L Commands

This chapter describes the Cisco Nexus 1010 commands that begin with the letter L.

line console

To enter console configuration mode, use the **line console** command. To exit console configuration mode, use the **no** form of this command.

line console

no line console

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Global configuration (config)

SupportedUserRoles network-admin

Command History

Release	Modification
4.0(4)SP1(1)	This command was introduced.

Examples This example shows how to enter console configuration mode:

```
switch# configure terminal
switch(config)# line console
switch(config-console)#
```

line vty

To enter line configuration mode, use the **line vty** command. To exit line configuration mode, use the **no** form of this command.

line vty

no line vty

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SP1(1)	This command was introduced.

Examples

This example shows how to enter line configuration mode:

```
switch# configure terminal
switch(config)# line vty
switch(config-line)#
```

Related Commands

Command	Description
exit	Exits a configuration mode.
line console	Enters console configuration mode.

logging console

To enable logging messages to the console session, use the **logging console** command. To disable logging messages to the console session, use the **no** form of this command.

logging console [*severity-level*]

no logging console

Syntax Description

severity-level — Severity level at which you want messages to be logged. When you set a severity level, such as 4, then messages at that severity level and higher (0 through 4) are logged.

Severity levels are as follows:

Level	Designation	Definition
0	Emergency	System unusable
1	Alert	Immediate action needed
2	Critical	Critical condition—default level
3	Error	Error condition
4	Warning	Warning condition
5	Notification	Normal but significant condition
6	Informational	Informational message only
7	Debugging	Condition that appears during debugging only

Note Level 0 is the highest severity level.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SP1(1)	This command was introduced.

Examples

This example shows how to enable logging messages with a severity level of 4 (warning) or higher to the console session:

```
switch# configure terminal
```

```
switch(config)# logging console 4
switch(config)#
```

Related Commands

Command	Description
show logging logfile	Displays the contents of the log file.
logging event	Logs interface events.
logging level	Enables the logging of messages from named facilities and for specified severity levels.
logging logfile	Configures the log file used to store system messages.
logging module	Starts logging of module messages to the log file.
logging server	Designate and configure a remote server for logging system messages.
logging timestamp	Set the unit of measure for the system messages timestamp.

logging event

To log interface events, use the **logging event** command. To disable logging of events, use the **no** version of this command.

logging event {link-status | trunk-status} {enable | default}

no logging event {link-status | trunk-status} {enable | default}

Syntax Description

link-status	Logs all up/down and change status messages.
trunk-status	Logs all trunk status messages.
default	Specifies that the default logging configuration is used.
enable	Enables interface logging to override the port level logging configuration.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SP1(1)	This command was introduced.

Examples

This example shows how to log interface events:

```
switch# configure terminal
switch(config)# logging event link-status default
switch(config)#
```

Related Commands

Command	Description
show logging logfile	Displays the contents of the log file.
logging console	Enables logging messages to the console session.
logging level	Enables the logging of messages from named facilities and for specified severity levels.
logging logfile	Configures the log file used to store system messages.
logging module	Starts logging of module messages to the log file.
logging server	Designate and configure a remote server for logging system messages.
logging timestamp	Set the unit of measure for the system messages timestamp.

logging level

To enable the logging of messages from a named facility and for specified severity levels, use the **logging level** command. To disable the logging of messages, use the **no** form of this command.

logging level *facility severity-level*

no logging level *facility severity-level*

Syntax Description

facility	Facility name.
severity-level	Severity level at which you want messages to be logged. When you set a severity level, for example 4, then messages at that severity level and higher (0 through 4) are logged. Severity levels are as follows:

Level	Designation	Definition
0	Emergency	System unusable
1	Alert	Immediate action needed
2	Critical	Critical condition—default level
3	Error	Error condition
4	Warning	Warning condition
5	Notification	Normal but significant condition
6	Informational	Informational message only
7	Debugging	Condition that appears during debugging only

Note Level 0 is the highest severity level.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SP1(1)	This command was introduced.

Usage Guidelines

To apply the same severity level to all facilities, use the following command:

- **logging level all** *level_number*

To list the available facilities for which messages can be logged, use the following command:

- **logging level ?**

Examples

This example shows how to enable logging messages from the AAA facility that have a severity level of 0 through 2:

```
switch# configure terminal
switch(config)# logging level aaa 2
switch(config)#
```

This example shows how to enable logging messages from the license facility with a severity level of 0 through 4 and then display the license logging configuration:

```
switch# configure terminal
switch(config)# logging level license 4
switch(config)# show logging level license
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
licmgr                  6                       4

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)

switch(config)#
```

Related Commands

Command	Description
show logging logfile	Displays the contents of the log file.
logging console	Enables logging messages to the console session.
logging event	Logs interface events.
logging logfile	Configures the log file used to store system messages.
logging module	Starts logging of module messages to the log file.
logging server	Designate and configure a remote server for logging system messages.
logging timestamp	Set the unit of measure for the system messages timestamp.

logging logfile

To configure the log file used to store system messages, use the **logging logfile** command. To remove a configuration, use the **no** form of this command.

logging logfile *logfile-name severity-level* **[size** *bytes***]**

no logging logfile [*logfile-name severity-level* **[size** *bytes***]]]**

Syntax Description

logfile-name	Name of the log file that stores system messages.
severity-level	Severity level at which you want messages to be logged. When you set a severity level, for example 4, then messages at that severity level and higher (0 through 4) are logged. Severity levels are as follows:

Level	Designation	Definition
0	Emergency	System unusable
1	Alert	Immediate action needed
2	Critical	Critical condition—default level
3	Error	Error condition
4	Warning	Warning condition
5	Notification	Normal but significant condition
6	Informational	Informational message only
7	Debugging	Condition that appears during debugging only

size *bytes*	(Optional) Specifies the log file size in bytes, from 4096 to 10485760 bytes. The default file size is 10485760 bytes.

Note Level 0 is the highest severity level.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SP1(1)	This command was introduced.

Examples

This example shows how to configure a log file named LogFile to store system messages and set its severity level to 4:

```
switch# config t
switch(config)# logging logfile LogFile 4
switch(config)#
```

Related Commands

Command	Description
show logging logfile	Displays the contents of the log file.
logging console	Enables logging messages to the console session.
logging event	Logs interface events.
logging level	Enables the logging of messages from named facilities and for specified severity levels.
logging module	Starts logging of module messages to the log file.
logging server	Designate and configure a remote server for logging system messages.
logging timestamp	Set the unit of measure for the system messages timestamp.

logging module

To start logging of module messages to the log file, use the **logging module** command. To stop module log messages, use the **no** form of this command.

logging module [*severity-level*]

no logging module [*severity-level*]

Syntax Description

severity-level — Severity level at which you want messages to be logged. If you do not specify a severity level, the default is used. When you set a severity level, for example 4, then messages at that severity level and higher (0 through 4) are logged.

Severity levels are as follows:

Level	Designation	Definition
0	Emergency	System unusable
1	Alert	Immediate action needed
2	Critical	Critical condition—default level
3	Error	Error condition
4	Warning	Warning condition
5	Notification	Normal but significant condition (the default)
6	Informational	Informational message only
7	Debugging	Condition that appears during debugging only

Note Level 0 is the highest severity level.

Defaults

Disabled

If you start logging of module messages, and do not specify a severity, then the default, Notification (5), is used.

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SP1(1)	This command was introduced.

Examples

This example shows how to start logging module messages to the log file at the default severity level (severity 4):

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

This example shows how to stop logging module messages to the log file:

```
switch# configure terminal
switch(config)# no logging module
switch#
```

Related Commands

Command	Description
show logging logfile	Displays the contents of the log file.
logging console	Enables logging messages to the console session.
logging event	Logs interface events.
logging level	Enables the logging of messages from named facilities and for specified severity levels.
logging logfile	Configures the log file used to store system messages.
logging server	Designate and configure a remote server for logging system messages.
logging timestamp	Set the unit of measure for the system messages timestamp.

logging server

To designate and configure a remote server for logging system messages, use the **logging server** command. Use the **no** form of this command to remove or change the configuration.

logging server *hostname* [*indicator* [**use-vrf** *name* [**facility** {**auth** | **authpriv** | **cron** | **daemon** | **ftp** | **kernel** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **syslog** | **user** | **uucp**}]]]

no logging server *hostname* [*indicator* [**use-vrf** *name* [**facility** {**auth** | **authpriv** | **cron** | **daemon** | **ftp** | **kernel** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **syslog** | **user** | **uucp**}]]]

Syntax Description

hostname	Hostname/IPv4/IPv6 address of the remote syslog server.
indicator	(Optional) One of the following indicators: 0–emerg, 1–alert, 2–crit, 3–err, 4–warn, 5–notif, 6–inform, 7–debug.
use-vrf *name*	(Optional) Specifies the VRF name. The default is management.
facility	(Optional) Specifies the facility to use when forwarding to the server.
auth	Specifies the auth facility.
authpriv	Specifies the authpriv facility.
cron	Specifies the Cron/at facility.
daemon	Specifies the daemon facility.
ftp	Specifies the file transfer system facility.
kernel	Specifies the kernel facility.
local0	Specifies the local0 facility.
local1	Specifies the local1 facility.
local2	Specifies the local2 facility.
local3	Specifies the local3 facility.
local4	Specifies the local4 facility.
local5	Specifies the local5 facility.
local6	Specifies the local6 facility.
local7	Specifies the local7 facility.
lpr	Specifies the lpr facility.
mail	Specifies the mail facility.
news	Specifies the USENET news facility.
syslog	Specifies the syslog facility.
user	Specifies the user facility.
uucp	Specifies the UNIX-to-UNIX copy system facility.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles network-admin

Command History

Release	Modification
4.0(4)SP1(1)	This command was introduced.

Examples

This example shows how to configure a remote syslog server at a specified IPv4 address using the default outgoing facility:

```
switch# configure terminal
switch(config)# logging server 172.28.254.253
switch(config)#
```

This example shows how to configure a remote syslog server at a specified host name with severity level 5 or higher:

```
switch# configure terminal
switch(config)# logging server syslogA 5
switch(config)#
```

Related Commands

Command	Description
show logging logfile	Displays the contents of the log file.
logging console	Enables logging messages to the console session.
logging event	Logs interface events.
logging level	Enables the logging of messages from named facilities and for specified severity levels.
logging logfile	Configures the log file used to store system messages.
logging module	Starts logging of module messages to the log file.
logging timestamp	Set the unit of measure for the system messages timestamp.

logging timestamp

To set the unit of measure for the system message time stamp, use the **logging timestamp** command. To restore the default unit of measure, use the **no** form of this command.

logging timestamp {**microseconds** | **milliseconds** | **seconds**}

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

Syntax Description

microseconds	Specifies the time stamp in microseconds.
milliseconds	Specifies the time stamp in milliseconds.
seconds	Specifies the time stamp in seconds (default).

Defaults

Seconds

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SP1(1)	This command was introduced.

Examples

This example shows how to set microseconds as the unit of measure for the system message time stamp:

```
switch# configure terminal
switch(config)# logging timestamp microseconds
switch(config)#
```

Related Commands

Command	Description
show logging logfile	Displays the contents of the log file.
logging console	Enables logging messages to the console session.
logging event	Logs interface events.
logging level	Enables the logging of messages from named facilities and for specified severity levels.
logging logfile	Configures the log file used to store system messages.
logging module	Starts logging of module messages to the log file.
logging server	Designate and configure a remote server for logging system messages.

login virtual-service-blade

To log in to a Virtual Service Blade (VSB), use the **login virtual-service-blade** command.

login virtual-service-blade *name* **[primary | secondary]**

Syntax Description

name	Name of an existing virtual service blade.
primary	(Optional) The Cisco Nexus 1010 that was assigned the primary role.
secondary	(Optional) The Cisco Nexus 1010 that was assigned the secondary role.

Defaults

None

Command Modes

EXEC

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1)SP1(2)	The optional **primary** and **secondary** keywords were added.
4.0(4)SP1(1)	This command was introduced.

Usage Guidelines

This command gives serial command access to a virtual service blade.

Examples

This example shows how to log into the Cisco Nexus 1000V CLI for the VSB named VSB-1 which is on the primary Cisco Nexus 1010.

```
switch# login virtual-service-blade VSB-1 primary
switch#
```

Related Commands

Command	Description
virtual-service-blade	Creates the named virtual service and places you into the configuration mode for that service.
show virtual-service-blade-type summary	Displays a summary of all virtual service configurations by the type name.
virtual-service-blade-type	Specifies the type and name of the software image file to add to this virtual service.
description	Adds a description to the virtual service.

Command	Description
show virtual-service-blade name	Displays information about a virtual service.
enable	Initiates the configuration of the virtual service and then enables it.
show virtual-service-blade	Displays information about the virtual service blades.