L Commands

- ldap search-map, on page 2
- ldap-server deadtime, on page 3
- ldap-server host, on page 4
- ldap-server timeout, on page 6
- lifetime seconds, on page 7
- line com1, on page 8
- line console, on page 11
- line vty, on page 14
- link-state-trap (SME), on page 15
- load-balancing, on page 16
- load-balancing (Cisco IOA cluster Configuration submode), on page 17
- locator-led, on page 18
- logging abort, on page 19
- logging commit, on page 20
- logging console, on page 21
- logging distribute, on page 22
- logging level, on page 23
- logging level pmon, on page 24
- logging level port , on page 26
- logging logfile, on page 28
- logging module, on page 29
- logging monitor, on page 30
- logging origin-id, on page 31
- logging server, on page 33
- logging timestamp, on page 36
- logging timezone utc, on page 37
- logging format rfc5424, on page 38
- logical-type, on page 39

ldap search-map

To configure a search map, use the ldap search-map command. To disable this feature, use the no form of the command.

ldap search-map *map-name*
no ldap search-map *map-name*

Syntax Description

map-name	Specifies the name of the search map. The maximum length is 128 characters.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to specify the LDAP search mapping table:

```
switch(config)# ldap search-map map1
switch(config-ldap-search-map)#
```

Related Commands

Command	Description
show ldap-server groups	Displays the configured LDAP server groups.

ldap-server deadtime

To configure global LDAP server deadtime period in seconds, use the **ldap-server deadtime** command To disable this feature, use the no form of the command.

ldap-server deadtime *minutes*
no ldap-server deadtime *minutes*

Syntax Description

minutes	Specifies LDAP server deadtime period in minutes. The range is from 1 to 60 minutes. Default is 5 minutes.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure global LDAP server deadtime period in seconds:

```
switch(config)# ldap-server deadtime 5
switch(config)#
```

Related Commands

Command	Description
show ldap-server groups	Displays the configured LDAP server groups.

ldap-server host

To configure global LDAP server IP address, use the **ldap-server host** command in configuration mode. To disable this feature, use the **no** form of the command.

{**ldap-server host** {**server-name** | **ip-address**} **enable-ssl** | [**port port number**] [**timeout timeout in seconds**] | **rootDN rootDN password** [**7 password** | **password**] [**port port number**] [**timeout timeout in seconds**] | **test rootDN DN string** [**username user-name**] [**password** [**7 password** | **password**]] [**idle-time n**]}
{**no ldap-server host** {**server-name** | **ip-address**} **enable-ssl** | [**port port number**] [**timeout timeout in seconds**] | **rootDN rootDN password** [**7 password** | **password**] [**port port number**] [**timeout timeout in seconds**] | **test rootDN DN string** [**username user-name**] [**password** [**7 password** | **password**]] [**idle-time n**]}

Syntax Description

server-name	Specifies LDAP server DNS name. The maximum length is 255 characters.
ip-address	Specifies LDAP server IP address.
enable-ssl	Specifies LDAP server, enable SSL. **Note** From Cisco MDS NX-OS Release 8.1(1) and later, LDAP over Secure Sockets Layer (SSL) supports SSL version 3 and Transport Layer Security (TLS) versions 1.0 and 1.2. From Cisco MDS NX-OS Release 6.2(29) and later, LDAP over Secure Sockets Layer (SSL) supports SSL version 3 and Transport Layer Security (TLS) versions 1.0 and 1.2.
port	Specifies LDAP server port.
port-number	Specifies port number. The range is from 1 to 65535.
root DN	Specifies LDAP rootDN for the LDAP server database.
rootDN	The maximum length is 63 characters and default is empty string.
password 7 *pasword*	Specifies encrypted bind password for root. The maximum length is 63 characters and default is empty string.
password *password*	Specifies bind password for root. The maximum length is 63 characters and default is empty string
test rootDN *DN string*	Specifies the test keyword which turns on automated testing for the feature. The rootDN keyword is mandatory and is followed by the rootDN to be used to bind to ldap server to verify its state.
username *user-name*	Specifies the username that would be used to do a test bind.
password *password*	Specifies the password to be used in the packets. When a password cannot be obtained, the default of test is used for test packets.

idle-time *n*	Specifies the time for which the server has to remain idle before test packet(s) are sent out. If any of the responses are not received, the server is assumed dead. The default idle-time is 0, but can be configured as low as 1 minute.
timeout *timeout in seconds*	Specifies the timeout period to wait for a response from the server before client can declare a timeout failure. The range is from 1 to 60 seconds.

Command Default

Port -Globally configured value ("ldap-server port <>"), in absence of which a value of 389. Timeout- Globally configured value ("ldap-server timeout <>"), in absence of which a value of 5 seconds.

idle-time- Default is 0.

testrootDN-Default value dc=test, dc=com.

username- default value is test.

Password- For test commands default value is test.

Command Modes

Configuration submode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.
NX-OS 6.2(29)	LDAP over Secure Sockets Layer (SSL) supports SSL version 3 and Transport Layer Security (TLS) versions 1.0 and 1.2 on Cisco MDS NX-OS Release 6.2(29) and later.
NX-OS 8.1(1)	LDAP over Secure Sockets Layer (SSL) supports SSL version 3 and Transport Layer Security (TLS) versions 1.0 and 1.2 on Cisco MDS NX-OS Release 8.1(1) and later.

Usage Guidelines

None.

Examples

The following example shows how to Specify the test keyword turns on automated testing for the feature:

```
switch(config)# ldap-server host 10.64.66.140 test rootDN cn=Manager,dc=acme,dc=com user
test password secret idle-time 1
```

The following example shows how to enable TLS while connecting to the server:

```
switch(config)# ldap-server host 10.64.66.140 enable-ssl
switch(config)#
```

The following example shows how to configure LDAP server port:

```
switch(config)# ldap-server host 10.64.66.140 root DN cn=Manager, dc=acme, dc=com password
 secret port 389
switch(config)#
```

Related Commands

Command	Description
show ldap-server groups	Displays the configured LDAP server groups.

ldap-server timeout

To configure global timeout period in seconds, use the ldap-server timeout command in configuration mode. To disable this feature, use the no form of the command.

ldap-server timeout *timeout in second*
no ldap-server timeout*timeout in second*

Syntax Description

timeout in seconds	Specifies timeout value in seconds. The default timeout value is 5 seconds and valid range is from 1 to 60 seconds. This value will be used only for those servers for which timeout is not configured at a per-server level.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure global LDAP server timeout in seconds:

```
switch(config)# no ldap-server timeout 1
switch(config)#
```

Related Commands

Command	Description
show ldap-server groups	Displays the configured LDAP server groups.

lifetime seconds

To configure the security association (SA) lifetime duration for an IKE protocol policy, use the **lifetime seconds** command in IKE policy configuration submode. To revert to the default, use the **no** form of the command.

lifetime seconds *seconds*
no lifetime seconds *seconds*

Syntax Description

seconds	Specifies the lifetime duration in seconds. The range is 600 to 86400.

Command Default

86,400 seconds.

Command Modes

IKE policy configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

The **lifetime seconds** command overrides the default.

Examples

The following example shows how to configure the SA lifetime duration for the IKE protocol:

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# policy 1
switch(config-ike-ipsec-policy)# lifetime seconds 6000
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
policy	Configures IKE protocol policy.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

line com1

To configure auxiliary COM 1 port, use the **line com1** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

linecom1->databits*number* | **flowcontrolhardware** | **modem** {**in** | **init-string** {**default** | **user-input**} | **set-stringuser-input***string*} | **parity** {**even** | **none** | **odd**} | **speed***speed* | **stopbits** {**1** | **2**}
nolinecom1->databitsnumber | **flowcontrolhardware** | **modem** {**in** | **init-string** | **set-stringuser-input**} | **parity** {**even** | **none** | **odd**} | **speedspeed** | **stopbits** {**1** | **2**}

Syntax Description

databits *number*	Specifies the number of databits per character. The range is 5 to 8.
flowcontrol hardware	Enables modem flow on the COM1 port control.
modem	Enables the modem mode.
in	Enables the COM 1 port to only connect to a modem.
init-string default	Writes the default initialization string to the modem.
set-string user-input *string*	Sets the user-specified initilization string to its corresponding profile. Maximum length is 80 characters.
init-string user-default	Writes the provided initialization string to the modem.
parity	Sets terminal parity.
even	Sets even parity.
none	Sets no parity.
odd	Sets odd parity.
speed *speed*	Sets the transmit and receive speeds. The range is 110 to 115, 200 baud.
stopbits	Sets async line stopbits.
1	Sets one stop bit.
2	Sets two stop bits.

Command Default

9600 Baud

8 databits

1 stopbit

Parity none

Default init string

Command Modes

Configuration mode.

Command History

Release	Modification
1.2(2)	This command was introduced.
3.0(1)	Added an example to show the user-input initialization string for the Supervisor-2 module.

Usage Guidelines

The **line com1** command available in config t command mode. The **line com1** configuration commands are available in **config-com1** submode.

You can perform the configuration specified in this section only if you are connected to the console port or the COM1 port.

We recommend you use the default initialization string. If the required options are not provided in the user-input string, the initialization string is not processed.

You must first set the user-input string before initializing the string.

Examples

The following example configures a line console and sets the options for that terminal line:

```
switch## config terminal
switch(config)#
switch(config)# line com1
switch(config-com1)# databits 6
switch(config-com1)# parity even
switch(config-com1)# stopbits 1
```

The following example disables the current modem from executing its functions:

```
switch# config terminal
switch(config)# line com1
switch(config-com1)# no modem in
```

The following example enables (default) the COM1 port to only connect to a modem:

```
switch# config terminal
switch(config)# line com1
switch(config-com1)# modem in
```

The following example writes the initialization string to the modem. This is the default.

```
switch# config terminal
switch(config)# line com1
switch(config-com1)# modem init-string default
```

The following example assigns the user-specified initialization string for a Supervisor-1 module to its corresponding profile:

```
switch# config terminal
switch(config)# line com1
switch(config-com1)# modem set-string user-input ATE0Q1&D2&C1S0=3\015
```

The following example assigns the user-specified initialization string for a Supervisor-2 module to its corresponding profile:

```
switch# config terminal
```

```
switch(config)# line com1
switch(config-com1)# modem set-string user-input ATE0Q0V1&D0&C0S0=1
```

The following example deletes the configured initialization string:

```
switch# config terminal
switch(config)# line com1
switch(config-com1)# no modem set-string user-input ATE0Q1&D2&C1S0=3\015
```

The following example writes the user-specified initialization string to the modem:

```
switch# config terminal
switch(config)# line com1
switch(config-com1)# modem init-string user-input
```

Related Commands

Command	Description
line console	Configures primary terminal line.
line vty	Configures virtual terminal line.
show line com1	Displays COM1 information.

line console

To configure a terminal line, use the **line console** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

lineconsole->databits*number* | **exec-timeout***minutes* | **modem** {**in** | **init-string** | **set-stringuser-inputstring**} | **parity** {**even** | **none** | **odd**} | **speed***speed* | **stopbits** {**1** | **2**}
nolineconsoledatabits *number* | **exec-timeout***minutes* | **modem** {**in** | **init-string** {**default** | **user-input**} | **set-stringuser-input***string*} | **parity** {**even** | **none** | **odd**} | **speed***speed* | **stopbits** {**1** | **2**}

Syntax Description

databits *number*	Specifies the number of databits per character. The range is 5 to 8.
exec-timeout *minutes*	Configures exec timeout in minutes. The range is 0 to 525,600. To disable, set to 0 minutes.
modem	Enables the modem mode.
in	Enables the COM 1 port to only connect to a modem.
init-string default	Writes the default initialization string to the modem.
init-string user-input	Writes the provided initialization string to the modem.
set-string user-input *string*	Sets the user-specified initilization string to its corresponding profile. Maximum length is 80 characters.
parity	Sets terminal parity.
even	Sets even parity.
none	Sets no parity.
odd	Sets odd parity.
speed *speed*	Sets the transmit and receive speeds. Valid values for Supervisor-1 modules are between 110 and 115,200 bps (110, 150, 300, 600, 1200, 2400, 4800, 9600, 19200, 28800, 38400, 57600, 115200). Valid values for Supervisor-2 modules are 9600, 19200, 38400, and 115200.
stopbits	Sets async line stopbits.
1	Sets one stop bit.
2	Sets two stop bits.

Command Default

9600 Baud.

8 databits.

1 stopbit.

Parity none.

Default init string.

Command Modes

Configuration mode.

Command History

Release	Modification
1.2(2)	This command was introduced.
3.0(1)	Modified the **speed** option by specifying speeds for the Supervisor-1 module and Supervisor-2 module.

Usage Guidelines

The **line console** command available in config t command mode. The **line console** configuration commands are available in config-console submode.

When setting the **speed** option, be sure to specify one of the exact values.

Examples

The following example configures a line console and sets the options for that terminal line:

```
switch## config terminal
switch(config)##
switch(config)# line console
switch(config-console)# databits 60
switch(config-console)# exec-timeout 60
switch(config-console)#

flowcontrol software
switch(config-console)# parity even
switch(config-console)# stopbits 1
```

The following example disables the current modem from executing its functions:

```
switch# config terminal
switch(config)# line console
switch(config-console)# no modem in
```

The following example enables (default) the COM1 port to only connect to a modem:

```
switch# config terminal
switch(config)# line console
switch(config-console)# modem in
```

The following example writes the initialization string to the modem. This is the default.

```
switch# config terminal
switch(config)# line console
switch(config-console)# modem init-string default
```

The following example assigns the user-specified initialization string to its corresponding profile:

```
switch# config terminal
switch(config)# line console
switch(config-console)# modem set-string user-input ATE0Q1&D2&C1S0=3\015
```

The following example deletes the configured initialization string:

```
switch# config terminal
```

```
switch(config)# line console
switch(config-console)# no modem set-string user-input ATE0Q1&D2&C1S0=3\015
```

The following example writes the user-specified initialization string to the modem:

```
switch# config terminal
switch(config)# line console
switch(config-console)# modem init-string user-input
```

Related Commands

Command	Description
line com1	Configures the auxiliary COM 1 port
line vty	Configures virtual terminal line.
show line console	Displays console information.

line vty

To configure a virtual terminal line, use the **line vty** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

linevty->exec-timeout*minutes* | **session-limit***number*
nolinevtyexec-timeout | **session-limit***number*

Syntax Description

exec-timeout *minutes*	Configures timeout in minutes. The range is 0 to 525600. To disable, set to 0 minutes.
session-limit *number*	Configures the number of VSH sessions. The range is 1 to 64.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The **line vty** command is available in config t command mode. The **line vty** configuration commands are available in config-line submode.

Examples

The following example configures a virtual terminal line and sets the timeout for that line:

```
switch## config terminal
switch(config)# line vty
switch(config-line)# exec-timeout 60
```

Related Commands

Command	Description
line com1	Configures the auxiliary COM 1 port.
line console	Configures primary terminal line.

link-state-trap (SME)

To enable an Simple Network Management Protocol (SNMP) link state trap on an interface, use the link-state-trap command. To disable this feature, use the no form of the command.

link-state-trap
no link-state-trap

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable the link-state-trap on the Fibre Channel interface:

```
switch# config t
switch(config)# interface fc 1/1
switch(config-if)# link-state-trap
switch(config-if)#
```

The following example shows how to disable the link-state-trap on the Fibre Channel interface:

```
switch# config t
switch(config)# interface fc 1/1
switch(config-if)# no link-state-trap
switch(config-if)#
```

Related Commands

Command	Description
show interface	Displays interface information.

load-balancing

To enable cluster reload balancing for all targets or specific targets, use the load-balancing command. To disable this command, use the no form of the command.

load-balancing {**enable** | *target wwn* }
no load-balancing {**enable** | *target wwn* }

Syntax Description

enable	Enables cluster load balancing.
target *wwn*	Specifies the world-wide name (WWN) of the target port.

Command Default

None.

Command Modes

Cisco SME cluster configuration submode.

Command History

Release	Modification
3.3(1a)	This command was introduced.

Usage Guidelines

The reload balancing operation is performed by the Cisco SME administrator for all or specific target ports. This operation first unbinds all the targets from the Cisco SME interfaces. The targets are then associated, one at a time, based on the load-balancing algorithm.

The reload balancing operation can be triggered if the targets remain unconnected due to errors in the prior load balancing opertions in the backend.

Examples

The following example enables reload balancing in Cisco SME:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# load-balancing enable
switch(config-sme-cl-node)#
```

The following example adds the host to the Cisco SME interface based on the load-balancing policy:

```
switch# config t
switch(config))# sme cluster c1
switch(config-sme-cl)# load-balancing 17:11:34:44:44:12:14:10
switch(config-sme-cl-node)#
```

Related Commands

Command	Description
show sme cluster	Displays Cisco SME information.

load-balancing (Cisco IOA cluster Configuration submode)

To enable cluster reload balancing of all flows in an IOA cluster, use the load-balancing command.

load-balancing {**enable** | *target wwn* }
no load-balancing {**enable** | *target wwn* }

Syntax Description

enables	Enables cluster load balancing.
target *pwwn*	Specifies the world-wide name (WWN) of the target port.

Command Default

None.

Command Modes

Cisco IOA cluster Configuration submode.

Command History

Release	Modification
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable cluster reload balancing of all targets:

```
rtp-sw1(config)# ioa cluster tape_vault
rtp-sw1(config-ioa-cl)# load-balancing enable
switch#(config-ioa-cl)# load-balancing10:00:00:00:00:00:00:00
This command will first disable all the IT nexuses (only for a target if specifi
ed) and then enable them back. This process is disruptive. Also, in case you abo
rt the request in the middle, you can enable load balancing back by executing th
e command 'load-balancing enable'.
Do you wish to continue? (yes/no) [no] y
Cluster config fails: This switch is not the master switch, configuration change
 not allowed. (0x420f003c)
switch#(config-ioa-cl)#
```

Related Commands

Command	Description
interface ioa	Configures the IOA interface.

locator-led

To blink an LED on the system, use the **locator-led** command. To restore the default LED state, use the no form of this command.

locator-led {**chassis** | **fan** *f-number* | **module** *slot* | **powersupply** *ps-number* | **xbar** *x-number*}
no locator-led {**chassis** | **fan** *f-number* | **module** *slot* | **powersupply** *ps-number* | **xbar** *x-number*}

Syntax Description

chassis	Blinks the chassis LED.
fan *f-number*	Blinks the LED that represents the configured fan number. The range depends on the platform. Use **?** to see the range.
module *slot*	Blinks the module LED. The range depends on the platform. Use **?** to see the range.
powersupply *ps-number*	Blinks the power supply LED. The range depends on the platform. Use **?** to see the range.
xbar *x-number*	Blinks the xbar module LED. The range depends on the platform. Use **?** to see the range.

Command Default

The locator LED is off.

Command Modes

Any command mode

network-admin network-operator vdc-admin vdc-operator

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

Use the **locator-led** command to flash the LED on a component in the system. You can use this blinking LED to identify the component to an administrator in the data center.

This command is available only in modular Cisco MDS switches.

Examples

This example shows how to blink the LED for module 4:

switch# **locator-led module 4**

Related Commands

Command	Description
show locator-led status	Displays the status of locator LEDs on the system.

logging abort

To discard the logging Cisco Fabric Services (CFS) distribution session in progress, use the **logging abort** command **in configuration mode.**

logging abort

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to discard logging CFS distribution session in progress:

```
switch# config terminal
switch(config)# logging abort
```

Related Commands

Command	Description
show logging	Displays logging information.

logging commit

To apply the pending configuration pertaining to the logging Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **logging commit** command **in configuration mode.**

logging commit

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to distribute the current logging configuration on this switch to all participating switches in the fabric:

```
switch# config terminal
switch(config)# logging commit
```

Related Commands

Command	Description
logging server	Sends system messages to a remote logging server.
show logging	Displays logging information.

logging console

To set console logging, use the **logging console** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

logging console [*severity-level*]
no logging console [*severity-level*]

Syntax Description

severity-level	(Optional) Specifies the maximum severity of messages logged. The range is 0 to 7, where 0 is emergency, 1 is alert, 2 is critical, 3 is error, 4 is warning, 5 is notify, 6 is informational, and 7 is debugging.

Command Default

Disabled.

The default severity level is 2.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The switch logs messages at or above the configured severity level.

Examples

The following example reverts console logging to the factory set default severity level of 2 (critical). Logging messages with a severity level of 2 or above will be displayed on the console.

```
switch# config terminal
switch(config)# logging console 2
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging distribute

To enable distribution of the logging configuration to other switches in the fabric via Cisco Fabric Services (CFS), use the **logging distribute** command. To disable this feature, use the **no** form of the command.

logging distribute
no logging distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This option must be enabled on all switches in the fabric for them to participate in fabric-wide updates of the logging configuration.

Examples

The following example shows how to enable distribution of the logging configuration on the local switch:

```
switch# configure terminal
switch(config)# logging distribute
```

Related Commands

Command	Description
logging commit	Commits the logging configuration to other switches in the fabric.
logging server	Configures details of a remote logging server.
show cfs	Displays the information of switches in the fabric that have CFS enabled.
show logging	Displays logging information.

logging level

To modify message logging facilities, use the **logging level** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

logging level *facility-name severity-level*
no logging level *facility-name severity-level*

Syntax Description

facility-name	Specifies the required facility name (for example **acl**, or **ivr**, or **port**, etc.)
severity-level	Specifies the maximum severity of messages logged. The range is 0 to 7, where 0 is emergency, 1 is alert, 2 is critical, 3 is error, 4 is warning, 5 is notify, 6 is informational, and 7 is debugging.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The switch logs messages at or above the configured severity level.

Examples

Configures Telnet or SSH logging for the kernel facility at level 4 (warning). As a result, logging messages with a severity level of 4 or above will be displayed:

```
switch# config terminal
switch(config)# logging level kernel 4
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging level pmon

To configure logging level for port monitor syslog messages, use the **logging level pmon** command. To remove this configuration, use the **no** form of this command.

logging level pmon *severity-level*
no logging level pmon

Syntax Description

severity-level	Specifies the severity of messages logged. The range is 0–7, where 0 is emergency, 1 is alert, 2 is critical, 3 is error, 4 is warning, 5 is notify, 6 is informational, and 7 is debugging.

Command Default

The default severity level is warning (4).

Command Modes

Configuration mode (config)

Command History

Release	Modification
8.4(1)	Added support for configuring severity level for port monitor.
1.3(1)	This command was introduced.

Usage Guidelines

Use the **show logging level pmon** command to verify the configured port monitor severity level.

Examples

The following example displays how to configure logging for port monitor at level 3 (error). As a result, logging messages with a severity level of 2–3 will be displayed:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# logging level pmon 3
```

The following example displays the syslog message when the severity level configured for port monitor is error (3):

```
PMON-SLOT1-3-RISING_THRESHOLD_REACHED: Invalid Words has reached the rising threshold
(port=fc1/1 [chars], value=90).
PMON-SLOT1-3-FALLING_THRESHOLD_REACHED: Invalid Words has reached the falling threshold
(port=fc1/1 [chars], value=0).
```

The following example displays the syslog message when the severity level configured for port monitor is warning (4):

```
PMON-SLOT1-4-WARNING_THRESHOLD_REACHED_UPWARD: Invalid Words has reached warning threshold
 in the upward direction (port fc1/1 [chars], value = 90).
PMON-SLOT1-3-RISING_THRESHOLD_REACHED: Invalid Words has reached the rising threshold
(port=fc1/1 [chars], value=90).
PMON-SLOT1-4-WARNING_THRESHOLD_REACHED_DOWNWARD: Invalid Words has reached warning threshold
 in the downward direction (port fc1/1 [chars], value = 0).
PMON-SLOT1-3-FALLING_THRESHOLD_REACHED: Invalid Words has reached the falling threshold
```

```
(port=fc1/1 [chars], value=0).
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging level port

To configure logging level for port syslog messages, use the **logging level port** command. To remove this configuration, use the **no** form of this command.

logging level port {*severity-level* | **link-failure** | {**critical** | **notif**}}

no logging level port {*severity-level* | **link-failure** | {**critical** | **notif**}}

Syntax Description

severity-level	Specifies the severity of messages logged. The range is from 0 to 7, where 0 is emergency, 1 is alert, 2 is critical, 3 is error, 4 is warning, 5 is notify, 6 is informational, and 7 is debugging.
link-failure	Specifies logging level for port link failure syslog messages.
critical	Specifies that when an active link fails, the message that is issued is a critical level (2) message: %PORT-2-IF_DOWN_LINK_FAILURE_CRIT.
notif	Specifies that when an active link fails, the message that is issued is a notification level (5) message: %PORT-5-IF_DOWN_LINK_FAILURE.

Command Default

The default severity is the notification level (5).

Command Modes

Configuration mode (config)

Command History

Release	Modification
1.3(1)	This command was introduced.

Examples

The following example displays how to configure Telnet or SSH logging for port at level 4 (warning). As a result, logging messages with a severity level of 4 or above will be displayed:

```
switch# configure
switch(config)# logging level port 4
```

The following example displays how to configure Telnet or SSH logging for critical port link failure messages. As a result, logging messages that are critical will be displayed:

```
switch# configure
switch(config)# logging level port link-failure critical
```

The following example displays the syslog message when a critical port link failure is configured:

```
PORT-2-IF_DOWN_LINK_FAILURE_CRIT: Interface [chars] is down (Link failure)
```

The following example displays the syslog message when a notification port link failure is configured:

```
PORT-5-IF_DOWN_LINK_FAILURE: Interface [chars] is down (Link failure [chars]) [chars] [chars]
```

Command	Description
show logging	Displays logging configuration information.

logging logfile

To set message logging for logfile, use the **logging logfile** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

logging logfile *filename severity-level* [**size** *filesize*]
no logging logfile *filename severity-level* [**size** *filesize*]

Syntax Description

filename	Specifies the log filename. Maximum length is 80 characters.
severity-level	Specifies the maximum severity of messages logged. The range is 0 to 7, where 0 is emergency, 1 is alert, 2 is critical, 3 is error, 4 is warning, 5 is notify, 6 is informational, and 7 is debugging.
size *filesize*	(Optional) Specifies the log file size. The range is 4096 to 4194304 bytes.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The switch logs messages at or above the configured severity level.

Examples

The following example configures logging information for errors or events above a severity level of 3 (errors) to be logged in a file named ManagerLogFile. By configuring this limit, the file size is restricted to 3,000,000 bytes:

```
switch# config terminal
switch(config)# logging logfile
ManagerLogFile 3 size 3000000
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging module

To set message logging for linecards, use the **logging module** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

logging module [[*severity-level*] | [**kernel** [*severity-level*]]]
no logging module [[*severity-level*] | [**kernel** [*severity-level*]]]

Syntax Description

severity-level	(Optional) Specifies the maximum severity of messages logged. The range is 0 to 7, where 0 is emergency, 1 is alert, 2 is critical, 3 is error, 4 is warning, 5 is notify, 6 is informational, and 7 is debugging.
kernel *severity-level*	(Optional) Logs the kernel system logs from the line cards into the Supervisor module.

Command Default

The command is disabled by default.

The logging module severity level is enabled at level 7

The logging module kernel severity level is enabled at level 2.

Command Modes

Configuration mode.

Command History

Release	Modification
9.4(3)	Added **kernel** *severity-level* keyword.
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example sets message logging for modules at level 7:

```
switch## config terminal
switch(config)# logging module 7
```

The following example logs the kernel system logs from the line cards into the Supervisor module.

```
switch(config)# logging module kernel
switch(config)# logging module kernel 1
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging monitor

To set monitor message logging, use the **logging monitor** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

logging monitor *severity level*

Syntax Description

logging monitor	Sets message logging.
severity level	Specifies the maximum severity of messages logged. The range is 0 to 7, where 0 is emergency, 1 is alert, 2 is critical, 3 is error, 4 is warning, 5 is notify, 6 is informational, and 7 is debugging.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example sets terminal line (monitor) message logging at level 2:

```
switch## config terminal
switch(config)# logging monitor 2
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging origin-id

To specify the hostname, IP address, or a text string in the system messages that are sent to remote syslog servers, use the **logging origin-id** command. To remove this configuration, use the **no** form of this command.

logging origin-id { **hostname** | **ip** *address* | **string** *word* } [**rfc-order**]

no logging origin-id { **hostname** | **ip** *address* | **string** *word* } [**rfc-order**]

Syntax Description

hostname	Specifies to use the switch name as the origin ID in system messages.
ip *address*	Specifies to use the specified IP address *address* as the origin ID in system messages.
string *word*	Specifies to use the single word *word* as the origin ID in system messages. No spaces or quoting is allowed. **word** is truncated to 200 characters in messages.

Command Default

This feature is disabled by default.

Command Modes

Configuration mode (config#)

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The **hostname** option has no arguments as it uses the name configured by the **switchname** configured command.

By default, header fields in remote logging messages are sent in the Cisco specific order of 'origin ID-timestamp-message'. If a remote syslog server does not accept this ordering use the **rfc-order** option to send message header fields ordering in the syslog RFC order of 'timestamp-origin ID-message'.

If the **system timestamp format** command is enabled it overrides the **rfc-order** option to make remote system logging messages RFC 5424 compliant. This is a standard format and allows messages from multiple platforms and vendors to be more easily managed together on remote servers.

Examples

The following example displays how to specify to add the host name to the system messages that are sent to the remote syslog servers:

```
switch# configure
switch(config)# logging origin-id hostname
```

The following example displays how to specify to add the IP address of the switch that is sending the system messages to the remote syslog servers:

```
switch# configure
switch(config)# logging origin-id ip 192.0.2.2
```

The following example displays how to specify to append a custom string to the system messages that are sent to the remote syslog servers:

```
switch# configure
switch(config)# logging origin-id word switch2
```

Command	Description
show logging	Displays logging configuration information.
switchname	Configure the switchname.
system timestamp format	Configures the system logging timestamp format.

logging server

To send system messages to a remote logging server, use the **logging server** command.

logging server *name* [*severity-level*] [**port** *number*] [**secure** [**trustpoint client-identity** *name*]] [**facility** *facility-name*]

Syntax Description

server *name*	Specifies the host name or IPv4/IPv6 address of the remote system logging server.
severity-level	(Optional) Specifies the minimum severity of messages logged. The range is 0 to 7, where 0 is emergency, 1 is alert, 2 is critical, 3 is error, 4 is warning, 5 is notify, 6 is informational, and 7 is debugging.
port *number*	(Optional) Specifies the port number. Range is from 1 - 65535. The default port number for unsecure connections is UDP 514 and for secure connections is TCP 6514.
secure	(Optional) Sets the transport to TCP, the destination port to the default secure port, and enables TLS and mutual authentication of switch and destination server using identity certificates signed by a trusted CA.
trustpoint client-identity *name*	(Optional) Specifies to use identity certificates from the specified trust point. When this option is not specified certificates from all trust points are tried until authentication succeeds. *name* is the name of a trust point configured on the switch.

facility *facility-name*	(Optional) Specifies the facility to tag the message with. The options are: • **auth** • **authpriv** • **cron** • **daemon** • **ftp** • **kernel** • **local0** • **local1** • **local2** • **local3** • **local4** • **local5** • **local6** • **local7** • **lpr** • **mail** • **news** • **syslog** • **user** • **uucp**

Command Default

The default unsecure port is UDP 514. The default secure port is TCP 6514 with TLS.

Command Modes

Configuration mode.

Command History

Release	Modification
9.2(1)	Added the **secure** and **trustpoint client-identity** *name* options.
1.0(2)	This command was introduced.

Usage Guidelines

Remote logging destinations may be specified by a name, IPv4 or IPv6 address. If using a name as the destination address then ensure that it exists as a local **ip host** configuration or is a valid DNS name and DNS lookup is enabled.

The maximum configurable remote logging destinations is 3.

If the connection to a secure remote logging destination is lost, then the switch will not attempt to reconnect until the next system message to that destination must be sent.

If the **secure** option is specified and no identity certificates are installed, then connection to the specified remote destination will not be established.

Examples

The following example displays how to enable message logging to the specified remote server for severity 7 and higher (up to severity 0) messages:

```
switch## config terminal
switch(config)# logging server sanjose 7
```

The following example displays how to configure a secure, encrypted connection to a remote syslog server using TCP destination port 55551 and only identity certificates installed in the trust point called *tp1*:

```
switch## config terminal
switch(config)# logging server 192.168.0.1 port 55551 secure trustpoint client-identity tp1
```

Related Commands

Command	Description
crypto ca trustpoint	Installs identity certificates from a trusted Certificate Authority.
ip host	Configures a name to IP address mapping.
show hosts	Displays local name to IP address mappings.
show logging	Displays system message logging configuration information.
system timestamp format	Configures the timestamp format of logs.

logging timestamp

To set the time increment for the message logging time stamp, use the **logging timestamp** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

logging timestamp {**microseconds** | **milliseconds** | **seconds**}
no logging timestamp {**microseconds** | **milliseconds** | **seconds**}

Syntax Description

microseconds	Sets the logging time stamp to microseconds.
milliseconds	Sets the logging time stamp to milliseconds.
seconds	Sets the logging time stamp to seconds.

Command Default

Seconds.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example sets the logging time stamp to milliseconds:

```
switch## config terminal
switch(config)# logging timestamp milliseconds
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging timezone utc

To set the timezone for syslog message to UTC, use the **logging timezone utc** command. To disable the feature, use the **no** form of the command.

logging timezone utc
no logging timezone utc

Syntax Description

timezone utc	Specifies the timezone in syslog messages to be UTC.

Command Default

Messages are stamped with the switch clock timezone.

Command Modes

Configuration mode.

Command History

Release	Modification
9.4(4)	This command was introduced.

Usage Guidelines

logging timezone utc only sets the timezone in timestamps of logging messages. It does not affect the switch clock timezone or other features such as the accounting log or debug logs.

UTC stamped syslog messages are useful when aggregating syslogs from multiple devices and timezones for event correlation and diagnosis.

Examples

The following example sets the timezone as UTC for system logs:

```
switch(config)# logging timezone utc
```

Related Commands

Command	Description
show logging	Displays logging information, including the `logging timezone utc` configuration.
show logging timezone	Displays the timezone used in syslog message timestamps

logging format rfc5424

To set system logging message format to comply with RFC 5424, use the **logging format rfc5424** command. To disable the feature, use the **no** form of the command.

logging format rfc5424
no logging format rfc5424

Syntax Description

format rfc5424	Enables system logging with all fields compliant to RFC 5424.

Command Default

Messages are logged locally and sent to remote servers with BSD (RFC 3164) format.

Command Modes

Configuration mode.

Command History

Release	Modification
9.4(4)	This command was introduced.

Usage Guidelines

logging format rfc5424 is only applicable to system logs.

Examples

The following example enables logging system logs with RFC5424 format:

```
switch(config)# logging format rfc5424
```

Related Commands

Command	Description
show logging	Displays logging configuration information including logging format rfc5424 configuration.
show logging format	Displays logging format used for syslog message.
system timestamp format rf5424	Configures system wide ISO style timestamps.

logical-type

To configure a logical-type policy, use the **logical-type** command. To disable a logical-type policy, use the **no** form of this command.

logical-type {**all** | **core** | **edge**}
no logical-type {**all** | **core** | **edge**}

Syntax Description

all	Specifies both core ports and edge ports. This is the default value.
core	Specifies the port's logical type as core or E.
edge	Specifies the port's logical type as edge or F.

Command Default

Specifies both core ports and edge ports.

Command Modes

Port monitor configuration (config-port-monitor)

Command History

Release	Modification
8.1(1)	This command was introduced.

Usage Guidelines

- From Cisco MDS NX-OS Release 8.1(x), the **port-type** {**access-port** | **trunks** | **all**} command is replaced with the **logical-type** {**core** | **edge** | **all**} command, and **port-type** is replaced with **logical-type**, **access-port** is replaced with **edge**, and **trunks** is replaced with **core**.
- The default policy uses its own internal logical type, which is the same for all ports.

Examples

The following example shows how to configure port monitoring for a core port:

```
switch# configure terminal
switch(config)# port-monitor name cisco
switch(config-port-monitor)# logical-type core
```

Related Commands

Command	Description
show interface	Displays the status of an interface.
show port-monitor	Displays all port-monitor policies.
switchport logical-type	Configures a logical type for a port in an interface and a port in a port channel.