

# set ntp key

Use the **set ntp key** command to define an NTP authentication key pair or to specify a key to be trusted or untrusted.

```
set ntp key public_keynum {trusted | untrusted} [md5 secret_keystring]
```

Syntax Description	
<i>public_keynum</i>	Number of the key pair; valid values are <b>1</b> to <b>4292945295</b> .
<b>trusted</b>	Keyword to specify the trusted key mode.
<b>untrusted</b>	Keyword to specify the untrusted key mode.
<b>md5</b>	(Optional) Keyword to specify the keystring of the key pair.
<i>secret_keystring</i>	(Optional) Key string; valid values are 1 to 32 printable characters.

## Defaults

This command has no default settings.

## Command Types

Switch command.

## Command Modes

Privileged.

## Usage Guidelines

If you enter the **set ntp key** command without the **md5** keyword, the trusted or untrusted mode of the key will change after it is entered into the key table. Enter the **set ntp key** command with the **md5** option to enter an authentication key pair into the system.

## Examples

This example shows how to define an NTP authentication key:

```
Console> (enable) set ntp key 435 trusted md5 have_a_smurfy_day
NTP key 435 added.
Console> (enable)
```

This example shows how to trust an NTP key:

```
Console> (enable) set ntp key 435 trusted
NTP key 435 configured to be trusted.
Console> (enable)
```

This example shows how to untrust an NTP key:

```
Console> (enable) set ntp key 9999 untrusted
NTP key 9999 configured not to be trusted.
Console> (enable)
```

## Related Commands

[clear ntp key](#)  
[show ntp](#)

# set ntp server

Use the **set ntp server** command to specify the NTP server address and to configure an NTP server authentication key.

```
set ntp server ip_addr [key public_keynum]
```

<b>Syntax Description</b>	<i>ip_addr</i>	IP address of the NTP server.
	<b>key</b> <i>public_keynum</i>	(Optional) Keyword to specify the key number; valid values are 1 to 4292945295.

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

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** If you enter the **set ntp server** command without the **key** argument, and the authentication feature is enabled, the following message appears:

```
A trusted key may be required to communicate with this server.
```

**Examples** This example shows how to configure an NTP server:

```
Console> (enable) set ntp server 172.20.52.3  
NTP server 172.20.52.3 added  
Console> (enable)
```

This example shows how to configure an NTP server with a key:

```
Console> (enable) set ntp server 111.222.111.222 key 879  
NTP server 111.222.111.222 with key 879 added  
Console> (enable)
```

This example shows how to assign a new key to an NTP server:

```
Console> (enable) set ntp server 111.222.111.222 key 4323423  
NTP server 111.222.111.222 has been updated with key 4323423  
Console> (enable)
```

**Related Commands** [clear ntp server](#)  
[show ntp](#)

# set ntp summertime

Use the **set ntp summertime** command set to specify whether the system should set the clock ahead one hour during daylight saving time.

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

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

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

## Syntax Description

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

## Defaults

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

## Command Types

Switch command.

## Command Modes

Privileged.

## Usage Guidelines

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

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

## Examples

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

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

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

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

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

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

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

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

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

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

## Related Commands

[clear ntp timezone](#)  
[show ntp](#)

# set ntp timezone

Use the **set ntp timezone** command to configure the time offset from Greenwich Mean Time.

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

Syntax Description	
<i>zone_name</i>	Name of the time zone.
<i>hours</i>	(Optional) Time offset (hours) from Greenwich Mean Time; valid values are from <b>-12</b> to <b>12</b> hours.
<i>minutes</i>	(Optional) Time offset (minutes) from Greenwich Mean Time; valid values are <b>0</b> to <b>59</b> minutes.

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

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** The **set ntp timezone** command is effective only when NTP is running. If you set the time explicitly and NTP is disengaged, the **set ntp timezone** command has no effect. If you have enabled NTP and have not entered the **set timezone** command, the Catalyst 5000 family switch displays UTC by default.

**Examples** This example shows how to set the time zone to Pacific Standard Time with an offset of minus 8 hours from UTC:

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

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

# set password

Use the **set password** command to change the login password on the CLI.

**set password**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** The default configuration has no password configured.

---

**Command Types** Switch command.

---

**Command Modes** Privileged.

---

**Usage Guidelines** Passwords are case sensitive and may be 0 to 30 characters in length, including spaces. The command prompts you for the old password. If the password you enter is valid, you are prompted to enter a new password and to verify the new password. A zero-length password is allowed by pressing **Return**.

---

**Examples** This example shows how to set the normal (login) mode password:

```
Console> (enable) set password
Enter old password: <old_password>
Enter new password: <new_password>
Retype new password: <new_password>
Password changed.
Console> (enable)
```

---

**Related Commands** [set enablepass](#)

# 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 <b>1</b> to <b>1000</b> .
<b>untagged</b>	Keyword to specify that the Cisco IP Phone 7960 send untagged packets without 802.1p priority.
<b>dot1p</b>	Keyword to specify that the Cisco IP Phone 7960 send packets with 802.1p priority.
<b>none</b>	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**

If you do not specify a port, all ports are selected.

The *vlan* option specifies that the connected device send packets tagged with a specific VLAN.

If you enter the **none** option, voice information will not be sent or received.

Dynamic VLAN support for VVID includes these restrictions to MVAP switch ports:

- You can configure any VVID on a dynamic port including **dot1p** and **untagged**, except when the VVID is equal to **dot1p** or **untagged**. If this is the case, you must configure VMPS with the MAC address of the IP phone. When you configure the VVID as **dot1p** or **untagged** on a dynamic port, the following warning message appears:
 

```
VMPS should be configured with the IP phone mac's.
```
- You cannot change the VVID of the port equal to the PVID assigned by the VMPS for the dynamic port.
- You cannot configure trunk ports as dynamic ports, but an MVAP can be configured as a dynamic port.

**Examples** 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.
```

**set port auxiliaryvlan**

```
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 Voice VLAN information.
Console> (enable)
```

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/multicast 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>	Number of packets-per-second of broadcast/multicast traffic allowed on the port or the percentage of total available bandwidth that can be used by broadcast/multicast traffic. Valid values are <b>0</b> to <b>150000</b> packets per second or <b>0.00</b> to <b>100.00</b> percent. <b>0</b> pps or <b>100%</b> unlimits broadcast traffic.
<i>%</i>	(Optional) Keyword used if <i>threshold</i> is expressed as a percentage of total available bandwidth that can be used by broadcast/multicast traffic.

**Defaults** The default value for the threshold is 100 percent.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** Use the [show port capabilities](#) command to determine whether your hardware supports broadcast/multicast suppression.



**Note**

Although the broadcast suppression threshold can be specified to 0.01%, not all modules adjust to that level of precision. Most module thresholds vary between 0.01% and 0.05%. If you specify a threshold more precise than that for a given module, the threshold percent adjusts as close as possible.

You can enter the *threshold* values as decimal numbers from 0.00% to 100% or whole numbers from 0% to 100%.

**Examples** This example shows how to limit broadcast/multicast traffic on port 2/1 to 15.65%:

```
Console> (enable) set port broadcast 2/1 15.65%
Port(s) 2/1 broadcast traffic limited to 15.65%.
Console> (enable)
```

**set port broadcast**

This example shows how to limit broadcast traffic to 500 packets per second on ports 2/1 through 2/24:

```
Console> (enable) set port broadcast 2/1-2/24 500  
Ports 2/1-2/24 broadcast traffic limited to 500 packets.  
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 mode off
```

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

```
set port channel all distribution {session} [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 <b>1</b> to <b>1024</b> .
<b>mode</b>	Keyword to specify the EtherChannel mode.
<b>on</b>	Keyword to enable and force specified ports to channel without PAgP.
<b>off</b>	Keyword to prevent ports from channeling.
<b>desirable</b>	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.
<b>auto</b>	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.
<b>silent</b>	(Optional) Keyword to use with <b>auto</b> or <b>desirable</b> when no traffic is expected from the other device to prevent the link from being reported to STP as down.
<b>non-silent</b>	(Optional) Keyword to use with <b>auto</b> or <b>desirable</b> when traffic is expected from the other device.
<b>all mode off</b>	Keywords to globally turn off channeling on all ports.
<b>all distribution</b>	Keywords to apply frame distribution to all ports in the switch.
<b>mac</b>	Keyword to specify the frame distribution method using MAC address values.
<b>source</b>	(Optional) Keyword to specify the frame distribution method using source address values.
<b>destination</b>	(Optional) Keyword to specify the frame distribution method using destination address values.
<b>both</b>	(Optional) Keyword to specify the frame distribution method using source and destination address values.
<b>session</b>	Keyword to allow frame distribution of Layer 4 traffic.
<b>both</b>	(Optional) Keyword to specify the frame distribution method using source and destination Layer 4 port number.

**Defaults**

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

**Command Types**

Switch command.

**Command Modes**

Privileged.

**Usage Guidelines**

Make sure that all ports you intend to channel are configured properly. For complete information on EtherChannel configuration restrictions, refer to the *Catalyst 5000 Family Software Configuration Guide*.

Administrative groups specify which ports can form an EtherChannel together. An administrative group can contain a maximum of eight ports. However, administrative group membership is restricted by hardware capabilities. Use the **show port capabilities** command to determine which ports can form a channel together.

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* value, it means that you want to create a new administrative group with *admin\_group* selected automatically. The next available administrative 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.

To support jumbo frames, channeling ports need to have the same jumbo frame setting on each port.

This command is not supported by non-EtherChannel-capable modules.

Hardware support for EtherChannel is as follows:

- On most Catalyst 5000 family modules, each EtherChannel port bundle must consist of two or four contiguous ports on the same module. The ports in an EtherChannel must belong to the same port group (ports that share the same EtherChannel bundling controller). Depending on the hardware, there might be additional restrictions. For example, on certain modules, you cannot form an EtherChannel with the last two ports in a port group unless the first two ports in the group already form an EtherChannel.

- On the Catalyst 5000 family Gigabit EtherChannel module (WS-X5010), an EtherChannel bundle can consist of any two to eight ports on the module. Ports in an EtherChannel do not have to be contiguous.
- Channeling is not supported on the Catalyst 5000 family three-port Gigabit Ethernet switching module (WS-X5403), the RSM, ATM modules, and Token Ring modules.

---

**Examples**

This example shows how to create an EtherChannel on ports 5–6 of module 7:

```
Console> (enable) set port channel 7/5-6 on  
Port(s) 7/5-6 are assigned to admin group 56.  
Port(s) 7/5-6 channel mode set to on.  
Console> (enable)
```

This example shows how to remove an EtherChannel on ports 5–6 of module 7:

```
Console> (enable) set port channel 7/5-6 mode auto  
Port(s) 7/5-6 channel mode set to auto.  
Console> (enable) show port channel
```

This example shows how to set the EtherChannel to desirable on ports 5–6 of module 7:

```
Console> (enable) set port channel 7/5-6 mode desirable  
Port(s) 7/5-6 channel mode set to desirable.  
Console> (enable) show port channel
```

---

**Related Commands**

[set channel cost](#)  
[set channel vlancost](#)  
[show channel](#)  
[show channel group](#)  
[show port channel](#)

# set port disable

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

**set port disable** *mod/port*

<b>Syntax Description</b>	<i>mod/port</i> Number of the module and the port on the module.
<b>Defaults</b>	The default system configuration has all ports enabled.
<b>Command Types</b>	Switch command.
<b>Command Modes</b>	Privileged.
<b>Usage Guidelines</b>	This command is not supported by the RSM.
<b>Examples</b>	<p>This example shows how to disable port 5/10:</p> <pre>Console&gt; (enable) <b>set port disable 5/10</b> Port 5/10 disabled. Console&gt; (enable)</pre>
<b>Related Commands</b>	<p><a href="#">set port enable</a>  <a href="#">show port</a></p>

# set port dot1x

Use the **set port dot1x** command to configure dot1x on a port.

```
set port dot1x mod/port {port-control port_control_value}
```

```
set port dot1x mod/port {initialize | re-authenticate}
```

```
set port dot1x mod/port re-authentication {enable | disable}
```

## Syntax Description

<i>mod</i>	Number of the module.
<i>port</i>	Number of the port on the module.
<b>port-control</b> <i>port_control_value</i>	Keyword and variable to specify the port control type; valid values are <b>force-authorized</b> , <b>force-unauthorized</b> , and <b>auto</b> .
<b>initialize</b>	Keyword to initialize dot1x on the port.
<b>re-authenticate</b>	Keyword to manually initiate a reauthentication of the entity connected to the port.
<b>re-authentication</b>	Keyword to automatically initiate reauthentication of the entity connected to the port within the reauthentication time period; see the “Usage Guidelines” section for more information.
<b>enable</b>	Keyword to enable automatic reauthentication.
<b>disable</b>	Keyword to disable automatic reauthentication.

## Defaults

The default settings are as follows:

- The default port control type is **force-authorized**.
- The reauthentication feature is disabled.

## Command Types

Switch command.

## Command Modes

Privileged.

## Usage Guidelines

When setting the port control type, the following applies:

- The force-authorized value forces the controlled port to transition to the authorized state unconditionally and is equivalent to disabling 802.1x restriction in the port.
- The force-unauthorized value forces the controlled port to transition to the unauthorized state unconditionally and prevents the authorized services of the authenticator to the supplicant.
- The auto value enables 802.1x control on the port.

The dot1x port will not be allowed to become a trunk port, MVAP, channel port, dynamic port, or secure port.

If you enable reauthentication, you can set the reauthentication time period in seconds by entering the **set dot1x re-authperiod** *seconds* command. The default for the reauthentication time period is 3600 seconds.

---

**Examples**

This example shows how to set the port control type to auto:

```
Console> (enable) set port dot1x 4/1 port-control auto  
Port 4/1 dot1x port-control is set to auto.  
Console> (enable)
```

This example shows how to initialize dot1x on a port:

```
Console> (enable) set port dot1x 4/1 initialize  
dot1x port 4/1 initializing...  
dot1x initialized on port 4/1.  
Console> (enable)
```

This example shows how to reauthenticate a port:

```
Console> (enable) set port dot1x 4/1 re-authenticate  
dot1x port 4/1 re-authenticating...  
dot1x re-authentication successful...  
dot1x port 4/1 authorized.  
Console> (enable)
```

This example shows how to enable automatic reauthentication on a port:

```
Console> (enable) set port dot1x 4/1 re-authentication enable  
Port 4/1 re-authentication enabled.  
Console> (enable)
```

---

**Related Commands**

[set dot1x](#)  
[show dot1x](#)  
[show port dot1x](#)

# set port duplex

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

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

<b>Syntax Description</b>	<i>mod/port</i>	Number of the module and the port on the module.
	<b>full</b>	Keyword to specify full-duplex transmission.
	<b>half</b>	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. The **set port duplex** command is not valid on the 24- and 48-port group switching modules (WS-X5020 and WS-X5223) or the RSM. The **set port duplex** command is not supported on Token Ring ports. Use the **set tokenring portmode** command instead. You cannot configure the duplex mode on Gigabit Ethernet ports (they are always in 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)
```

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

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

<b>Syntax Description</b>	<i>mod/port</i> Number of the module and the port on the module.
<b>Defaults</b>	The default is all ports are enabled.
<b>Command Types</b>	Switch command.
<b>Command Modes</b>	Privileged.
<b>Usage Guidelines</b>	This command is not supported on the RSM.
<b>Examples</b>	This example shows how to enable port 3 on module 2: <pre>Console&gt; (enable) <b>set port enable 2/3</b> Port 2/3 enabled. Console&gt; (enable)</pre>
<b>Related Commands</b>	<a href="#">set port disable</a> <a href="#">show port</a>

# set port filter

Use the **set port filter** command to configure a MAC address filter or a protocol filter for ports on the Token Ring module.

```
set port filter mod/port {mac_addr | protocol_type} {permit | deny}
```

## Syntax Description

<i>mod/port</i>	Number of the module and the port on the module.
<i>mac_addr</i>	MAC address contained in the packets to be filtered.
<i>protocol_type</i>	Protocol type that you want to filter. For a list of the protocol types that you can filter, see <a href="#">Table 2-6</a> through <a href="#">Table 2-8</a> .
<b>permit</b>	Keyword to specify the filter can permit packets with the specified MAC address or protocol type.
<b>deny</b>	Keyword to specify the filter can deny packets with the specified MAC address or protocol type.

## Defaults

This command has no default settings.

## Command Types

Switch command.

## Command Modes

Privileged.

## Usage Guidelines

You can configure up to 16 MAC address filters or 16 protocol (eight SAPs and eight DSAPs) filters per port on the Token Ring module. See [Table 2-6](#) through [Table 2-8](#) for lists of SAPs and Ethertypes that you can use when defining protocol filters.

You can enter the MAC address in canonical format (00-11-33-44-55) or noncanonical format (00:11:22:33:44:55).

[Table 2-6](#) and [Table 2-7](#) list the SAPs that you can use to define protocol classes.

**Table 2-6 IEEE-Defined SAPs**

Hexadecimal Value	Description
X'02'	LLC Sublayer Management
X'06'	DoD Internet
X'x6'	National Standards Bodies
X'0E'	Proway Network Management
X'4E'	Manufacturing Message Service
X'7E'	ISO 8208
X'8E'	Proway Active Station List Maintenance

**Table 2-6 IEEE-Defined SAPs (continued)**

Hexadecimal Value	Description
X'FE'	OSI Network Layer Protocols
X'42'	Bridge Spanning Tree Protocol

**Table 2-7 IBM-Defined SAPs**

Hexadecimal Value	Description
X'04'	SNA Path Control Individual
X'F0'	NetBIOS
X'F4'	LAN Management Individual
X'F8'	IMPL
X'FC'	Discovery
X'DC'	Dynamic Address Resolution
X'D4'	Resource Management

Table 2-8 lists the possible Ethertypes that you can use to define protocol filters.

**Table 2-8 Ethertypes**

Hexadecimal Value	Description
X'0000' through X'05DC'	IEEE 802.3
X'0600'	Xerox XNS IDP
X'0800'	DoD IP
X'0801'	X.75 Internet
X'0802'	NBS Internet
X'0803'	ECMA Internet
X'0804'	CHAOSnet
X'0805'	X.25 Level 3
X'0806'	ARP (for IP and CHAOS)
X'6001'	DEC MOP Dump/Load Assistance
X'6002'	DEC MOP Remote Console
X'6003'	DEC DECnet Phase IV
X'6004'	DEC LAT
X'6005'	DEC DECnet Diagnostics
X'6010' through X'6014'	3Com Corporation
X'7000' through X'7002'	Ungermann-Bass download
X'7030'	Proteon
X'7034'	Cabletron
X'8035'	Reverse ARP

**Table 2-8** Ethertypes (continued)

Hexadecimal Value	Description
X'8046' through X'8047'	AT&T
X'8088' through X'808A'	Xyplex
X'809B'	Kinetics Ethertalk (Appletalk over Ethernet)
X'80C0' through X'80C3'	Digital Communications Associates
X'80D5'	IBM SNA Services over Ethernet
X'80F2'	Retix
X'80F3' through X'80F5'	Kinetics
X'80F7'	Apollo Computer
X'80FF' through X'8103'	Wellfleet Communications
X'8137' through X'8138'	Novell

**Examples**

This example shows how to configure a port filter on port 2 MAC address 00:40:0b:01:bc:65 of module 3 to permit packets from a specific MAC address:

```
Console> (enable) set port filter 3/2 00:40:0b:01:bc:65 permit
Port 3/2 filter Mac Address 00:40:0b:01:bc:65 set to permit.
Console> (enable)
```

This example shows how to configure a port filter on port 2 MAC address 00:40:0b:01:bc:65 of module 3 to deny packets from a specific MAC address:

```
Console> (enable) set port filter 3/2 00:40:0b:01:bc:65 deny
Port 3/2 filter Mac Address 00:40:0b:01:bc:65 set to deny.
Console> (enable)
```

**Related Commands**

[clear port filter](#)  
[show port filter](#)

# 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.
<b>receive</b>	Keyword to configure a port to process pause frames.
<b>send</b>	Keyword to configure a port to send pause frames.
<b>off</b>	Keyword to prevent a local port from receiving and processing pause frames from remote ports or from sending pause frames to remote ports.
<b>on</b>	Keyword to enable a local port to receive and process pause frames from remote ports or send pause frames to remote ports.
<b>desired</b>	Keyword to obtain predictable results whether a remote port is set to <b>on</b> , <b>off</b> , or <b>desired</b> .

## 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 (Rx) and **on** for transmit (Tx)

## Command Types

Switch command.

## Command Modes

Privileged.

## Usage Guidelines

[Table 2-9](#) describes guidelines for using different configurations of the **send** and **receive** keywords with the **set port flowcontrol** command.

**Table 2-9 send and receive Keyword Configurations**

Configuration	Description
<b>send on</b>	Enables a local port to send pause frames to remote ports. To obtain predictable results, use <b>send on</b> only when remote ports are set to <b>receive on</b> or <b>receive desired</b> .
<b>send off</b>	Prevents a local port from sending pause frames to remote ports. To obtain predictable results, use <b>send off</b> only when remote ports are set to <b>receive off</b> or <b>receive desired</b> .
<b>send desired</b>	Obtains predictable results whether a remote port is set to <b>receive on</b> , <b>receive off</b> , or <b>receive desired</b> .

**Table 2-9** send and receive Keyword Configurations (continued)

Configuration	Description
<b>receive on</b>	Enables a local port to process pause frames that a remote port sends. To obtain predictable results, use <b>receive on</b> only when remote ports are set to <b>send on</b> or <b>send desired</b> .
<b>receive off</b>	Prevents remote ports from sending pause frames to local port. To obtain predictable results, use <b>send off</b> only when remote ports are set to <b>receive off</b> or <b>receive desired</b> .
<b>receive desired</b>	Obtains predictable results whether a remote port is set to <b>send on</b> , <b>send off</b> , or <b>send desired</b> .

All Catalyst Gigabit Ethernet ports can receive and process pause frames from remote devices. However, not all Catalyst Gigabit Ethernet ports can send pause frames to remote devices.

Table 2-10 identifies the Catalyst Gigabit Ethernet switches, modules, and ports that can send pause frames to remote devices.

**Table 2-10** Send Capability by Module and Port

Module	Ports	Send
All modules except WS-X5410	All ports except WS-X5410	Yes
WS-X5410	Uplink ports	No
WS-X5410	Oversubscribed ports	Yes

## 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)
```

This example shows how to configure port 1 of module 5 to not send pause frames:

```
Console> (enable) set port flowcontrol send 5/1 off  
Port 5/1 flow control send administration status set to off  
(port will not send flowcontrol to far end)  
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/ports... {enable | disable}
```

<b>Syntax Description</b>	<i>mod/ports...</i>	Module number and port number list.
	<b>enable</b>	Keyword to enable GMRP on a specified port.
	<b>disable</b>	Keyword to disable GMRP on a specified port.

**Defaults** The default is GMRP is disabled.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** You can modify the per-port GMRP configuration, but you must enable GMRP globally using the **set gmrp enable** command before the per-port GMRP configuration takes effect.

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

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

**Related Commands** [show gmrp configuration](#)

# set port gvrp

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

**set port gvrp** *mod/ports...* { **enable** | **disable** }

Syntax Description	
<i>mod/ports...</i>	Module number and port number list.
<b>enable</b>	Keyword to enable GVRP on the specified ports.
<b>disable</b>	Keyword to disable GVRP on the specified ports.

**Defaults** The default is GVRP is disabled.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines**

GVRP can only be enabled on IEEE 802.1Q trunks.

When VTP pruning is enabled, VTP pruning runs on all GVRP-disabled trunks.

To run GVRP on a trunk, GVRP needs to be enabled both globally on the switch and enabled individually on the trunk.

You can configure GVRP on a port even when GVRP is globally disabled. However, the port will not become a GVRP participant until GVRP is also globally enabled.

**Examples** This example shows how to enable GVRP on module 3, port 2:

```
Console> (enable) set port gvrp 3/2 enable
GVRP enabled on 3/2.
Console> (enable)
```

This example shows how to disable GVRP on module 3, port 2:

```
Console> (enable) set port gvrp 3/2 disable
GVRP disabled on 3/2.
Console> (enable)
```

This example shows what happens if you try to enable GVRP on a port that is not an 802.1Q trunk:

```
Console> (enable) set port gvrp 4/1 enable
Failed to set port 4/1 to GVRP enable. Port not allow GVRP.
Console> (enable)
```

This example shows what happens if you try to enable GVRP on a specific port when GVRP has not first been enabled using the [set gvrp](#) command:

```
Console> (enable) set port gvrp 5/1 enable  
GVRP enabled on 5/1.  
GVRP feature is currently disabled on the switch.  
Console> (enable)
```

---

**Related Commands**

[clear gvrp statistics](#)  
[set gvrp](#)  
[show gvrp configuration](#)

# set port host

Use the **set port host** command to optimize the port configuration for a host connection.

**set port host** *mod/ports...*

---

<b>Syntax Description</b>	<i>mod/ports...</i> Module number and port number list.
---------------------------	---

---



---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

---



---

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

---



---

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

---



---

<b>Usage Guidelines</b>	The <b>set port host</b> command sets channel mode to off, enables spanning tree PortFast, and sets trunk mode to off. Only an end station can accept this configuration.
-------------------------	---

Enable spanning tree PortFast start 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.

---

<b>Examples</b>	This example shows how to optimize the port configuration for end station/host connections on ports 2/1 and 3/1:
-----------------	--

```
Console> (enable) set port host 2/1,3/1
```

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

```
Spantree 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.
```

```
Console> (enable)
```

---

<b>Related Commands</b>	<a href="#">clear port host</a>
-------------------------	---------------------------------

# set port jumbo

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.
<b>enable</b>		Keyword to enable jumbo frames on a specified port.
<b>disable</b>		Keyword to disable jumbo frames on a specified port.

**Defaults** The default is disabled on all ports.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** This command is not supported by the NAM.

The jumbo frame feature is supported on all Ethernet ports, except for the ports on the Catalyst 5000 family Gigabit EtherChannel switching module (WS-X5410).

You can use the jumbo frame feature to transfer large frames or jumbo frames through Catalyst 5000 family switches to optimize server-to-server performance. The jumbo frame feature applies to incoming traffic only.

If the jumbo frame feature cannot be enabled on some ports at system start-up time, the CLI displays a message that the system failed to enable the jumbo frame feature on those ports. This means that the feature is enabled in NVRAM, but operationally disabled on the module.

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.

**Examples** This example shows how to enable the jumbo frame feature on module 3, port 2:

```
Console> (enable) set port jumbo 3/2 enable
Jumbo frames enabled on port 5/3.
Console> (enable)
```

**Related Commands** [show port jumbo](#)

# set port level

Use the **set port level** command to set the priority level of a port or range of ports on the switching bus.

**set port level** *mod/port* { **normal** | **high** }

Syntax Description		
	<i>mod/port</i>	Number of the module and the port on the module.
	<b>normal</b>	Keyword to set the port priority to normal.
	<b>high</b>	Keyword to set the port priority to high.

**Defaults** The default configuration has all ports at normal priority level.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** Packets traveling through a port set at normal priority are served only after packets traveling through a port set at high priority are served.

**Examples** This example shows how to set the priority level for port 2 on module 1 to high:

```
Console> (enable) set port level 1/2 high
Port 1/2 port level set to high.
Console> (enable)
```

This example shows how to set the priority level for port 2 on module 1 to normal:

```
Console> (enable) set port level 1/2 normal
Port 1/2 level set to normal.
Console> (enable)
```

**Related Commands**

- [set port disable](#)
- [set port enable](#)
- [set port name](#)
- [set port speed](#)
- [show port](#)

# set port membership

Use the **set port membership** command to configure ports for dynamic or static VLAN membership.

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

Syntax Description	
<i>mod/port</i>	Number of the module and the port on the module.
<b>dynamic</b>	Keyword to configure the port for dynamic VLAN membership.
<b>static</b>	Keyword to configure the port for static VLAN membership.

**Defaults** Default port membership is static.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** This command is not supported on the following:

- RSM
- Three-port Gigabit Ethernet switching module (WS-X5403)
- Token Ring

Ports configured for dynamic VLAN membership obtain their VLAN assignment through VMPS. Ports configured for static VLAN membership obtain their VLAN assignment through the **set vlan** command.

When a port is assigned a VLAN dynamically, the **show port** command output identifies the VLAN as dynamic. If the dynamic port is shut down by a VMPS, its status is shown as shutdown.

Dynamic VLAN support for VVID imposes these restrictions to the following configuration of multiple VLAN access port (MVAP) on the switch port:

- You can configure any VVID on a dynamic port including **dot1p** and **untagged**, except when the VVID is equal to **dot1p** or **untagged**. If this is the case, then you must configure VMPS with the MAC address of the IP phone. When you configure the VVID as **dot1p** or **untagged** on a dynamic port, the following warning message appears:
 

```
VMPS should be configured with the IP phone mac's.
```
- You cannot change the VVID of the port equal to the PVID assigned by the VMPS for the dynamic port.
- You cannot configure trunk ports as dynamic ports, but an MVAP can be configured as a dynamic port.

---

**Examples**

This example shows how to configure a port for dynamic VLAN membership:

```
Console> (enable) set port membership 3/1-3 dynamic
Ports 3/1-3 vlan assignment set to dynamic.
Spantree port fast start option enabled for ports 3/1-3.
Console> (enable)
```

---

**Related Commands**

[set port enable](#)  
[show port](#)

# set port name

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

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

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

**Defaults** The default configuration has no port name configured for any port.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** 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)
```

**Related Commands** [show port](#)

# set port negotiation

Use the **set port negotiation** command to enable link negotiation on the port that you specify. Link negotiation autonegotiates flow control, duplex mode, and remote fault information.

**set port negotiation** *mod/port* [**enable** | **disable**]

Syntax Description	
<i>mod/port</i>	Number of the module and the port on the module.
<b>enable</b>	(Optional) Keyword to enable the link negotiation protocol.
<b>disable</b>	(Optional) Keyword to disable the link negotiation protocol.

**Defaults** The default is link negotiation protocol 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.
```

N/N is the module and port number.

When you enable link negotiation with the **set port negotiation** command, 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 enable link negotiation on port 1, module 3:

```
Console> (enable) set port negotiation 3/1 enable
Link negotiation protocol disabled on port 3/1.
Console> (enable)
```

This example shows how to disable link negotiation 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 set the protocol filtering group 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.
<b>ip</b>	Keyword to specify the IP protocol filtering group.
<b>ipx</b>	Keyword to specify the IPX protocol filtering group.
<b>group</b>	Keyword to specify the Group protocol filtering group.
<b>on</b>	Keyword to indicate the port will receive all the flood traffic for that protocol.
<b>off</b>	Keyword to indicate the port will not receive any flood traffic for that protocol.
<b>auto</b>	Keyword to indicate the port will receive the flood traffic for that protocol only after transmitting packets of that specific protocol.

**Defaults** By default, ports are configured to **on** for the IP protocol group and **auto** for the IPX and Group protocol groups.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** Protocol filtering is supported only on nontrunking Ethernet, Fast Ethernet, and Gigabit Ethernet ports. Trunking ports are always members of all the protocol groups.

You must enable protocol filtering globally on the switch using the **set protocolfilter** command.

If the configuration for one of the protocol groups is set to **auto**, the port initially does not receive any flood packets for that protocol. If the connected device transmits packets of that protocol, the port is added to the protocol group and flood traffic for that protocol is transmitted on that port.

Ports configured as **auto** are removed from the protocol group if the connected device does not transmit the protocol packets within 60 minutes. The ports are also removed from the protocol group on detection of a link down.

On Catalyst 5000 family switches, packets are classified into the following protocol groups:

- IP
- IPX
- AppleTalk, DECnet, and Banyan VINES (“group”)
- Packets not belonging to any of these protocols

---

**Examples**

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

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

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)
```

This example shows how to disable group IP membership of port 1 on module 1:

```
Console> (enable) set port protocol 1/1 group off  
Group protocol disabled on port 1/1.  
Console> (enable)
```

---

**Related Commands**

[set protocolfilter](#)  
[show port protocol](#)

# set port qos

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

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

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

**Defaults** The default is that ports are port-based.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** This command is not supported by the NAM.

You can use the **set port qos** command on Supervisor Engines III or Supervisor Engines II G and III G. 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, QoS policy-source is COPS, or DSBM-election is enabled. The VLAN-based setting is 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 configuraiton ...
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 configuraiton ...
QoS interface is set to VLAN-based for ports 3/1-48.
Console> (enable)
```

**set port qos**

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  
Ports 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

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

**Defaults** 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.  
 You can use the **set port qos cos** command on Supervisor Engines III or Supervisor Engines II G and III G.

**Examples** This example shows how to set the default CoS 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 extension 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](#)
- [set port qos](#)
- [show 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.
	<b>untrusted</b>	Keyword to specify that packets need to be reclassified from the matching ACE.
	<b>trust-cos</b>	Keyword to specify that even though 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.
	<b>trust-ipprec</b>	Keyword to specify that even though the ToS and CoS bits in the incoming packets are trusted, the ToS is invalid and the ToS is set as IP precedence.
	<b>trust-dscp</b>	Keyword to specify that the ToS and 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** This command is not supported by the NAM.

You can use the **set port qos trust** command on Supervisor Engines III or Supervisor Engines II G and III G.

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

**Examples** This example shows how to set the trusted state of a module:

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

**Related Commands** [set port qos](#)  
[show port qos](#)

# set port qos trust-ext

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

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

<b>Syntax Description</b>	<i>mod/ports...</i> Number of the module and the ports on the module.
<b>untrusted</b>	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.
<b>trusted</b>	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 port qos](#)

# set port security

Use the **set port security** command 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.
<b>enable</b>	(Optional) Keyword to enable port security.
<b>disable</b>	(Optional) Keyword to disable port security.
<i>mac_addr</i>	(Optional) Secure MAC address of the enabled port.
<b>age</b> <i>age_time</i>	(Optional) Keyword and variable to specify the duration for which addresses on the port will be secured; valid values are from <b>10</b> to <b>1440</b> minutes.
<b>maximum</b> <i>num_of_mac</i>	(Optional) Keyword to specify the maximum number of MAC addresses to secure on the port; valid values are from <b>1</b> to <b>1025</b> .
<b>shutdown</b> <i>shutdown_time</i>	(Optional) Keyword and variable to specify the duration of time a port will remain disabled in case of a security violation; valid values are from <b>10</b> to <b>1440</b> minutes.
<b>violation</b>	(Optional) Action to be taken in the event of a security violation.
<b>shutdown</b>	(Optional) Keyword to shut down the port in the event of a security violation.
<b>restrict</b>	(Optional) 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

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 only to insecure MAC addresses. You can specify the duration of the shutdown time 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 security enabled.  
Trunking disabled for Port 1/1 due to Security Mode.  
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 security enabled.  
Mac address 01-02-03-04-05-06 set for port 1/1.  
Console> (enable)
```

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

```
Console> (enable) set port security 7/7 shutdown 600  
Port 7/7 security shutdown time 600.  
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 7/7 security violation mode restrict.  
Console> (enable)
```

---

**Related Commands**

[clear qos config](#)  
[show port security](#)

# set port speed

Use the **set port speed** command to configure transmission speed or autonegotiation.

```
set port speed mod/port {4 | 10 | 16 | 100 | auto}
```

Syntax Description		
<i>mod/port</i>		Number of the module and the port on the module.
<b>auto</b>		Keyword to specify autonegotiation for transmission speed and duplex mode on 10/100 Fast Ethernet ports.
<b>4</b>		Keyword to specify a transmission rate of 4-Mbps on Token Ring ports.
<b>10</b>		Keyword to specify a transmission rate of 10-Mbps on 10/100 Fast Ethernet ports.
<b>16</b>		Keywords to specify a transmission rate of 16-Mbps on Token Ring ports.
<b>100</b>		Keyword to specify a transmission rate of 100-Mbps on 10/100 Fast Ethernet ports.

**Defaults** The default configuration has all module ports set to **auto**.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** You can configure Ethernet interfaces on the 10/100-Mbps Ethernet switching modules to either 10 Mbps or 100 Mbps, or to autosensing mode, allowing them to sense and distinguish between 10-Mbps 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 mode, they automatically configure themselves to operate at the proper speed and transmission type.

You can configure Token Ring interfaces on the Token Ring module to either 4 Mbps or 16 Mbps, or to autospeed detection mode, allowing them to sense and distinguish between 4-Mbps and 16-Mbps port transmission speed. If you set the interfaces to autospeed detection mode, they automatically configure themselves to operate at the proper speed.

If you change the transmission speed of a port that is open to 4 or 16 Mbps, the port will close and reopen at the new transmission speed. If a port closes and reopens on an existing ring using a transmission speed different from that which the ring is operating, the ring will beacon.

If you set the port speed to **auto**, duplex mode is automatically set to auto.

If the ports on the Token Ring module are configured to detect the speed of the ring automatically, the first port inserted on the ring does not set the speed because it is unable to detect the speed.

---

**Examples**

This example shows how to configure port 1 on 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 port 2 on module 2 port speed to 10 Mbps:

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

This example shows how to configure port 4 on module 3 port speed to 16 Mbps:

```
Console> (enable) set port speed 3/4 16  
Port(s) 3/4 speed set to 16Mbps.  
Console> (enable)
```

---

**Related Commands**

[set port duplex](#)  
[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.
<b>enable</b>		Keyword to activate the SNMP link trap.
<b>disable</b>		Keyword to deactivate the SNMP link trap.

**Defaults** The default configuration has all port traps disabled.

**Command Types** Switch command.

**Command Modes** Privileged.

**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 name](#)
- [set port speed](#)
- [show port](#)

# set prompt

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

```
set prompt prompt_string
```

---

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

---

---

<b>Defaults</b>	The default configuration has the prompt set to Console>.
-----------------	---

---

---

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

---

---

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

---

---

<b>Usage Guidelines</b>	If you use the <b>set system name</b> 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 <b>set prompt</b> command, that string is used for the prompt.
-------------------------	--

---

---

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

---

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

---

<b>Related Commands</b>	<a href="#">set system name</a>
-------------------------	---------------------------------

---

# set protocolfilter

Use the **set protocolfilter** command to activate or deactivate protocol filtering.

```
set protocolfilter { enable | disable }
```

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

**Defaults** The default configuration has protocol filtering disabled.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** Use the **set protocolfilter** command to activate/deactivate protocol filtering on the switch. Use the **set port protocol** command to configure protocol filtering group membership on switch 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** [set port protocol](#)

# set qos

Use the **set qos** command to enable and disable QoS on the switch.

```
set qos {enable | disable}
```

<b>Syntax Description</b>	<b>enable</b>	Keyword to enable QoS on the switch.
	<b>disable</b>	Keyword to disable QoS on the switch.

**Defaults** The default is QoS is disabled.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** Do not enable and disable QoS in quick succession (within 2 seconds of each other).

**Examples** This example shows how to enable QoS:

```
Console> (enable) set qos enable
QoS is enabled.
Console> (enable)
```

This example shows how to disable QoS:

```
Console> (enable) set qos disable
QoS is disabled.
Console> (enable)
```

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

## set qos ip-filter

Use the **set qos ip-filter** command to create ACEs with Layer 3 values or with both Layer 3 and 4 values.

```
set qos ip-filter cos {src_ip_addr_spec} {dest_ip_addr_spec} [before ACE# | modify ACE#]
```

```
set qos ip-filter cos protocol {src_ip_addr_spec} {src_port} {dest_ip_addr_spec} {dest_port}  
[before ACE# | modify ACE#]
```

### Syntax Description

<i>cos</i>	CoS to assign to packets matching this filter; valid values are from <b>0</b> to <b>7</b> .
<i>src_ip_addr_spec</i>	Source IP address. See the “Usage Guidelines” section for information regarding formatting.
<i>dest_ip_addr_spec</i>	Destination IP address. See the “Usage Guidelines” section for information regarding formatting.
<b>before</b> <i>ACE#</i>	(Optional) Keyword and variable to insert an ACE in front of the specified ACE.
<b>modify</b> <i>ACE#</i>	(Optional) Keyword and variable to replace an ACE with the new ACE.
<i>protocol</i>	Type of protocol that the ACE matches; valid values are <b>tcp</b> , <b>udp</b> , or <b>any</b> .
<i>src_port</i>	Number of the source port.
<i>dest_port</i>	Number of the destination port.

### Defaults

This command has no default settings.

### Command Types

Switch command.

### Command Modes

Privileged.

### Usage Guidelines

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

If you do not specify the **before** *ACE#* argument, the new entry is placed after the last. The ACE number of any entry is its current position in the list. These can be viewed by the **show qos ip** command.

If you do not enter the *protocol* variable, the **set qos ip-filter** command specifies an ACE that is independent of the Layer 4 protocol and port. If you enter the *protocol* variable, the command specifies an ACE that matches specific Layer 4 protocols and ports.

The *dest\_ip\_addr\_spec* and *src\_ip\_addr\_spec* variables are entered in the following format:

```
{any | {host ip_addr} | {ip_addr ip_addr_mask}}
```

where:

- **any** is a keyword that specifies the *ip\_addr ip\_addr\_mask* as 0.0.0.0 255.255.255.255.
- **host ip\_addr** is a keyword and variable that specifies the IP address of the host and the subnet mask of the specified IP address.

Layer 4 ports can only be specified for unicast addresses. If the destination address specifies a multicast address, and you enter the **set qos ip-filter** *{dest\_ip\_addr} {src\_ip\_addr mask} protocol [dst\_port src\_port] cos [before ACE#]* command, an error is displayed. If the destination address includes multicast addresses and the same command is used, a message displays that the command only applies to unicast addresses.

If you enter a 0 for the *src\_port* variable, it means any source port matches.

If you enter a 0 for the *dest\_port* variable, it means any destination port matches.

### Examples

This example shows how to create ACEs and an ACE within the list and verify the configuration using the **show qos ip** command:

```
Console>(enable) set qos ip-filter 7 100.100.1.1 255.255.255.0 200.200.1.1 255.255.255.0
qos ip-filter is set successfully.
Console> (enable)
```

```
Console> (enable) show qos ip
There are 1 IP filter(s).
ACE# Dest IP and Mask                               Src IP and Mask
-----
  1 100.100.1.1 255.255.255.0           200.200.1.1 255.255.255.0
    Protocol Dst Port Src Port CoS
    -----
    both     0         0         7
Console> (enable)
```

```
Console> (enable) set qos ip-filter 4 tcp 120.100.1.1 255.255.255.0 47 210.210.1.1 255.255.255.0 23
qos ip-filter is set successfully.
```

```
Console> (enable) show qos ip
There are 2 IP filter(s).
ACE# Dest IP and Mask                               Src IP and Mask
-----
  1 100.100.1.1 255.255.255.0           200.200.1.1 255.255.255.0
    Protocol Dst Port Src Port CoS
    -----
    both     0         0         7

  2 120.100.1.1 255.255.255.0           210.210.1.1 255.255.255.0
    Protocol Dst Port Src Port CoS
    -----
    tcp      23        47         4
Console> (enable)
```

```
Console> (enable) set qos ip-filter 1 20.20.20.1 255.0.0.0 30.30.1.1 255.0.0.0 before 1
qos ip-filter is set successfully.
Console> (enable)
```

```
Console> (enable) show qos ip
There are 3 IP filter(s).
```

**set qos ip-filter**

```

ACE# Dest IP and Mask                               Src IP and Mask
-----
 1 20.20.20.1 255.0.0.0                             30.30.1.1 255.0.0.0
   Protocol Dst Port Src Port CoS
   -----
   both     0       0       1

 2 100.100.1.1 255.255.255.0                       200.200.1.1 255.255.255.0
   Protocol Dst Port Src Port CoS
   -----
   both     0       0       7

 3 120.100.1.1 255.255.255.0                       210.210.1.1 255.255.255.0
   Protocol Dst Port Src Port CoS
   -----
   tcp      23      47      4
Console> (enable)

```

**Related Commands**    [clear qos ip-filter](#)  
[show qos ip](#)