



## L Commands

---

This chapter describes the Cisco NX-OS system management commands that begin with the letter L.

### 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**

<b>Syntax Description</b>	<i>severity-level</i>	<p>(Optional) The number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows:</p> <ul style="list-style-type: none"> <li>• <b>0</b>—emergency: System unusable</li> <li>• <b>1</b>—alert: Immediate action needed</li> <li>• <b>2</b>—critical: Critical condition—default level</li> <li>• <b>3</b>—error: Error condition</li> <li>• <b>4</b>—warning: Warning condition</li> <li>• <b>5</b>—notification: Normal but significant condition</li> <li>• <b>6</b>—informational: Informational message only</li> <li>• <b>7</b>—debugging: Appears during debugging only</li> </ul>
<b>Defaults</b>	None	
<b>Command Modes</b>	Global configuration	

## ***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

**SupportedUserRoles** Super user  
VDC administrator  
VDC user

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

**Usage Guidelines** This command does not require a license.

**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
	<b>show logging console</b>	Displays the console logging configuration.

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-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
<b>link-status</b>	Log all UP/DOWN and CHANGE messages.
<b>trunk-status</b>	Log all TRUNK status messages.
<b>default</b>	The default logging configuration is used by interfaces not explicitly configured.
<b>enable</b>	To enable logging overriding port level configuration.

**Defaults** None

**Command Modes** Global configuration

**Supported User Roles** Super user  
VDC administrator  
VDC user

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

**Usage Guidelines** This command does not require a license.

**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
	<b>show logging</b>	Displays the logging status.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## logging ip access-list cache

Use the **logging ip access-list cache** command to configure the Optimized ACL Logging (OAL) parameters.

To reset to the default settings, use the **no** form of this command.

```
logging ip access-list cache {{entries num_entries} | {interval seconds} | {threshold
num_packets}}
```

```
no logging ip access-list cache {{entries num_entries} | {interval seconds} | {threshold
num_packets}}
```

Syntax Description		
<b>entries</b> <i>num_entries</i>	Specifies the maximum number of log entries that are cached in the software; valid values are from 0 to 1048576 entries. The default value is 8000 entries.	
<b>interval</b> <i>seconds</i>	Specifies the maximum time interval before an entry is sent to syslog; valid values are from 5 to 86400 seconds. The default value is 300 seconds.	
<b>threshold</b> <i>num_packets</i>	Specifies the number of packet matches (hits) before an entry is sent to syslog; valid values are from 0 to 1000000 packets. The default value is 0 packets—rate limiting is off; the system log is not triggered by the number of packet matches.	

**Defaults** None

**Command Modes** Global configuration

**Supported User Roles** Super user  
VDC administrator  
VDC user

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

**Usage Guidelines** This command does not require a license.

**Examples** This example shows how to specify the maximum number of log entries that are cached in the software:

```
switch# configure terminal
switch(config)# logging ip access-list cache entries 200
switch(config)#
```

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

This example shows how to specify the maximum time interval before an entry is sent to the system log:

```
switch# configure terminal
switch(config)# logging ip access-list cache interval 350
switch(config)#
```

This example shows how to specify the number of packet matches before an entry is sent to the system log:

```
switch# configure terminal
switch(config)# logging ip access-list cache threshold 125
switch(config)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show logging ip access-list</b>	Displays the status of IP access list logging.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

## logging level

Use the **logging level** command to enable logging messages from the defined facility that have the specified severity level or higher.

To disable logging messages from the defined facility, use the **no** form of this command.

**logging level** *facility severity-level*

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

<b>Syntax Description</b>	<i>facility</i>	Define the appropriate <i>facility</i> . The facilities are listed in the <a href="#">“System Message Logging Facilities”</a> section on page 317.  To apply the same severity level to all facilities, use the <b>all</b> facility.
	<i>severity-level</i>	The number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows: <ul style="list-style-type: none"> <li>• <b>0</b>—emergency: System unusable</li> <li>• <b>1</b>—alert: Immediate action needed</li> <li>• <b>2</b>—critical: Critical condition—default level</li> <li>• <b>3</b>—error: Error condition</li> <li>• <b>4</b>—warning: Warning condition</li> <li>• <b>5</b>—notification: Normal but significant condition</li> <li>• <b>6</b>—informational: Informational message only</li> <li>• <b>7</b>—debugging: Appears during debugging only</li> </ul>

**Defaults** None

**Command Modes** Global configuration

**Supported User Roles** Super user  
VDC administrator  
VDC user

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

**Usage Guidelines** This command does not require a license.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*****Examples**

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

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show logging level</b>	Displays the facility logging level configuration.

**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

## logging logfile

Use the **logging logfile** command to configure the name of the log file used to store system messages and the minimum severity level to log.

To disable logging to the log file, 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>	Configure the name of the log file to be used to store system messages.
<i>severity-level</i>	The number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows: <ul style="list-style-type: none"> <li>• <b>0</b>—emergency: System unusable</li> <li>• <b>1</b>—alert: Immediate action needed</li> <li>• <b>2</b>—critical: Critical condition—default level</li> <li>• <b>3</b>—error: Error condition</li> <li>• <b>4</b>—warning: Warning condition</li> <li>• <b>5</b>—notification: Normal but significant condition</li> <li>• <b>6</b>—informational: Informational message only</li> <li>• <b>7</b>—debugging: Appears during debugging only</li> </ul>
<i>size bytes</i>	(Optional) Specify a maximum file size. The default file size is 10485760 bytes and can be configured from 4096 to 10485760 bytes.

### Defaults

None

### Command Modes

Global configuration

### Supported User Roles

Super user  
VDC administrator  
VDC user

### Command History

Release	Modification
4.0(1)	This command was introduced.

### Usage Guidelines

This command does not require a license.

## ***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

### **Examples**

This example shows how to configure a log file called *logfile* to store system messages and set its severity level to 4:

```
switch# configure terminal
switch(config)# logging logfile logfile 4
switch(config)#
```

### **Related Commands**

<b>Command</b>	<b>Description</b>
<b>show logging logfile</b>	Displays the log file.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

## logging module

Use the **logging module** command to enable module log messages. Set a specified severity level or use the default.

To disable module log messages, use the **no** form of this command.

**logging module** [*severity-level*]

**no logging module**

<b>Syntax Description</b>	<i>severity-level</i>	(Optional) The number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows/:
		<ul style="list-style-type: none"> <li>• <b>0</b>—emergency: System unusable</li> <li>• <b>1</b>—alert: Immediate action needed</li> <li>• <b>2</b>—critical: Critical condition</li> <li>• <b>3</b>—error: Error condition</li> <li>• <b>4</b>—warning: Warning condition</li> <li>• <b>5</b>—notification: Normal but significant condition—default level</li> <li>• <b>6</b>—informational: Informational message only</li> <li>• <b>7</b>—debugging: Appears during debugging only</li> </ul>

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>SupportedUserRoles</b>	Super user VDC administrator VDC user
---------------------------	---

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

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*****Examples**

This example shows how to enable module log messages:

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show logging module</b>	Displays the module logging status.

**[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

## logging monitor

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

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

**logging monitor** [*severity-level*]

**no logging monitor**

<b>Syntax Description</b>	<i>severity-level</i>	(Optional) The number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows/:
		<ul style="list-style-type: none"> <li>• <b>0</b>—emergency: System unusable</li> <li>• <b>1</b>—alert: Immediate action needed</li> <li>• <b>2</b>—critical: Critical condition—default level</li> <li>• <b>3</b>—error: Error condition</li> <li>• <b>4</b>—warning: Warning condition</li> <li>• <b>5</b>—notification: Normal but significant condition</li> <li>• <b>6</b>—informational: Informational message only</li> <li>• <b>7</b>—debugging: Appears during debugging only</li> </ul>

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>SupportedUserRoles</b>	Super user VDC administrator VDC user
---------------------------	---

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

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*****Examples**

This example shows how to enable monitor log messages:

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show logging monitor</b>	Displays the status of monitor logging.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## logging server

Use the **logging server** command to configure a Remote Syslog Server at the specified host name or IPv4/IPv6 address.

To disable the Remote Syslog Server, use the **no** form of this command.

```
logging server host [severity-level [use-vrf 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 host
```

Syntax Description	
<i>host</i>	Configure the host name or IPv4/IPv6 address of the Remote Syslog Server.
<i>severity-level</i>	(Optional) The number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows: <ul style="list-style-type: none"> <li>• <b>0</b>—emergency: System unusable</li> <li>• <b>1</b>—alert: Immediate action needed</li> <li>• <b>2</b>—critical: Critical condition—default level</li> <li>• <b>3</b>—error: Error condition</li> <li>• <b>4</b>—warning: Warning condition</li> <li>• <b>5</b>—notification: Normal but significant condition</li> <li>• <b>6</b>—informational: Informational message only</li> <li>• <b>7</b>—debugging: Appears during debugging only</li> </ul>
<b>use-vrf</b> <i>VRF_name</i>	(Optional) Enable VPN routing and forwarding (VRF) and create a VRF instance named <i>VRF_name</i> .
<b>facility</b> <i>facility</i>	(Optional) Define the appropriate outgoing <i>facility</i> . The facilities are listed in the <a href="#">“System Message Logging Facilities”</a> section on page 317.  The default outgoing facility is <b>local7</b> .

**Defaults** None

**Command Modes** Global configuration

**Supported User Roles** Super user  
VDC administrator  
VDC user

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

## ***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

### **Usage Guidelines**

This command does not require a license.

### **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**

<b>Command</b>	<b>Description</b>
<b>show logging server</b>	Displays the configured syslog servers.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## logging source-interface

Use the **logging source-interface** command to enable a source interface for the Remote Syslog Server. To disable the source interface, use the **no** form of this command.

**logging source-interface loopback** *virtual\_interface*

**no logging source-interface loopback** *virtual\_interface*

<b>Syntax Description</b>	<b>loopback</b> Enable the loopback interface selecting the virtual interface number from 0 to <i>virtual_interface</i> 1023.				
<b>Defaults</b>	None				
<b>Command Modes</b>	Global configuration				
<b>SupportedUserRoles</b>	Super user VDC administrator VDC user				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	4.0(1)	This command was introduced.
Release	Modification				
4.0(1)	This command was introduced.				
<b>Usage Guidelines</b>	This command does not require a license.				
<b>Examples</b>	<p>This example shows how to enable a source interface for the syslog server:</p> <pre>switch# <b>configure terminal</b> switch(config)# <b>logging source-interface loopback 5</b> switch(config)#</pre>				

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## logging timestamp

Use the **logging timestamp** command to set the logging timestamp units. By default, the units are seconds.

To reset the logging timestamp units to the default, use the **no** form of this command.

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

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

<b>Syntax Description</b>	<b>microseconds   milliseconds   seconds</b> Select the units to use for logging timestamps. The default units are <b>seconds</b> .				
<b>Defaults</b>	None				
<b>Command Modes</b>	Global configuration				
<b>SupportedUserRoles</b>	Super user VDC administrator VDC user				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	4.0(1)	This command was introduced.
Release	Modification				
4.0(1)	This command was introduced.				
<b>Usage Guidelines</b>	This command does not require a license.				
<b>Examples</b>	<p>This example shows how to set the logging timestamp units to microseconds:</p> <pre>switch# <b>configure terminal</b> switch(config)# <b>logging timestamp microseconds</b> switch(config)#</pre>				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>show logging timestamp</b></td> <td>Displays the logging timestamp configuration.</td> </tr> </tbody> </table>	Command	Description	<b>show logging timestamp</b>	Displays the logging timestamp configuration.
Command	Description				
<b>show logging timestamp</b>	Displays the logging timestamp configuration.				

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*

## match (NetFlow)

To specify match criteria for Flexible NetFlow flow records, use the **match** flow record configuration mode subcommand. To remove match criteria for Flexible NetFlow flow records, use the **no** form of this command.

```
match { flow direction | interface { input | output } | ip { protocol | tos } | ipv4 { destination address
| source address } | transport { destination-port | source-port } }
```

```
match { flow direction | interface { input | output } | ip { protocol | tos } | ipv4 { destination address
| source address } | transport { destination-port | source-port } }
```

### Syntax Description

<b>flow direction</b>	Direction of the flow to be matched.
<b>interface input</b>	Specifies that the match criterion is based on the input interface.
<b>interface output</b>	Specifies that the match criterion is based on the output interface.
<b>ip protocol</b>	Specifies that the match criterion is based on protocol.
<b>ip tos</b>	Specifies that the match criterion is based on type of service (ToS).
<b>ipv4 destination address</b>	Specifies that the match criterion is based on the destination IPv4 address.
<b>ipv4 source address</b>	Specifies that the match criterion is based on the source IPv4 address.
<b>transport destination-port</b>	Specifies that the match criterion for transport layer fields is based on the destination port.
<b>transport source-port</b>	Specifies that the match criterion for transport layer fields is based on the destination port.

### Command Default

No matching criteria are specified by default.

### Command Modes

Flow record configuration

### Supported User Roles

network-admin  
vdc-admin

### Command History

Release	Modification
4.0(1)	This command was introduced.

### Usage Guidelines

A Flexible NetFlow flow record must be enabled before you can use the **match** command. This command does not require a license.

## Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

### Examples

The following example shows how to specify the direction of the flow to be matched:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# match flow direction
```

Specifies that the match criterion is based on the input interface.

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# match interface input
```

Specifies that the match criterion is based on the output interface.

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# match interface output
```

Specifies that the match criterion is based on protocol.

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# match ip protocol
```

Specifies that the match criterion is based on type of service (ToS).

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# match ip tos
```

Specifies that the match criterion is based on the destination IPv4 address.

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# match ipv4 destination address
```

Specifies that the match criterion is based on the source IPv4 address.

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# match ipv4 source address
```

Specifies that the match criterion for transport layer fields is based on the destination port.

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# match ipv4 transport destination-port
```

Specifies that the match criterion for transport layer fields is based on the source port.

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# match ipv4 transport source-port
```

### Related Commands

Command	Description
<b>flow record</b>	Creates a flow record.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***