example shows how to set the priority of port 1 on module 4 to 63:

```
Console> (enable) set spantree portpri 4/1 63
Bridge port 4/1 priority set to 63.
Console> (enable)
```

Related Commands [show spantree](#)

set spantree portstate

Use the **set spantree portstate** command to manually set the state of a TrCRF.

```
set spantree portstate trcrf {block | forward | auto} [trbrf]
```

Syntax Description	
<i>trcrf</i>	Number of the TrCRF for which you are manually setting the state.
block forward auto	Keywords to set the TrCRF to a blocked state (block), forwarding state (forward), or to have the Spanning Tree Protocol determine the correct state automatically (auto).
<i>trbrf</i>	(Optional) Number of the parent TrBRF.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines Use this command only to set the port state when the TrCRF is in SRT mode and the TrBRF is running the IBM Spanning Tree Protocol, or the TrCRF is in SRB mode and the TrBRF is running the IEEE Spanning Tree Protocol.

When you enable Spanning Tree Protocol, every switch in the network goes through the blocking state and the transitory states of listening and learning at power up. If properly configured, the ports then stabilize to the forwarding or blocking state. However, with TrBRFs and TrCRFs, there are two exceptions to this rule that require you to manually set the state of the logical ports of a TrBRF:

- The TrBRF is running the IBM Spanning Tree Protocol, and the TrCRF is in SRT mode.
- The TrBRF is running the IEEE Spanning Tree Protocol, and the TrCRF is in SRB mode.

If either condition exists, use the **set spantree portstate** command to manually set the state of a TrCRF to blocked or forwarding mode or set the Spanning Tree Protocol to determine the correct state automatically.

Examples This example shows the manual setting of TrCRF 900 to a forwarding state:

```
Console> (enable) set spantree portstate 900 forward
reserve_nvram : requested by block = 0
reserve_nvram : granted to block = 0
release_nvram : releasing block = 0
Console> (enable)
```

Related Commands [show spantree](#)
[show spantree portstate](#)

set spantree portvlancost

Use the **set spantree portvlancost** command to assign a lower path cost to a set of VLANs on a port.

```
set spantree portvlancost mod/port [cost cost_value] [preferred_vlans]
```

Syntax Description		
<i>mod/port</i>		Number of the module and the port on the module.
cost <i>cost_value</i>		(Optional) Keyword to indicate the path cost. The port VLAN cost applies only to trunk ports; valid values are from 1 to 65535 .
<i>preferred_vlans</i>		(Optional) Number of the preferred VLAN; valid values are from 1 to 1005 .

Defaults The value specified is used as the path cost of the port for the specified set of VLANs. The rest of the VLANs have a path cost equal to the port path cost, set with the **set spantree portcost** command (if not set, the value is the default path cost of the port).

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines Follow these guidelines when you set the path cost for VLANs on a port:

- The *cost* value specified is used as the path cost of the port for the specified set of VLANs. The rest of the VLANs have a path cost equal to the port path cost set through the **set spantree portcost** command. If not set, the value is the default path cost of the port.
- You must supply a *vlan_list* argument when you first set the cost value. When you subsequently set a new *cost* value, all *cost* values previously set by entering this command are changed to the new *cost* value. If you have never explicitly set a *cost* value for a VLAN by entering this command, the *cost* value for the VLAN does not change.
- If you do not explicitly specify a cost value but cost values were specified previously, the port VLAN cost is set to 1 less than the current port cost for a port. However, this reduction might not assure load balancing in all cases.
- When setting the path cost for extended-range VLANs, you can create a maximum of 64 nondefault entries or create entries until NVRAM is full.

Examples These examples show various ways to use the **set spantree portvlancost** command:

```
Console> (enable) set spantree portvlancost 2/10 cost 25 1-20
Cannot set portvlancost to a higher value than the port cost, 10, for port 2/10.
Console> (enable)
```

```
Console> (enable) set spantree portvlancost 2/10 1-20
Port 2/10 VLANs 1-20 have a path cost of 9.
Console> (enable)
```

```
Console> (enable) set spantree portvlancost 2/10 cost 4 1-20  
Port 2/10 VLANs 1-20 have path cost 4.  
Port 2/10 VLANs 21-1000 have path cost 10.  
Console> (enable)
```

```
Console> (enable) set spantree portvlancost 2/10 cost 6 21  
Port 2/10 VLANs 1-21 have path cost 6.  
Port 2/10 VLANs 22-1000 have path cost 10.  
Console> (enable)
```

These examples show how to use the **set spantree portvlancost** command without explicitly specifying cost:

```
Console> (enable) set spantree portvlancost 1/2  
Port 1/2 VLANs 1-1005 have path cost 3100.  
Console> (enable)
```

```
Console> (enable) set spantree portvlancost 1/2 21  
Port 1/2 VLANs 1-20,22-1005 have path cost 3100.  
Port 1/2 VLANs 21 have path cost 3099.  
Console> (enable)
```

Related Commands

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

set spantree portvlanpri

Use the **set spantree portvlanpri** command to set the port priority for a subset of VLANs in the trunk port.

set spantree portvlanpri *mod/port priority [vlans]*

Syntax Description	
<i>mod/port</i>	Number of the module and the port on the module.
<i>priority</i>	Number that represents the cost of a link in a spanning tree bridge. The priority level is from 0 to 63 , with 0 indicating high priority and 63 indicating low priority.
<i>vlans</i>	(Optional) VLANs that use the specified priority level.

Defaults The default configuration has the port VLAN priority set to 0 with no VLANs specified.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines You can use this command to add VLANs to a specified port priority level. Subsequent attempts to use this command do not replace VLANs that are already set at a specified port priority level.

This feature is not supported for the RSM.

The **set spantree portvlanpri** command applies only to trunk ports. Do not use Token Ring ports as trunk ports. If you enter this command on Token Ring ports, you see this message:

```
Port xx is not a trunk-capable port
```

Examples This example shows how to set the port priority for module 1, port 2, on VLANs 21 to 40:

```
Console> (enable) set spantree portvlanpri 1/2 16 21-40
Port 1/2 vlans 3,6-20,41-1000 using portpri 32
Port 1/2 vlans 1-2,4-5,21-40 using portpri 16
Console> (enable)
```

Related Commands [clear spantree portvlanpri](#)
[show spantree](#)