

# set rcp username

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

**set rcp username** *username*

---

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

---

---

<b>Defaults</b>	There are no default settings for this command.
-----------------	---

---

---

<b>Command Types</b>	Switch command.
----------------------	-----------------

---

---

<b>Command Modes</b>	Privileged.
----------------------	-------------

---

---

<b>Usage Guidelines</b>	The username must be different from “root” and not a null string. The only case where you cannot configure the rcp <i>username</i> is for the VMPS database where you will use an rcp VMPS username.
-------------------------	--

---

---

<b>Examples</b>	This example shows how to set the username for rcp:
-----------------	---

---

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

# set rgmp

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

**set rgmp { enable | disable }**

---

## Syntax Description

<b>enable</b>	Keyword to enable RGMP on the switch.
<b>disable</b>	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

**show rgmp group**  
**show rgmp statistics**  
**clear rgmp statistics**  
**set igmp**

# set rspan

Use the **set rspan** command set to create remote SPAN sessions.

```
set rspan disable source [rspan_vlan | all]
```

```
set rspan disable destination [mod/port | all]
```

```
set rspan source {src_mod/src_ports... | vlangs... | sc0} {rspan_vlan} [rx | tx | both]  
[multicast {enable | disable}] [filter vlangs...] [create]
```

```
set rspan destination {mod/port} {rspan_vlan} [inpkts {enable | disable}]  
[learning {enable | disable}] [create]
```

## Syntax Description

<b>disable source</b>	Keywords to disable remote SPAN source information.
<i>rspan_vlan</i>	(Optional) Remote SPAN VLAN.
<b>all</b>	(Optional) Keyword to disable all remote SPAN source or destination sessions.
<b>disable destination</b>	Keywords to disable remote SPAN destination information.
<i>mod/port</i>	(Optional) Remote SPAN destination port.
<i>src_mod/src_ports...</i>	Monitored ports (remote SPAN source).
<i>vlangs...</i>	Monitored VLANs (remote SPAN source).
<b>sc0</b>	Keyword to specify the inband port is a valid source.
<b>rx</b>	(Optional) Keyword to specify that information received at the source (ingress SPAN) is monitored.
<b>tx</b>	(Optional) Keyword to specify that information transmitted from the source (egress SPAN) is monitored.
<b>both</b>	(Optional) Keyword to specify that information both transmitted from the source (ingress SPAN) and received (egress SPAN) at the source are monitored.
<b>multicast enable</b>	(Optional) Keywords to enable monitoring multicast traffic (egress traffic only).
<b>multicast disable</b>	(Optional) Keywords to disable monitoring multicast traffic (egress traffic only).
<b>filter</b> <i>vlangs</i>	(Optional) Keywords to monitor traffic on selected VLANs on source trunk ports.
<b>create</b>	(Optional) Keyword to create a new remote SPAN session instead of overwriting the previous SPAN session.
<b>inpkts enable</b>	(Optional) Keywords to allow the remote SPAN destination port to receive normal ingress traffic (from the network to the bus) while forwarding the remote SPAN traffic.

<b>inpkts disable</b>	(Optional) Keywords to disable the receiving of normal inbound traffic on the remote SPAN destination port.
<b>learning enable</b>	(Optional) Keywords to enable learning for the remote SPAN destination port.
<b>learning disable</b>	(Optional) Keywords to disable learning for the remote SPAN destination port.

### Defaults

The defaults are as follows:

- Remote SPAN is disabled.
- No VLAN filtering.
- Monitoring multicast traffic is enabled.
- Learning is enabled.
- inpkts is disabled.

### Command Types

Switch command.

### Command Modes

Privileged.

### Usage Guidelines

The *rspan\_vlan* variable is optional in the **set rspan disable source** command and required in the **set rspan source** and **set rspan destination** command set.

After you enable SPAN, system defaults are used if no parameters were ever set. If you changed parameters, these are stored in NVRAM, and the new parameters are used.

Use a network analyzer to monitor ports.

Use the **inpkts** keyword with the **enable** option to allow the remote SPAN destination port to receive normal incoming traffic in addition to the traffic mirrored from the remote SPAN source. Use the **disable** option to prevent the remote SPAN destination port from receiving normal incoming traffic.

You can specify an MSM port as the remote SPAN source port. However, you cannot specify an MSM port as the remote SPAN destination port.

When you enable the **inpkts** option, a warning message notifies you that the destination port does not join STP and may cause loops if this option is enabled.

If you do not specify the keyword **create** and you have only one session, the session will be overwritten. If a matching *rspan\_vlan* or destination port exists, the particular session will be overwritten (with or without specifying **create**). If you specify the keyword **create** and there is no matching *rspan\_vlan* or destination port, the session will be created.

Each switch can source only one remote SPAN session (ingress, egress, or both). When you configure a remote ingress or bidirectional SPAN session in a source switch, the limit for local ingress or bidirectional SPAN session is reduced to one. There are no limits on the number of remote SPAN sessions carried across the network within the remote SPAN session limits.

You can configure any VLAN as a remote SPAN VLAN as long as these conditions are met:

- The same remote SPAN VLAN is used for a remote SPAN session in the switches.

- All the participating switches have appropriate hardware and software.
- No unwanted access port is configured in the remote SPAN VLAN.

---

**Examples**

This example shows how to disable all enabled source sessions:

```
Console> (enable) set rspan disable source all  
This command will disable all remote span source session(s).  
Do you want to continue (y/n) [n]? y  
Disabled monitoring of all source(s) on the switch for remote span.  
Console> (enable)
```

This example shows how to disable one source session to a specific VLAN:

```
Console> (enable) set rspan disable source 903  
Disabled monitoring of all source(s) on the switch for rspan_vlan 903.  
Console> (enable)
```

This example shows how to disable all enabled destination sessions:

```
Console> (enable) set rspan disable destination all  
This command will disable all remote span destination session(s).  
Do you want to continue (y/n) [n]? y  
Disabled monitoring of remote span traffic on ports 9/1,9/2,9/3,9/4,9/5,9/6.  
Console> (enable)
```

This example shows how to disable one destination session to a specific port:

```
Console> (enable) set rspan disable destination 4/1  
Disabled monitoring of remote span traffic on port 4/1.  
Console> (enable)
```

---

**Related Commands**

**show rspan**

# set security acl capture-ports

Use the **set security acl capture-ports** command to set the ports (specified with the **capture** option in the **set security acl ip**, **set security acl ipx**, and **set security acl mac** commands) to show traffic captured on these ports.

```
set security acl capture-ports {mod/ports...}
```

---

## Syntax Description

*mod/ports...* Module and port number.

---



---

## Defaults

This command has no default setting.

---

## Command Types

Switch command.

---

## Command Modes

Privileged.

---

## Usage Guidelines

Configurations you make by entering this command are saved in NVRAM. This command *does not* require that you enter the **commit** command.

The module and port specified in this command are added to the current ports configuration list.

This command works with Ethernet ports only; you cannot set ATM ports.

The ACL capture will not work unless the capture port is in the spanning tree forwarding state for the VLAN.

---

## Examples

This example shows how to set a port to capture traffic:

```
Console> (enable) set security acl capture 3/1
Successfully set 3/1 to capture ACL traffic.
Console> (enable)
```

This example shows how to set multiple ports to capture traffic:

```
Console> (enable) set security acl capture 1/1-10
Successfully set the following ports to capture ACL traffic: 1/1-2.
Console> (enable)
```

---

## Related Commands

**clear security acl capture-ports**  
**show security acl capture-ports**

# set security acl ip

Use the **set security acl ip** command set to create a new entry in a standard IP VACL and append the new entry at the end of VACL.

```
set security acl ip {acl_name} {permit | deny} {src_ip_spec} [before editbuffer_index |
modify editbuffer_index]
```

```
set security acl ip {acl_name} {permit | deny | redirect mod_num/port_num} {protocol}
{src_ip_spec} {dest_ip_spec} [precedence precedence] [tos tos] [capture] [before
editbuffer_index | modify editbuffer_index]
```

```
set security acl ip {acl_name} {permit | deny | redirect {mod_num/port_num}} [ip | 0]
{src_ip_spec} {dest_ip_spec} [precedence precedence] [tos tos] [capture]
[before editbuffer_index | modify editbuffer_index]
```

```
set security acl ip {acl_name} {permit | deny | redirect {mod_num/port_num}} [icmp | 1]
{src_ip_spec} {dest_ip_spec} [icmp_type] [icmp_code] | [icmp_message]
[precedence precedence] [tos tos] [capture] [before editbuffer_index |
modify editbuffer_index]
```

```
set security acl ip {acl_name} {permit | deny | redirect {mod_num/port_num}} [igmp | 2]
{src_ip_spec} {dest_ip_spec} [igmp_type] [precedence precedence] [tos tos] [capture]
[before editbuffer_index | modify editbuffer_index]
```

```
set security acl ip {acl_name} {permit | deny | redirect {mod_num/port_num}} [tcp | 6]
{src_ip_spec} [operator port [port]] {dest_ip_spec} [operator port [port]] [established]
[precedence precedence] [tos tos] [capture] [before editbuffer_index |
modify editbuffer_index]
```

```
set security acl ip {acl_name} {permit | deny | redirect {mod_num/port_num}} [udp | 17]
{src_ip_spec} [operator port [port]] {dest_ip_spec} [operator port [port]]
[precedence precedence] [tos tos] [capture] [before editbuffer_index |
modify editbuffer_index]
```

Syntax Description		
<i>acl_name</i>		Unique name that identifies the lists to which the entry belongs.
<b>permit</b>		Keyword to allow traffic from the source IP address.
<b>deny</b>		Keyword to block traffic from the source IP address.
<i>src_ip_spec</i>		Source IP address and the source mask. See the “Usage Guidelines” section for the format.
<b>before</b> <i>editbuffer_index</i>		(Optional) Keyword and variable to insert the new ACE in front of another ACE.
<b>modify</b> <i>editbuffer_index</i>		(Optional) Keyword and variable to replace an ACE with the new ACE.
<b>redirect</b>		Keyword to specify to which switched ports the packet is redirected.
<i>mod_num/port_num</i>		Number of the module and port.
<i>protocol</i>		Keyword or number of an IP protocol; valid numbers are from 0 to 255 representing an IP protocol number. See the “Usage Guidelines” section for the list of valid keywords.

<i>dest_ip_spec</i>	Destination IP address and the destination mask. See the “Usage Guidelines” section for the format.
<b>precedence</b> <i>precedence</i>	(Optional) Keyword and variable to specify the precedence level; valid values are from 0 to 7 or by name. See the “Usage Guidelines” section for a list of valid names.
<b>tos</b> <i>tos</i>	(Optional) Keyword and variable to specify the type of service level; valid values are from 0 to 15 or by name. See the “Usage Guidelines” section for a list of valid names.
<b>capture</b>	(Optional) Keyword to specify packets are switched normally and captured; <b>permit</b> must also be enabled.
<b>ip</b>   <b>0</b>	(Optional) Keyword or number to match any Internet Protocol packets.
<b>icmp</b>   <b>1</b>	(Optional) Keyword or number to match ICMP packets.
<i>icmp-type</i>	(Optional) ICMP message type name or a number; valid values are from 0 to 255. See the “Usage Guidelines” section for a list of valid names.
<i>icmp-code</i>	(Optional) ICMP message code name or a number; valid values are from 0 to 255. See the “Usage Guidelines” section for a list of valid names.
<i>icmp-message</i>	(Optional) ICMP message type name or ICMP message type and code name. See the “Usage Guidelines” section for a list of valid names.
<b>igmp</b>   <b>2</b>	(Optional) Keyword or number to match IGMP packets.
<i>igmp-type</i>	(Optional) IGMP message type or message name; valid message type numbers are from 0 to 15. See the “Usage Guidelines” section for a list of valid names and corresponding numbers.
<b>tcp</b>   <b>6</b>	(Optional) Keyword or number to match TCP packets.
<i>operator</i>	(Optional) Operands; valid values include <b>lt</b> (less than), <b>gt</b> (greater than), <b>eq</b> (equal), <b>neq</b> (not equal), and <b>range</b> (inclusive range).
<i>port</i>	(Optional) Number or name of a TCP or UDP port; valid port numbers are from 0 to 65535. See the “Usage Guidelines” section for a list of valid names.
<b>established</b>	(Optional) Keyword to specify an established connection; used only for TCP protocol.
<b>udp</b>   <b>17</b>	(Optional) Keyword or number to match UDP packets.

**Defaults**

There are no default ACLs and no default ACL-VLAN mappings.

**Command Types**

Switch command.

**Command Modes**

Privileged.

**Usage Guidelines**

Configurations you make by entering this command are saved to NVRAM and hardware only after you enter the **commit** command. Enter ACEs in batches and then enter the **commit** command to save them in NVRAM and in the hardware.

If you use the **redirect** keyword, the destination must be 255.255.255.255.

If you use the **capture** keyword, the ports that capture the traffic and transmit out are specified by entering the **set security acl capture-ports** command.

When you enter the ACL name, follow these naming conventions:

- Maximum of 32 characters long and may include a-z, A-Z, 0-9, the dash character (-), the underscore character (\_), and the period character (.)
- Must start with an alpha character and must be unique across all ACLs of all types
- Case sensitive
- Cannot be a number
- Must not be a keyword; keywords to avoid are all, default-action, map, help, and editbuffer

When you specify the source IP address and the source mask, use the form *source\_ip\_address source\_mask* and follow these guidelines:

- The *source\_mask* is required; 0 indicates a care bit, 1 indicates a don't-care bit.
- Use a 32-bit quantity in four-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** source as an abbreviation for a *source* and *source-wildcard* of source 0.0.0.0.

When you enter a destination IP address and the destination mask, use the form *destination\_ip\_address destination\_mask*. The destination mask is required.

- Use a 32-bit quantity in a four-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host**/source as an abbreviation for a *destination* and *destination-wildcard* of destination 0.0.0.0.

Valid names for *precedence* are critical, flash, flash-override, immediate, internet, network, priority, and routine.

Valid names for *tos* are max-reliability, max-throughput, min-delay, min-monetary-cost, and normal.

Valid *protocol* keywords include **icmp** (1), **igmp** (2), **ip** (0), **ipinip** (4), **tcp** (6), **udp** (17), **igrp** (9), **eigrp** (88), **gre** (47), **nos** (94), **ospf** (89), **ahp** (51), **esp** (50), **pcp** (108), and **pim** (103). The IP number is displayed in parentheses. Use the keyword **ip** to match any Internet Protocol.

ICMP packets that are matched by ICMP message type can also be matched by the ICMP message code.

Valid names for *icmp\_type* and *icmp\_code* are administratively-prohibited, alternate-address, conversion-error, dod-host-prohibited, dod-net-prohibited, echo, echo-reply, general-parameter-problem, host-isolated, host-precedence-unreachable, host-redirect, host-tos-redirect, host-tos-unreachable, host-unknown, host-unreachable, information-reply, information-request, mask-reply, mask-request, mobile-redirect, net-redirect, net-tos-redirect, net-tos-unreachable, net-unreachable, network-unknown, no-room-for-option, option-missing, packet-too-big, parameter-problem, port-unreachable, precedence-unreachable, protocol-unreachable,

reassembly-timeout, redirect, router-advertisement, router-solicitation, source-quench, source-route-failed, time-exceeded, timestamp-reply, timestamp-request, traceroute, ttl-exceeded, and unreachable.

Valid names and corresponding numbers for *igmp\_message* are dvmrp (3), host-query (1), host-report (2), pim (4), and trace (5).

If the operator is positioned after the source and source-wildcard, it must match the source port. If the operator is positioned after the destination and destination-wildcard, it must match the destination port. The range operator requires two port numbers. All other operators require one port number.

TCP port names can be used only when filtering TCP. Valid names for TCP ports are bgp, chargen, daytime, discard, domain, echo, finger, ftp, ftp-data, gopher, hostname, irc, klogin, kshell, lpd, nntp, pop2, pop3, smtp, sunrpc, syslog, tacacs-ds, talk, telnet, time, uucp, whois, and www.

UDP port names can be used only when filtering UDP. Valid names for UDP ports are biff, bootpc, bootps, discard, dns, dnsix, echo, mobile-ip, nameserver, netbios-dgm, netbios-ns, ntp, rip, snmp, snmptrap, sunrpc, syslog, tacacs-ds, talk, tftp, time, who, and xdmcp.

The number listed with the protocol type is the layer protocol number (for example, **udp | 17**).

If no layer protocol number is entered, you can enter the following syntax:

```
set security acl ip {acl_name} {permit | deny} {src_ip_spec} [before editbuffer_index |
  modify editbuffer_index]
```

If a Layer 4 protocol is specified, you can enter the following syntax:

```
set security acl ip {acl_name} {permit | deny | redirect mod_num/port_num} {protocol}
  {src_ip_spec} {dest_ip_spec} [precedence precedence] [tos tos] [capture]
  [before editbuffer_index | modify editbuffer_index]
```

For IP, you can enter the following syntax:

```
set security acl ip {acl_name} {permit | deny | redirect {mod_num/port_num}} [ip | 0]
  {src_ip_spec} {dest_ip_spec} [precedence precedence] [tos tos] [capture]
  [before editbuffer_index | modify editbuffer_index]
```

For ICMP, you can enter the following syntax:

```
set security acl ip {acl_name} {permit | deny | redirect {mod_num/port_num}} [icmp | 1]
  {src_ip_spec} {dest_ip_spec} [icmp_type] [icmp_code] | [icmp_message]
  [precedence precedence] [tos tos] [capture] [before editbuffer_index |
  modify editbuffer_index]
```

For IGMP, you can use the following syntax:

```
set security acl ip {acl_name} {permit | deny | redirect {mod_num/port_num}} [igmp | 2]
  {src_ip_spec} {dest_ip_spec} [igmp_type] [precedence precedence] [tos tos] [capture]
  [before editbuffer_index | modify editbuffer_index]
```

For TCP, you can use the following syntax:

```
set security acl ip {acl_name} {permit | deny | redirect {mod_num/port_num}} [tcp | 6]
  {src_ip_spec} [operator port [port]] {dest_ip_spec} [operator port [port]] [established]
  [precedence precedence] [tos tos] [capture] [before editbuffer_index |
  modify editbuffer_index]
```

For UDP, you can use the following syntax:

```
set security acl ip {acl_name} {permit | deny | redirect {mod_num/port_num}} [udp | 17]
  {src_ip_spec} [operator port [port]] {dest_ip_spec} [operator port [port]]
  [precedence precedence] [tos tos] [capture] [before editbuffer_index |
  modify editbuffer_index]
```

## Examples

These examples show different ways to use the **set security acl ip** commands to configure IP security ACL:

```
Console> (enable) set security acl ip IPACL1 deny 1.2.3.4 0.0.0.0
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

```
Console> (enable) set security acl ip IPACL1 deny host 171.3.8.2 before 2
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

```
Console> (enable) set security acl ip IPACL1 permit any any
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

```
Console> (enable) set security acl ip IPACL1 redirect 3/1 ip 3.7.1.2 0.0.0.255 host
255.255.255.255 precedence 1 tos min-delay
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

```
Console> (enable) set security acl ip IPACL1 permit ip host 60.1.1.1 host 60.1.1.98
capture
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
```

## Related Commands

```
clear security acl
clear security acl capture-ports
clear security acl map
commit
show security acl
show security acl capture-ports
set security acl map
set security acl capture-ports
```

## set security acl ipx

Use the **set security acl ipx** command to create a new entry in a standard IPX VACL and to append the new entry at the end of the VACL.

```
set security acl ipx {acl_name} {permit | deny | redirect mod_num/port_num} {protocol}
  {src_net} [dest_net.dest_node] [[dest_net_mask.]dest_node_mask]] [capture]
  [before editbuffer_index | modify editbuffer_index]
```

Syntax Description		
<i>acl_name</i>		Unique name that identifies the list to which the entry belongs.
<b>permit</b>		Keyword to allow traffic from the specified source IPX address.
<b>deny</b>		Keyword to block traffic from the specified source IPX address.
<b>redirect</b>		Keyword to redirect traffic from the specified source IPX address.
<i>mod_num/port_num</i>		Number of the module and port.
<i>protocol</i>		Keyword or number of an IPX protocol; valid values are from 0 to 255 representing an IPX protocol number. See the “Usage Guidelines” section for a list of valid keywords and corresponding numbers.
<i>src_net</i>		Number of the network from which the packet is being sent. See the “Usage Guidelines” section for format guidelines.
<i>dest_net</i> .		(Optional) Number of the network from which the packet is being sent.
<i>.dest_node</i>		(Optional) Node on destination-network to which the packet is being sent.
<i>dest_net_mask</i> .		(Optional) Mask to be applied to the destination network. See the “Usage Guidelines” section for format guidelines.
<i>dest_node_mask</i>		(Optional) Mask to be applied to the destination-node. See the “Usage Guidelines” section for format guidelines.
<b>capture</b>		(Optional) Keyword to specify packets are switched normally and captured.
<b>before</b> <i>editbuffer_index</i>		(Optional) Keyword and variable to insert the new ACE in front of another ACE.
<b>modify</b> <i>editbuffer_index</i>		(Optional) Keyword and variable to replace an ACE with the new ACE.

**Defaults** There are no default ACLs and no default ACL-VLAN mappings.

**Command Types** Switch command.

**Command Modes** Privileged.

## Usage Guidelines

Configurations you make by entering this command are saved to NVRAM and hardware only after you enter the **commit** command. Enter ACEs in batches and then enter the **commit** command to save all of them in NVRAM and in the hardware.

If you use the **capture** keyword, the ports that capture the traffic and transmit out are specified by entering the **set security acl capture-ports** command.

When you enter the ACL name, follow these naming conventions:

- Maximum of 32 characters long and may include a-z, A-Z, 0-9, the dash character (-), the underscore character (\_), and the period character (.)
- Must start with an alpha character and must be unique across all ACLs of all types
- Case sensitive
- Cannot be a number
- Must not be a keyword; keywords to avoid are all, default-action, map, help, and editbuffer

Valid *protocol* keywords include **ncp** (17), **netbios** (20), **rip** (1), **sap** (4), and **spx** (5).

The *src\_net* and *dest\_net* variables are eight-digit hexadecimal numbers that uniquely identify network cable segments. When you specify the *src\_net* or *dest\_net*, use the following guidelines:

- It can be a number in the range 0 to FFFFFFFF. A network number of -1 or **any** matches all networks.
- You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.

The *.dest\_node* is a 48-bit value represented by a dotted triplet of 4-digit hexadecimal numbers (xxxx.xxxx.xxxx).

The *dest\_net\_mask* is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must be immediately followed by a period, which must in turn be immediately followed by the destination-node-mask. You can enter this value only when *dest\_node* is specified.

The *dest\_node\_mask* is a 48-bit value represented as a dotted triplet of 4-digit hexadecimal numbers (xxxx.xxxx.xxxx). Place ones in the bit positions you want to mask. You can enter this value only when *dest\_node* is specified.

The *dest\_net\_mask* is an eight-digit hexadecimal number that uniquely identifies the network cable segment. It can be a number in the range 0 to FFFFFFFF. A network number of -1 or **any** matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA. Following are *dest\_net\_mask* examples:

- 123A
- 123A.1.2.3
- 123A.1.2.3 ffff.fff.fff
- 1.2.3.4 ffff.fff.fff.fff

Use the **show security acl** command to display the list.

## Examples

This example shows how to block traffic from a specified source IP address:

```
Console> (enable) set security acl ipx IPXACL1 deny 1.a
IPXACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

■ set security acl ipx

---

**Related Commands**

**clear security acl**  
**clear security acl capture-ports**  
**clear security acl map**  
**commit**  
**show security acl**  
**show security acl capture-ports**  
**set security acl map**  
**set security acl capture-ports**

# set security acl mac

Use the **set security acl mac** command to create a new entry in a non-IP or non-IPX protocol VACL and to append the new entry at the end of the VACL.

```
set security acl mac {acl_name} {permit | deny} {src_mac_addr_spec}
  {dest_mac_addr_spec} [ether-type] [capture] [before editbuffer_index |
  modify editbuffer_index]
```

Syntax Description	
<i>acl_name</i>	Unique name that identifies the list to which the entry belongs.
<b>permit</b>	Keyword to allow traffic from the specified source MAC address.
<b>deny</b>	Keyword to block traffic from the specified source MAC address.
<i>src_mac_addr_spec</i>	Source MAC address and mask in the form <i>source_mac_address source_mac_address_mask</i> .
<i>dest_mac_addr_spec</i>	Destination MAC address and mask.
<i>ether-type</i>	(Optional) Number or name that matches the ethertype for Ethernet-encapsulated packets; valid values are 0x0600, 0x0601, 0x0BAD, 0x0BAF, 0x6000-0x6009, 0x8038-0x8042, 0x809b, and 0x80f3. See the “Usage Guidelines” section for a list of valid names.
<b>capture</b>	(Optional) Keyword to specify packets are switched normally and captured.
<b>before editbuffer_index</b>	(Optional) Keyword and variable to insert the new ACE in front of another ACE.
<b>modify editbuffer_index</b>	(Optional) Keyword and variable to replace an ACE with the new ACE.

**Defaults** There are no default ACLs and no default ACL-VLAN mappings.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** Configurations you make by entering this command are saved to NVRAM and hardware only after you enter the **commit** command. Enter ACEs in batches and then enter the **commit** command to save all of them in NVRAM and in the hardware.

If you use the **capture** keyword, the ports that capture the traffic and transmit out are specified by entering the **set security acl capture-ports** command.

When you enter the ACL name, follow these naming conventions:

- Maximum of 32 characters long and may include a-z, A-Z, 0-9, the dash character (-), the underscore character (\_), and the period character (.)
- Must start with an alpha character and must be unique across all ACLs of all types

- Case sensitive
- Cannot be a number
- Must not be a keyword; keywords to avoid are all, default-action, map, help, and editbuffer

The *src\_mac\_addr\_spec* is a 48-bit source MAC address and mask and entered in the form of *source\_mac\_address source\_mac\_address\_mask* (for example, 08-11-22-33-44-55 ff-ff-ff-ff-ff). Place ones in the bit positions you want to mask. When you specify the *src\_mac\_addr\_spec*, follow these guidelines:

- The *source\_mask* is required; 0 indicates a care bit, 1 indicates a don't care bit.
- Use a 32-bit quantity in four-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** source as an abbreviation for a *source* and *source-wildcard* of source 0.0.0.0.

The *dest\_mac\_spec* is a 48-bit destination MAC address and mask and entered in the form of *dest\_mac\_address dest\_mac\_address\_mask* (for example, 08-00-00-00-02-00/ff-ff-ff-00-00-00). Place ones in the bit positions you want to mask. The destination mask is mandatory. When you specify the *dest\_mac\_spec*, use the following guidelines:

- Use a 48-bit quantity in 6-part dotted-hexadecimal format for source address and mask.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0-0-0-0-0-0 ff-ff-ff-ff-ff-ff.
- Use **host** source as an abbreviation for a *destination* and *destination-wildcard* of destination 0-0-0-0-0-0.

Valid names for Ethertypes (and corresponding numbers) are Ethertalk (0x809B), AARP (0x8053), dec-mop-dump (0x6001), dec-mop-remote-console (0x6002), dec-phase-iv (0x6003), dec-lat (0x6004), dec-diagnostic-protocol (0x6005), dec-lavc-sca (0x6007), dec-amber (0x6008), dec-mumps (0x6009), dec-lanbridge (0x8038), dec-dsm (0x8039), dec-netbios (0x8040), dec-msdos (0x8041), banyan-vines-echo (0x0baf), xerox-ns-idp (0x0600), and xerox-address-translation (0x0601).

Use the **show security acl** command to display the list.

---

## Examples

This example shows how to block traffic to an IP address:

```
Console> (enable) set security acl mac MACACL1 deny 01-02-02-03-04-05
MACACL1 editbuffer modified. User 'commit' command to apply changes.
Console> (enable)
```

---


## Related Commands

```
clear security acl
clear security acl capture-ports
clear security acl map
commit
show security acl
show security acl capture-ports
set security acl map
set security acl capture-ports
```

# set security acl map

Use the **set security acl map** command to map an existing VACL to a VLAN.

```
set security acl map acl_name vlan
```

<b>Syntax Description</b>	<i>acl_name</i> Unique name that identifies the list to which the entry belongs.
	<i>vlan</i> Number of the VLAN to be mapped to the VACL.
<b>Defaults</b>	There are no default ACLs and no default ACL-VLAN mappings.
<b>Command Types</b>	Switch command.
<b>Command Modes</b>	Privileged.
<b>Usage Guidelines</b>	<p>Configurations you make by entering this command are saved in NVRAM. This command <i>does not</i> require that you enter the <b>commit</b> command. Each VLAN can be mapped to only one ACL of each type (IP, IPX, and MAC). An ACL can be mapped to a VLAN only after you have committed the ACL.</p> <p>When you enter the ACL name, follow these naming conventions:</p> <ul style="list-style-type: none"> <li>• Maximum of 32 characters long and may include a-z, A-Z, 0-9, the dash character (-), the underscore character (_), and the period character (.)</li> <li>• Must start with an alpha character and must be unique across all ACLs of all types</li> <li>• Case sensitive</li> <li>• Cannot be a number</li> <li>• Must not be a keyword; keywords to avoid are all, default-action, map, help, and editbuffer</li> </ul>
<b>Caution</b>	 <p>Use the <b>copy</b> command to save the ACL configuration to Flash memory.</p>

## Examples

This example shows how to map an existing VACL to a VLAN:

```
Console> (enable) set security acl map IPACL1 1
ACL IPACL1 mapped to vlan 1
Console> (enable)
```

This example shows the output if you try to map an ACL that has not been committed:

```
Console> (enable) set security acl map IPACL1 1
Commit ACL IPACL1 before mapping.
Console> (enable)
```

This example shows the output if you try to map an ACL that is already mapped to a VLAN for the ACL type (IP, IPX, or MAC):

```
Console> (enable) set security acl map IPACL2 1
Mapping for this type already exists for this VLAN.
Console> (enable)
```

---

**Related Commands**

**clear security acl**  
**clear security acl map**  
**commit**  
**show security acl**

## set snmp access

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

# 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]
```

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

**Defaults** The default is the following communities and access types are 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.

To support the access types, you also need to configure four MIB tables: vacmContextTable, vacmSecurityToGroupTable, vacmAccessTable, and vacmViewTreeFamilyTable. Use the **clear config snmp** command to reset these tables to the default values.

**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 to yappledapple.
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 config**  
**show snmp**

# set snmp extendedrmon netflow

Use the **set snmp extendedrmon netflow** command to enable or disable the SNMP extended RMON support for the NAM.

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

Syntax Description	enable	disable	mod
	enable	disable	mod
	Keyword to enable the extended RMON support.	Keyword to disable the extended RMON support.	Module number of the extended RMON NAM.

**Defaults** The default is SNMP-extended RMON NetFlow is disabled.

**Command Types** Switch command.

**Command Modes** Privileged.

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

```
Console> (enable) set snmp extendedrmon netflow enable 2
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 2
Snm extended RMON netflow disabled
Console> (enable)
```

This example shows the response when the SNMP-extended RMON NetFlow feature is not supported:

```
Console> (enable) set snmp extendedrmon enable 4
NAM card is not installed.
Console> (enable)
```

**Related Commands** **set snmp rmon**  
**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		
<b>-hex</b>	(Optional) Keyword to display the <i>groupname</i> and <i>username</i> in a hexadecimal format.	
<i>groupname</i>	Name of the SNMP group that defines an access control; the maximum length is 32 bytes.	
<b>user</b>	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.	
<b>security-model</b> <b>v1</b>   <b>v2c</b>   <b>v3</b>	Keywords to specify security-model v1, v2c, or v3.	
<b>volatile</b>	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.	
<b>nonvolatile</b>	(Optional) Keyword to specify that the storage type is defined 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		
<b>-hex</b>	(Optional) Keyword to display the <i>notifyname</i> and <i>notifytag</i> in a hexadecimal format.	
<i>notifyname</i>	Identifier to index the <i>snmpNotifyTable</i> .	
<b>tag</b>	Keyword to specify the tag name in the taglist.	
<i>notifytag</i>	Name of entries in the <i>snmpTargetAddrTable</i> .	
<b>trap</b>	(Optional) Keyword to specify all messages that contain <i>snmpv2-Trap</i> PDUs.	
<b>inform</b>	(Optional) Keyword to specify all messages that contain <i>InfoRequest</i> PDUs.	
<b>volatile</b>	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.	
<b>nonvolatile</b>	(Optional) Keyword to specify that the storage type is defined 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**.
- 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 is RMON support is disabled.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** RMON statistics are collected on a segment basis.

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

When you enable RMON, the supported RMON groups for Ethernet ports are Statistics, History, Alarms, and Events as specified in RFC 1757.

Use of this command requires a separate software license.

**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 port counters**

# 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		
<b>-hex</b>	(Optional) Keyword to display <i>addrname</i> , <i>paramsname</i> , <i>tagvalue</i> , and <i>tag</i> in a hexadecimal format.	
<i>addrname</i>	Unique identifier to index the snmpTargetAddrTable; the maximum length is 32 bytes.	
<b>param</b>	Keyword to specify an entry in the snmpTargetParamsTable that 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.	
<b>udpport</b> <i>port</i>	(Optional) Keyword and variable to specify which UDP port of the target host to use.	
<b>timeout</b> <i>value</i>	(Optional) Keyword and variable to specify the number of timeouts.	
<b>retries</b> <i>value</i>	(Optional) Keyword and variable to specify the number of retries.	
<b>volatile</b>	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.	
<b>nonvolatile</b>	(Optional) Keyword to specify that the storage type is defined as persistent memory and the content remains after the device is turned off and on again.	
<b>taglist</b> <i>tag</i>	(Optional) Keyword and variable to specify a tag name in the taglist.	
<b>tag</b> <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		
<b>-hex</b>	(Optional) Keyword to display the <i>paramsname</i> and <i>username</i> in a hexadecimal format.	
<i>paramsname</i>	Name of the parameter in the snmpTargetParamsTable; the maximum length is 32 bytes.	
<b>user</b>	Keyword to specify the SNMP group username.	
<i>username</i>	Name of the SNMP user that belongs to the SNMP group; the maximum length is 32 bytes.	
<b>security-model v1   v2c</b>	Keywords to specify security-model v1 or v2c.	
<b>message-processing v1   v2c   v3</b>	Keywords to specify the version number used by the message processing model.	
<b>security-model v3</b>	Keyword to specify security-model v3.	
<b>message-processing v3</b>	Keywords to specify v3 is used by the message-processing model.	
<b>noauthentication</b>	Keyword to specify security model is not set to use authentication protocol.	
<b>authentication</b>	Keyword to specify the type of authentication protocol.	
<b>privacy</b>	Keyword to specify the messages sent on behalf of the user are protected from disclosure.	
<b>volatile</b>	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.	
<b>nonvolatile</b>	(Optional) Keyword to specify that the storage type is defined as persistent memory and the content remains after the device is turned off and on again.	

**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 | auth | bridge | chassis | config | entity | ippermit |
module | stpx | syslog | vmps | vtp]
```

```
set snmp trap rcvr_addr rcvr_community
```

Syntax Description	
<b>enable</b>	Keyword to enable SNMP traps.
<b>disable</b>	Keyword to disable SNMP traps.
<b>all</b>	(Optional) Keyword to specify all trap types and all port traps. See the “Usage Guidelines” section before using this option.
<b>auth</b>	(Optional) Keyword to specify the authenticationFailure trap from RFC 1157.
<b>bridge</b>	(Optional) Keyword to specify the newRoot and topologyChange traps from RFC 1493 (the BRIDGE-MIB).
<b>chassis</b>	(Optional) Keyword to specify the chassisAlarmOn and chassisAlarmOff traps from the CISCO-STACK-MIB.
<b>config</b>	(Optional) Keyword to specify the sysConfigChange trap from the CISCO-STACK-MIB.
<b>entity</b>	(Optional) Keyword to specify the entityMIB trap from the ENTITY-MIB.
<b>ippermit</b>	(Optional) Keyword to specify the IP Permit Denied access from the CISCO-STACK-MIB.
<b>module</b>	(Optional) Keyword to specify the moduleUp and moduleDown traps from the CISCO-STACK-MIB.
<b>stp</b> x	(Optional) Keyword to specify the STPX trap.
<b>syslog</b>	(Optional) Keyword to specify the syslog notification traps.
<b>vmps</b>	(Optional) Keyword to specify the vmVmpsChange trap from the CISCO-VLAN-MEMBERSHIP-MIB.
<b>vtp</b>	(Optional) Keyword to specify the VTP from the CISCO-VTP-MIB.
<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 is SNMP traps are 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 the appropriate traps were configured. To use this command, you must configure all notification tables: snmpTargetAddrTable, snmpTargetParamsTable, and snmpNotifyTable. Use the **all** option to enable or disable all trap types and all port traps. Use the **set port trap** command to enable or disable a single port or a range of ports.

---

**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**

- show snmp**
- test snmp trap**
- clear snmp trap**
- set port 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		
<b>-hex</b>	(Optional) Keyword to display <i>username</i> in a hexadecimal format.	
<i>username</i>	Name of the SNMP user.	
<b>remote</b> <i>engineid</i>	Keyword and variable to specify the remote SNMP engine ID.	
<b>authentication</b>	(Optional) Keyword to specify the authentication protocol.	
<b>md5</b>	Keyword to specify HMAC-MD5-96 authentication protocol.	
<b>sha</b>	Keyword to specify HMAC-SHA-96 authentication protocol.	
<i>authpassword</i>	Password for authentication.	
<b>privacy</b> <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.	
<b>volatile</b>	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.	
<b>nonvolatile</b>	(Optional) Keyword to specify that the storage type is defined as persistent memory and the content remains after the device is turned off and on again.	

**Defaults** The default storage type is **volatile**. If you do not specify **authentication**, the security level default will be **noauthentication**. If you do not specify **privacy**, the default will be no privacy.

**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.

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

---

**Examples**

This example shows how to set a specific username:

```
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 username, 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	
<b>-hex</b>	(Optional) Keyword to display the <i>viewname</i> in a hexadecimal format.
<i>viewname</i>	Name of a MIB view.
<i>subtree</i>	MIB subtree.
<b>mask</b>	(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.
<b>included</b>   <b>excluded</b>	(Optional) Keywords to specify that the MIB subtree is included or excluded.
<b>volatile</b>	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
<b>nonvolatile</b>	(Optional) Keyword to specify that the storage type is defined 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 MIB 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 set to configure and display SPAN.

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

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

## Syntax Description

<b>disable</b>	Keyword to disable SPAN.
<i>dest_mod</i>	(Optional) Monitoring module (SPAN destination).
<i>dest_port</i>	(Optional) Monitoring port (SPAN destination).
<b>all</b>	(Optional) Keyword to disable all SPAN sessions.
<i>src_mod</i>	Monitored module (SPAN source).
<i>src_ports</i>	Monitored ports (SPAN source).
<i>src_vlans</i>	Monitored VLANs (SPAN source).
<b>sc0</b>	Keyword to specify the inband port is a valid source.
<b>rx</b>	(Optional) Keyword to specify that information received at the source (ingress SPAN) is monitored.
<b>tx</b>	(Optional) Keyword to specify that information transmitted from the source (egress SPAN) is monitored.
<b>both</b>	(Optional) Keyword to specify that information both transmitted from the source (ingress SPAN) and received (egress SPAN) at the source are monitored.
<b>inpkts enable</b>	(Optional) Keywords to enable the receiving of normal inbound traffic on the SPAN destination port.
<b>inpkts disable</b>	(Optional) Keywords to disable the receiving of normal inbound traffic on the SPAN destination port.
<b>learning enable</b>	(Optional) Keywords to enable learning for the SPAN destination port.
<b>learning disable</b>	(Optional) Keywords to disable learning for the SPAN destination port.
<b>multicast enable</b>	(Optional) Keywords to enable monitoring multicast traffic (egress traffic only).
<b>multicast disable</b>	(Optional) Keywords to disable monitoring multicast traffic (egress traffic only).
<b>filter</b> <i>vlans</i>	(Optional) Keyword and variable to monitor traffic on selected VLANs on source trunk ports.
<b>create</b>	(Optional) Keyword to create a SPAN port.

## Defaults

The default is SPAN is disabled, no VLAN filtering is enabled, multicast is enabled, input packets are disabled, and learning is enabled.

## Command Types

Switch command.

## Command Modes

Privileged.

**Usage Guidelines**

After you enable SPAN, system defaults are used if no parameters were ever set. If you changed parameters, the old parameters are stored in NVRAM, and the new parameters are used.

Use a network analyzer to monitor ports.

If you specify multiple SPAN source ports, the ports can belong to different VLANs.

A maximum of two **rx** or **both** SPAN sessions and four **tx** SPAN sessions can exist simultaneously. If you use a remote SPAN station, the maximum number of **rx** or **both** SPAN sessions is one.

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.

You can specify an MSM port as the SPAN source port. However, you cannot specify an MSM port as the SPAN destination port.

When you enable the **inpkts** option, a warning message notifies you that the destination port does not join STP and may cause loops if this option is enabled.

When you configure multiple SPAN sessions, the destination module number/port number must be known to index the particular SPAN session.

If you do not specify the keyword **create** and you have only one session, the session will be overwritten. If a matching destination port exists, the particular session will be overwritten (with or without specifying **create**). If you specify the keyword **create** and there is no matching destination port, the session will be created.

**Examples**

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

```
Console> (enable) set span 1/1 2/1
Enabled monitoring of Port 1/1 transmit/receive traffic by Port 2/1
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)
```

This example shows how to set VLAN 522 as the SPAN source and port 3/12 as the SPAN destination. Only transmit traffic is monitored. Normal incoming packets on the SPAN destination port are allowed.

```
Console> (enable) set span 522 2/12 tx inpkts enable
SPAN destination port incoming packets enabled.
Enabled monitoring of VLAN 522 transmit traffic by Port 2/12
Console> (enable)
```

This example shows how to set port 3/2 as the SPAN source and port 2/2 as the SPAN destination:

```
Console> (enable) set span 3/2 2/2 tx create
Enabled monitoring of port 3/2 transmit traffic by Port 2/1
Console> (enable)
```

This example shows what happens if you try to enter the **set span disable** command (without the destination module number/port number defined) and multiple SPAN sessions are defined:

```
Console> (enable) set span disable
Multiple active span sessions. Please specify span destination to disable.
Console> (enable)
```

**Related Commands**

**clear config**  
**show span**

# set spantree backbonefast

Use the **set spantree backbonefast** command to enable or disable the spanning tree Backbone Fast Convergence feature.

**set spantree backbonefast {enable | disable}**

Syntax Description	enable	disable
	Keyword to enable Backbone Fast Convergence.	Keyword to disable Backbone Fast Convergence.

**Defaults** The default is Backbone Fast Convergence is disabled.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** For Backbone Fast Convergence to work, you must enable it on all switches in the network.

**Examples** This example shows how to enable Backbone Fast Convergence:

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

**Related Commands** **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]
```

<b>Syntax Description</b>	<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.

**Defaults** The default is the bridge forward delay is set to 15 seconds for all VLANs.

**Command Types** Switch command.

**Command Modes** Privileged.

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

**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 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 seconds.
	<i>vlan</i>	(Optional) Number of the VLAN.

**Defaults** The default is the bridge hello time is set to 2 seconds for all VLANs.

**Command Types** Switch command.

**Command Modes** Privileged.

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

**Examples** This example shows how to set the spantree hello time for VLAN 100 to 3 seconds:

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

<b>Syntax Description</b>	<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.

**Defaults** The default configuration is 20 seconds for all VLANs.

**Command Types** Switch command.

**Command Modes** Privileged.

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

**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 portcost

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

**set spantree portcost** {*mod/port*} *cost*

<b>Syntax Description</b>	<i>mod/port</i>	Number of the module and the port on the module.
	<i>cost</i>	Number of the path cost; valid values are from 0 to 65535, where 0 is low cost and 65535 is high cost.

**Defaults** The default is portcost is 4.

**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.

This 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.
<b>enable</b>	Keyword to enable the spanning tree port fast-start feature on the port.
<b>disable</b>	Keyword to disable the spanning tree port fast-start feature on the port.

**Defaults** The default is the port fast-start feature is 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 rather than 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-guard

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

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

## Syntax Description

<b>enable</b>	Keyword to enable the spanning tree PortFast BPDU guard.
<b>disable</b>	Keyword to disable the spanning tree PortFast BPDU guard.

## Defaults

The default is PortFast BPDU guard is disabled.

## Command Types

Switch command.

## Command Modes

Privileged.

## Usage Guidelines

When you enable PortFast BPDU guard, a nontrunking PortFast-enabled port is moved into an errdisable state when a BPDU is received on that port. When you disable a PortFast BPDU guard, a PortFast enabled nontrunking 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 or TrCRF.

**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.
<b>trcrf</b>		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 to 63, with 0 indicating high priority and 63, low priority.
<i>trcrf_priority</i>		(Optional) Number that represents the cost of the TrCRF; valid values are from 0 to 7, with 0 indicating high priority and 7, low priority.

**Defaults** The default is all ports with bridge priority are set to 32.

**Command Types** Switch command.

**Command Modes** Privileged.

**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 set the state of a TrCRF manually.

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

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

**Defaults** There is no default configuration for this command.

**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 set the state of the logical ports of a TrBRF manually:

- 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 set the state of a TrCRF manually 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**

# 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] [vlan_list]
```

<b>Syntax Description</b>	<i>mod/port</i>	Number of the module and the port on the module.
	<b>cost</b> <i>cost</i>	(Optional) Keyword to indicate the path cost. The portvlancost applies only to trunk ports.
	<i>vlan_list</i>	(Optional) If you do not list a VLAN explicitly, the VLANs listed in prior invocations of this command are affected. If no cost is listed explicitly, and previous cost values are specified in prior invocations, then the portvlancost is set to 1 less than the current port cost for a port. However, this may not assure load balancing in all cases.

**Defaults** The default is portvlancost is 3.

**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. This command is not supported in MISTP mode.

---

**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**    **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 [vlangs]
```

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>vlangs</i>	(Optional) VLANs that use the specified priority level.

**Defaults** The default is the port VLAN priority is set to 0, with no VLANs specified.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** Use this command to add VLANs to a specified port priority level. Subsequent calls to this command do not replace VLANs that are already set at a specified port priority level.

This feature is not supported for the MSM.

The **set spantree portvlanpri** command applies only to trunk ports. If you enter this command, 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 portvlancost**
- show spantree**

# set spantree priority

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

**set spantree priority** *bridge\_priority* [*vlan*]

<b>Syntax Description</b>	<i>bridge_priority</i>	Number representing the priority of the bridge. The priority level is from 0 to 65535, with 0 indicating high priority and 65535, low priority.
	<i>vlan</i>	(Optional) Number of the VLAN. If you do not specify a VLAN number, VLAN 1 is used.

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

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** This feature is not supported for the MSM.

**Examples** This example shows how to set the bridge priority of VLAN 1 to 4096:

```
Console> (enable) set spantree priority 4096
VLAN 1 bridge priority set to 4096.
Console> (enable)
```

**Related Commands** **show spantree**

## set spantree root

Use the **set spantree root** command to set the primary or secondary root for specific VLANs or for all VLANs of the switch.

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

### Syntax Description

<b>secondary</b>	(Optional) Keyword to designate this switch as a secondary root, should the primary root fail.
<i>vlan_list</i>	(Optional) Number of the VLAN.
<b>dia</b> <i>network_diameter</i>	(Optional) Keyword to specify the maximum number of bridges between any two points of attachment of end stations; valid values are from 1 through 7.
<b>hello</b> <i>hello_time</i>	(Optional) Keyword to specify in seconds, the duration between the generation of configuration messages by the root switch.

### 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*, the current value of *hello\_time* from the NVRAM is used.

### 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 secondary command reduces the bridge priority value to 16384. This command increases path costs to a value greater than 3000.

### Command Types

Switch command.

### Command Modes

Privileged.

### Examples

This example shows how to use the **set spantree root** command:

```
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)
```

These examples show that setting the bridge priority to 8192 was not sufficient to make this switch the root. So, 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.  
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

Use the **set spantree uplinkfast** command to enable fast switchover to alternate ports when the root port fails. 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		
<b>enable</b>		Keyword to enable fast switchover.
<b>disable</b>		Keyword to disable fast switchover.
<b>rate</b>		(Optional) Keyword to specify the number of multicast packets transmitted per 100 ms when an alternate port is chosen after the root port goes down.
<i>station_update_rate</i>		(Optional) Number of multicast packets transmitted per 100 ms when an alternate port is chosen after the root port goes down.
<b>all-protocols</b>		(Optional) Keyword to specify whether or not to generate multicast packets for all protocols (IP, IPX, AppleTalk, and Layer 2 packets).
<b>off</b>		(Optional) Keyword to turn off the all-protocols feature.
<b>on</b>		(Optional) Keyword to turn on the all-protocols feature.

**Defaults** The default *station\_update\_rate* is 15 packets per 100 ms.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** 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 **set spantree uplinkfast enable** 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 **set spantree uplinkfast disable** on a switch, the UplinkFast feature is disabled but the switch priority and port cost values are not reset to the factory-set defaults. To reset the values to the factory-set defaults, enter the **clear spantree uplinkfast** command.

The default *station\_update\_rate* value is 15 packets per 100 ms, which is equivalent to a 1 percent load on a 10-Mbps Ethernet. 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 6000 family switches that have both the UplinkFast and protocol filtering features enabled. Use the all-protocols feature only on Catalyst 6000 family 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 ms:

```
Console> (enable) set spantree uplinkfast enable rate 40
VLANs 1-1000 bridge priority set to 49152.
The port cost and portvlancost of all ports increased to above 3000.
Station update rate set to 40 packets/100ms.
uplinkfast turned on 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 already 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)
```

---

### Related Commands

**show spantree**



■ set spantree uplinkfast