set logging level

Use the **set logging level** command to set the facility and severity level used when logging system messages.

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

Syntax Description

facility	Value for the type of system messages to capture; see the "Usage Guidelines" section for valid values.
severity	Value for the severity level of system messages to capture; see the "Usage Guidelines" section for valid values.
default	(Optional) Keyword to specify the logging level to apply to all sessions.

Defaults

The default is *facility* is set to **all**, and *level* is set to **0**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Facility types are shown in Table 2-4.

Table 2-4 Facility Types

Facility Name	Definition
all	all facilities
cdp	Cisco Discovery Protocol
cops	Common Open Policy Service
drip	Dual Ring Protocol
dtp	Dynamic Trunk Protocol
earl	Encoded Address Recognition Logic
fddi	Fiber Distributed Data Interface
filesys	file system
gvrp	GARP VLAN Registration Protocol
ip	Internet Protocol
kernel	Kernel
mcast	Multicast
mgmt	Management
mls	Multilayer Switching
pagp	Port Aggregation Protocol

Table 2-4 Facility Types (continued)

Facility Name	Definition
protfilt	Protocol Filter
pruning	VTP pruning
qos	Quality of Service
radius	Remote Access Dial-In User Service
security	Security
snmp	Simple Network Management Protocol
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

Severity level definitions are shown in Table 2-5.

Table 2-5 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

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

Use the **set logging server** command to enable and disable system message logging to configured syslog servers and to add a syslog server to the system logging server table.

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	Keyword to enable system message logging to configured syslog servers.
disable	Keyword to disable system message logging to configured syslog servers.
ip_addr	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	Keyword to set the type of system messages to capture.
server_facility_parameter	Value to specify the logging facility of syslog server; valid values are **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local6**, **local7**, and **syslog**.
severity	Keyword to set the severity level of system messages to capture.
server_severity_level	Value to specify the severity level of system messages to capture; valid values are from **0** through **7**. Severity level definitions are shown in Table 2-5.

Defaults

By default, no syslog servers are configured to receive system messages.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Severity logging to a configured syslog server depends on the configuration set by **set logging level** command. The server severity level must be greater than or equal to the default severity level of those message facility that you expect to receive in syslog messages on the syslog server.

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

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

set logging session {**enable** | **disable**}

Syntax Description

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

Defaults

By default, system message logging to the current login session is 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 timestamp

Use the **set logging timestamp** command to enable or disable the timestamp display on system logging messages.

set logging timestamp {**enable** | **disable**}

Syntax Description

enable	Keyword to enable the timestamp display.
disable	Keyword to disable the timestamp display.

Defaults

By default, system message logging timestamp is 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

Use the **set logout** command to set the number of minutes until the system disconnects an idle session automatically.

set logout *timeout*

Syntax Description

timeout	Number of minutes until the system disconnects an idle session automatically; valid values are from **0** to **10,000** minutes.

Defaults

The default value is 20 minutes.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Setting the value to 0 disables the automatic disconnection of idle sessions.

The **show tech-support** command may time out if the configuration file output takes longer to display than the configured session timeout time. If this happens, enter a **set logout** *timeout* value of 0 to disable automatic disconnection of idle sessions or enter a longer *timeout* value.

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 mls

Use the **set mls** command to enable and disable IP or IPX MLS on the switch.

set mls {**enable** | **disable**} {**ip** | **ipx**}

Syntax Description

enable	Keyword to enable MLS on the switch.
disable	Keyword to disable MLS on the switch.
ip	Keyword to specify IP MLS.
ipx	Keyword to specify IPX MLS.

Defaults

By default, IP MLS is enabled and IPX MLS is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **ipx** keyword is supported only on Supervisor Engine II G or III G, or Supervisor Engine III.

If you do not specify the **ip** or **ipx** keyword, **ip** is assumed.

Examples

This example shows how to disable IP MLS on the switch:

```
Console> (enable) set mls disable ip
IP Multilayer switching is disabled.
Console> (enable)
```

This example shows how to enable IPX MLS on the switch:

```
Console> (enable) set mls enable ipx
IPX Multilayer switching is enabled
Console> (enable)
```

Related Commands

clear mls entry ip
clear mls entry ipx
clear mls include ip
clear mls include ipx
clear mls nde flow
clear mls statistics
set mls nde
show mls rp

set mls agingtime

Use the **set mls agingtime** command to configure the IP and IPX MLS entry aging time.

set mls agingtime {**ip** | **ipx**} *agingtime*

Syntax Description

ip	Keyword to specify IP MLS agingtime.
ipx	Keyword to specify IPX MLS agingtime.
agingtime	(Optional) Aging time of MLS entries, in seconds.

Defaults

The default MLS entry aging time is set to 256 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **ipx** keyword is supported only on Supervisor Engine II G or III G, or Supervisor Engine III.

If you do not specify the **ip** or **ipx** keyword, **ip** is assumed.

The *agingtime* value must be specified as a multiple of 8 seconds in the range of 8 to 2024 seconds. If you enter a value for *agingtime* that is not a multiple of 8 seconds, the value is adjusted to the closest one. For example, 65 is adjusted to 64, while 127 is adjusted to 128.

Examples

This example shows how to set the IP MLS aging time to 512 seconds:

```
Console>(enable) set mls agingtime 512
IP Multilayer switching aging time set to 512 seconds.
Console> (enable)
```

Related Commands

clear mls entry ip
clear mls entry ipx
clear mls include ip
clear mls include ipx
clear mls nde flow
clear mls statistics
set mls agingtime fast
show mls rp

set mls agingtime fast

Use the **set mls agingtime fast** command to specify the MLS aging time of shortcuts to an MLS entry that has no more than *pkt_threshold* packets switched within *fastagingtime* seconds after it is created.

set mls agingtime fast *fastagingtime pkt_threshold*

Syntax Description

fastagingtime	Fast aging time; valid values are multiples of 8 to any value in the range of **0** to **128** seconds. **0** disables fast aging. If a value is not specified, the default value is used.
pkt_threshold	Packet threshold; valid values are **0**, **1**, **3**, **7**, **15**, **31**, **63**, and **127** packets. If a value is not specified, the default value is used.

Defaults

The default *fastagingtime* is 0, no fast aging. The default *pkt_threshold* is 0.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not available for IPX MLS.

When you set the *fastagingtime* value, it can be configured as multiples of 8 to any value in the range of 0 to 128 seconds.

The default *pkt_threshold* value is 0. It can be configured as one of the 0, 1, 3, 7, 15, 31, 63, and 127 (the values picked for efficient aging). If the *fastagingtime* value is not configured exactly the same among these values, it is adjusted to the closest one. A typical value for *fastagingtime* and *pkt_threshold* is 32 seconds and 0 packet, respectively (it means no packet switched within 32 seconds after the entry created).

Agingtime applies to an MLS entry that has no more than *pkt_threshold* packets switched within *fastagingtime* seconds after it is created. A typical example is the MLS entry destined to or sourced from a DNS or TFTP server. This entry may never be used again after it is created. For example, only one request goes to a server and one reply returns from the server, and then the connection is closed.

The *fastagingtime* option is used to purge entries associated with very short flows, such as DNS and TFTP.

We recommend that you keep the number of MLS entries in the MLS cache below 32K. If the number of MLS entries is more than 32K, some flows (less than 1 percent) are sent to the router.

To keep the number of MLS cache entries below 32K, decrease the aging time. Aging time can be decreased up to 8 seconds. If your switch has a lot of short flows that are used by only a few packets, then you can use fast aging.

If cache entries continue to exceed 32K, decrease the normal aging time in 64-second increments from the 256-second default.

Examples

This example shows how to use the **set mls agingtime fast** command to set the agingtime:

```
Console>(enable) set mls agingtime fast 32 0
Multilayer switching fast aging time set to 32 seconds for entries with no more than 0
packet switched.
Console> (enable)
```

Related Commands

clear mls entry ip
clear mls entry ipx
clear mls include ip
clear mls include ipx
clear mls nde flow
clear mls statistics
set mls nde
show mls rp
show mls statistics

set mls flow

Use the **set mls flow** command to specify the minimum flow mask used for MLS. This command is needed to collect statistics for the supervisor engine module.

set mls flow {**destination** | **destination-source** | **full**}

Caution **Use this command carefully.** This command *purges all existing shortcuts* and affects the number of active shortcuts. This command can increase the cache usage and increase the load on the router.

Caution Be extremely careful if you enter this command on a switch that already has a large number of shortcuts (greater than 16K).

Caution Do not place this command in scripts that are frequently executed—changing the MLS flow mask purges all MLS cache entries.

Syntax Description

destination	Keyword to set the minimum flow mask to destination flow.
destination-source	Keyword to set the minimum flow mask to source flow.
full	Keyword to set the minimum flow mask to an extended access list.

Defaults

If there are no access lists on any MLS-RP, the flow mask is set to destination flow.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command specifies the minimum MLS flow mask. Depending on the MLS-RP configuration, the actual flow mask used might be more specific than the specified minimum flow mask. For example, if you configure the minimum flow mask to **destination-source**, but an MLS-RP interface is configured with IP extended access lists, the actual flow mask used will be **full**.

If you configure a more specific flow mask (for example, **destination-source** or **full**), the number of active flow entries increases. To limit the number of active flow entries, you might need to decrease the MLS aging time.

This command is intended to be used for gathering very detailed statistics at the protocol port level; for example, when NetFlow data is exported to an RMON2 probe.

Examples

These examples show how to specify that only expired flows to subnet 171.69.194.0 are exported:

```
Console> (enable) set mls flow destination
Configured flow mask is set to destination flow.
Console> (enable)

Console> (enable) set mls flow destination-source
Configured flow mask is set to destination-source flow.
Console> (enable)

Console> (enable) set mls flow full
Configured flow mask is set to full flow.
Console> (enable)
```

Related Commands

clear mls entry ip
clear mls entry ipx
clear mls include ip
clear mls include ipx
clear mls nde flow
clear mls statistics
set mls agingtime
show mls rp

set mls include

Use the **set mls include** command to specify routers to add to the IP or IPX MLS-RP include list.

set mls include {**ip** | **ipx**} *ip_addr1* [*ip_addr2...*]

Syntax Description

ip	Keyword to specify the IP MLS-RP include list.
ipx	Keyword to specify the IPX MLS-RP include list.
ip_addr1	IP address or DNS host name of the first router to include.
ip_addr2...	(Optional) IP addresses or DNS host names of additional routers to include (you can include up to 16 routers to participate in IP MLS).

Defaults

If a Catalyst 5000 family RSM or RSFC is installed in the switch, it is added to the MLS-RP include list automatically.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **ipx** keyword is supported only on Supervisor Engine II G or III G, or Supervisor Engine III.

If you do not specify the **ip** or **ipx** keyword, **ip** is assumed.

You must use the IP address or DNS host name of the router to add to the IP or IPX MLS-RP include list. You cannot specify the router IPX address.

You can specify the IP addresses of multiple MLS-RPs on the same command line. Up to 16 MLS-RPs can be selected to participate in MLS.

The switch does not process MLSP messages from routers that are not in the MLS-RP include list.

Examples

This example shows how to add a router to the IP MLS-RP include list:

```
Console> (enable) set mls include ip 172.170.2.1
IP Multilayer switching is enabled for router 172.170.2.1
Console> (enable)
```

This example shows how to add a router to the IPX MLS-RP include list:

```
Console> (enable) set mls include ipx 172.170.2.1
IPX Multilayer switching is enabled for router 172.170.2.1
Console> (enable)
```

Related Commands

clear mls entry ip
clear mls entry ipx
clear mls include ip
clear mls include ipx
clear mls nde flow
clear mls statistics
set mls nde
show mls rp
show mls statistics

set mls multicast

Use the **set mls multicast** command to enable and disable IP multicast MLS on the switch.

set mls multicast {**enable** | **disable**}

Syntax Description

enable	Keyword to enable IP multicast MLS on the switch.
disable	Keyword to disable IP multicast MLS on the switch.

Defaults

The default is that IP multicast MLS is disabled.

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.

You must enable one of the Layer 2 multicast protocols (CGMP, IGMP snooping, or GMRP) on the switch before you enable IP multicast MLS.

Examples

This example shows how to enable IP multicast MLS on the switch:

```
Console> (enable) set mls multicast enable
Multilayer switching for Multicast is enabled for this device.
Console> (enable)
```

Related Commands

clear mls multicast include
clear mls multicast statistics
set mls multicast include
show mls multicast entry

set mls multicast include

Use the **set mls multicast include** command to specify routers to add to the IP MMLS-RP include list.

set mls multicast include *ip_addr*

Syntax Description

ip_addr	IP address or DNS host name of the router to include.

Defaults

The default is no routers are in the IP MMLS-RP include list.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can specify only one router IP address at a time. You can configure a maximum of two internal or directly attached participating routers.

The switch does not process MLSP messages from routers that are not in the MMLS-RP include list.

Examples

This example shows how to add a router to the MMLS-RP include list:

```
Console> (enable) set mls multicast include 172.170.2.1
Multilayer switching enabled for router 172.170.2.1
Console> (enable)
```

Related Commands

clear mls multicast include
clear mls multicast statistics
clear mls nde flow
show mls multicast entry

set mls nde

Use the **set mls nde** command to enable and disable NDE on the switch and to configure the switch to export statistics to the specified collector.

set mls nde {**disable** | **enable**}

set mls nde {*collector_ip*} {*udp_port_num*}

set mls nde flow [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**protocol** *protocol*] [**src-port** *port_number*] [**dst-port** *port_number*]

Syntax Description

disable	Keyword to disable NDE.
enable	Keyword to enable NDE.
collector_ip	IP address of the collector if DNS is enabled.
udp_port_num	Number of the UDP port to receive the exported statistics.
flow	Keyword to add filtering to NDE.
destination	(Optional) Keyword to specify the destination IP address.
ip_addr_spec	(Optional) Full IP address or a subnet address in these formats: *ip_subnet_addr*, *ip_addr*/*subnet_mask*, or *ip_addr*/#*subnet_mask_bits*.
source	(Optional) Keyword to specify the source IP address.
protocol *protocol*	(Optional) Keyword and variable to specify the protocol type; valid values can be **0**, **tcp**, **udp**, **icmp**, or a decimal number for other protocol families. **0** indicates “do not care.”
src-port *port_number*	(Optional) Keyword and variable to specify the number of the source port.
dst-port *port_number*	(Optional) Keyword and variable to specify the number of the destination port.

Defaults

All expired flows are exported until the filter is specified explicitly.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Before you use the **set mls nde** command for the first time, you must configure the host to collect the MLS statistics. You do not need to specify the host name and UDP port number because they are saved in NVRAM. If you specify a host name and UDP port, values in NVRAM overwrite the old values. Collector’s values in NVRAM do not clear when NDE is disabled; this command configures the collector, but does not enable NDE automatically.

The **set mls nde enable** command enables NDE, exporting statistics to the preconfigured collector.

The **set mls nde flow** command adds filtering to the NDE. Expired flows matching the specified criteria are exported. These values are stored in NVRAM. They are not cleared when NDE is disabled. If any option is not specified in this command, it is treated as a wildcard. The NDE filter in NVRAM does not clear when NDE is disabled.

Use the following syntax to specify an IP subnet address:

- *ip_subnet_addr*—This is the short subnet address format. The trailing decimal number 00 in an IP address YY.YY.YY.00 specifies the boundary for an IP subnet address. For example, 172.22.36.00 indicates a 24-bit subnet address (subnet mask 172.22.36.00/255.255.255.0), and 173.24.00.00 indicates a 16-bit subnet address (subnet mask 173.24.00.00/255.255.0.0). However, this format can identify only a subnet address of 8, 16, or 24 bits.
- *ip_addr/subnet_mask*—This is the long subnet address format, for example, 172.22.252.00/255.255.252.00 indicates a 22-bit subnet address. This format can specify a subnet address of any bit number. To provide more flexibility, the *ip_addr* is a full host address, such as 172.22.253.1/255.255.252.00.
- *ip_addr/maskbits*—This is the simplified long subnet address format. The mask bits specify the number of bits of the network masks. For example, 172.22.252.00/22 indicates a 22-bit subnet address. The *ip_addr* is a full host address, such as 193.22.253.1/22, which has the same subnet address as the *ip_subnet_addr*.

If the *protocol* value is not set to TCP or UDP, we recommend you set the *dst_port* and *src_port* values to 0; otherwise, no flows will be displayed.

The **src-port** *port_number* is used with **dst-port** *port_number* to specify the port pair if the protocol is TCP or UDP. If you enter a **src-port** value of 0, this indicates "do not care." If the protocol is not TCP or UDP, we recommend that you set the **src-port** or **dst-port** value to 0; otherwise, no flows are displayed.

Examples

These examples show how to use the **set mls nde** command set to configure NDE:

```
Console> (enable) set mls nde Stargate 120
Netflow data export not enabled.
Netflow data export to port 120 on 172.20.15.1(Stargate)
Console> (enable)

Console>(enable) set mls nde enable
Netflow data export enabled.
Netflow data export to port 120 on 172.20.15.1 (Stargate)
Console> (enable)

Console> (enable) set mls nde disabled
Netflow data export disabled.
Console> (enable)

Console> (enable) set mls nde flow destination 171.69.194.140/24
Netflow data export: destination filter set to 171.69.194.0/24
Console> (enable)

Console> (enable) set mls nde flow destination 171.69.194.140
Netflow data export: destination filter set to 171.69.194.140/32
Console> (enable)

Console>(enable) set mls nde flow destination 171.69.194.140/24 source 171.69.173.5/24
Netflow data export: destination filter set to 171.69.194.0/24
Netflow data export: source filter set to 171.69.173.0/24
Console>(enable)
```

```
Console> (enable) set mls nde flow source 171.69.194.140 protocol 51
Netflow data export: source filter set to 171.69.194.140/32
Netflow data export: protocol filter set to 51.
Console> (enable)

Console>(enable) set mls nde flow dst-port 23
Netflow data export: destination port filter set to 23.
Console>(enable)

Console>(enable) set mls nde flow source 171.69.194.140 dst-port 23
Netflow data export: destination port filter set to 23
Netflow data export: source filter set to 171.69.194.140/32
Console>(enable)
```

Related Commands

clear mls entry ip
clear mls entry ipx
clear mls include ip
clear mls include ipx
clear mls nde flow
clear mls statistics
set mls agingtime
set mls agingtime fast
show mls rp
show mls statistics

set mls statistics protocol

Use the **set mls statistics protocol** command to add protocols to the protocols statistics list.

set mls statistics protocol *protocol src_port*

Syntax Description

protocol	Number of the protocol.
port	Number of the port.

Defaults

The default is no protocols are specified for statistics collection.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can configure a maximum of 64 ports on which to collect protocol statistics. Use the **show mls statistics** command to view MLS statistics for the specified protocols.

Examples

This example shows how to specify a protocol and port for which to gather MLS statistics:

```
Console>(enable) set mls statistics protocol 17 1934
Protocol 17 port 1934 is added to protocol statistics list.
Console> (enable)
```

Related Commands

show mls statistics

set module disable

Use the **set module disable** command to disable a module.

set module disable *mod*

Syntax Description

mod	Number of the module.

Defaults

The default configuration has all modules 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 dash 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.
```

Related Commands

set module enable
show module

set module enable

Use the **set module enable** command to enable a module.

set module enable *mod*

Syntax Description

mod	Number of the module to enable.

Defaults

The default setting has all modules 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

Use the **set module name** command to set the name for a module.

set module name *mod* [*mod_name*]

Syntax Description

mod	Number of the module.
mod_name	(Optional) Name to assign to the module.

Defaults

The default configuration has no module names configured for any modules.

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 the name for module 1 to Supervisor:

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

Related Commands

show module

set multicast router

Use the **set multicast router** command to manually configure a port as a multicast router port.

set multicast router *mod/port*

Syntax Description

mod/port	Number of the module and the port on the module.

Defaults

By default, 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

This example shows how to configure a multicast router port:

```
Console> (enable) set multicast router 3/1
Port 3/1 added to multicast router port list.
Console> (enable)
```

Related Commands

clear multicast router
set cgmp
set igmp
show multicast group count
show multicast router

set ntp authentication

Use the **set ntp authentication** command to enable or disable the NTP authentication feature.

set ntp authentication {**enable** | **disable**}

Syntax Description

enable	Keyword to enable NTP authentication.
disable	Keyword to disable NTP authentication.

Defaults

The default is NTP authentication.

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

Use the **set ntp broadcastclient** command to enable or disable NTP broadcast-client mode.

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

Syntax Description

enable	Keyword to enable NTP broadcast-client mode.
disable	Keyword to disable NTP broadcast-client mode.

Defaults

The default setting for this command is 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

set port broadcast

set ntp broadcastdelay

Use the **set ntp broadcastdelay** command to configure a time-adjustment factor so the switch can receive broadcast packets.

set ntp broadcastdelay *microseconds*

Syntax Description

microseconds	Estimated round-trip time, in microseconds, for NTP broadcasts. Allowable range is from **1** to **999999**.

Defaults

By default, the NTP broadcast delay is set to 3000.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the NTP broadcast delay to 4000 microseconds:

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

Related Commands

set port broadcast

set ntp client

Use the **set ntp client** command to enable or disable the switch as an NTP client.

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

Syntax Description

enable	Keyword to enable the NTP client.
disable	Keyword to disable the NTP client.

Defaults

The default is NTP client mode is 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

set port broadcast