

set port auxiliaryvlan

Use the **set port auxiliaryvlan** command to configure the auxiliary VLAN ports.

```
set port auxiliaryvlan mod[/ports] { vlan / untagged / dot1p / none }
```

Syntax Description	
<i>mod</i> [/ports]	Number of the module and (optional) ports.
<i>vlan</i>	Number of the VLAN; valid values are from 1 to 1000.
untagged	Keyword to specify the IP Phone 7960 send untagged packets without 802.1p priority.
dot1p	Keyword to specify the IP Phone 7960 send packets with 802.1p priority.
none	Keyword to specify that the switch does not send any auxiliary VLAN information in the CDP packets from that port.

Defaults The default setting is **none**.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines

Examples If you do not specify a port, all ports are selected. The *vlan* option specifies that the IP Phone 7960 send packets tagged with a specific VLAN.

This example shows how to set the auxiliary VLAN port to untagged:

```
Console> (enable) set port auxiliaryvlan 5/7 untagged
Port 5/7 allows the connected device send and receive untagged packets and without 802.1p
priority.
Console> (enable)
```

This example shows how to set the auxiliary VLAN port to dot1p:

```
Console> (enable) set port auxiliaryvlan 5/9 dot1p
Port 5/9 allows the connected device send and receive packets with 802.1p priority.
Console> (enable)
```

This example shows how to set the auxiliary VLAN port to none:

```
Console> (enable) set port auxiliaryvlan 5/12 none
Port 5/12 will not allow sending CDP packets with AuxiliaryVLAN information.
Console> (enable)
```

set port auxiliaryvlan

This example shows how to set the auxiliary VLAN port to a specific module, port, and VLAN:

```
Console> (enable) set port auxiliaryvlan 2/1-3 222
Auxiliaryvlan 222 configuration successful.
AuxiliaryVlan AuxVlanStatus Mod/Ports
-----
222          active          1/2,2/1-3
Console> (enable)
```

Related Commands **show port auxiliaryvlan**

set port broadcast

Use the **set port broadcast** command to set the broadcast suppression for one or more ports. The broadcast threshold limits the backplane traffic received from the module.

set port broadcast *mod/port threshold%*

Syntax Description	<i>mod/port</i>	Number of the module and the port on the module.
	<i>threshold%</i>	Percentage of total available bandwidth that can be used by broadcast traffic.

Defaults The default is broadcast suppression is disabled (no broadcast limit).

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command is not supported by the NAM.

Examples This example shows how to limit broadcast traffic to 20 percent to all ports on module 4:

```
Console> (enable) set port broadcast 4/3 20%
Port 4/1-24 broadcast traffic limited to 20.00%.
Console> (enable)
```

This example shows how to allow unlimited broadcast traffic to all ports on module 4:

```
Console> (enable) set port broadcast 4/3 100%
Port 4/1-24 broadcast traffic unlimited.
Console> (enable)
```

Related Commands

- clear port broadcast**
- show port broadcast**

set port channel

Use the **set port channel** command set to configure EtherChannel on Ethernet module ports.

```
set port channel mod/port [admin_group]
```

```
set port channel mod/port mode {on | off | desirable | auto} [silent | non-silent]
```

```
set port channel all distribution {ip | mac} [source | destination | both]
```

Syntax Description		
<i>mod/port</i>		Number of the module and the port on the module.
<i>admin_group</i>		(Optional) Number of administrative group; valid values are from 1 to 1024.
mode		Keyword to specify the EtherChannel mode.
on		Keyword to enable and force specified ports to channel without PAgP.
off		Keyword to prevent ports from channeling.
desirable		Keyword to set a PAgP mode that places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending PAgP packets.
auto		Keyword to set a PAgP mode that places a port into a passive negotiating state, in which the port responds to PAgP packets it receives, but does not initiate PAgP packet negotiation.
silent		(Optional) Keyword to use with auto or desirable when no traffic is expected from the other device to prevent the link from being reported to STP as down.
non-silent		(Optional) Keyword to use with auto or desirable when traffic is expected from the other device.
all distribution		Keywords to apply frame distribution to all ports in the switch.
ip		Keyword to specify the frame distribution method using IP address values.
mac		Keyword to specify the frame distribution method using MAC address values.
source		(Optional) Keyword to specify the frame distribution method using source address values.
destination		(Optional) Keyword to specify the frame distribution method using destination address values.
both		(Optional) Keyword to specify the frame distribution method using source and destination address values.

Defaults

The default is EtherChannel is set to **auto** and **silent** on all module ports. The defaults for frame distribution are **ip** and **both**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Make sure that all ports in the channel are configured with the same port speed, duplex mode, and so forth. For more information on EtherChannel, refer to the *Catalyst 6000 Family Software Configuration Guide*.

With the **on** mode, a usable EtherChannel exists only when a port group in **on** mode is connected to another port group in **on** mode.

If you are running QoS, make sure that bundled ports are all of the same trust types and have similar queueing and drop capabilities.

Disable the port security feature on the channeled ports (see the **set port security** command). If you enable port security for a channeled port, the port shuts down when it receives packets with source addresses that do not match the secure address of the port.

You can configure up to eight ports on the same switch in each administrative group.

When you assign ports to an existing admin group, the original ports associated with the admin group will move to an automatically picked new admin group. You cannot add ports to the same admin group.

If you do not enter an *admin_group*, it means that you want to create a new administrative group with *admin_group* selected automatically. The next available *admin_group* is automatically selected.

If you do not enter the channel mode, the channel mode of the ports addressed are not modified.

The **silent** | **non-silent** parameters only apply if **desirable** or **auto** modes are entered.

If you do not specify **silent** or **non-silent**, the current setting is not affected.

Examples

This example shows how to set the channel mode to **desirable**:

```
Console> (enable) set port channel 2/2-8 mode desirable
Ports 2/2-8 channel mode set to desirable.
```

This example shows how to set the channel mode to **auto**:

```
Console> (enable) set port channel 2/7-8,3/1 mode auto
Ports 2/7-8,3/1 channel mode set to auto.
Console> (enable)
```

This example shows how to group ports 4/1 through 4 in an admin group:

```
Console> (enable) set port channel 4/1-4 96
Port(s) 4/1-4 are assigned to admin group 96.
Console> (enable)
```

This example shows the display when the port list is exceeded:

```
Console> (enable) set port channel 2/1-9 1
No more than 8 ports can be assigned to an admin group.
Console> (enable)
```

This example shows how to disable EtherChannel on module 4, ports 4 through 6:

```
Console> (enable) set port channel 4/4-6 mode off
Port(s) 4/4-6 channel mode set to off.
Console> (enable)
```

This example shows the display output when you assign ports to an existing admin group. This example moves ports in admin group 96 to another admin group and assigns ports 4/4 through 6 to admin group 96:

```
Console> (enable) set port channel 4/4-6 96  
Port(s) 4/1-3 are moved to admin group 97.  
Port(s) 4/4-6 are assigned to admin group 96.  
Console> (enable)
```

This example shows how to set the channel mode to **off** for ports 4/4 through 6 and assign ports 4/4 through 6 to an automatically selected admin group:

```
Console> (enable) set port channel 4/4-6 off  
Port(s) 4/4-6 channel mode set to off.  
Port(s) 4/4-6 are assigned to admin group 23.  
Console> (enable)
```

This example shows how to configure the EtherChannel load-balancing feature:

```
Console> (enable) set port channel all distribution ip destination  
Channel distribution is set to ip destination.  
Console> (enable)
```

Related Commands

show port channel
show channel
show channel group

set port cops

Use the **set port cops** command to create port roles.

```
set port cops mod/port roles role1 [role2]...
```

Syntax Description	<i>mod/port</i> Number of the module and the port on the module.
	roles <i>role#</i> Keyword and variable to specify the roles.
Defaults	The default is all ports have a default role of null string, for example, the string of length 0.
Command Types	Switch command.
Command Modes	Privileged.
Usage Guidelines	<p>This command is not supported by the NAM.</p> <p>A port may have multiple roles. You can configure a maximum of 64 total roles per switch. You can specify multiple roles in a single command.</p>
Examples	<p>This example shows how to create roles on a port:</p> <pre>Console> (enable) set port cops 3/1 roles backbone_port main_port New role 'backbone_port' created. New role 'main_port' created. Roles added for port 3/1-4. Console> (enable)</pre> <p>This example shows the display if you attempt to create a roll and exceed the maximum allowable number of roles:</p> <pre>Console> (enable) set port cops 3/1 roles access_port Unable to add new role. Maximum number of roles is 64. Console> (enable)</pre>
Related Commands	<pre>clear port cops show port cops</pre>

set port disable

Use the **set port disable** command to disable a port or a range of ports.

set port disable *mod/port*

Syntax Description	<i>mod/port</i> Number of the module and the port on the module.
Defaults	The default system configuration has all ports enabled.
Command Types	Switch command.
Command Modes	Privileged.
Usage Guidelines	This command is not supported by the NAM. It takes approximately 30 seconds for this command to take effect.
Examples	This example shows how to disable a port using the set port disable command: <pre>Console> (enable) set port disable 5/10 Port 5/10 disabled. Console> (enable)</pre>
Related Commands	set port enable show port

set port duplex

Use the **set port duplex** command to configure the duplex type of an Ethernet port or a range of ports.

set port duplex *mod/port* {**full** | **half**}

Syntax Description	<i>mod/port</i>	Number of the module and the port on the module.
	full	Keyword to specify full-duplex transmission.
	half	Keyword to specify half-duplex transmission.

Defaults The default configuration for 10-Mbps and 100-Mbps modules has all Ethernet ports set to half duplex.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines You can configure Ethernet and Fast Ethernet interfaces to either full duplex or half duplex. Gigabit ports only support full-duplex mode.

Examples This example shows how to set port 1 on module 2 to full duplex:

```
Console> (enable) set port duplex 2/1 full
Port 2/1 set to full-duplex.
Console> (enable)
```

Related Commands **show port**

set port enable

Use the **set port enable** command to enable a port or a range of ports.

set port enable *mod/port*

Syntax Description	<i>mod/port</i> Number of the module and the port on the module.
Defaults	The default is all ports are enabled.
Command Types	Switch command.
Command Modes	Privileged.
Usage Guidelines	This command is not supported by the NAM. It takes approximately 30 seconds for this command to take effect.
Examples	This example shows how to enable port 3 on module 2: <pre>Console> (enable) set port enable 2/3 Port 2/3 enabled. Console> (enable)</pre>
Related Commands	set port disable show port

set port flowcontrol

Use the **set port flowcontrol** command to configure a port to send or receive pause frames. Pause frames are special packets that signal a source to stop sending frames for a specific period of time because the buffers are full.

```
set port flowcontrol {mod/port} {receive | send} {off | on | desired}
```

Syntax Description	
<i>mod/port</i>	Number of the module and the port on the module.
receive	Keyword to specify a port processes pause frames.
send	Keyword to specify a port sends pause frames.
off	Keyword to prevent a local port from receiving and processing pause frames from remote ports or from sending pause frames to remote ports.
on	Keyword to enable a local port to receive and process pause frames from remote ports or send pause frames to remote ports.
desired	Keyword to obtain predictable results regardless of whether a remote port is set to on , off , or desired .

Defaults

Flow-control defaults vary depending upon port speed:

- Gigabit Ethernet ports default to **off** for receive (Rx) and **desired** for transmit (Tx)
- Fast Ethernet ports default to **off** for receive and **on** for transmit

On the 24-port 100BaseFX and 48-port 10/100 BaseTX RJ-45 modules, the default is **off** for receive and **off** for send.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

When you configure the 24-port 100BaseFX and 48-port 10/100 BaseTX RJ-45 modules, you can set the receive flow control to **on** or **off** and the send flow control to **off**.

All Catalyst Gigabit Ethernet ports can receive and process pause frames from remote devices.

To obtain predictable results, use these guidelines:

- Use **send on** only when remote ports are set to **receive on** or **receive desired**.
- Use **send off** only when remote ports are set to **receive off** or **receive desired**.
- Use **receive on** only when remote ports are set to **send on** or **send desired**.
- Use **send off** only when remote ports are set to **receive off** or **receive desired**.

Table 2-11 describes guidelines for different configurations of the **send** and **receive** keywords.

Table 2-11 *send and receive Keyword Configurations*

Configuration	Description
send on	Enables a local port to send pause frames to remote ports.
send off	Prevents a local port from sending pause frames to remote ports.
send desired	Obtains predictable results whether a remote port is set to receive on , receive off , or receive desired .
receive on	Enables a local port to process pause frames that a remote port sends.
receive off	Prevents a local port from sending pause frames to remote ports.
receive desired	Obtains predictable results whether a remote port is set to send on , send off , or send desired .

Examples

This example shows how to configure port 1 of module 5 to receive and process pause frames:

```
Console> (enable) set port flowcontrol receive 5/1 on
Port 5/1 flow control receive administration status set to on
(port will require far end to send flowcontrol)
Console> (enable)
```

This example shows how to configure port 1 of module 5 to receive and process pause frames if the remote port is configured to send pause frames:

```
Console> (enable) set port flowcontrol receive 5/1 desired
Port 5/1 flow control receive administration status set to desired
(port will allow far end to send flowcontrol if far end supports it)
Console> (enable)
```

This example shows how to configure port 1 of module 5 to receive but NOT process pause frames on port 1 of module 5:

```
Console> (enable) set port flowcontrol receive 5/1 off
Port 5/1 flow control receive administration status set to off
(port will not allow far end to send flowcontrol)
Console> (enable)
```

This example shows how to configure port 1 of module 5 to send pause frames:

```
Console> (enable) set port flowcontrol send 5/1 on
Port 5/1 flow control send administration status set to on
(port will send flowcontrol to far end)
Console> (enable)
```

This example shows how to configure port 1 of module 5 to send pause frames and yield predictable results even if the remote port is set to **receive off**:

```
Console> (enable) set port flowcontrol send 5/1 desired
Port 5/1 flow control send administration status set to desired
(port will send flowcontrol to far end if far end supports it)
Console> (enable)
```

Related Commands

show port flowcontrol

set port gmrp

Use the **set port gmrp** command to enable or disable GMRP on the specified ports in all VLANs.

```
set port gmrp {mod/port} {enable | disable}
```

Syntax Description		
	<i>mod/port</i>	Number of the module and the port on the module.
	enable	Keyword to enable GVRP on a specified port.
	disable	Keyword to disable GVRP on a specified port.

Defaults The default is GMRP is disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command is not supported by the NAM.
You can enter this command even when GMRP is not enabled, but the values come into effect only when you enable GMRP using the **set gmrp enable** command.

Examples This example shows how to enable GMRP on module 3, port 1:

```
Console> (enable) set port gmrp 3/1 enable
GMRP enabled on port(s) 3/1.
GMRP feature is currently disabled on the switch.
Console> (enable)
```

This example shows how to disable GMRP on module 3, ports 1 through 5:

```
Console> (enable) set port gmrp 3/1-5 disable
GMRP disabled on port(s) 3/1-5.
Console> (enable)
```

Related Commands **show gmrp configuration**

Use the **set port gvrp** command to enable or disable GVRP on the specified ports in all VLANs.

```
set port gvrp {mod/port} {enable | disable}
```

Syntax Description		
	<i>mod/port</i>	Number of the module and the port on the module.
	enable	Keyword to enable GVRP on a specified port.
	disable	Keyword to disable GVRP on a specified port.

Usage Guidelines

This command is not supported by the NAM.

You can configure GVRP on a port even when you globally enable GVRP. However, the port will not become a GVRP participant until you globally enable GVRP.

```
GVRP enabled on port(s) 5/1.
```

GVRP feature is currently disabled on the switch. Use the **set port host** command to optimize the port configuration for a host connection.

```
set port host {mod/port}
```

Syntax Description

<i>mod/port</i>	Number of the module and the port on the module.
-----------------	--

Usage Guidelines

This command is not supported by the NAM.

Because you should enter the **set port host** only on ports connected to a single host. Connecting hubs, concentrators, switches, and bridges to a fast-start port can cause temporary spanning tree loops.

Enable the **set port host** command to decrease the time it takes to start up packet forwarding.

```
Spantree ports 2/1,3/1 fast start enabled.
```

```
Port(s) 2/1,3/1 trunk mode set to off.
```

```
Port(s) 2/1 channel mode set to off.
```

set port inlinepower

Use the **set port inlinepower** command to set the inline power mode of a port or group of ports.

```
set port inlinepower mod/ports {off | auto}
```

Syntax Description		
	<i>mod/ports</i>	Number of the module and the ports on the module.
	off	Keyword to not power up the port even if an unpowered phone is connected.
	auto	Keyword to power up the port only if the switching module has discovered the phone.

Defaults The default is **auto**.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command is not supported by the NAM.
 If you enter this command on a port that does not support the IP phone power feature, an error message is displayed.
 You can enter a single port or a range of ports, but you cannot enter the module number only.
 An inline power-capable device can still be detected even if the inlinepower mode is set to off.



Caution

Damage can occur to equipment connected to the port if you are not using a phone that can be configured for the IP phone phantom power feature.

Examples This example shows how to set the inlinepower to off:

```
Console> (enable) set port inlinepower 2/5 off
Inline power for port 2/5 set to off.
Console> (enable)
```

This example shows the output if the inlinepower feature is not supported:

```
Console> (enable) set port inlinepower 2/3-9 auto
Feature not supported on module 2.
Console> (enable)
```

Related Commands **set inlinepower defaultallocation**
show environment power

Use the **set port jumbo** command to enable or disable the jumbo frame feature on a per-port basis.

set port jumbo {*mod/port*} {**enable** | **disable**}

Syntax Description

<i>mod/port</i>	Number of the module and the port on the module.
enable	Keyword to enable jumbo frames on a specified port.
disable	Keyword to disable jumbo frames on a specified port.

Usage Guidelines

MTU size for packet acceptance is 9216 bytes for nontrunking ports

This command is not supported by the NAM.

You can use the jumbo frame feature to transfer large frames or jumbo frames through Catalyst 6000 family switches to optimize server-to-server performance.

The jumbo frames feature is only supported on Layer 2-switched frames.

The MSFC and MSM do not support the routing of jumbo frames; if jumbo frames are sent to these routers, router performance is significantly degraded.

The GSR supports jumbo frames.

- The port must be a Gigabit Ethernet port.
- The trunking mode on the port must be set to OFF.
- The channeling mode on the port must be set to OFF.

For information on how to set the jumbo frame MTU size, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com.

Jumbo frames enabled on port 5/3.

```
Jumbo framesGigabit Ethernet portConsole> (enable) set port jumbo 3/1 enable
Feature not supported on port 3/1.
```

```
trunking mode set to OFFConsole> (enable) set port jumbo 6/1 enable
Failed to enable the port jumbo frame feature on port 6/1.
The trunking mode for jumbo enabled ports must be set to off.
```

```
channeling mode set to OFFConsole> (enable) set port jumbo 6/2 enable
Failed to enable the port jumbo frame feature on port 6/2.
The channelling mode for jumbo enabled ports must be set to off.
```

set port channel
set trunk
show port jumbo

set port membership

Use the **set port membership** command to set the VLAN membership assignment to a port.

```
set port membership mod/port {dynamic | static}
```

Syntax Description	<i>mod/port</i>	Number of the module and the port on the module.
	dynamic	Keyword to specify the port become a member of dynamic VLANs.
	static	Keyword to specify the port become a member of static VLANs.

Defaults This command has no default setting.

Command Types Switch command.

Command Modes Privileged.

Examples This example shows how to set the port membership VLAN assignment to dynamic:

```
Console> (enable) set port membership 5/5 dynamic
Port 5/5 vlan assignment set to dynamic.
Spantree port fast start option enabled for ports 5/5.
Console> (enable)
```

This example shows how to set the port membership VLAN assignment to static:

```
Console> (enable) set port membership 5/5 static
Port 5/5 vlan assignment set to static.
Console> (enable)
```

Related Commands

- set vlan**
- set vlan mapping**
- set pvlan**
- set pvlan mapping**

set port name

Use the **set port name** command to configure a name for a port.

```
set port name mod/port [port_name]
```

Syntax Description	<i>mod/port</i>	Number of the module and the port on the module.
	<i>port_name</i>	(Optional) Name of the module.

Defaults The default is no port name is configured for any port.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command is not supported by the NAM.
If you do not specify the name string, the port name is cleared.

Examples This example shows how to set port 1 on module 4 to Snowy:

```
Console> (enable) set port name 4/1 Snowy
Port 4/1 name set.
Console> (enable)
show port
```

set port negotiation

Use the **set port negotiation** command to enable or disable the link negotiation protocol on the specified port.

```
set port negotiation 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 link negotiation protocol.
disable	Keyword to disable the link negotiation protocol.

Defaults

link negotiation protocol is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set port negotiation** command is supported on 1000Base (SX, LX, and ZX) modules only.

If the port does not support this command, the following message appears:

```
Feature not supported on Port N/N.
```

where N/N is the module and port number.

When you enable link negotiation, the system autonegotiates flow control, duplex mode, and remote fault information.

You must either enable or disable link negotiation on both ends of the link. Both ends of the link must be set to the same value or the link cannot connect.

Examples

This example shows how to disable link negotiation protocol on port 1, module 4:

```
Console> (enable) set port negotiation 4/1 disable
Link negotiation protocol disabled on port 4/1.
Console> (enable)
```

Related Commands

show port negotiation

set port protocol

Use the **set port protocol** command to enable or disable protocol membership of ports.

```
set port protocol mod/port { ip | ipx | group } { on | off | auto }
```

Syntax Description		
	<i>mod/port</i>	Number of the module and the port on the module.
	ip	Keyword to specify IP.
	ipx	Keyword to specify IPX.
	group	Keyword to specify VINES, AppleTalk, and DECnet protocols.
	on	Keyword to indicate the port will receive all the flood traffic for that protocol.
	off	Keyword to indicate the port will not receive any flood traffic for that protocol.
	auto	Keyword to indicate the port will not receive any flood traffic for that protocol.

Defaults The default is that the ports are configured to **on** for the IP protocol groups and **auto** for IPX and group protocols.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command is not supported by the NAM.

Protocol filtering is supported only on nontrunking EtherChannel ports. Trunking ports are always members of all the protocol groups.

If the port configuration is set to **auto**, the port initially does not receive any flood packets for that protocol. When the corresponding protocol packets are received on that port, the supervisor engine detects this and adds the port to the protocol group.

Ports configured as **auto** are removed from the protocol group if no packets are received for that protocol within a certain period of time. This aging time is set to 60 minutes. They are also removed from the protocol group on detection of a link down.

Examples This example shows how to disable IPX protocol membership of port 1 on module 2:

```
Console> (enable) set port protocol 2/1 ipx off
IPX protocol disabled on port 2/1.
Console> (enable)
```

This example shows how to enable automatic IP membership of port 1 on module 5:

```
Console> (enable) set port protocol 5/1 ip auto
IP protocol set to auto mode on module 5/1.
Console> (enable)
```

Related Commands **show port protocol**

set port qos

Use the **set port qos** command to specify whether an interface is interpreted as a physical port or as a VLAN.

set port qos *mod/ports...* **port-based** | **vlan-based**

Syntax Description	<i>mod/ports...</i> Number of the module and the ports on the module.
port-based	Keyword to interpret the interface as a physical port.
vlan-based	Keyword to interpret the interface as part of a VLAN.

Defaults The default is ports are port-based.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command is not supported by the NAM.

Changing a port from port-based to VLAN-based QoS detaches all ACLs from the port. Any ACLs attached to the VLAN apply to the port immediately.

When you set a port to VLAN-based using the **set port qos** command with RSVP or COPS enabled on that port, the QoS policy-source is COPS or DSBM-election is enabled. The VLAN-based setting has been saved in NVRAM only.

Examples This example shows how to specify an interface as a physical port:

```
Console> (enable) set port qos 1/1-2 port-based
Updating configuration ...
QoS interface is set to port-based for ports 1/1-2.
Console> (enable)
```

This example shows how to specify an interface as a VLAN:

```
Console> (enable) set port qos 3/1-48 vlan-based
Updating configuration ...
QoS interface is set to VLAN-based for ports 3/1-48.
Console> (enable)
```

This example shows the output if you change from port-based to VLAN-based with either RSVP or COPS enabled on the port:

```
Console> (enable) set port qos 3/1-48 vlan
QoS interface is set to vlan-based for ports 3/1-48
Port(s) 3/1-48 - QoS policy-source is Cops or DSBM-election is enabled.
Vlan-based setting has been saved in NVRAM only.
Console> (enable)
```

Related Commands

show port qos
set port qos cos
set port qos trust
show qos info

set port qos cos

Use the **set port qos cos** command to set the default value for all packets that have arrived through an untrusted port.

```
set port qos mod/ports cos cos_value
```

```
set port qos mod/ports cos-ext cos_value
```

Syntax Description		
<i>mod/ports</i>		Number of the module and ports.
cos <i>cos_value</i>		Keyword and variable to specify the CoS value for a port; valid values are from 0 to 7.
cos-ext <i>cos_value</i>		Keyword and variable to specify the CoS extension for a phone port; valid values are from 0 to 8.

Defaults The default is CoS 0.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command is not supported by the NAM.
If the default is enforced when you disable QoS, CoS is enforced when you enable QoS.

Examples This example shows how to set the CoS default value on a port:

```
Console> (enable) set port qos 2/1 cos 3
Port 2/1 qos cos set to 3.
Console> (enable)
```

This example shows how to set the CoS-ext default value on a port:

```
Console> (enable) set port qos 2/1 cos-ext 3
Port 2/1 qos cos-ext set to 3.
Console> (enable)
```

Related Commands

- clear port qos cos**
- show port qos**
- show qos info**
- set port qos trust**
- set port qos**
- show qos info**

set port qos trust

Use the **set port qos trust** command to set the trusted state of a port; for example, whether the packets arriving at a port are trusted to carry the correct classification.

```
set port qos mod/ports... trust { untrusted | trust-cos | trust-ipprec | trust-dscp }
```

Syntax Description

<i>mod/ports...</i>	Number of the module and the ports on the module.
untrusted	Keyword to specify that packets need to be reclassified from the matching ACE.
trust-cos	Keyword to specify that although the CoS bits in the incoming packets are trusted, the ToS is invalid and a valid value needs to be derived from the CoS bits.
trust-ipprec	Keyword to specify that although the ToS/CoS bits in the incoming packets are trusted, the ToS is invalid and the ToS is set as IP Precedence.
trust-dscp	Keyword to specify that the ToS/CoS bits in the incoming packets can be accepted as is with no change.

Defaults

The default when you enable QoS is **untrusted**; when you disable QoS, the default is **trust-cos** on Layer 2 switches and **trust-dscp** on Layer 3 switches.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you disable QoS, the default is **trust-cos** on Layer 2 switches and **trust-dscp** on Layer 3 switches.

This command is not supported by the NAM.

On 10/100 ports, you can use only the **set port qos trust** command to activate the receive drop thresholds. To configure a trusted state, you have to convert the port to port-based QoS, define an ACL that defines all (or the desired subset) of ACEs to be trusted, and attach the ACL to that port.

Examples

This example shows how to set the port to a trusted state:

```
Console> (enable) set port qos 3/7 trust trust-cos
Port 3/7 qos set to trust-cos.
Console> (enable)
```

This example shows how to set the trust extension on ports on the connected phone to a trusted state:

```
Console> (enable) set port qos 3/7 trust-ext trusted
Port in the phone device connected to port 3/7 is configured to be trusted.
Console> (enable)
```

■ set port qos trust

Related Commands

show qos info
show port qos
set port qos
set port qos cos

set port qos trust-ext

Use the **set port qos trust-ext** command to configure the access port on an IP phone connected to the switch port.

```
set port qos mod/ports... trust-ext { trusted | untrusted }
```

Syntax Description	<i>mod/ports...</i> Number of the module and the ports on the module.
untrusted	Keyword to specify that all traffic in 802.1Q or 802.1p frames received through the access port is marked with a configured Layer 2 CoS value.
trusted	Keyword to specify that all traffic received through the access port passes through the phone switch unchanged.

Defaults The default when the phone is connected to a Cisco LAN switch is untrusted mode; trusted mode is the default when the phone is not connected to a Cisco LAN switch.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command is not supported by the NAM.
Traffic in frame types other than 802.1Q or 802.1p passes through the phone switch unchanged, regardless of the access port trust state.

Examples This example shows how to set the trust extension on ports on the connected phone to a trusted state:

```
Console> (enable) set port qos 3/7 trust-ext trusted
Port in the phone device connected to port 3/7 is configured to be trusted.
Console> (enable)
```

Related Commands

- show qos info
- show port qos
- set port qos
- set port qos cos

set port rsvp dsbm-election

Use the **set port rsvp dsbm-election** command to specify whether or not the switch participates in the DSBM election on that particular segment.

set port rsvp *mod/port* dsbm-election enable | disable [*dsbm_priority*]

Syntax Description		
	<i>mod/port</i>	Number of the module and the port.
	enable	Keyword to enable participation in the DSBM election.
	disable	Keyword to disable participation in the DSBM election.
	<i>dsbm_priority</i>	(Optional) DSBM priority; valid values are from 128 to 255.

Defaults The default is DSBM is disabled; the default *dsbm_priority* is 128.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command is not supported by the NAM.

Examples This example shows how to enable participation in the DSBM election:

```
Console> (enable) set port rsvp 2/1,3/2 dsbm-election enable 232
DSBM election enabled for ports 2/1,3/2.
DSBM priority set to 232 for ports 2/1,3/2.
This DSBM priority will be used during the next election process.
Console> (enable)
```

This example shows how to disable participation in the DSBM election:

```
Console> (enable) set port rsvp 2/1 dsbm-election disable
DSBM election disabled for ports(s) 2/1.
Console> (enable)
```

This example shows the output when you enable participation in the DSBM election on a port that is not forwarding:

```
Console> (enable) set port rsvp 2/1,3/2 dsbm-election enable 232
DSBM enabled and priority set to 232 for ports 2/1,3/2.
Warning: Port 2/1 not forwarding. DSBM negotiation will start after port starts forwarding on the native
vlan.
Console> (enable)
```

Related Commands **show port rsvp**

set port security

Use the **set port security** command set to configure port security on a port or range of ports.

```
set port security mod/ports... [enable | disable] [mac_addr] [age {age_time}]
[maximum {num_of_mac}] [shutdown {shutdown_time}] [violation
{shutdown | restrict}]
```

Syntax Description	
<i>mod/ports...</i>	Number of the module and the ports on the module.
enable	(Optional) Keyword to enable port security.
disable	(Optional) Keyword to disable port security.
<i>mac_addr</i>	(Optional) Secure MAC address of the enabled port.
age <i>age_time</i>	(Optional) Keyword and variable to specify the duration for which addresses on the port will be secured; valid values are 0 (to disable) and from 10 to 1440 (minutes).
maximum <i>num_of_mac</i>	(Optional) Keyword and variable to specify the maximum number of MAC addresses to secure on the port; valid values are from 1 to 1025.
shutdown <i>shutdown_time</i>	(Optional) Keyword and variable to specify the duration for which a port will remain disabled in case of a security violation; valid values are 0 (to disable) and from 10 to 1440 (minutes).
violation	(Optional) Keyword to specify the action to be taken in the event of a security violation.
shutdown	Keyword to shut down the port in the event of a security violation.
restrict	Keyword to restrict packets from unsecure hosts.

Defaults

The default port security configuration is as follows:

- Port security is disabled.
- Number of secure addresses per port is one.
- Violation action is shutdown.
- Age is permanent (addresses are not aged out).
- Shutdown time is indefinite.

Command Types

Switch command.

Command Modes Privileged.

Usage Guidelines This command is not supported by the NAM.

If you enter the **set port security enable** command but do not specify a MAC address, the first MAC address seen on the port becomes the secure MAC address.

You can specify the number of MAC addresses to secure on a port. You can add MAC addresses to this list of secure addresses. The maximum number is 1024.

The **set port security violation** command allows you to specify whether you want the port to shut down or to restrict access to insecure MAC addresses only. The shutdown time allows you to specify the duration of shutdown in the event of a security violation.

Examples This example shows how to set port security with a learned MAC address:

```
Console> (enable) set port security 3/1 enable
Port 3/1 port security enabled with the learned mac address.
Console> (enable)
```

This example shows how to set port security with a specific MAC address:

```
Console> (enable) set port security 3/1 enable 01-02-03-04-05-06
Port 3/1 port security enabled with 01-02-03-04-05-06 as the secure mac address.
Console> (enable)
```

This example sets the shutdown time to 600 minutes on port 7/7:

```
Console> (enable) set port security 7/7 shutdown 600
Secure address shutdown time set to 600 minutes for port 7/7.
Console> (enable)
```

This example sets the port to drop all packets that are coming in on the port from insecure hosts:

```
Console> (enable) set port security 7/7 violation restrict
Port security violation on port 7/7 will cause insecure packets to be dropped.
Console> (enable)
```

Related Commands **show port security**
clear port security

set port speed

Use the **set port speed** command to configure the speed of a port interface. You can configure the speed of a Fast Ethernet interface.

```
set port speed mod/port { 10 | 100 | auto }
```

Syntax Description	<i>mod/port</i> Number of the module and the port on the module.
	10 100 auto Keyword to set a port speed to 10 Mbps, 100 Mbps, or autospeed detection mode.

Defaults The default is **auto**.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines You can configure Fast Ethernet interfaces on the 10/100-Mbps Fast Ethernet switching module to either 10 or 100 Mbps, or to autosensing mode, allowing the interfaces to sense and distinguish between 10- and 100-Mbps port transmission speeds and full-duplex or half-duplex port transmission types at a remote port connection. If you set the interfaces to autosensing, they configure themselves automatically to operate at the proper speed and transmission type.

This command is not supported by the Gigabit Ethernet switching module or the NAM.

Examples This example shows how to configure port 1, module 2 to auto:

```
Console> (enable) set port speed 2/1 auto
Port 2/1 speed set to auto-sensing mode.
Console> (enable)
```

This example shows how to configure the port speed on port 2, module 2 to 10 Mbps:

```
Console> (enable) set port speed 2/2 10
Port 2/2 speed set to 10 Mbps.
Console> (enable)
```

Related Commands **show port**

set port trap

Use the **set port trap** command to enable or disable the operation of the standard SNMP link trap (up or down) for a port or range of ports.

```
set port trap mod/port {enable | disable}
```

Syntax Description	<i>mod/port</i>	Number of the module and the port on the module.
	enable	Keyword to activate the SNMP link trap.
	disable	Keyword to deactivate the SNMP link trap.

Defaults The default is all port traps are disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command is not supported by the NAM.
To set SNMP traps, enter the **set snmp trap** command.

Examples This example shows how to enable the SNMP link trap for module 1, port 2:

```
Console> (enable) set port trap 1/2 enable
Port 1/2 up/down trap enabled.
Console> (enable)
```

Related Commands

- set port disable**
- set port duplex**
- set port enable**
- set port speed**
- show port**

set port voice interface dhcp

Use the **set port voice interface dhcp** command to set the port voice interface for the DHCP, TFTP, and DNS servers.

```
set port voice interface mod/port dhcp enable [vlan vlan]
```

```
set port voice interface mod/port dhcp disable {ipaddrspec} {tftp ipaddr} [vlan vlan]  
[gateway ipaddr] [dns [ipaddr] [domain_name]]
```

Syntax Description		
<i>mod/port</i>		Number of the module and the port on the module.
enable		Keyword to activate the SNMP link trap.
vlan <i>vlan</i>		(Optional) Keyword and variable to specify a VLAN interface.
disable		Keyword to deactivate the SNMP link trap.
<i>ipaddrspec</i>		IP address and mask; see the “Usage Guidelines” section for format instructions.
tftp <i>ipaddr</i>		Keyword and variable to specify the number of the TFTP server IP address or IP alias in dot notation a.b.c.d.
gateway <i>ipaddr</i>		(Optional) Keyword and variable to specify the number of the gateway server IP address or IP alias in dot notation a.b.c.d.
dns		(Optional) Keyword to specify the DNS server.
<i>ipaddr</i>		(Optional) Number of the DNS IP address or IP alias in dot notation a.b.c.d.
<i>domain_name</i>		(Optional) Name of the domain.

Defaults This command has no default setting.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The *ipaddrspec* format is {*ipaddr*} {*mask*} or {*ipaddr*}/{*mask*} {*mask*}. The *mask* is a dotted format (255.255.255.0) or number of bits (0 to 31).

You can specify a single port only when setting the IP address.

If you enable DHCP on a port, the port obtains all other configuration information from the TFTP server. When you disable DHCP on a port, the following mandatory parameters must be specified:

- If you do not specify DNS parameters, the software uses the system DNS configuration on the supervisor engine to configure the port.
- You cannot specify more than one port at a time because a unique IP address must be set for each port.

Examples

This example shows how to enable the port voice interface for the DHCP server:

```
Console> (enable) set port voice interface 7/4-8 dhcp enable
Port 7/4 DHCP enabled.
Console> (enable)
```

This example shows how to disable the set port voice interface DHCP server:

```
Console> (enable) set port voice interface 7/3 dhcp disable 171.68.111.41/24 tftp
173.32.43.11 dns 172.20.34.204 cisco.com
Port 7/3 dhcp disabled.
System DNS configurations applied.
Console> (enable)
```

This example shows how to enable the port voice interface for the DHCP server with a specified VLAN:

```
Console> (enable) set port voice interface 7/4-6 dhcp enable vlan 3
Vlan 3 configuration successful
Ports 7/4-6 DHCP enabled.
Console> (enable)
```

This example shows how to enable the port voice interface for the TFTP, DHCP, and DNS servers:

```
Console> (enable) set port voice interface dhcp enable 4/2 171.68.111.41 tftp
173.32.43.11 dhcp 198.98.4.1 dns 189.69.24.192
Port 4/2 interface set.
IP address: 171.68.111.41 netmask 255.255.0.0
TFTP server: 173.32.43.11
DHCP server: 198.98.4.1
DNS server: 189.69.24.192
Console> (enable)
```

This example shows how to enable a single port voice interface:

```
Console> (enable) set port voice interface 4/2-9 123.23.32.1/24
Single port must be used when setting the IP address.
Console> (enable)
```

Related Commands **show port voice interface**

set power redundancy

Use the **set power redundancy** command to turn redundancy between the power supplies on or off.

set power redundancy enable | disable

Syntax Description	<table><tr><td>enable</td><td>Keyword to activate redundancy between the power supplies.</td></tr><tr><td>disable</td><td>Keyword to deactivate redundancy between the power supplies.</td></tr></table>	enable	Keyword to activate redundancy between the power supplies.	disable	Keyword to deactivate redundancy between the power supplies.
enable	Keyword to activate redundancy between the power supplies.				
disable	Keyword to deactivate redundancy between the power supplies.				
Defaults	The default is power redundancy is enabled.				
Command Types	Switch command.				
Command Modes	Privileged.				
Usage Guidelines	<p>In a system with dual power supplies, this command turns redundancy between the power supplies on or off. In a redundant configuration, the power available to the system is the maximum power capability of the weakest supply.</p> <p>In a nonredundant configuration, the power available to the system is the sum of the power capability of both supplies.</p>				
Examples	<p>This example shows how to activate redundancy between power supplies:</p> <pre>Console> (enable) set power redundancy enable Power supply redundancy enabled.</pre> <p>This example shows how to deactivate redundancy between power supplies:</p> <pre>Console> (enable) set power redundancy disable Power supply redundancy disabled. Console> (enable)</pre>				
Related Commands	<p>show system</p> <p>show environment</p>				

set prompt

Use the **set prompt** command to change the prompt for the CLI.

set prompt *prompt_string*

Syntax Description	<i>prompt_string</i> String to use as the command prompt.
---------------------------	---

Defaults	The default is the prompt is set to Console>.
-----------------	---

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

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

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

Examples	This example shows how to set the prompt to system100>:
-----------------	---

```
Console> (enable) set prompt system100>
system100> (enable)
```

Related Commands	set system name
-------------------------	------------------------

set protocolfilter

Use the **set protocolfilter** command to activate or deactivate protocol filtering on Ethernet VLANs and on nontrunking Ethernet, Fast Ethernet, and Gigabit Ethernet ports.

set protocolfilter { enable | disable }

Syntax Description

enable	Keyword to activate protocol filtering.
disable	Keyword to deactivate protocol filtering.

Defaults

The default is protocol filtering is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Protocol filtering is supported only on Ethernet VLANs and on nontrunking EtherChannel ports.

Examples

This example shows how to activate protocol filtering:

```
Console> (enable) set protocolfilter enable
Protocol filtering enabled on this switch.
Console> (enable)
```

This example shows how to deactivate protocol filtering:

```
Console> (enable) set protocolfilter disable
Protocol filtering disabled on this switch.
Console> (enable)
```

Related Commands

show protocolfilter

set pvlan

Use the **set pvlan** command to bind the isolated or community VLAN to the primary VLAN and assign the isolated or community ports to the private VLAN.

```
set pvlan primary_vlan {isolated_vlan | community_vlan} [mod/port]
```



Caution

We recommend that you read and understand the “Configuring VLANs” chapter in the *Catalyst 6000 Family Software Configuration Guide* before using this command.

Syntax Description	
<i>primary_vlan</i>	Number of the primary VLAN.
<i>isolated_vlan</i>	Number of the isolated VLAN.
<i>community_vlan</i>	Number of the community VLAN.
<i>mod/port</i>	(Optional) Module and port numbers of the isolated or community ports.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines You must set the primary VLAN, isolated VLAN, and community VLANs using the **set vlan pvlan-type** command before making the association with the **set pvlan** command.

Each isolated or community VLAN can have only one primary VLAN associated with it. A primary VLAN may have one isolated and/or multiple community VLANs associated to it.

Examples This example shows how to map VLANs 901, 902, and 903 (isolated or community VLANs) to VLAN 7 (the primary VLAN):

```
Console> (enable) set pvlan 7 901 4/3
Port 4/3 is successfully assigned to vlan 7, 901 and is made an isolated port.
Console> (enable) set pvlan 7 902 4/4-5
Ports 4/4-5 are successfully assigned to vlan 7, 902 and are made community ports.
Console> (enable) set pvlan 7 903 4/6-7
Ports 4/6-7 are successfully assigned to vlan 7, 903 and are made community ports.
Console> (enable)
```

Related Commands

set vlan
show vlan
set pvlan mapping
clear vlan
clear config pvlan
clear pvlan mapping
show pvlan
show pvlan mapping

set pvlan mapping

Use the **set pvlan mapping** command to map isolated or community VLANs to the primary VLAN on the promiscuous port.

```
set pvlan mapping primary_vlan {isolated_vlan | community_vlan} {mod/port}
```

Syntax Description		
	<i>primary_vlan</i>	Number of the primary VLAN.
	<i>isolated_vlan</i>	Number of the isolated VLAN.
	<i>community_vlan</i>	Number of the community VLAN.
	<i>mod/port</i>	Module and port number of the promiscuous port.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines You must set the primary VLAN, isolated VLANs, and community VLANs using the **set vlan pvlan-type** command bound with the **set pvlan** command, before you can apply the VLANs on any of the promiscuous ports with the **set pvlan mapping** command.

You should connect the promiscuous port to an external device for the ports in the private VLAN to communicate with any other device outside the private VLAN.

You should apply this command for each primary or isolated (community) association in the private VLAN.

Examples This example shows how to remap community VLAN 903 to the primary VLAN 901 on ports 3 through 5 on module 8:

```
Console> (enable) set pvlan mapping 901 903 8/3-5
Successfully set mapping between 901 and 903 on 8/3-5.
Console> (enable)
```

Related Commands

- set vlan**
- show vlan**
- set pvlan**
- clear vlan**
- clear pvlan mapping**
- show pvlan**
- show pvlan mapping**

set qos

Use the **set qos** command to turn on or turn off QoS functionality on the switch.

set qos enable | disable

Syntax Description	enable Keyword to activate QoS functionality.
	disable Keyword to deactivate QoS functionality.
Defaults	The default is QoS functionality is disabled.
Command Types	Switch command.
Command Modes	Privileged.
Usage Guidelines	<p>Refer to the <i>Catalyst 6000 Family Software Configuration Guide</i> for information on how to change the QoS default configurations.</p> <p>When you enable and disable QoS in quick succession, a bus timeout might occur.</p> <p>If you enable or disable QoS on channel ports with different port types, channels might break or form.</p>
Examples	<p>This example shows how to enable QoS:</p> <pre>Console> (enable) set qos enable <...trunking reset messages deleted ...> QoS is enabled. Console> (enable)</pre> <p>This example shows how to disable QoS:</p> <pre>Console> (enable) set qos disable <...trunking reset messages deleted ...> QoS is disabled. Console> (enable)</pre>
Related Commands	show qos info

set qos acl default-action

Use the **set qos acl default-action** command set to set the ACL default actions.

```
set qos acl default-action ip {dscp {dscp} | trust-cos | trust-ipprec | trust-dscp}
[microflow microflow_name] [aggregate aggregate_name]
```

```
set qos acl default-action ipx {dscp {dscp} | trust-cos} [microflow microflow_name]
[aggregate aggregate_name]
```

```
set qos acl default-action ipx | mac {dscp {dscp} | trust-cos}
[aggregate aggregate_name]
```

Syntax Description		
ip		Keyword to specify the IP ACL default actions.
dscp <i>dscp</i>		Keyword and variable to set the DSCP to be associated with packets matching this stream.
trust-cos		Keyword to specify DSCP is derived from the packet CoS.
trust-ipprec		Keyword to specify DSCP is derived from the packet's IP precedence.
trust-dscp		Keyword to specify DSCP is contained in the packet already.
microflow <i>microflow_name</i>	(Optional)	Keyword and variable to specify the name of the microflow policing rule to be applied to packets matching the ACE.
aggregate <i>aggregate_name</i>	(Optional)	Keyword and variable to specify the name of the aggregate policing rule to be applied to packets matching the ACE.
ipx		Keyword to specify the IPX ACL default actions.
mac		Keyword to specify the MAC ACL default actions.

Defaults The default is no ACL is set up. When you enable QoS, the default-action is to classify everything to best effort and to do no policing. When you disable QoS, the default-action is **trust-dscp** on all packets and no policing.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines Configurations you make by entering this command are saved to NVRAM and the switch and do not require that you enter the **commit** command.

Examples

This example shows how to set up the IP ACL default actions:

```
Console> (enable) set qos acl default-action ip dscp 5 microflow micro aggregate agg
QoS default-action for IP ACL is set successfully.
Console> (enable)
```

This example shows how to set up the IPX ACL default actions:

```
Console> (enable) set qos acl default-action ipx dscp 5 microflow micro aggregate agg
QoS default-action for IPX ACL is set successfully.
Console> (enable)
```

This example shows how to set up the MAC ACL default actions:

```
Console> (enable) set qos acl default-action mac dscp 5 microflow micro aggregate agg
QoS default-action for MAC ACL is set successfully.
Console> (enable)
```

Related Commands

show qos acl info
clear qos acl

set qos acl ip

Use the **set qos acl ip** command set to create or add IP access lists.

```
set qos acl ip {acl_name} {dscp dscp | trust-cos | trust-ipprec | trust-dscp}
[microflow microflow_name] [aggregate aggregate_name] {src_ip_spec}
[before editbuffer_index | modify editbuffer_index]
```

```
set qos acl ip {acl_name} {dscp dscp | trust-cos | trust-ipprec | trust-dscp}
[microflow microflow_name] [aggregate aggregate_name] {protocol} {src_ip_spec}
{dest_ip_spec} [precedence precedence | dscp-field dscp] [before editbuffer_index |
modify editbuffer_index]
```

```
set qos acl ip {acl_name} {dscp dscp | trust-cos | trust-ipprec | trust-dscp}
[microflow microflow_name] [aggregate aggregate_name] icmp {src_ip_spec}
{dest_ip_spec} [icmp_type [icmp_code] | icmp_message] [precedence precedence |
dscp-field dscp] [before editbuffer_index | modify editbuffer_index]
```

```
set qos acl ip {acl_name} {dscp dscp | trust-cos | trust-ipprec | trust-dscp}
[microflow microflow_name] [aggregate aggregate_name] igmp {src_ip_spec}
{dest_ip_spec} [igmp_type] [precedence precedence | dscp-field dscp]
[before editbuffer_index | modify editbuffer_index]
```

```
set qos acl ip {acl_name} {dscp dscp | trust-cos | trust-ipprec | trust-dscp}
[microflow microflow_name] [aggregate aggregate_name] tcp {src_ip_spec} [{operator}
{port} [port]] {dest_ip_spec} [{operator} {port} [port]] [established]
[precedence precedence | dscp-field dscp] [before editbuffer_index |
modify editbuffer_index]
```

```
set qos acl ip {acl_name} {dscp dscp | trust-cos | trust-ipprec | trust-dscp}
[microflow microflow_name] [aggregate aggregate_name] udp {src_ip_spec} [{operator}
{port} [port]] {dest_ip_spec} [{operator} {port} [port]] [precedence precedence |
dscp-field dscp] [before editbuffer_index | modify editbuffer_index]
```

Syntax Description

<i>acl_name</i>	Unique name that identifies the list to which the entry belongs.
dscp <i>dscp</i>	Keyword and variable to set CoS and DSCP from configured DSCP values.
trust-cos	Keyword to specify DSCP is derived from the packet CoS.
trust-ipprec	Keyword to specify DSCP is derived from the packet's IP precedence.
trust-dscp	Keyword to specify DSCP is contained in the packet already.
microflow <i>microflow_name</i>	(Optional) Keyword and variable to specify the name of the microflow policing rule to be applied to packets matching the ACE.
aggregate <i>aggregate_name</i>	(Optional) Keyword and variable to specify the name of the aggregate policing rule to be applied to packets matching the ACE.
<i>src_ip_spec</i>	Source IP address and the source mask. See the "Usage Guidelines" section for the format.
before <i>editbuffer_index</i>	(Optional) Keyword and variable to insert the new ACE in front of another ACE.
modify <i>editbuffer_index</i>	(Optional) Keyword and variable to replace an ACE with the new ACE.

<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 and corresponding numbers.
<i>dest_ip_spec</i>	Destination IP address and the destination mask. See the “Usage Guidelines” section for the format.
precedence <i>precedence</i>	(Optional) Keyword and variable to specify the precedence level to compare with in incoming packet; valid values are from 0 to 7 or by name. See the “Usage Guidelines” section for a list of valid names.
dscp-field <i>dscp</i>	(Optional) Keyword and variable to specify the DSCP field level to compare with an incoming packet. Valid values are from 0 to 7 or by name; valid names are critical, flash, flash-override, immediate, internet, network, priority, and routine.
icmp	Keyword to specify ICMP.
<i>icmp-type</i>	(Optional) ICMP message type; valid values are from 0 to 255.
<i>icmp-code</i>	(Optional) ICMP message code; valid values are from 0 to 255.
<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.
igmp	Keyword to specify IGMP.
<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 numbers.
tcp	Keyword to specify TCP.
<i>operator</i>	(Optional) Operands; valid values include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).
<i>port</i>	(Optional) TCP or UDP port number or name; valid port numbers are from 0 to 65535. See the “Usage Guidelines” section for a list of valid names.
established	(Optional) For TCP protocol only—Keyword to specify an established connection.
udp	Keyword to specify UDP.

Defaults The default is there are no ACLs.

Command Types Switch command.

Command Modes Privileged.

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

Use the **show qos acl info** command to view the edit buffer.

The **dscp** *dscp*, **trust-cos**, **trust-ipprec**, and **trust-dscp** keywords and variables are used to select a marking rule. Refer to the *Catalyst 6000 Family Software Configuration Guide* for additional marking rule information.

The optional **microflow** *microflow_name*, **aggregate** *aggregate_name* keywords and variables are used to configure policing in the ACE. Refer to the *Catalyst 6000 Family Software Configuration Guide* for additional policing rule information.

The *src_ip_spec*, optional **precedence** *precedence*, or **dscp-field** *dscp* keywords and variables, are used to configure filtering.

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

- Maximum of 31 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 protocol 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 only.

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.

If no layer protocol number is entered, you can use this syntax:

```
set qos acl ip {acl_name} {dscp dscp | trust-cos | trust-ipprec | trust-dscp}
    [microflow microflow_name] [aggregate aggregate_name] {src_ip_spec}
    [before editbuffer_index | modify editbuffer_index]
```

If a Layer 4 protocol is specified, you can use this syntax:

```
set qos acl ip {acl_name} {dscp dscp | trust-cos | trust-ipprec | trust-dscp}
    [microflow microflow_name] [aggregate aggregate_name] {protocol} {src_ip_spec}
    {dest_ip_spec} [precedence precedence | dscp-field dscp] [before editbuffer_index |
    modify editbuffer_index]
```

If ICMP is used, you can use this syntax:

```
set qos acl ip {acl_name} {dscp dscp | trust-cos | trust-ipprec | trust-dscp}
    [microflow microflow_name] [aggregate aggregate_name] icmp {src_ip_spec}
    {dest_ip_spec} [icmp_type icmp_code] | icmp_message] [precedence precedence |
    dscp-field dscp] [before editbuffer_index | modify editbuffer_index]
```

If IGMP is used, you can use this syntax:

```
set qos acl ip {acl_name} {dscp dscp | trust-cos | trust-ipprec | trust-dscp}
    [microflow microflow_name] [aggregate aggregate_name] igmp {src_ip_spec}
    {dest_ip_spec} [igmp_type] [precedence precedence | dscp-field dscp]
    [before editbuffer_index | modify editbuffer_index]
```

If TCP is used, you can use this syntax:

```
set qos acl ip {acl_name} {dscp dscp | trust-cos | trust-ipprec | trust-dscp}
    [microflow microflow_name] [aggregate aggregate_name] tcp {src_ip_spec} [{operator}
    {port} [port]] {dest_ip_spec} [{operator} {port} [port]] [established]
    [precedence precedence | dscp-field dscp] [before editbuffer_index |
    modify editbuffer_index]
```

If UDP is used, you can use this syntax:

```
set qos acl ip {acl_name} {dscp dscp | trust-cos | trust-ipprec | trust-dscp}
  [microflow microflow_name] [aggregate aggregate_name] udp {src_ip_spec} [{operator}
  {port} [port]] {dest_ip_spec} [{operator {port} [port]}] [precedence precedence |
  dscp-field dscp] [before editbuffer_index | modify editbuffer_index]
```

Examples

This example shows how to define a TCP access list:

```
Console> (enable) set qos acl ip my_acl trust-dscp microflow my-micro tcp 1.2.3.4
255.0.0.0 eq port 21 172.20.20.1 255.255.255.0
my_acl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

This example shows how to define an ICMP access list:

```
Console> (enable) set qos acl ip icmp_acl trust-dscp microflow my-micro icmp 1.2.3.4
255.255.0.0 172.20.20.1 255.255.255.0 precedence 3
my_acl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

Related Commands

```
show qos acl info
clear qos acl
rollback
commit
```

set qos acl ipx

Use the **set qos acl ipx** command set to define IPX access lists.

```
set qos acl ipx {acl_name} {dscp dscp | trust-cos} [aggregate aggregate_name] {protocol}
  {src_net} [dest_net.dest_node] [[dest_net_mask.]dest_node_mask]
  [before editbuffer_index | modify editbuffer_index]
```

Syntax Description	
<i>acl_name</i>	Unique name that identifies the list to which the entry belongs.
dscp <i>dscp</i>	Keyword and variable to set CoS and DSCP from configured DSCP values.
trust-cos	Keyword to specify that the DSCP is derived from the packet CoS.
aggregate <i>aggregate_name</i>	(Optional) Keyword and variable to specify the name of the aggregate policing rule to be applied to packets matching the ACE.
<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) Mask to be applied to destination-node. See the “Usage Guidelines” section for format guidelines.
<i>dest_node</i>	(Optional) Node on destination-network of the packet being sent.
<i>dest_net_mask</i> .	(Optional) Mask to be applied to the the destination network. See the “Usage Guidelines” section for format guidelines.
<i>dest_node_mask</i>	(Optional) Mask to be applied to destination-node. See the “Usage Guidelines” section for format guidelines.
before <i>editbuffer_index</i>	(Optional) Keyword and variable to insert the new ACE in front of another ACE.
modify <i>editbuffer_index</i>	(Optional) Keyword and variable to replace an ACE with the new ACE.

Defaults There are no default ACL mappings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines

The **dscp** *dscp* and **trust-cos** keywords and variables are used to select a marking rule. Refer to the *Catalyst 6000 Family Software Configuration Guide* for additional marking rule information.

The optional **aggregate** *aggregate_name* keyword and variable are used to configure policing in the ACE. Refer to the *Catalyst 6000 Family Software Configuration Guide* for additional policing rule information.

The *src_ip_spec*, optional **precedence** *precedence*, or **dscp-field** *dscp* keywords and variables, are used to configure filtering.

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

- Maximum of 31 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 **nbp** (17), **rip** (1), **sap** (4), and **spx** (5). The IP network number is listed in parentheses.

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 four-digit hexadecimal numbers (xxxx.xxxx.xxxx).

The *destination_mask* is of the form N.H.H.H or H.H.H where N is the destination network mask and H is the node mask. It can be specified only when the destination node is also specified for the destination address.

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 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.ffff.ffff
- 1.2.3.4 ffff.ffff.ffff.ffff

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

Examples This example shows how to create an IPX ACE:

```
Console> (enable) set qos acl ipx my_IPXacl trust-cos aggregate my-agg -1
my_IPXacl editbuffer modified. Use `commit' command to apply changes.
Console> (enable)
```

Related Commands

- show qos acl info**
- clear qos acl**
- rollback**
- commit**

set qos acl mac

Use the **set qos acl mac** command to define MAC access lists.

```
set qos acl mac {acl_name} {dscp dscp | trust-cos} [aggregate aggregate_name]
  {src_mac_addr_spec} {dest_mac_addr_spec} [ether-type] [before editbuffer_index |
  modify editbuffer_index]
```

Syntax Description		
<i>acl_name</i>		Unique name that identifies the list to which the entry belongs.
dscp <i>dscp</i>		Keyword and variable to set CoS and DSCP from configured DSCP values.
trust-cos		Keyword to specify that the DSCP is derived from the packet CoS.
aggregate <i>aggregate_name</i>		(Optional) Keyword and variable to specify the name of the aggregate policing rule to be applied to packets matching the ACE.
<i>src_mac_addr_spec</i>		Number of the source MAC address in the form <i>source_mac_address source_mac_address_mask</i> .
<i>dest_mac_addr_spec</i>		(Optional) Number of the destination MAC address.
<i>ether-type</i>		(Optional) Name or number that matches the ethertype for Ethernet-encapsulated packets. See the “Usage Guidelines” section for a list of valid names and numbers.
before <i>editbuffer_index</i>		(Optional) Keyword and variable to insert the new ACE in front of another ACE.
modify <i>editbuffer_index</i>		(Optional) Keyword and variable to replace an ACE with the new ACE.

Defaults There are no default ACL mappings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The **dscp** *dscp* and **trust-cos** keywords and variables are used to select a marking rule. Refer to the *Catalyst 6000 Family Software Configuration Guide* for additional marking rule information.

The optional **aggregate** *aggregate_name* keyword and variable are used to configure policing in the ACE. Refer to the *Catalyst 6000 Family Software Configuration Guide* for additional policing rule information.

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

- Maximum of 31 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-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 4-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 ff-ff-ff-ff-ff-ff.
- Use **host** source as an abbreviation for a *destination* and *destination-wildcard* of destination 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-lave-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).

The *ether-type* is a 16-bit hexadecimal number written with a leading 0x.

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

Examples

This example shows how to create an Ethernet ACE:

```
Console> (enable) set qos acl ip my_MACacl trust-cos microflow my-micro aggregate my-agg
any any
my_IPXacl editbuffer modified. Use `commit' command to apply changes.
Console> (enable)
```

Related Commands

show qos acl info
clear qos acl
rollback
commit

set qos acl map

Use the **set qos acl map** command to attach an ACL to a specified port or VLAN.

```
set qos acl map acl_name mod/port | vlan
```

Syntax Description	<i>acl_name</i>	Name of the list to which the entry belongs.
	<i>mod/port</i>	Number of the module and the port on the module.
	<i>vlan</i>	Number of the VLAN.

Defaults There are no default ACL mappings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines



Caution

Use the **copy** command to save the ACL configuration to Flash memory.

Examples

This example shows how to attach an ACL to a port:

```
Console> (enable) set qos acl map my_acl 2/1
ACL my_acl is attached to port 2/1.
```

This example shows how to attach an ACL to a VLAN:

```
Console> (enable) set qos acl map ftp_acl 4
ACL ftp_acl is attached to vlan 4.
Console> (enable)
```

This example shows what happens if you try to attach an ACL that has not been committed:

```
Console> (enable) set qos acl map new_acl 4
Commit ACL new_acl before mapping.
Console> (enable)
```

Related Commands

```
show qos acl map
clear qos acl
rollback
commit
```

set qos bridged-microflow-policing

Use the **set qos bridged-microflow-policing** command to enable or disable microflow policing of bridged packets on a per-VLAN basis.

set qos bridged-microflow-policing {enable | disable} *vlanlist*

Syntax Description

enable	Keyword to activate microflow policing functionality.
disable	Keyword to deactivate microflow policing functionality.
<i>vlanlist</i>	List of VLANs; valid values are from 1 to 1000.

Defaults

The default is intraVLAN QoS is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Layer 3 switching engine-based systems do not create NetFlow entries for bridged packets. Without a NetFlow entry, these packets cannot be policed at the microflow level. You must enter the **set qos bridged-microflow-policing enable** command if you want the bridged packets to be microflow policed.

This command is supported on systems configured with a Layer 3 switching engine only.

Examples

This example shows how to enable microflow policing:

```
Console> (enable) set qos bridged-microflow-policing enable 1-1000
QoS microflow policing is enabled for bridged packets on vlans 1-1000.
Console> (enable)
```

This example shows how to disable microflow policing:

```
Console> (enable) set qos bridged-microflow-policing disable 10
QoS microflow policing is disabled for bridged packets on VLAN 10.
Console> (enable)
```

Related Commands

show qos bridged-packet-policing

set qos cos-dscp-map

Use the **set qos cos-dscp map** command to set the CoS-to-DSCP mapping.

```
set qos cos-dscp-map dscp1 dscp2... dscp8
```

Syntax Description	<i>dscp#</i>	Number of the DSCP; valid values are from 0 to 63.
--------------------	--------------	--

Defaults	The default CoS-to-DSCP configuration is listed in Table 2-12.
----------	--

Table 2-12 CoS-to-DSCP Mapping

CoS	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

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

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

Usage Guidelines	The CoS-to-DSCP map is used to map the CoS of packets arriving on trusted ports (or flows) to a DSCP where the trust type is trust-cos . This map is a table of eight CoS values (0 through 7) and their corresponding DSCP values. The switch has one map.
------------------	--

This command is supported on systems configured with a Layer 3 switching engine only.

Examples	This example shows how to set the CoS-to-DSCP mapping:
----------	--

```
Console> (enable) set qos cos-dscp-map 20 30 1 43 63 12 13 8
QoS cos-dscp-map set successfully.
Console> (enable)
```

Related Commands	clear qos cos-dscp-map show qos maps
------------------	---

set qos drop-threshold

Use the **set qos drop-threshold** command to program the transmit and receive drop thresholds on all ports in the system.

```
set qos drop-threshold 2q2t tx queue q# thr1 thr2
```

```
set qos drop-threshold {1q4t | 1p1q4t} rx queue q# thr1 thr2 thr3 thr4
```

Syntax Description	
2q2t tx	Keywords to specify the transmit drop threshold.
1q4t 1p1q4t rx	Keywords to specify the receive drop threshold.
queue q#	Keyword and variable to specify the queue; valid values are 1 and 2.
<i>thr1, thr2, thr3, thr4</i>	Threshold percentage; valid values are from 1 to 100.

Defaults

If you enable QoS, the following defaults apply:

- Transmit drop thresholds:
 - queue 1—80%, 100%
 - queue 2—80%, 100%
- Receive drop thresholds:
 - queue 1—50%, 60%, 80%, 100% if the port is trusted
 - queue 2—100%, 100%, 100%, 100% if the port is untrusted

If you disable QoS, the following defaults apply:

- Transmit drop thresholds:
 - queue 1—100%, 100%
 - queue 2—100%, 100%
- Receive drop thresholds: queue 1—100%, 100%, 100%, 100%

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The number preceding the **t** letter in the *port_type* (**2q2t**, **1q4t**, or **1p1q4t**) determines the number of threshold values the hardware supports. For example, with **2q2t**, the number of thresholds specified is two; with **1q4t** and **1p1q4t**, the number of thresholds specified is four. Due to the granularity of programming the hardware, the values set in hardware will be close approximations of the values provided.

The number preceding the **q** letter in the *port_type* determines the number of the queues that the hardware supports. For example, with **2q2t**, the number of queues specified is two; with **1q4t** and **1p1q4t**, the number of queues specified is four. The system defaults for the transmit queues attempt to keep the maximum latency through a port at a maximum of 10 ms.

The number preceding the **p** letter in the **1p1q4t** port types determines the threshold in the priority queue.

When you configure the drop threshold for **1q1q4t**, the drop threshold for the second queue is 100 percent and is not configurable.

The thresholds are all specified as percentages; 10 indicates a threshold when the buffer is 10 percent full.

The single-port ATM OC-12 module does not support transmit queue drop thresholds.

Examples

This example shows how to assign the transmit drop threshold:

```
Console> (enable) set qos drop-threshold 2q2t tx queue 1 40 80
Transmit drop thresholds for queue 1 set at 40% and 80%
Console> (enable)
```

These examples show how to assign the receive drop threshold:

```
Console> (enable) set qos drop-threshold 1q4t rx queue 1 40 50 60 100
Receive drop thresholds for queue 1 set at 40% 50% 60% 100%
Console> (enable)
```

```
Console> (enable) set qos drop-threshold 1p1q4t rx queue 1 40 50 60 100
Receive drop thresholds for queue 1 set at 40% 50% 60% 100%
Console> (enable)
```

Related Commands

show qos info

set qos dscp-cos-map

Use the **set qos dscp-cos-map** command to set the DSCP-to-CoS mapping.

```
set qos dscp-cos-map dscp_list:cos_value ...
```

Syntax Description	
<i>dscp_list</i>	Number of the DSCP; valid values are from 0 to 63.
<i>cos_value...</i>	Number of the CoS; valid values are from 0 to 7.

Defaults

The default DSCP-to-CoS configuration is listed in Table 2-13.

Table 2-13 DSCP-to-CoS Mapping

DSCP	0 to 7	8 to 15	16 to 23	24 to 31	32 to 39	40 to 47	48 to 55	56 to 63
CoS	0	1	2	3	4	5	6	7

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The DSCP-to-CoS map is used to map the final DSCP classification to a final CoS. This final map determines the output queue and threshold to which the packet is assigned. The CoS map is written into the ISL header or 802.1Q tag of the transmitted packet on trunk ports and contains a table of 64 DSCP values and their corresponding CoS values. The switch has one map.

This command is supported on systems configured with a Layer 3 switching engine only.

Examples

This example shows how to set the DSCP-to-CoS mapping:

```
Console> (enable) set qos dscp-cos-map 20-25:7 33-38:3
QoS dscp-cos-map set successfully.
Console> (enable)
```

Related Commands

```
show qos maps
clear qos map
```

set qos ipprec-dscp-map

Use the **set qos ipprec-dscp-map** command to set the IP precedence-to-DSCP map. This command applies to all packets and all ports.

set qos ipprec-dscp-map *dscp1 ... dscp8*

Syntax Description	<i>dscp1#</i> Number of the IP precedence value; up to eight values can be specified.
---------------------------	---

Defaults	The default IP precedence-to-DSCP configuration is listed in Table 2-14.
-----------------	--

Table 2-14 IP Precedence-to-DSCP Mapping

IPPREC	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

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

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

Usage Guidelines	Use this command to map the IP precedence of IP packets arriving on trusted ports (or flows) to a DSCP when the trust type is trust-ipprec . This map is a table of eight precedence values (0 through 7) and their corresponding DSCP values. The switch has one map. The IP precedence values are as follows:
-------------------------	--

- network 7
- internet 6
- critical 5
- flash-override 4
- flash 3
- immediate 2
- priority 1
- routine 0

This command is supported on systems configured with a Layer 3 switching engine only.

Examples	This example shows how to assign IP precedence-to-DSCP mapping and return to the default:
-----------------	---

```
Console> (enable) set qos ipprec-dscp-map 20 30 1 43 63 12 13 8
QoS ipprec-dscp-map set successfully.
Console> (enable)
```

Related Commands

show qos maps
clear qos ipprec-dscp-map

set qos mac-cos

Use the **set qos mac-cos** command to set the CoS value to the 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, higher numbers represent higher priority.

Defaults This command has no default setting.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command has no effect on a switch configured with a PFC because the Layer 3 switching engine's result always overrides the Layer 2 result.

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

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

The CoS for a packet going to the specified MAC address is overwritten even if it is coming from a trusted port.

If you enter the **show cam** command, entries made with the **set qos mac-cos** command display as dynamic because QoS considers them to be dynamic, but they do not age out.

Examples This example shows how to assign the CoS value 3 to VLAN 2:

```
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 map a specific CoS value to one of the transmit or receive priority queues and one of the thresholds per available priority queue for all ports.

```
set qos map port_type tx | rx q# thr# cos coslist
```

Syntax Description

<i>port_type</i>	Port type; valid values are 2q2t and 1p2q2t for transmit and 1p1q4t for receive. The same mapping is used for both the receive and transmit directions.
tx	Keyword to specify the transmit queue.
rx	Keyword to specify the receive queue.
<i>q#</i>	Value determined by the number of priority queues provided at the transmit or receive end; valid values are 1 and 2, with the higher value indicating a higher priority queue.
<i>thr#</i>	Value determined by the number of drop thresholds available at a port; valid values are 1 and 2, with the higher value indicating lower chances of being dropped.
cos coslist	Keyword and variable to specify CoS values; valid values are from 0 through 7, with the higher numbers representing a higher priority.

Defaults

The default mappings for all ports are shown in Table 2-4 and Table 2-5.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can enter the *cos_list* variable as a single CoS value, multiple noncontiguous CoS values, a range of CoS values, or a mix of values. For example, you can enter any of the following: 0, or 0,2,3, or 0-3,7.

When specifying the priority queue for the **1p2q2t** *port_type*, the priority queue number is 3 and the threshold number is 1.

The receive and transmit drop thresholds have this relationship:

- Receive queue 1 (standard) threshold 1 = transmit queue 1 (standard low priority) threshold 1
- Receive queue 1 (standard) threshold 2 = transmit queue 1 (standard low priority) threshold 2
- Receive queue 1 (standard) threshold 3 = transmit queue 2 (standard high priority) threshold 1
- Receive queue 1 (standard) threshold 4 = transmit queue 2 (standard high priority) threshold 2

Examples

This example shows how to assign the CoS values 1, 2, and 5 to the first queue and the first drop threshold in that queue:

```
Console> (enable) set qos map 2q2t tx 1 1 cos 1,2,5
Qos tx priority queue and threshold mapped to cos successfully.
Console> (enable)
```

This example shows how to assign the CoS values to queue 1 and threshold 2 in that queue:

```
Console> (enable) set qos map 2q2t tx 1 2 cos 3-4,7
Qos tx priority queue and threshold mapped to cos successfully.
Console> (enable)
```

This example shows how to assign the CoS values 1, 2, and 5 to the first queue and the first drop threshold in that queue:

```
Console> (enable) set qos map 1p2q2t tx 1 1 cos 1,2,5
Qos tx priority queue and threshold mapped to cos successfully.
Console> (enable)
```

This example shows how to map the CoS value 7 to strict priority transmit queue 3/drop threshold 1:

```
Console> (enable) set qos map 1p2q2t tx 3 1 cos 7

Qos tx strict queue and threshold mapped to cos successfully.
Console> (enable)
```

Related Commands

clear qos map
show qos info

set qos policed-dscp-map

Use the **set qos policed-dscp-map** command to set the mapping of policed in-profile DSCPs.

```
set qos policed-dscp-map in_profile_dscp:policed_dscp...
```

Syntax Description	<i>in_profile_dscp</i> Number of the in-profile DSCP; valid values are from 0 through 63.
	<i>policed_dscp</i> Number of the policed DSCP; valid values are 0 through 63.
Defaults	The default map is no markdown.
Command Types	Switch command.
Command Modes	Privileged.
Usage Guidelines	<p>You can enter <i>in_profile_dscp</i> as a single DSCP, multiple DSCPs, or a range of DSCPs (for example, 1 or 1,2,3 or 1-3,7).</p> <p>The colon between <i>in_profile_dscp</i> and <i>policed_dscp</i> is required.</p> <p>This command is supported on systems configured with a Layer 3 switching engine only.</p>
Examples	<p>This example shows how to set the mapping of policed in-profile DSCPs:</p> <pre>Console> (enable) set qos policed-dscp-map 60-63:60 20-40:5 QoS policed-dscp-map set successfully. Console> (enable)</pre>
Related Commands	<pre>clear qos policed-dscp-map show qos policer show qos maps</pre>

set qos policer

Use the **set qos policer** command to create a policing rule for ACL.

set qos policer microflow *microflow_name* **rate** *rate* **burst** *burst* **drop** | **policed-dscp**

set qos policer aggregate *aggregate_name* **rate** *rate* **burst** *burst* **drop** | **policed-dscp**

Syntax Description		
microflow	<i>microflow_name</i>	Keyword and variable to specify the name of the microflow policing rule.
rate	<i>rate</i>	Keyword and variable to specify the average rate; valid values are from 0 and 32 Kbps to 8 Gbps.
burst	<i>burst</i>	Keyword and variable to specify the burst size; valid values are from 1 Kb to 32 Mb.
drop		Keyword to specify drop traffic.
policed-dscp		Keyword to specify policed DSCP.
aggregate	<i>aggregate_name</i>	Keyword and variable to specify the name of the aggregate policing rule.

Defaults The default is no policing rules or aggregates are configured.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines

Before microflow policing can occur, you must define a microflow policing rule. Policing allows the switch to limit the bandwidth consumed by a flow of traffic.

The Catalyst 6000 family switch supports up to 63 microflow policing rules. When a microflow policer is used in any ACL that is attached to any port or VLAN, the NetFlow flowmask is bumped up to full flow.

Before aggregate policing can occur, you must create an aggregate and a policing rule for that aggregate. The Catalyst 6000 family switch supports up to 1023 aggregates and 1023 policing rules.

The **set qos policer aggregate** command allows you to configure an aggregate flow and a policing rule for that aggregate. When you enter the **microflow** *microflow_name* **rate** *rate* **burst** *burst*, the range for the average rate is 32 Kbps to 8 Gbps and the range for the burst size is 1 Kb (entered as 1) to 32 Mb (entered as 32000). The burst can be set lower, higher, or equal to the rate. Modifying an existing aggregate rate limit entry causes that entry to be modified in NVRAM and in the switch if that entry is currently being used.

**Note**

We recommend a 32-Kb minimum value burst size. Due to the nature of the traffic at different customer sites, coupled with the hardware granularity, smaller values occasionally result in lower rates than the specified rate. If you experiment with smaller values but problems occur, increase the burst rate to this minimum recommended value.

Modifying an existing microflow or aggregate rate limit modifies that entry in NVRAM as well as in the switch if it is currently being used.

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

- Maximum of 31 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

Examples

This example shows how to create a microflow policing rule for ACL:

```
Console> (enable) set qos policer microflow my-micro rate 1000 burst 10000 policed-dscp
QoS policer for microflow my-micro set successfully.
Console> (enable)
```

This example shows how to create an aggregate policing rule for ACL:

```
Console> (enable) set qos policer aggregate my-agg rate 1000 burst 2000 drop
QoS policer for aggregate my-aggset successfully.
Console> (enable)
```

Related Commands

```
clear qos policer
show qos policer
```

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 no COPS servers 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 policy-source**

set qos rsvp

Use the **set qos rsvp** command set to turn on or turn off the RSVP+ feature on the switch, set the time in minutes after which the RSVP+ databases get flushed (when the policy server dies), and set the local policy.

set qos rsvp enable | disable

set qos rsvp policy-timeout *timeout*

set qos rsvp local-policy forward | reject

Syntax Description	enable	disable
	Keyword to activate the RSVP+ feature.	Keyword to deactivate the RSVP+ feature.
	policy-timeout <i>timeout</i>	Keyword and variable to specify the time in minutes after which the RSVP+ databases get flushed; valid values are from 1 to 65535 minutes.
	local-policy forward reject	Keywords to specify the policy configuration local to the network device to either accept existing flows and forward them or not accept new flows.

Defaults The default is the RSVP+ feature is disabled, policy-timeout is 30 minutes, and local-policy is forward.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The local-policy guidelines are as follows:

- There is no connection with the policy server
- New flows that come up after connection with the policy server has been lost
- Old flows after the PDP policy times out

Examples This example shows how to enable RSVP+:

```
Console> (enable) set qos rsvp enable
RSVP enabled. Only RSVP qualitative service supported.
QoS must be enabled for RSVP.
Console> (enable)
```

This example shows how to disable RSVP+:

```
Console> (enable) set qos rsvp disable
RSVP disabled on the switch.
Console> (enable)
```

This example shows how to set the policy-timeout interval:

```
Console> (enable) set qos rsvp policy-timeout 45  
RSVP database policy timeout set to 45 minutes.  
Console> (enable)
```

This example shows how to set the policy-timeout interval:

```
Console> (enable) set qos rsvp local-policy forward  
RSVP local policy set to forward.  
Console> (enable)
```

Related Commands **show qos rsvp**

set qos txq-ratio

Use the **set qos txq-ratio** command to set the amount of packet buffer memory allocated to high-priority traffic and low-priority traffic.

```
set qos txq-ratio port_type queue1_val queue2_val... queueN_val
```

Syntax Description

<i>port_type</i>	Port type; valid values are 2q2t and 1p2q2t .
<i>queue1_val</i>	Percentage of low-priority traffic; valid values are from 1 to 99 and must total 100 with the <i>queue2_val</i> value.
<i>queue2_val</i>	Percentage of high-priority traffic; valid values are from 1 to 99 and must total 100 with the <i>queue1_val</i> value.
<i>queueN_val</i>	Percentage of strict-priority traffic; valid values are from 1 to 99 and must total 100.

Defaults

The default for **2q2t** is 80:20 if you enable QoS, and 100:0 if you disable QoS. The default for **1p2q2t** is 70:15:15 if you enable QoS and 100:0:0 if you disable QoS.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Use caution when using this command. When entering the **set qos txq-ratio** command, all ports go through a link up and down condition.

The values set in hardware will be close approximations of the values provided. For example, even if you specify 0 percent, the actual value programmed will not necessarily be 0.

The **txq** ratio is determined by the traffic mix in the network. Since high-priority traffic is typically a smaller fraction of the traffic and since the high-priority queue gets more service, you should set the high-priority queue lower than the low-priority queue.

The strict priority queue requires no configuration.

Examples

This example shows how to set the transmit queue size ratio:

```
Console> (enable) set qos txq-ratio 2q2t 75 25
QoS txq-ratio is set successfully.
Console> (enable)
```

Related Commands

```
clear qos config
show qos info
```

set qos wred-threshold

Use the **set qos wred-threshold** command to configure the WRED threshold parameters for the specified port type.

```
set qos wred-threshold 1p2q2t tx queue q# thr1 thr2
```

Syntax Description	1p2q2t	Keyword to specify the port type; only valid value is 1p2q2t .
	tx	Keyword to specify the parameters for output queuing; only valid value is tx .
	queue q#	Keyword and variable to specify the queue to which the arguments apply.
	thr1 thr2	Percentage of the buffer size.

Defaults The defaults are queue type is **tx**, threshold 1 is 80 percent, threshold 2 is 100 percent, and the low threshold is picked automatically by the system.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The queue number is 1 for the low-priority standard transmit queue and 2 for the high-priority standard transmit queue. The strict priority queue is not configurable; it uses threshold 2 as specified for queue 2. The thresholds are all specified as percentages, ranging from 1 to 100. A value of 10 indicates a threshold when the buffer is 10 percent full.

Examples This example shows how to configure the low-priority transmit queue drop thresholds:

```
Console> (enable) set qos wred-threshold 1p2q2t tx queue 1 50 60
WRED thresholds for queue 1 set to 50%,60% on all WRED-capable 1p2q2t ports.
Console> (enable)
```

Related Commands

- clear qos config**
- show qos info**

set qos wrr

Use the **set qos wrr** command to specify the weights that determine how many packets will transmit out of one queue before switching to the other queue.

```
set qos wrr port_type queue1_val queue2_val
```

Syntax Description	<p><i>port_type</i> Port type; valid values are 2q2t and 1p2q2t.</p> <p><i>queue1_val</i> Number of weights for queues 1 and 2; valid values are from 1 to 255.</p> <p><i>queue2_val</i></p>
Defaults	The default WRR is 4:255.
Command Types	Switch command.
Command Modes	Privileged.
Usage Guidelines	<p>The WRR weights are used to partition the bandwidth between the queues in the event all queues are not empty. For example, weights of 1:3 mean that one queue gets 25 percent of the bandwidth and the other gets 75 percent as long as both queues have data.</p> <p>Weights of 1:3 do not necessarily lead to the same results as when the weights are 10:30. In the latter case, more data is serviced from each queue and the latency of packets serviced from the other queue goes up. For best results, set the weights so that at least one packet (maximum size) can be serviced from the lower priority queue at a time. For the higher priority queue, set the weights so that multiple packets are serviced at any one time.</p> <p>The values set in hardware will be close approximations of the values provided. For example, even if you specify 0 percent, the actual value programmed will not necessarily be 0. Whatever weights you choose, make sure that the resulting byte values programmed (see the show qos info command with the runtime keyword) are at least equal to the MTU size.</p> <p>The ratio achieved is only an approximation of what you specify since the cutoff is on a packet and midway through a packet. For example, if you specify that the ratio services 1000 bytes out of the low-priority queue, and there is a 1500-byte packet in the low-priority queue, the entire 1500-byte packet is transmitted because the hardware services an entire packet.</p> <p>For 1p2q2t, only two queues can be set; the third queue is strict priority.</p>
Examples	<p>This example shows how to specify the weights for queue 1 and queue 2 to 30 and 70:</p> <pre>Console> (enable) set qos wrr 2q2t 30 70 QoS wrr ratio is set successfully. Console> (enable)</pre>

■ set qos wrr

Related Commands

show qos info
show qos statistics

set radius deadline

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

set radius deadline *minutes*

Syntax Description	<i>minutes</i>	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 since no alternate servers are available. By default, the deadline is 0 minutes; the RADIUS servers are not 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	<p>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 characters except tabs.</p> <p>If you configure a RADIUS key on the switch, make sure you configure an identical key on the RADIUS server.</p>
-------------------------	---

Examples	<p>This example shows how to set the RADIUS encryption and authentication key to Make my day:</p> <pre>Console> (enable) set radius key Make my day Radius key set to Make my day. Console> (enable)</pre>
-----------------	---

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 this server be contacted first.	

Defaults The default **auth-port** is 181, and the default **acct-port** is 1813.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines If you configure multiple RADIUS servers, the first server configured is the primary. Authentication requests are sent to this server first. You can specify a particular server as primary by using the **primary** keyword. You can add up to three RADIUS servers.

The *ipaddr* value can be entered as an IP alias or an IP address in dot notation a.b.c.d.

If you set the **auth-port** *port* to 0, the RADIUS server will not be used for authentication. If you set the **acct-port** *port* to 0, the RADIUS server will not be used for accounting.

If you configure a RADIUS key on the switch, make sure you configure an identical key on the RADIUS server.

You must specify a RADIUS server before enabling RADIUS on the switch.

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

```
Console> (enable) set radius server everquest.com auth-port 0 acct-port 1646 primary
everquest.com added to RADIUS server table as primary server.
Console> (enable)
```

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

```
Console> (enable) set radius server 172.22.11.12 auth-port 0 acct-port 1722 primary
172.22.11.12 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 radius timeout

■ set radius timeout