



L Commands

This chapter describes the Cisco Nexus 1000V commands that begin with the letter L.

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

limit-resource erspan-flow-id minimum

To configure the range of allowed ERSPAN flow IDs, use the **limit-resource erspan-flow-id minimum** command. To remove the configuration, use the **no** form of this command.

limit-resource erspan-flow-id minimum *min-val* **maximum** *max-val*

no limit-resource erspan-flow-id

Syntax Description	Parameter	Description
	<i>min-val</i>	Minimum ERSPAN flow ID number allowed.
	maximum	Configures the maximum range value for ERSPAN flow IDs.
	<i>max-val</i>	Maximum ERSPAN flow ID number allowed.

Defaults None

Command Modes Global configuration (config)

Supported User Roles network-admin

Command History	Release	Modification
	4.0(4)SV1(2)	This command was introduced.

Examples This example shows how to restrict the range of allowed ERSPAN flow IDs to the range, 1-80:

```
n1000v(config)# limit-resource erspan-flow-id minimum 1 maximum 80
```

This example shows how to restore the default range of ERSPAN flow IDs:

```
n1000v(config)# no limit-resource erspan-flow-id
```

Related Commands	Command	Description
	erspan-id	Adds an ERSPAN ID (1-1023) to the session configuration and saves it in the running configuration.
	show monitor session	Displays the ERSPAN session configuration as it exists in the running configuration.
	monitor session	Creates an ERSPAN session.

Send document comments to nexus1k-docfeedback@cisco.com.

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)SV1(1)	This command was introduced.

Examples This example shows how to enter console configuration mode:

```
n1000v# configure terminal
n1000v(config)# line console
n1000v(config-console)#
```

Send document comments to nexus1k-docfeedback@cisco.com.

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)SV1(1)	This command was introduced.

Examples This example shows how to enter line configuration mode:

```
n1000v# configure terminal
n1000v(config)# line vty
n1000v(config-line)#
```

Send document comments to nexus1k-docfeedback@cisco.com.

logging console

Use the **logging console** command to enable logging messages to the console session.

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 The 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 *the highest level*
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	Appears during debugging only

Defaults

None

Command Modes

Global configuration (config)

Supported User Roles

network-admin

Command History

Release	Modification
4.0(4)SV1(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:

```
n1000v# configure terminal
n1000v(config)# logging console 4
n1000v(config)#
```

Send document comments to nexus1k-docfeedback@cisco.com.

Related Commands

Command	Description
show logging console	Displays the console logging configuration.

Send document comments to nexus1k-docfeedback@cisco.com.

logging event

Use the **logging event** command to log interface events.

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

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

Syntax Description	link-status	Log all up/down and change status messages.
	trunk-status	Log all trunk status messages.
	default	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)SV1(1)	This command was introduced.

Examples This example shows how to log interface events:

```
n1000v# configure terminal
n1000v(config)# logging event link-status default
n1000v(config)#
```

Related Commands	Command	Description
	show logging	Displays the logging configuration and contents of logfile.

Send document comments to nexus1k-docfeedback@cisco.com.

logging level

Use the **logging level** command to enable the logging of messages as follows:

- from a named facility (such as license or aaa)
- of a specified severity level or higher

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

<i>facility</i>	Names the <i>facility</i> .
<i>severity-level</i>	The 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 *the highest level*
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	Appears during debugging only

Defaults

None

Command Modes

Global configuration (config)

Supported User Roles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Send document comments to nexus1k-docfeedback@cisco.com.

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:

```
n1000v# configure terminal
n1000v(config)# logging level aaa 2
n1000v(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:

```
n1000v# configure terminal
n1000v(config)# logging level license 4
n1000v(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)
```

n1000v(config)#

Related Commands

Command	Description
show logging level	Displays the facility logging level configuration.
logging level ?	Lists the available facilities for which messages can be logged.

Send document comments to nexus1k-docfeedback@cisco.com.

logging logfile

Use the **logging logfile** command to configure the log file used to store system messages.

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

<i>logfile-name</i>	Specifies the name of the log file that stores system messages.																											
<i>severity-level</i>	The 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:																											
	<table border="1"> <thead> <tr> <th>Level</th> <th>Designation</th> <th>Definition</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Emergency</td> <td>System unusable *the highest level*</td> </tr> <tr> <td>1</td> <td>Alert</td> <td>Immediate action needed</td> </tr> <tr> <td>2</td> <td>Critical</td> <td>Critical condition—default level</td> </tr> <tr> <td>3</td> <td>Error</td> <td>Error condition</td> </tr> <tr> <td>4</td> <td>Warning</td> <td>Warning condition</td> </tr> <tr> <td>5</td> <td>Notification</td> <td>Normal but significant condition</td> </tr> <tr> <td>6</td> <td>Informational</td> <td>Informational message only</td> </tr> <tr> <td>7</td> <td>Debugging</td> <td>Appears during debugging only</td> </tr> </tbody> </table>	Level	Designation	Definition	0	Emergency	System unusable *the highest level*	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	Appears during debugging only
Level	Designation	Definition																										
0	Emergency	System unusable *the highest level*																										
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	Appears during debugging only																										
<i>size bytes</i>	(Optional) Specifies the log file size in bytes, from 4096 to 10485760 bytes. The default file size is 10485760 bytes.																											

Defaults

None

Command Modes

Global configuration (config)

Supported User Roles

network-admin

Command History

Release	Modification
4.0(4)SV1(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:

```
n1000v# config t
n1000v(config)# logging logfile LogFile 4
```

Send document comments to nexus1k-docfeedback@cisco.com.

```
n1000v(config)#
```

Related Commands

Command	Description
show logging logfile	Displays the contents of the log file.

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

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 logging module** form of this command.

logging module [*severity*]

no logging module [*severity*]

Syntax Description

severity-level

The 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 *the highest level*
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	Appears during debugging only

Defaults

Disabled

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

Command Modes

Global configuration (config)

Supported User Roles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

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

```
n1000v# configure terminal
n1000v(config)# logging module
n1000v(config)#
```

Send document comments to nexus1k-docfeedback@cisco.com.

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

```
n1000v# configure terminal
n1000v(config)# no logging module
n1000v#
```

Related Commands

Command	Description
show logging module	Displays the current configuration for logging module messages to the log file.

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

logging monitor

Use the **logging monitor** command to enable the logging of messages to the monitor (terminal line). This configuration applies to telnet and Secure Shell (SSH) sessions.

To disable monitor logging, use the **no** form of this command.

logging monitor [*severity-level*]

no logging monitor

Syntax Description

severity-level

The 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 *the highest level*
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	Appears during debugging only

Defaults

None

Command Modes

Global configuration (config)

Supported User Roles

Network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to enable monitor log messages:

```
n1000v# configure terminal
n1000v(config)# logging monitor
n1000v(config)#
```

Send document comments to nexus1k-docfeedback@cisco.com.

Related Commands

Command	Description
show logging monitor	Displays the monitor logging configuration.

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

logging server

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

```
logging server host0 [i1 [use-vrf s0 [facility {auth | authpriv | cron | daemon | ftp | kernel | local0
| local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news | syslog | user |
uucp}]]]
```

```
no logging server host0 [i1 [use-vrf s0 [facility {auth | authpriv | cron | daemon | ftp | kernel |
local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news | syslog | user |
uucp}]]]
```

Syntax Description

<i>host0</i>	Hostname/IPv4/IPv6 address of the Remote Syslog Server.
<i>i1</i>	(Optional) 0-emerg;1-alert;2-crit;3-err;4-warn;5-notif;6-inform;7-debug.
use-vrf <i>s0</i>	(Optional) Enter VRF name, default is management + VRF name,default management.
facility	(Optional) Facility to use when forwarding to server.
auth	Use auth facility.
authpriv	Use authpriv facility.
cron	Use Cron/at facility.
daemon	Use daemon facility.
ftp	Use file transfer system facility.
kernel	Use kernel facility.
local0	Use local0 facility.
local1	Use local1 facility.
local2	Use local2 facility.
local3	Use local3 facility.
local4	Use local4 facility.
local5	Use local5 facility.
local6	Use local6 facility.
local7	Use local7 facility.
lpr	Use lpr facility.
mail	Use mail facility.
news	Use USENET news facility.
syslog	Use syslog facility.
user	Use user facility.
uucp	Use Unix-to-Unix copy system facility.

Defaults

None

Send document comments to nexus1k-docfeedback@cisco.com.

Command Modes Global configuration (config)

SupportedUserRoles network-admin

Command History	Release	Modification
	4.0(4)SV1(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:

```
n1000v# configure terminal
n1000v(config)# logging server 172.28.254.253
n1000v(config)#
```

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

```
n1000v# configure terminal
n1000v(config)# logging server syslogA 5
n1000v(config)#
```

Related Commands	Command	Description
	show logging server	Displays the current server configuration for logging system messages.

Send document comments to nexus1k-docfeedback@cisco.com.

logging timestamp

To set the unit of measure for the system messages timestamp, 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	Timestamp in micro-seconds.
	milliseconds	Timestamp in milli-seconds.
	seconds	Timestamp in seconds (Default).

Defaults Seconds

Command Modes Global configuration (config)

SupportedUserRoles network-admin

Command History	Release	Modification
	4.0(4)SV1(1)	This command was introduced.

Examples This example shows how to set microseconds as the unit of measure for the system messages timestamp:

```
n1000v# configure terminal
n1000v(config)# logging timestamp microseconds
n1000v(config)#
```

Related Commands	Command	Description
	show logging timestamp	Displays the logging timestamp configuration.