L Commands

This chapter describes the system management commands that begin with L.

logging abort

To discard the pending changes to the syslog server configuration, use the **logging abort** command.

logging abort

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

This example shows how to discard the changes made to the syslog server configuration:

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

Related Commands

Command	Description
logging distribute	Enables the distribution of the syslog server configuration to network switches using the CFS infrastructure.
show logging pending	Displays the pending changes to the syslog server configuration.
show logging status	Displays the logging status.

logging commit

To commit the pending changes to the syslog server configuration for distribution to the switches in the fabric, use the **logging commit** command.

logging commit

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

This example shows how to commit the distribution of the syslog server configuration:

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

Related Commands

Command	Description
logging distribute	Enables the distribution of the syslog server configuration to network switches using the CFS infrastructure.
show logging status	Displays the logging status.

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	(Optional) 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: • **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: Appears during debugging only

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(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
```

Related Commands

Command	Description
show logging console	Displays the console logging configuration.

logging distribute

To enable the distribution of the syslog server configuration to network switches using the Cisco Fabric Services (CFS) infrastructure, use the **logging distribute** command. To disable the distribution, use the **no** form of this command.

logging distribute

no logging distribute

Syntax Description

This command has no arguments or keywords.

Command Default

Distribution is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

This example shows how to enable the distribution of the syslog server configuration:

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

This example shows how to disable the distribution of the syslog server configuration:

```
switch(config)# no logging distribute
switch(config)#
```

Related Commands

Command	Description
logging abort	Cancels the pending changes to the syslog server configuration.
logging commit	Commits the changes to the syslog server configuration for distribution to the switches in the fabric.
show logging status	Displays the logging status.

logging event

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

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

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

Syntax Description

link-status	Specifies to log all UP/DOWN and CHANGE messages.
trunk-status	Specifies to log all TRUNK status messages.
default	Specifies to the default logging configuration is used by interfaces not explicitly configured.
enable	Enables the logging to override the port level configuration.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

This example shows how to log interface events:

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

Related Commands

Command	Description
show logging	Displays the logging status.

logging event port

To log events on an interface, use the **logging event port** command. To disable logging of interface events, use the **no** form of this command.

logging event port {**link-status** | **trunk-status**} [**default**]

no logging event port {**link-status** | **trunk-status**}

Syntax Description

link-status	Specifies to log all UP/DOWN and CHANGE messages.
trunk-status	Specifies to log all TRUNK status messages.
default	(Optional) Specifies the default logging configuration that is used by interfaces not explicitly configured.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

This example shows how to log interface events:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# logging event port link-status default
```

Related Commands

Command	Description
show interface	Displays the interface configuration information.
show logging	Displays the logging status.

logging ip access-list cache

To configure the Optimized ACL Logging (OAL) parameters, use the **logging ip access-list cache** command. 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

entries *num_entries*	Specifies the maximum number of log entries that are cached in the software. The range is from 0 to 1048576. The default value is 8000 entries.
interval *seconds*	Specifies the maximum time interval before an entry is sent to a syslog. The range is from 5 to 86400. The default value is 300 seconds.
threshold *num_packets*	Specifies the number of packet matches (hits) before an entry is sent to a syslog. The range is from 0 to 1000000. 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

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to 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)#
```

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

Command	Description
show logging ip access-list	Displays the status of IP access list logging.

logging level

To enable logging messages from a defined facility that have the specified severity level or higher, use the **logging level** command. To disable logging messages from a defined facility, use the **no** form of this command.

logging level *facility severity-level*

no logging level *facility severity-level*

Syntax Description

facility	Facility. The facilities are listed in Table A-1 of Appendix A, "System Message Logging Facilities." To apply the same severity level to all facilities, use the **all** facility.
severity-level	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: • **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: Appears during debugging only

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

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

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

Related Commands

Command	Description
show logging level	Displays the facility logging level configuration.

logging logfile

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

logfile-name	Name of the log file to be used to store system messages.
severity-level	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: • **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: Appears during debugging only
size *bytes*	(Optional) Specifies a maximum file size. The default file size is 4194304 bytes and can be configured from 4096 to 4194304 bytes.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

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

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

Related Commands

Command	Description
show logging logfile	Displays the log file.

logging module

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

logging module [*severity-level*]

no logging module

Syntax Description

severity-level	(Optional) 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*:* • **0**—emergency: System unusable • **1**—alert: Immediate action needed • **2**—critical: Critical condition • **3**—error: Error condition • **4**—warning: Warning condition • **5**—notification: Normal but significant condition—default level • **6**—informational: Informational message only • **7**—debugging: Appears during debugging only

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

Set a specified severity level or use the default.

Examples

This example shows how to enable module log messages:

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

Related Commands

Command	Description
show logging module	Displays the module logging status.

logging monitor

To enable the device to log messages to the monitor (terminal line), use the **logging monitor** command. To disable monitor log messages, use the **no** form of this command.

logging monitor [*severity-level*]

no logging monitor

Syntax Description

severity-level	(Optional) 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: • **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: Appears during debugging only

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

This configuration applies to Telnet and Secure Shell (SSH) sessions.

Examples

This example shows how to enable monitor log messages:

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

Related Commands

Command	Description
show logging monitor	Displays the status of monitor logging.

logging server

To configure a remote syslog server at the specified hostname or IPv4/IPv6 address, use the **logging server** command. To disable the remote syslog server, use the **no** form of this command.

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

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

Syntax Description

host	Hostname or IPv4/IPv6 address of the remote syslog server.
severity-level	(Optional) 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: • **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: Appears during debugging only
facility *facility*	(Optional) Specifies the outgoing *facility*. The facilities are listed in Table A-1 of Appendix A, "System Message Logging Facilities." The default outgoing facility is **local7**.
vrf *vrf_name*	(Optional) Specifies the virtual routing and forwarding (VRF) to be used in the remote server. The name can be a maximum of 32 alphanumeric characters.
management	Specifies the management VRF. This is the default VRF.

Command Default

The default outgoing facility is **local7**.
The default VRF is **management**.

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(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(config)# logging server 192.168.2.253
```

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

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

Related Commands

Command	Description
show logging server	Displays the configured syslog servers.

logging timestamp

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

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

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

Syntax Description

microseconds	Specifies the units to use for logging timestamps in microseconds. The default units are **seconds**.
milliseconds	Specifies the units to use for logging timestamps in milliseconds.
seconds	Specifies the units to use for logging timestamps in seconds. The default units are **seconds**.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

By default, the units are seconds.

Examples

This example shows how to set the logging time-stamp units to microseconds:

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

Related Commands

Command	Description
show logging timestamp	Displays the logging time-stamp configuration.