L Commands

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

lacp offload

To offload management of LACP from the VSM to the VEMs, use the **lacp offload** command. To return management of LACP to the VSM, use the **no** form of this command.

lacp offload

no lacp offload

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1) SV1(4))	This command was introduced.

Usage Guidelines

After changing the management of LACP from the VSM to the VEM, or back from VEM to VSM, you must copy the running configuration to the startup configuration and then reload the VSM for the change to take effect.

Examples

This example shows how to offload management of LACP from the VSM to the VEMs and then reload the switch for the change to take effect:

```
n1000v# config t
n1000v(config)# lacp offload
Please do a "copy running startup" to ensure the new setting takes effect on next reboot
LACP Offload Status can be verified using "show lacp offload status"
Change in LACP Offload Status takes effect only on the next VSM Reboot
This can potentially cause modules with LACP uplinks to flap
n1000v(config)# copy running-config startup-config
[################################] 100%
n1000v(config)# reload
!!!WARNING! there is unsaved configuration!!!
This command will reboot the system. (y/n)?  [n] y
2010 Sep  3 11:33:35 bl-n1000v %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from
Command Line Interface
```

This example shows how to return management of LACP to the VSM and then reload the switch for the change to take effect:

```
n1000v# config t
```

```
n1000v(config)# no lacp offload
Please do a "copy running startup" to ensure the new setting takes effect on next reboot
LACP Offload Status can be verified using "show lacp offload status"
Change in LACP Offload Status takes effect only on the next VSM Reboot
This can potentially cause modules with LACP uplinks to flap
n1000v(config)# copy running-config startup-config
[################################] 100%
n1000v(config)# reload
!!!WARNING! there is unsaved configuration!!!
This command will reboot the system. (y/n)?  [n] y
2010 Sep  3 11:33:35 bl-n1000v %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from
Command Line Interface
```

Related Commands

Command	Description
show lacp offload status	Displays the LACP offload status for verification.
show lacp port-channel [**interface port-channel** *channel-number*]	Displays information about LACP port channels.
show lacp interface ethernet *slot/port*	Displays information about specific LACP interfaces.
channel-group auto [**mode** {**on** | **active** | **passive**}] **mac-pinning**	Configures port channel mode (active and passive) used by LACP in the port profile.

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

min-val	Minimum ERSPAN flow ID number allowed.
maximum	Configures the maximum range value for ERSPAN flow IDs.
max-val	Maximum ERSPAN flow ID number allowed.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

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.

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)#
```

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)#
```

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)

SupportedUserRoles

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)#
```

Related Commands

Command	Description
show logging console	Displays the console logging configuration.

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.

logging ip access-list cache

To enable ACL logging on all the Virtual Ethernet Modules (VEMs), use the **logging ip access-list cache** command. To disable ACL logging, use the **no** form of this command.

logging ip access-list cache {{**interval** *seconds*} | {**max-deny-flows** *deny*} | {**max-permit-flows** *permit*} | {**module** *vem*}}

no logging ip access-list cache {{**interval** *seconds*} | {**max-deny-flows** *deny*} | {**max-permit-flows** *permit*} | {**module** *vem*}}

Syntax Description

interval *seconds*	Sets the time interval in seconds to accumulate packet counters before they are reported to the syslog servers, where *seconds* is the number of seconds. the range is from 5 to 86,400 seconds. The default is 300 seconds.
max-deny-flows *deny*	Sets the number of deny flows, where deny is the number of flows. The range is from 0 to 5000 flows. The default is 3000 flows.
max-permit-flows *permit*	Sets the number of permit flows where permit is the number of flows. The range is from 0 to 5000 flows. The default is 3000 flows.
module *vem*	Enables ACL logging on the specified VEM where vem is the ID of the VEM.

Defaults

By default, ACL logging is the enabled on all VEMs.

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1)SV1(5.1)	This command was introduced.

Usage Guidelines

Examples

This example shows how to enable ACL logging on VEM 5:

```
n1000v# configure terminal
n1000v(config)# logging ip access-list cache module 5
```

This example shows how to disable ACL logging on VEM 5:

```
n1000v# configure terminal
n1000v(config)# no logging ip access-list cache module 5
```

Related Commands

Command	Description
show logging ip access-list status	Displays the status of the ACL logging configuration for a VSM.
show logging ip access-list cache module	Displays the ACL logging configuration for the specified VEM module.

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

facility	Names the *facility.*
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)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(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:

```
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.

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

logfile-name	Specifies the name of the log file that stores system messages.
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

size *bytes*	(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)

SupportedUserRoles

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
```

```
n1000v(config)#
```

Related Commands

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

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*]

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)

SupportedUserRoles

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)#
```

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.

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)

SupportedUserRoles

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)#
```

Related Commands

Command	Description
show logging monitor	Displays the monitor logging configuration.

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

host0	Hostname/IPv4/IPv6 address of the Remote Syslog Server.
i1	(Optional) 0-emerg;1-alert;2-crit;3-err;4-warn;5-notif;6-inform;7-debug.
use-vrf *s0*	(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

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.

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.