

set logging level

To set the facility and severity level to be used when system messages are logged, use the **set logging level** command.

set logging level *facility severity* [**default**]

Syntax Description

<i>facility</i>	Value for the type of system messages to capture. Facility types are shown in Table 2-3 .
<i>severity</i>	Value for the severity level of system messages to capture. Severity level definitions are shown in Table 2-4 .
default	(Optional) Logging level to apply to all sessions. If default is not used, the specified logging level applies only to the current session.

Table 2-3 Facility Types

Facility Type	Definition
all	All facilities
cdp	Cisco Discovery Protocol
cops	Common Open Policy Service
dot1x	IEEE 802.1x
dtp	Dynamic Trunking Protocol
dvlan	Dynamic VLAN
earl	Enhanced Address Recognition Logic
filesys	File system
gvrp	GARP VLAN Registration Protocol
ip	Internet Protocol
kernel	Kernel
mcast	Multicast
mgmt	Management
mls	Multilayer Switching
pagp	Port Aggregation Protocol
protfilt	Protocol Filter
pruning	VTP pruning
qos	Quality of Service
radius	Remote Access Dial-In User Service
security	Security
snmp	Simple Network Management Protocol

Table 2-3 Facility Types (continued)

Facility Type	Definition
spantree	Spanning Tree Protocol
sys	System
tac	Terminal Access Controller
tcp	Transmission Control Protocol
telnet	Terminal Emulation Protocol
tftp	Trivial File Transfer Protocol
udld	User Datagram Protocol
vtp	Virtual Terminal Protocol

Table 2-4 Severity Level Definitions

Severity Level	Severity Type	Description
0	Emergencies	System unusable
1	Alerts	Immediate action required
2	Critical	Critical condition
3	Errors	Error conditions
4	Warnings	Warning conditions
5	Notifications	Normal bug significant condition
6	Informational	Informational messages
7	Debugging	Debugging messages

Defaults

The defaults are shown in the following table:

Configuration Parameter	Default Setting
system message logging to the console	enabled
system message logging to Telnet sessions	enabled
logging server	disabled
syslog server	unconfigured
server facility	LOCAL7
server severity	Warnings (4)
logging buffer	500
logging history size	1

Configuration Parameter	Default Setting
timestamp option	disabled
facility/severity level for system messages	sys/5 dtp/5 pagp/5 mgmt/5 mls/5 all other facilities/2

Command Types Switch command

Command Modes Privileged

Usage Guidelines You can also set the logging level by using the **set logging server** command. If you do not use the **default** keyword, the specified logging level applies only to the current session.

Examples This example shows how to set the default system message logging severity level for the SNMP facility:

```
Console> (enable) set logging level snmp 2 default
System logging facility <snmp> set to severity 2(critical).
Console> (enable)
```

Related Commands [show logging](#)
[show logging buffer](#)

set logging server

To enable or disable system message logging to configured syslog servers and to add a syslog server to the system logging server table, use the **set logging server** command.

```
set logging server { enable | disable }
```

```
set logging server ip_addr
```

```
set logging server facility server_facility_parameter
```

```
set logging server severity server_severity_level
```

Syntax Description		
enable		Enables system message logging to configured syslog servers.
disable		Disables system message logging to configured syslog servers.
<i>ip_addr</i>		IP address of the syslog server to be added to the configuration. An IP alias or a host name that can be resolved through DNS can also be used.
facility		Type of system messages to capture.
<i>server_facility_parameter</i>		Logging facility of syslog server; valid values are local0 , local1 , local2 , local3 , local4 , local5 , local6 , local7 , and syslog .
severity		Sets the severity level of system messages to capture.
<i>server_severity_level</i>		Severity level of system messages to capture; valid values are from 0 to 7. Severity level definitions are shown in Table 2-4 .

Defaults No syslog servers are configured to receive system messages.

Command Types Switch command

Command Modes Privileged

Examples This example shows how to enable system message logging to the console:

```
Console> (enable) set logging server enable
System logging messages will be sent to the configured syslog servers.
Console> (enable)
```

This example shows how to add a syslog server to the system logging server table:

```
Console> (enable) set logging server 192.168.255.255
192.168.255.255 added to the System logging server table.
Console> (enable)
```

This example shows how to set the syslog server facility to local7:

```
Console> (enable) set logging server facility local7
System logging server facility set to <local7>
Console> (enable)
```

This example shows how to set the syslog server severity level to 4:

```
Console> (enable) set logging server severity 4
System logging server severity set to <4>
Console> (enable)
```

This example shows how to set the syslog history table size to 400:

```
Console> (enable) set logging history 400
System logging history table size set to <400>
Console> (enable)
```

Related Commands

[clear logging server](#)

[show logging](#)

set logging session

To enable or disable the sending of system logging messages to the current login session, use the **set logging session** command.

set logging session { enable | disable }

Syntax Description

enable Enables the sending of system logging messages to the current login session.

disable Disables the sending of system logging messages to the current login session.

Defaults

Enabled

Command Types

Switch command

Command Modes

Privileged

Examples

This example shows how to prevent system logging messages from being sent to the current login session:

```
Console> (enable) set logging session disable
System logging messages will not be sent to the current login session.
Console> (enable)
```

This example shows how to cause system logging messages to be sent to the current login session:

```
Console> (enable) set logging session enable
System logging messages will be sent to the current login session.
Console> (enable)
```

Related Commands

[set logging buffer](#)
[set logging level](#)
[show logging](#)
[show logging buffer](#)

set logging telnet

To enable or disable logging on Telnet sessions, use the **set logging telnet** command.

```
set logging telnet {enable | disable}
```

Syntax Description	enable	enable
	enable	Enables logging on Telnet sessions.
	disable	Disables logging on Telnet sessions.

Defaults Enabled

Command Types Switch command

Command Modes Privileged

Examples This example shows how to allow system logging messages to be sent to new Telnet sessions:

```
Console> (enable) set logging telnet enable
System logging messages will be sent to the new telnet sessions.
Console> (enable)
```

This example shows how to prevent system logging messages from being sent to new Telnet sessions:

```
Console> (enable) set logging telnet disable
System logging messages will not be sent to the new telnet sessions.
Console> (enable)
```

Related Commands

- [set logging console](#)
- [set logging history](#)
- [show logging](#)
- [show logging buffer](#)

set logging timestamp

To enable or disable the timestamp display on system logging messages, use the **set logging timestamp** command.

set logging timestamp {enable | disable}

Syntax Description	enable	Disables the timestamp display.
	disable	Enables the timestamp display.

Defaults Enabled

Command Types Switch command

Command Modes Privileged

Examples

This example shows how to enable the timestamp display:

```
Console> (enable) set logging timestamp enable
System logging messages timestamp will be enabled.
Console> (enable)
```

This example shows how to disable the timestamp display:

```
Console> (enable) set logging timestamp disable
System logging messages timestamp will be disabled.
Console> (enable)
```

Related Commands [show logging](#)

set logout

To specify the number of minutes the system waits before automatically disconnecting an idle session, use the **set logout** command.

set logout *timeout*

Syntax Description	<i>timeout</i>	Number of minutes until the system disconnects an idle session automatically; valid values are from 0 to 10000. Setting the value to zero (0) disables the automatic disconnection of idle sessions.
---------------------------	----------------	--

Defaults	20 minutes
-----------------	------------

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

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

Examples This example shows how to set the number of minutes until the system disconnects an idle session automatically:

```
Console> (enable) set logout 20  
Sessions will be automatically logged out after 20 minutes of idle time.  
Console> (enable)
```

This example shows how to disable the automatic disconnection of idle sessions:

```
Console> (enable) set logout 0  
Sessions will not be automatically logged out.  
Console> (enable)
```

set module disable

To disable a module, use the **set module disable** command.

```
set module disable mod
```

Syntax Description	<i>mod</i> Module number.
---------------------------	---------------------------

Defaults	All modules are enabled.
-----------------	--------------------------

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

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

Usage Guidelines	Avoid disabling a module when you are connected through a Telnet session; if you disable the module that contains the port through which your Telnet session was established, you will disconnect your Telnet session.
-------------------------	--

If there are no other network connections to the switch, you must connect to the switch through the console port to reenable the module.

You can specify a series of modules by entering a comma between each module number (for example, 2,3,5). You can specify a range of modules by entering a hyphen between module numbers (for example, 2-5).

Examples	This example shows how to disable module 3 when connected through the console port:
-----------------	---

```
Console> (enable) set module disable 3
Module 3 disabled.
Console> (enable)
```

This example shows how to disable module 2 when connected through a Telnet session:

```
Console> (enable) set module disable 2
This command may disconnect your telnet session.
Do you want to continue (y/n) [n]? y
Module 2 disabled.
Console> (enable)
```

Related Commands	set module enable show module
-------------------------	--

set module enable

To enable a module, use the **set module enable** command.

```
set module enable mod
```

Syntax Description

mod Module number.

Defaults

All modules are enabled.

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

If an individual port on a module was previously disabled, enabling the module does not enable the disabled port.

Examples

This example shows how to enable module 2:

```
Console> (enable) set module enable 2  
Module 2 enabled.  
Console> (enable)
```

Related Commands

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

set module name

To set the name for a module, use the **set module name** command.

```
set module name mod [mod_name]
```

Syntax Description

<i>mod</i>	Module number.
<i>mod_name</i>	(Optional) Specifies a name to assign to the module.

Defaults

No module names are configured.

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

If you do not specify a *mod_name* value, any previously specified name is cleared.

Module names configured using the **set module name** command are displayed in the output of the **show module** command and other commands.

Examples

This example shows how to set Supervisor as the name for module 1:

```
Console> (enable) set module name 1 Supervisor
Module name set.
Console> (enable)
```

Related Commands

[show module](#)

set multicast router

To manually configure a port as a multicast router port, use the **set multicast router** command.

set multicast router *mod/port*

Syntax Description	<i>mod/port</i> Number of the module and the port.
Defaults	No ports are configured as multicast router ports.
Command Types	Switch command
Command Modes	Privileged
Usage Guidelines	When you enable CGMP or IGMP snooping, the ports to which a multicast-capable router is attached are identified automatically. The set multicast router command allows you to configure multicast router ports statically.
Examples	<p>This example shows how to manually configure module 3 port 1 as a multicast router port:</p> <pre>Console> (enable) set multicast router 3/1 Port 3/1 added to multicast router port list. Console> (enable)</pre>
Related Commands	<p>clear multicast router set cgmp show multicast group count show multicast router</p>

set ntp authentication

To enable or disable the Network Time Protocol (NTP) authentication feature, use the **set ntp authentication** command.

set ntp authentication {enable | disable}

Syntax Description	enable	enable
	enable	Enables NTP authentication.
	disable	Disables NTP authentication.

Defaults Enabled

Command Types Switch command

Command Modes Privileged

Examples

This example shows how to enable NTP authentication:

```
Console> (enable) set ntp authentication enable
NTP authentication feature enabled.
At least one trusted key must be set for NTP to work.
Console> (enable)
```

This example shows how to disable NTP authentication:

```
Console> (enable) set ntp authentication disable
NTP authentication feature disabled.
Console> (enable)
```

Related Commands [show ntp](#)

set ntp broadcastclient

To enable or disable Network Time Protocol (NTP) broadcast-client mode, use the **set ntp broadcastclient** command.

```
set ntp broadcastclient {enable | disable}
```

Syntax Description

enable	Enables NTP broadcast-client mode.
disable	Disables NTP broadcast-client mode.

Defaults

Disabled

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

You can configure NTP in either broadcast-client mode or client mode. The broadcast-client mode assumes that a broadcast server, such as a router, sends time-of-day information regularly to the switch.

Examples

This example shows how to enable NTP broadcast client:

```
Console> (enable) set ntp broadcastclient enable  
NTP Broadcast Client mode enabled.  
Console> (enable)
```

This example shows how to disable NTP broadcast client:

```
Console> (enable) set ntp broadcastclient disable  
NTP Broadcast Client mode disabled.  
Console> (enable)
```

Related Commands[show ntp](#)

set ntp broadcastdelay

To configure a time-adjustment factor so the switch can receive broadcast packets, use the **set ntp broadcastdelay** command.

set ntp broadcastdelay *microseconds*

Syntax Description	<i>microseconds</i>	Estimated round-trip time, in microseconds, for Network Time Protocol (NTP) broadcasts; valid values are from 1 to 999999.
---------------------------	---------------------	--

Defaults	NTP broadcast delay is set to 3000 microseconds.
-----------------	--

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

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

Examples	This example shows how to set the NTP broadcast delay to 4000 microseconds (4 seconds):
-----------------	---

```
Console> (enable) set ntp broadcastdelay 4000
NTP broadcast delay set to 4000 microseconds.
Console> (enable)
```

Related Commands	show ntp
-------------------------	--------------------------

set ntp client

To enable or disable the switch as a Network Time Protocol (NTP) client, use the **set ntp client** command.

```
set ntp client {enable | disable}
```

Syntax Description

enable	Enables the NTP client.
disable	Disables the NTP client.

Defaults

Disabled

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

You can configure NTP in either broadcast-client mode or client mode. The client mode assumes that the client switch regularly sends time-of-day requests to the NTP server.

Examples

This example shows how to enable NTP client mode:

```
Console> (enable) set ntp client enable  
NTP client mode enabled.  
Console> (enable)
```

Related Commands[show ntp](#)

set ntp key

To define an Network Time Protocol (NTP) authentication key pair or to specify a key to be trusted or untrusted, use the **set ntp key** command.

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

Syntax Description	
<i>public_keynum</i>	Number of the key pair; valid values are from 1 to 4,292,945,295.
trusted	Trusted key mode.
untrusted	Untrusted key mode.
md5	(Optional) Sets the keystring of the key pair.
<i>secret_keystring</i>	(Optional) Key string; valid values are from 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 keyword 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_good_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

To specify the Network Time Protocol (NTP) server address and to configure an NTP server authentication key, use the **set ntp server** command.

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

Syntax Description		
	<i>ip_addr</i>	IP address of the NTP server.
	key	(Optional) Key number.
	<i>public_keynum</i>	(Optional) Number of the key pair; valid values are from 1 to 4,292,945,295.

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 specifying the **key** keyword, and the authentication feature is enabled, the following message is displayed:

```
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

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

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

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

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

Syntax Description		
enable	Sets the clock ahead one hour to accommodate daylight saving time.	
disable	Prevents the system from setting the clock ahead one hour during daylight saving time.	
<i>zone</i>	(Optional) Time zone used by the set summertime command.	
recurring	Summertime dates that recur every year.	
<i>week</i>	Week of the month; valid values are first , second , third , fourth , last , 1 , 2 , 3 , 4 , and 5 .	
<i>day</i>	Day of the week; valid values are sunday , monday , tuesday , wednesday , thursday , friday , and saturday .	
<i>month</i>	Month of the year; valid values are january , february , march , and so on.	
<i>hh:mm</i>	Hours and minutes.	
<i>offset</i>	(Optional) Offset in minutes; valid values are from 1 to 1440 minutes.	
date	Daylight savings begins and ends on a particular, nonrecurring date.	
<i>date</i>	Day of the month; valid values are from 1 to 31.	
<i>year</i>	Year; valid values are from 1993 to 2035.	

Defaults

Disabled



Note

When the command is 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 return to default (US summertime). Unless you configure it otherwise, this command advances the clock one hour at 2:00 a.m. on the first Sunday in April and moves the clock back one hour at 2:00 a.m. on the last Sunday in October.

Examples

This example shows how to configure the system to set the clock ahead one hour for daylight saving time to Pacific daylight time (PDT):

```
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 for daylight saving time:

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

This example shows how to set daylight saving time to 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 recurring 3 mon feb 12:00 2 saturday aug 15:00 30
Summertime is disabled and set to ''
  Start : Mon Feb 19 2001, 12:00:00
  End   : Sat Aug 11 2001, 15:00:00
  Offset: 30 minutes
  Recurring: yes, starting at 12:00pm of third Monday of February and ending on
15:00pm of second Saturday of August.
Console> (enable)
```

This example shows how to set 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 default to the standard US daylight savings:

```
Console> (enable) set ntp summertime recurring 3 mon feb 2:00 4 thurs oct 2:00 60
Summertime is disabled and set to ''
  Start : Mon Feb 19 2001, 02:00:00
  End   : Thu Oct 25 2001, 02:00:00
  Offset: 60 minutes
  Recurring: yes, starting at 02:00am of third Monday of February and ending on
02:00am of fourth Thursday of October.
Console> (enable)
```

Related Commands

[show ntp](#)

set ntp timezone

To configure the time offset from Greenwich Mean Time, use the **set ntp timezone** command.

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

Syntax Description	
<i>zone_name</i>	Name of the timezone.
<i>hours</i>	(Optional) Time offset (in hours) from Greenwich Mean Time; valid values are from –12 to 12 hours.
<i>minutes</i>	(Optional) Time offset (in minutes) from Greenwich Mean Time; valid values are from 0 to 59 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 4000 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

To change the Normal (login) mode password on the switch, use the **set password** command.

set password

Syntax Description This command has no arguments or keywords.

Defaults No password is configured.

Command Types Switch command

Command Modes Privileged

Usage Guidelines Passwords are case sensitive; they can be from 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

To configure the auxiliary VLAN ports, use the **set port auxiliaryvlan** command.

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

Syntax Description	
<i>mod</i> [/ports]	Number of the module and (optional) ports.
vlan	Number of the VLAN; valid values are from 1 to 1000.
untagged	Port sends untagged packets.
none	Port does not send any auxiliary VLAN information in the CDP packets from that port.

Defaults Auxiliary VLAN ports are set to 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.

Dynamic VLAN support for VVID includes these restrictions to the following configuration of 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 **untagged**. If this is the case, you must configure VMPS with the MAC address of the IP phone. When you configure the VVID as **untagged** on a dynamic port, the following warning message is displayed:


```
VMPS should be configured with the IP phone mac's.
```
- You cannot change the VVID of the port equal to 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 3/7 untagged
Port 3/7 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 none:

```
Console> (enable) set port auxiliaryvlan 3/12 none  
Port 3/12 will not allow sending CDP packets with AuxiliaryVlan 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 channel

To configure EtherChannel on Ethernet module ports, use the **set port channel** command set.

```
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 [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	EtherChannel mode.
on	Forces the specified ports to channel without PAgP.
off	Prevents ports from channeling.
desirable	Sets 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	Sets 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) Used 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) Used with auto or desirable when traffic is expected from the other device.
all mode off	Turns off channeling on all ports.
all distribution	Applies frame distribution to all ports in the switch.
mac	Frame distribution method using MAC address values.
both	(Optional) Frame distribution method using source and destination address values.

Defaults

The default settings are as follows:

- EtherChannel is set to **auto** and **silent** on all module ports.
- Frame distribution are **mac** and **both**.

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

Ensure that all ports you intend to channel are configured properly. For complete information on EtherChannel configuration restrictions, refer to the *Software Configuration Guide—Catalyst 4000 Family, Catalyst 2948G, and Catalyst 2980G Switches*.

Because of the port ID handling by the spanning tree feature, the maximum supported number of channels is 126 for a 6-slot chassis.

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.

On the Catalyst 4000 family switches, an EtherChannel bundle can consist of any two to eight ports. Ports in an EtherChannel do not have to be contiguous, nor do they have to be on the same module.

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 queuing 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.

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

Examples

This example shows how to create an EtherChannel on ports 5 and 6 of module 4:

```
Console> (enable) set port channel 4/5-6 on
Port(s) 4/5-6 are assigned to admin group 56.
Port(s) 4/5-6 channel mode set to on.
Console> (enable)
```

This example shows how to remove an EtherChannel on ports 5 and 6 of module 4:

```
Console> (enable) set port channel 4/5-6 mode auto
Port(s) 4/5-6 channel mode set to auto.
Console> (enable) show port channel
```

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 to 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 module 4, ports 4 to 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 module 4, ports 4 to 6 and assign those ports 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)
```

Related Commands

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

set port debounce

To enable or disable the debounce timer setting on a per port basis, use the **set port debounce** command.

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

Syntax Description	<i>mod/port</i>	Number of the module and the port on the module.
	enable	Enables the debounce timer.
	disable	Disables the debounce timer.

Defaults Debounce timer is disabled on all ports.

Command Types Switch command

Command Modes Privileged

Usage Guidelines The debounce timer is the time the firmware waits before notifying the main processor for the supervisor engine of a link change at the physical layer.

Examples This example shows how to enable the debounce timer for a specific port on a specific module:

```
Console> (enable) set port debounce 1/1 enable
Debounce is enabled on port 1/1.
Warning:Enabling port debounce causes Link Up/Down detections to be delayed.
It results in loss of data traffic during debouncing period, which might
affect the convergence/reconvergence of various Layer 2 and Layer 3
protocols.
Use with caution.
Console> (enable)
```

Related Commands [show port debounce](#)

set port disable

To disable a port or a range of ports, use the **set port disable** command.

```
set port disable mod/port
```

Syntax Description	<i>mod/port</i> Number of the module and the port on the module.
Defaults	All ports are enabled.
Command Types	Switch command
Command Modes	Privileged
Usage Guidelines	This command is not supported by the Access Gateway module.
Examples	<p>This example shows how to disable port 5/10:</p> <pre>Console> (enable) set port disable 5/10 Port 5/10 disabled. Console> (enable)</pre>
Related Commands	<p>set port enable show port</p>

set port dot1x

To configure dot1x on a port, use the **set port dot1x** command set.

```
set port dot1x mod/port multiple-host {enable | disable}
```

```
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}
```

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

Syntax Description

<i>mod/port</i>	Number of the module and port on the module.
multiple-host	Multiple-user access; see “Usage Guidelines” for more information.
enable	Enables multiple-user access.
disable	Disables multiple-user access.
port-control <i>port_control_value</i>	Port control type; valid values are force-authorized , force-unauthorized , and auto .
initialize	Initializes dot1x on the port.
re-authenticate	Initiates a reauthentication of the entity connected to the port.
re-authentication	Initiates reauthentication of the entity connected to the port within the reauthentication time period; see “Usage Guidelines” for more information.
enable	Enables automatic reauthentication.
disable	Disables automatic reauthentication.
multiple-authentication	Multiple authentications so that more than one host can gain access to the port; see “Usage Guidelines” for more information.
enable	Enables multiple authentication.
disable	Disables multiple authentication.

Defaults

The default settings are as follows:

- Default *port_control_value* is **force-authorized**.
- Multiple host feature is disabled.
- Reauthentication feature is disabled.
- Multiple authentication feature is disabled.

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

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

When setting the port control type, the following applies:

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

If you disable the multiple host feature, once a dot1x port is authorized through a successful authentication of a supplicant, only that particular host (MAC address) is allowed on that port. When the system detects another host (different MAC address) on the authorized port, it shuts down the port and displays a syslog message. This is the default system behavior.

If you enable the multiple host feature, once a dot1x port is authorized through a successful authentication of a supplicant, any host (any MAC address) is allowed to send or receive traffic on that 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.

You can enable either multiple host mode or multiple authentication mode.

Examples

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

```
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 manually 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 multiple-user access on a specific port:

```
Console> (enable) set port dot1x 4/1 multiple-host enable
Multiple hosts allowed on port 4/1.
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

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

set port duplex

To configure the duplex type of an Ethernet or Fast Ethernet port or range of ports, use the **set port duplex** command.

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

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

Defaults 10-Mbps and 100-Mbps modules have 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 supported on Token Ring ports. 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

To enable a port or a range of ports, use the **set port enable** command.

```
set port enable mod/port
```

Syntax Description	<i>mod/port</i> Number of the module and the port on the module.
Defaults	All ports are enabled.
Command Types	Switch command
Command Modes	Privileged
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 errdisable-timeout

To prevent an errdisabled port from being enabled, use the **set port errdisable-timeout** command.

set port errdisable-timeout *mod/port* {enable | disable}

Syntax Description	
<i>mod/port</i>	Number of the module and the port on the module.
enable	Enables errdisable timeout.
disable	Disables errdisable timeout.

Defaults The errdisable-timeout feature for each port is enabled.



Note

This means that when the global timer times out the port will be re-enabled.

Command Types Switch command

Command Modes Privileged

Usage Guidelines The **set port errdisable-timeout** command is helpful during troubleshooting if you intend for a port to remain in the errdisabled state until the problem is fixed.

Examples This example shows how to prevent port 3/3 from being re-enabled at timeout after it goes into errdisabled state:

```
Console> (enable) set port errdisable-timeout 3/3 disable
Successfully disabled errdisable-timeout for port 3/3.
Console> (enable)
```

Related Commands [set errdisable-timeout](#)
[show errdisable-timeout](#)

set port flowcontrol

To configure a port to send or receive pause frames, use the **set port flowcontrol** command.

```
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	Allows a port processes pause frames.
send	Designates if a port sends pause frames.
off	Prevents a local port from receiving and processing pause frames from remote ports or from sending pause frames to remote ports.
on	Enables a local port to receive and process pause frames from remote ports or send pause frames to remote ports.
desired	Obtains predictable results whether a remote port is set to on , off , or desired .

Defaults

The default settings are as follows:

- Gigabit Ethernet ports default to **off** for receive and **desired** for transmit.
 - Oversubscribed Gigabit Ethernet ports (ports 3-18) on the Catalyst 4000 family 18-port Gigabit Ethernet switching module (WS-X4418-GB) default to **desired** for receive and **on** for transmit.
- Fast Ethernet ports default to **off** for receive and **on** for transmit.

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

Pause frames are special packets that signal a source to stop sending frames for a specific period of time because the buffers are full.

When you install an Access Gateway module, the switch enables the internal Gigabit Ethernet port and forces flow control for send and receive actions to the off position.

[Table 2-5](#) describes guidelines for using different configurations of the **send** and **receive** keywords with the **set port flowcontrol** command.

Table 2-5 Send and Receive Keyword Configurations

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

Table 2-5 Send and Receive Keyword Configurations (continued)

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

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

Table 2-6 identifies the Catalyst Gigabit Ethernet switches, modules, and ports that can send pause frames to remote devices.

Table 2-6 Send Capability by Switch Type, Module, and Port

Module	Ports	Send
All modules except WS-X4418-GB, WS-X4412-2GB-TX, and WS-X4416-2GB-TX)	All ports except for the oversubscribed ports listed below	No
WS-X4418-GB	Uplink ports (1-2)	No
WS-X4418-GB	Oversubscribed ports (3-18)	Yes
WS-X4412-2GB-TX	Uplink ports (13-14)	No
WS-X4412-2GB-TX	Oversubscribed ports (1-12)	Yes
WS-X4416-2GB-TX	Uplink ports (17-18)	No

Examples

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

```
Console> (enable) set port flowcontrol 5/1 receive 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 5/1 receive 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 5/1 receive 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 5/1 send 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 5/1 send 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 5/1 send 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

To enable or disable GARP Multicast Registration Protocol (GMRP) on the specified ports in all VLANs, use the **set port gmrp** command.

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

Syntax Description		
	<i>mod/ports...</i>	Number of the module and port number list.
	enable	Enables GMRP on a specified port.
	disable	Disables GMRP on a specified port.

Defaults 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.

This command is not supported by the Access Gateway module.

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 to 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](#)

set port gvrp

To enable or disable GARP VLAN Registration Protocol (GVRP) on a specified port in all VLANs, use the **set port gvrp** command.

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

Syntax Description

mod/ports... Number of the module and port number list.

enable Enables GVRP on the specified ports.

disable Disables GVRP on the specified ports.

Defaults

Disabled

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

GVRP can be enabled only 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.

This command is not supported by the Access Gateway module.

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 port 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

To optimize the port configuration for a host connection, use the **set port host** command.

set port host *mod/ports...*

Syntax Description

mod/ports... Number of the module and port number list.

Defaults

This command has no default settings.

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

The **set port host** 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.

Examples

This example shows how to optimize the port configuration for end station/host connections on port 1 of modules 2 and 3:

```
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)
```

Related Commands

[clear port host](#)

set port inlinepower

To set the inline power mode of a port or group of ports, use the **set port inlinepower** command.

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

Syntax Description	
<i>mod/ports</i>	Number of the module and the ports on the module.
off	Disables power up the port even if an unpowered phone is connected.
auto	Enables power up the port only if the switching module has discovered the phone.

Defaults The inline power mode is set to auto.

Command Types Switch command

Command Modes Privileged

Usage Guidelines 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 only the module number.

An inline power-capable device can still be detected even if the inline power 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 inline power to off for module 2, port 5:

```
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 inline power feature is not supported for module 2, ports 3 to 9:

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

Console> (enable)
```

Related Commands

- [set inlinepower defaultallocation](#)
- [show environment](#)
- [show port inlinepower](#)

set port lacp-channel

To set the priority for physical ports, to assign an administrative key to a particular set of ports, or to change the channel mode for a set of ports that were previously assigned to the same administrative key, use the **set port lacp-channel** command.

```
set port lacp-channel mod/ports port-priority value
```

```
set port lacp-channel mod/ports [admin-key]
```

```
set port lacp-channel mod/ports mode {on | off | active | passive}
```

Syntax Description		
<i>mod/ports</i>		Number of the module and the port(s) on the module.
port-priority		Priority for physical ports.
<i>value</i>		Number of the port priority; valid values are from 1 to 255. See the “Usage Guidelines” section for more information.
<i>admin-key</i>		(Optional) Number of the administrative key; valid values are from 1 to 1024. See the “Usage Guidelines” section for more information.
mode		Channel mode for a set or ports.
on off active passive		Status of the channel mode.

Defaults

The default settings are as follows:

- Port priority is set to 128.
- All ports that are assigned the administrative key are **passive**.

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

This command is allowed for ports belonging to LACP modules only and is rejected by those ports running in PAgP mode.

Higher priority values correspond to lower priority levels.

The following usage guidelines apply when you assign an administrative key to ports:

- If you do not enter a value for the administrative key, the system chooses a value automatically.
- If the value you specify for the administrative key has already been used in your system, the ports that are associated with the value are moved to a new administrative key that is automatically assigned by the system. The previously used value is now associated with new ports.
- You can assign a maximum of 8 ports to an administrative key.
- If you assign an administrative key to a channel that was previously assigned a particular mode, the channel will maintain that mode after you enter the administrative key value.

Examples

This example shows how to Set the priority of ports 1/1 to 1/4 and 2/6 to 2/8 to 10:

```
Console> (enable) set port lacp-channel 1/1-4,2/6-8 port-priority 10
LACP Port(s) priority set to 10 for ports 1/1-4 2/6-8
Console> (enable)
```

This example shows how to assign ports 4/1-4 to an administrative key that the switch automatically chooses:

```
Console> (enable) set port lacp-channel 4/1-4
Ports 4/1-4 being assigned admin key 96.
Port(s) 4/1-4 channel mode set to passive.
Console> (enable)
```

This example shows what happens when you try to assign ports 4/4-6 to administrative key 96 when administrative key 96 has previously been used:

```
Console> (enable) set port lacp-channel 4/4-6 96
admin key 96 already assigned to port 4/1-3.
Port(s) 4/1-3 being assigned to admin key 97.
Port(s) 4/4-6 being assigned to admin key 96.
Port(s) 4/4-6 channel mode set to passive.
Console> (enable)
```

Related Commands

- [clear lacp-channel statistics](#)
- [set channelprotocol](#)
- [set lacp-channel system-priority](#)
- [set spantree channelcost](#)
- [set spantree channelvlancost](#)
- [show lacp-channel](#)
- [show port lacp-channel](#)

set port level

To set the priority level of a port or range of ports on the switching bus, use the **set port level** command.

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

Syntax Description	<table border="1"> <tbody> <tr> <td data-bbox="383 455 548 489"><i>mod/port</i></td> <td data-bbox="553 455 1312 489">Number of the module and the port on the module.</td> </tr> <tr> <td data-bbox="383 495 548 529">Normal</td> <td data-bbox="553 495 1312 529">Sets the port priority to normal.</td> </tr> <tr> <td data-bbox="383 535 548 569">high</td> <td data-bbox="553 535 1312 569">Sets the port priority to high.</td> </tr> </tbody> </table>	<i>mod/port</i>	Number of the module and the port on the module.	Normal	Sets the port priority to normal.	high	Sets the port priority to high.
<i>mod/port</i>	Number of the module and the port on the module.						
Normal	Sets the port priority to normal.						
high	Sets the port priority to high.						
Defaults	All ports are set to the 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	<p>This example shows how to set the priority level for port 2 on module 1 to high:</p> <pre>Console> (enable) set port level 1/2 high Port 1/2 port level set to high. Console> (enable)</pre> <p>This example shows how to set the priority level for port 2 on module 1 to normal:</p> <pre>Console> (enable) set port level 1/2 normal Port 1/2 level set to Normal Console> (enable)</pre>						
Related Commands	<p>set port disable set port enable set port name set port speed show port</p>						

set port membership

To configure ports for dynamic or static VLAN membership, use the **set port membership** command.

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

Syntax Description	<table border="1"> <tbody> <tr> <td><i>mod/port</i></td> <td>Number of the module and the port on the module.</td> </tr> <tr> <td>dynamic</td> <td>Configures the port for dynamic VLAN membership.</td> </tr> <tr> <td>static</td> <td>Configures the port for static VLAN membership.</td> </tr> </tbody> </table>	<i>mod/port</i>	Number of the module and the port on the module.	dynamic	Configures the port for dynamic VLAN membership.	static	Configures the port for static VLAN membership.
<i>mod/port</i>	Number of the module and the port on the module.						
dynamic	Configures the port for dynamic VLAN membership.						
static	Configures the port for static VLAN membership.						
Defaults	Static membership						
Command Types	Switch command						
Command Modes	Privileged						
Usage Guidelines	<p>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.</p> <p>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.</p> <p>This command is not supported by the Access Gateway module.</p> <p>Dynamic VLAN support for VVID includes these restrictions to the following configuration of MVAP on the switch port:</p> <ul style="list-style-type: none"> 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 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, this warning message is displayed: <pre>VMPS should be configured with the IP phone mac's.</pre> You cannot change the VVID of the port equal to 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	<p>This example shows how to set the port membership VLAN assignment to dynamic on module 3, ports 1 to 3:</p> <pre>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)</pre>						

This example shows how to configure a port for static VLAN membership on module 3, ports 1 to 3:

```
Console> (enable) set port membership 3/1-3 static  
Ports 3/1-3 vlan assignment set to static.  
Console> (enable)
```

Related Commands

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

set port name

To assign a name to a port, use the **set port name** command.

```
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 port.

Defaults No port names are configured for any ports.

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

To enable link negotiation on the port that you specify, use the **set port negotiation** command.

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

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

Defaults Link negotiation is enabled.

Command Types Switch command

Command Modes Privileged

Usage Guidelines



Note

Use the **set port negotiation** command only on 1000BASE [SX, LX, and ZX].

Link negotiation autonegotiates flow control, duplex mode, and remote fault information.

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

```
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

To set the protocol filtering group membership of ports, use the **set port protocol** command.

```
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	IP protocol filtering group.
ipx	IPX protocol filtering group.
group	Group protocol filtering group.
on	Indicates the port will receive all the flood traffic for that protocol.
off	Indicates the port will not receive any flood traffic for that protocol.
auto	Indicates the port will receive the flood traffic for that protocol only after transmitting packets of that specific protocol.

Defaults

The default settings are as follows:

- IP protocol group ports are **on**.
- IPX and group protocol group ports are **auto**.

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 the Catalyst 4000 family switches, packets are classified into the following protocol groups:

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

Examples

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

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

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

```
Console> (enable) set port protocol 2/1 ip 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 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 IPX membership of port 1 on module 5:

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

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

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

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

```
Console> (enable) set port protocol 1/1 group auto  
Group protocol set to auto mode on port 1/1.  
Console> (enable)
```

Related Commands

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

set port security

To configure port security and unicast flood on a port or range of ports, use the **set port security** command.

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

Syntax Description

<i>mod/port...</i>	Number of the module and the port on the module.
enable	(Optional) Enables port security or unicast flood.
disable	(Optional) Disables port security or unicast flood.
<i>mac_addr</i>	(Optional) Secure MAC address of the enabled port.
age <i>age_time</i>	(Optional) Duration for which addresses on the port will be secured; valid values are 0 (to disable) and from 1 to 1440 (minutes).
maximum <i>num_of_mac</i>	(Optional) Maximum number of MAC addresses to secure on the port; valid values are from 1 to 1025.
shutdown <i>shutdown_time</i>	(Optional) Duration for which a port will remain disabled in case of a security violation; valid values are 0 (to disable) and from 1 to 1440 (minutes).
unicast-flood	(Optional) Unicast flood.
violation	(Optional) Action to be taken in the event of a security violation.
shutdown	Shuts down the port in the event of a security violation.
restrict	Restricts packets from unsecure hosts.

Defaults

The default settings are 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.
- Unicast flood is enabled.

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.

We recommend that you configure the age timer and the shutdown timer if you want to move a host from one port to another when port security is enabled on those ports. If the *age_time* value is less than or equal to the *shutdown_time* value, the moved host will function again in an amount of time equal to the *shutdown_time* value. The age timer begins upon learning the first MAC address, and the disable timer begins when there is a security violation.

When you configure the switch to disable unicast flood packets on a port the packets are dropped once the address limit has been reached.

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)
```

This example shows how to enable unicast flood on port 4/1:

```
Console> (enable) set port security 4/1 unicast-flood enable
Port 4/1 security flood mode set to enable.
Console> (enable)
```

This example shows how to disable unicast flood on port 4/1:

```
Console> (enable) set port security 4/1 unicast-flood disable
WARNING: Trunking & Channelling will be disabled on the port.
Port 4/1 security flood mode set to disable.
Console> (enable)
```

Related Commands

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

set port speed

To configure transmission speed or autonegotiation, use the **set port speed** command.

```
set port speed mod/port {10 | 100 | 1000 | auto}
```

Syntax Description	
<i>mod/port</i>	Number of the module and the port on the module.
10	Transmission rate of 10 Mbps on 10/100 Fast Ethernet ports.
100	Transmission rate of 100 Mbps on 10/100 Fast Ethernet ports.
1000	Transmission rate of 1000 Mbps on a 1000BASE-T port.
auto	Autonegotiation for transmission speed and duplex mode on 10/100 Fast Ethernet ports. On 1000BASE-T Gigabit Ethernet ports, this keyword specifies that autonegotiation determines the master and slave links.

Defaults All module ports are set to auto.

Command Types Switch command

Command Modes Privileged

Usage Guidelines

In the default mode, autonegotiation manages the transmission speed, duplex mode, master link, and slave link.

On 1000BASE-T Gigabit Ethernet ports, autonegotiation determines which side of the link is master and which side is slave.

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.

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.

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

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

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

Syntax Description	<i>mod/port</i>	Number of the module and the port on the module.
	enable	Activates the SNMP link trap.
	disable	Deactivates the SNMP link trap.

Defaults All port traps are 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 port unicast-flood

To configure the switch to drop Unicast Flood traffic on an Ethernet port, use the **set port unicast-flood** command.

```
set port unicast-flood mod/port {enable | disable}
```

Syntax Description

<i>mod/port</i>	Number of the module and the port on the module.
enable	Enables unicast flood and disables unicast flood blocking.
disable	Disables unicast flood and enables unicast flood blocking.

Defaults

Unicast flood blocking is disabled on all ports.

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

Only Ethernet ports can block unicast flood traffic.

You must have a static CAM entry associated with the Ethernet port before you disable unicast flood on the port, or you will lose network connectivity when you disable unicast flood. You can verify a static CAM entry exists by entering the **show cam static** command.

You cannot configure a port channel on a unicast flood disabled port and you cannot disable unicast flood on a port channel.

You cannot disable unicast flood on a SPAN destination port and you cannot configure a SPAN destination on a unicast flood disabled port.

You cannot disable unicast flood on a trunk port. If you attempt to do so, an error message will be displayed.

If you disable unicast flood traffic on an Ethernet port that has port security enabled, the switch stops sending Unicast Flood packets to the port when the maximum number of MAC addresses allowed is reached. When the MAC address count drops below the maximum number allowed unicast flooding is automatically re-enabled.

Unicast flood blocking and GARP VLAN Registration Protocol (GVRP) are mutually exclusive. You cannot disable unicast flood and exchange VLAN configuration information with GVRP switches at the same time.

Examples

This example shows how to enable unicast flood traffic on module 4, port 1 of a switch:

```
Console> (enable) set port unicast-flood 4/1 disable
WARNING: Trunking & Channelling will be disabled on the port.
Unicast Flooding is successfully disabled on the port 4/1.
Console> (enable)
```

set port unicast-flood

This example shows how to disable unicast flood traffic on module 4, port 1 of a switch:

```
Console> (enable) set port unicast-flood 4/1 enable  
Unicast Flooding is successfully enabled on the port 4/1.  
Console> (enable)
```

Related Commands [show port unicast-flood](#)

set power budget

To configure the power settings for the chassis, use the **set power budget** command.

set power budget {1 | 2}

Syntax Description	1	2
	Configures the chassis for one power supply.	Configures the chassis for two power supplies.

Defaults This command has no default settings.

Command Types Switch command

Command Modes Privileged

Usage Guidelines If the chassis is has two power supplies and is configured to a power budget of 2, and you try to set the power budget to 1, it is disallowed. You must pull out the extra linecards and design a valid and supported configuration in order to change the power budget to 1.

Examples This example shows how to set the power budget to 1 for the chassis:

```
Console>(enable) set power budget 1
Warning: Your power supply budget will be constrained to one power supply and may cause
one or more linecards to be disabled depending upon your chassis configuration.
Do you want to continue ? [confirm (y/n)]:y
Console>(enable)
```

set power dcinput

To configure the DC power input setting for the Catalyst 4500 series switch, use the **set power dcinput** command.

set power dcinput *watts*

Syntax Description	<i>watts</i> Number of watts; valid range is from 300 to 7500.
Defaults	2500 watts
Command Types	Switch command
Command Modes	Privileged
Usage Guidelines	The command works only on Catalyst 4500 series switches with a Supervisor Engine II.
Examples	This example shows how to set DC power to 3000 watts: <pre>Console>(enable) set power dcinput 3000 Console>(enable)</pre>
Related Commands	show environment

set prompt

To change the prompt for the CLI, use the **set prompt** command.

```
set prompt prompt_string
```

Syntax Description	<i>prompt_string</i> String to use as the command prompt.
Defaults	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. Use the set prompt command to change the text that is displayed in the system prompt.
Examples	This example shows how to set the prompt to system100>: <pre>Console> (enable) set prompt system100> system100> (enable)</pre>
Related Commands	set system name

set protocolfilter

To activate or deactivate protocol filtering, use the **set protocolfilter** command.

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

Syntax Description	enable	Disables protocol filtering.
	disable	Deactivates protocol filtering.

Defaults Protocol filtering is disabled.

Command Types Switch command

Command Modes Privileged

Usage Guidelines 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](#)
[show protocolfilter](#)

set pvlan

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

```
set pvlan primary_vlan { isolated_vlan | community_vlan } [mod/port | sc0]
```



Caution

Before using this command, we recommend that you read and understand the “Configuring VLANs” chapter in the *Software Configuration Guide—Catalyst 4000 Family, Catalyst 2948G, and Catalyst 2980G*.

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) Number of the module and port numbers of the isolated or community ports.
sc0	(Optional) Inband port sc0.

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** *pvlan_type* command before making the association using the **set pvlan** command.

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

Although you can configure sc0 as a private VLAN port, you cannot configure sc0 as a promiscuous port.

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)
```

This example shows how to assign the sc0 interface to private VLANs 300 (the primary VLAN) and 301 (isolated, community, or two-way community VLANs):

```
Console> (enable) set pvlan 300 301 sc0
Successfully set the following ports to Private Vlan 300, 301:
sc0
Console> (enable)
```

Related Commands

- [clear config pvlan](#)
- [clear pvlan mapping](#)
- [clear vlan](#)
- [set pvlan mapping](#)
- [set vlan](#)
- [show vlan](#)
- [show pvlan](#)
- [show pvlan capability](#)
- [show pvlan mapping](#)