1 Syslog Commands

Command	Function
clear logging	Clear the logs from the memory buffer.
logging	Configure a syslog server for receiving logs.
logging buffered	Configure parameters (log severity level and buffer size) of the memory buffer for storing logs.
logging console	Configure the level of logs displayed on the console.
logging count	Enable log statistics collection.
logging delay-send file flash:	Configure the name of the log file that is buffered on the local device in the case of delayed reporting.
logging delay-send interval	Configure the interval for delayed log reporting.
logging delay-send server	Configure the IP address of the server and the reporting method for delayed log reporting.
logging delay-send terminal	Enable delayed log reporting to the console and remote terminal.
logging facility	Configure the facility value of logs.
logging file	Save logs to files. Log files can be stored in the hard disk, extended flash space, USB flash drive, or SD card.
logging file numbers	Configure the number of system log files that are written into the extended flash space.
logging flash flush	Immediately write logs in the system buffer into the flash space.
logging flash interval	Configure the interval at which you write system logs into the extended flash space.
logging filter direction	Filter the logs sent to a direction.
logging filter type	Configure the log filtering type.
logging filter rule	Configure the log filtering rule.
logging life-time level	Configure the storage time of log files in the extended flash space.

logging monitor	Configure the level of logs that are displayed in the window of the monitor terminal.
logging on	Allow the display of logs on different devices.
* MERGEFORMAT	Configure a level-based log reporting policy.
logging rate-limit	Enable logging rate limiting to limit the logs that are output per second.
logging rd on	Enable log redirection in a virtual switching unit (VSU) environment, to redirect the logs of the slave or standby device to the active device.
logging rd rate-limit	Enable log redirection rate limiting in a VSU environment to limit the logs that are redirected from the slave or standby device to the active device per second.
logging server	Configure a syslog server for receiving logs.
logging source interface	Set the source interface for log packets.
logging source ip	Configure the source IPv4 address for log packets.
logging source ipv6	Configure the source IPv6 address for log packets.
logging statistic enable	Enable periodical log reporting.
logging statistic mnemonic interval	Configure the interval of periodical log reporting.
logging statistic terminal	Enable periodical log reporting (system performance statistics logs) to the console and the remote terminal.
logging synchronous	Enable the synchronization of user input and log output to prevent interruption of user input.
logging trap	Configure the severity level of logs that are sent to the syslog server.
* MERGEFORMAT	Enable user login/logout logging.
logging userinfo command-log	Enable user operation logging.
logging performance switch	Enable performance log output.
service log-format rfc5424	Switch to the RFC5424 log format.
show logging	Display the log parameter configurations and log statistics as well as the log packets in the memory buffer. Log packets are displayed based on the timestamp from earliest to latest.

show logging config	Display the log parameter configurations and log statistics.
show logging count	Display the number of times logs are generated by each module and the last generation time.
show logging reverse	Display the log parameter configurations and log statistics as well as the log packets in the memory buffer. Log messages are displayed based on the timestamp from latest to earliest.
terminal monitor	Enable log display in the window of the current monitor terminal.

1.1 clear logging

Function

Run the **clear logging** command to clear the logs from the memory buffer.

Syntax

clear logging

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

1

Usage Guidelines

This command is used to clear log packets from the memory buffer, but cannot clear the log packet statistics.

Examples

The following example clears log packets from the memory buffer.

```
Hostname> enable
Hostname# clear logging
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 logging

Function

Run the **logging** command to configure a syslog server for receiving logs.

Run the **no** form of this command to remove this configuration.

Run the **no logging udp-port** command to restore the default configuration.

No syslog server is configured by default.

Syntax

logging { *ipv4-address* | **ipv6** *ipv6-address* } [**vrf** *vrf-name*] [**udp-prot** *port-number*] [**facility** *facility-type*] [**level** *inform-level*]

no logging { *ipv4-address* | **ipv6** *ipv6-address* } [**vrf** *vrf-name*] [**udp-prot**]

Parameter Description

ipv4-address: IPv4 address of the syslog server that receives logs.

vrf *vrf-name*: Specifies the VPN routing and forwarding table (VRF) instance connected to the syslog server. Here, *vrf-name* indicates the name of the instance.

ipv6 *ipv6-address*: Specifies the IPv6 address of the syslog server that receives logs. Here, *ipv6-address* indicates the IPv6 address of the syslog server.

udp-port *port-number*: Specifies the port number of the syslog server. Here, *port-number* indicates the port number. The range is from 1 to 65535 and the default value is **514**.

facility *facility-type*: Facility value of logs that are received by the syslog server. If the RFC5424 log format is disabled, the default facility value for logs sent to the server is **local7 (23)**. If the RFC5424 log format is enabled, such default facility value is **local0 (16)**.

level *inform-level*: Level of logs that are received by the syslog server. The value range is from 0 to 7. The default level of logs sent to the log server is information (level 6). The severity level can be a level name or a digit.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure a syslog server to receive logs of the device. Up to five syslog servers can be configured for a user. Logs are sent to all the configured syslog servers at the same time.

Examples

The following example configures a syslog server with IP address 10.1.1.100 and port 8099.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging 202.101.11.1 udp-port 8099
```

The following example configures a syslog server with IPv6 address AAAA:BBBB::FFFF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging ipv6 AAAA:BBBB::FFFF
```

Notifications

When more than five syslog servers are configured, the following notification will be displayed:

```
You can't configure more than 5 syslog servers!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 logging buffered

Function

Run the **logging buffered** command to configure parameters (log severity level and buffer size) of the memory buffer for storing logs.

Run the **no** form of this command to prohibit recording logs in the memory buffer.

Run the **default** form of this command to restore the default configuration.

The buffer size is 1 mega-byte and the log severity level is **7** by default.

Syntax

logging buffered [*buffer-size*] [*severity-level*]

no logging buffered

default logging buffered

Parameter Description

buffer-size: Buffer size in bytes. The value range is from 4096 to 10485760 (4 Kb to 10 Mb) and the default value is **1048576** (1 Mb).

severity-level: Log severity level. The value range is from 0 to 7. The severity level can be a level name or a digit. For details about the severity levels of logs, see Table 1-1.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- The memory buffer space is used cyclically. If the memory buffer of specified size is fully occupied, the earliest logs are overwritten. The **show logging** command is used to display logs in the memory buffer.
- Logs in the memory buffer are stored temporarily. When the device restarts or runs the **clear logging** command, logs in the buffer are cleared. Logs should be written into the extended flash space or sent to a syslog server to track problems.
- After the system has run for a long time, modifying the log buffer size, especially a larger one, may fail, and a failure prompt will appear. The general cause is that the continuous memory space for allocation is insufficient after the system has run for a long time. You are advised to modify the log buffer size when the

system starts up.

- The logs are classified into eight levels. A smaller value indicates a higher log severity level. Logs of level 0 have the highest severity level. After the level of logs that can be displayed on the device is set, logs with a level equal to or lower than the set level will be displayed. For details, see Table 1-1.

Table 1-1Details of Log Severity Levels

Keyword	Level	Description
Emergencies	0	Indicates that an emergency occurs and the system cannot run normally.
Alerts	1	Indicates that corrective measures must be taken immediately.
Critical	2	Indicates a critical circumstance.
Errors	3	Indicates an error message.
Warnings	4	Indicates a warning.
Notifications	5	Indicates a common but important message that requires attention.
Informational	6	Indicates an informational message.
Debugging	7	Indicates debugging information.

Examples

The following example allows only the logs of level 6 or below to be recorded in a memory buffer of 10,000 bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging buffered 10000 6
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 logging console

Function

Run the **logging console** command to configure the level of logs displayed on the console.

Run the **no** form of this command to prohibit you from printing log packets on the console.

The default level of logs that can be displayed on the console is **7** (debugging information).

Syntax

logging console [*severity-level*]

no logging console

Parameter Description

severity-level: Severity level of log packets. The value range is from 0 to 7. Here, the severity level can be a level name or a digit. For details about the severity levels of logs, see 1.3 Table 1-1.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- After a log severity level is configured, log packets with the level equal to or lower than the configured severity level will be displayed on the console.
- The **show logging** command is used to display the log parameter configuration and relevant log statistics.

Examples

The following example sets the level of logs that can be displayed on the console to 6.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging console informational
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 logging count

Function

Run the **logging count** command to enable log statistics collection.

Run the **no** form of this command to clear the log statistics and disable log statistics collection.

Log statistics collection is disabled by default.

Syntax

logging count

no logging count

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to enable log statistics collection. Statistics collection starts when the command is run. When the **no logging count** command is run, statistics collection is disabled and the statistics are cleared.

Examples

The following example enables log statistics collection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging count
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 logging delay-send file flash:

Function

Run the **logging delay-send file flash:** command to configure the name of the log file that is buffered on the local device in the case of delayed reporting.

Run the **no** form of this command to restore the default configuration.

The default format of the log file name is file size_device IP address_index.txt.

Syntax

logging delay-send file flash:*delay-send-filename*

no logging delay-send file

Parameter Description

delay-send-filename: Name of the log file for delayed reporting.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- The configured file name cannot contain any dot (.) because the system automatically adds the index and the suffix (**.txt**) to the file name when generating a locally buffered file. The index increases each time a new file is generated. In addition, the file name cannot contain characters prohibited by your file system, such as \, /, :, *, ", <, >, and |. For example, the configured file name is **log_server**, the current file index is 5, the file size is 1000 bytes, and the IP address of the device that sends the log file is 10.2.3.5. The name of the log file sent to the remote server is **log_server_1000_10.2.3.5_5.txt** while the name of the log file stored on the device is **log_server_5.txt**.
- If the source IP address is an IPv6 address, the colon (:) in the IPv6 address must be replaced by the hyphen (-) because the colon (:) is prohibited by the file system. For example, the file name is **log_server**, the current file index is 6, the file size is 1000 bytes, and the source IPv6 address of the device sending the log file is 2001::1. The name of the log file sent to the remote server is **log_server_1000_2001-1_6.txt** while the name of the log file stored on the device is **log_server_6.txt**.

Examples

The following example sets the name of the log file for delayed reporting to **log_server**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# service log-format rfc5424
Hostname(config)# logging delay-send file flash: log_server
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 logging delay-send interval

Function

Run the **logging delay-send interval** command to configure the interval for delayed log reporting.

Run the **no** form of this command to restore the default configuration.

The default interval for delayed log reporting is 3600s.

Syntax

logging delay-send interval *delay-send-interval*

no logging delay-send interval

Parameter Description

delay-send-interval: Interval for delayed log reporting in seconds. The value range is from 600 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the interval for delayed log reporting to 600s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# service log-format rfc5424
Hostname(config)# logging delay-send interval 600
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 logging delay-send server

Function

Run the **logging delay-send server** command to configure the IP address of the server and the reporting method for delayed log reporting.

Run the **no** form of this command to remove this configuration.

Delayed log reporting is disabled by default.

Syntax

logging delay-send server [**oob**] { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* | } [**vrf** *vrf-name*] [**via** *mgmt-name*] **mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** }**no logging delay-send server** [**oob**] { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**vrf** *vrf-name*] [**via** *mgmt-name*]

Parameter Description

oob: Indicates that the data is sent to the server through the MGMT interface of the device, that is, the data is sent to the server in the form of out-of-band communication. This parameter is available only when the device has an MGMT interface.

hostname: Domain name of the server receiving logs.

ipv-address:-address: IPv4 address of the server receiving logs.

ipv6 *ipv6-address*: Specifies the IPv6 address of the server receiving logs. *ipv6-address* indicates the IPv6 address of the server.

vrf *vrf-name*: Specifies the VPN routing and forwarding table (VRF) instance connected to the log server. *vrf-name* indicates the instance name.

via *mgmt-name*: Specifies the MGMT interface used by the syslog server when the **oob** option is included in the command.

username: Username of the FTP server.

password [**0** | **7**] *password*: Configures the password of the FTP server. **0** indicates using a plaintext password; **7** indicates using a simply encrypted ciphertext password; *password* indicates the ciphertext.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

At most five File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP) servers can be configured, and each server can be configured only as the FTP server or TFTP server. Logs are simultaneously sent to all the configured FTP or TFTP servers.

Examples

The following example configures an FTP server with IP address 192.168.23.12, username of **admin**, and password of **admin**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#service log-format rfc5424
Hostname(config)# logging delay-send server 192.168.23.12 mode ftp user admin
password admin
```

The following example configures a TFTP server withIPv6 address 2000::1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#service log-format rfc5424
Hostname(config)# logging delay-send server ipv6 2000::1 mode tftp
```

Related Commands

N/A

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

1.9 logging delay-send terminal

Function

Run the **logging delay-send terminal** command to enable delayed log reporting to the console and remote terminal.

Run the **no** form of this command to disable this feature.

Delayed log reporting to the console and remote terminal is disabled by default.

Syntax

logging delay-send terminal

no logging delay-send terminal

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables delayed log reporting to the console and remote terminal.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# service log-format rfc5424
Hostname(config)# logging delay-send terminal
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 logging facility

Function

Run the **logging facility** command to configure the facility value of logs.

Run the **no** form of this command to restore the facility value to the default value (**23**).

When the RFC5424 log format is enabled, the default facility value is 16 (Local0, Local use); otherwise, the default facility value is **23** (Local7, Local use).

Syntax

logging facility *facility-type*

no logging facility

Parameter Description

facility-type: Syslog facility value. For the specific values, see *Usage Guidelines*.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The facility value of logs is used to construct the priority of logs. The calculation formula is as follows:

Priority = Facility value × 8 + Severity.

As one part of log packets, the calculated log priority is sent to the log server. The log server can be used to identify different log sources, and search and filter logs of log sources. For description of the possible facility values of Syslog, see Table 1-1.

Table 1-1Description of Syslog Facility Values

Numerical Code	Facility
0 (kern)	Kernel messages
1 (user)	User-level messages
2 (mail)	Mail system
3 (daemon)	System daemons
4 (auth1)	Security/Authorization message
5 (syslog)	Messages generated internally by syslogd
6 (lpr)	Line printer system
7 (news)	USENET news
8 (uucp)	Unix-to-Unix copy system
9 (clock1)	Clock daemon
10 (auth2)	Security/Authorization message
11 (ftp)	FTP daemon
12 (ntp)	NTP daemon
13 (logaudit)	Log audit
14 (logalert)	Log alert
15 (clock2)	Clock daemon
16 (local0)	Local use
17 (local1)	Local use
18 (local2)	Local use
19 (local3)	Local use
20 (local4)	Local use
21 (local5)	Local use
22 (local6)	Local use
23 (local7)	Local use

Examples

The following example sets the facility value of syslog to **kern**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging facility kern
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 logging file

Function

Run the **logging file** command to save logs to files. Log files can be stored in the hard disk, extended flash space, USB flash drive, or SD card.

Run the **no** form of this command to remove the configuration.

Logs are not recorded in the extended flash space by default.

Syntax

logging file { **flash:***filename* **| usb0:***filename* } [*max-file-size*] [*inform-level*]

no logging file

Parameter Description

flash:: Saves log files to the extended flash drive (when there is flash2, the log files will be saved to flash2).

usb0:: Saves log files to USB0. This parameter is available only when the device has one USB port with a USB flash drive inserted. Whether this parameter is supported depends on the actual product version.

filename: Name of a log file. The name does not contain the file name extension, which is always **txt**.

max-file-size: Maximum size of a log file in bytes. The value range is from 131072 to 6291456 (128 kilobytes to 6 megabytes) and the default value is **131072** (128 kilobytes).

inform-level: Level of the logs that can be recorded in log files. The level can be a level name or a digit. The default level of logs that can be written into the extended flash space is **6**. For the levels of logs, see "Usage Guidelines".

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- If there is no syslog server or logs should not be transmitted on the network for security reasons, you can save the logs to the extended flash space.
- To record the logs in extended flash space, you must purchase an extended flash disk separately. Otherwise, **logging file flash** will be automatically hidden and cannot be configured. If no FLASH2 is available, **logging file flash2** is hidden automatically and cannot be configured. Otherwise, the logs are recorded in FLASH2 after **logging file flash** is configured.
- The log file name extension is fixed to **txt**. If other types of file name extensions are configured, the system prompts a configuration failure.

Examples

The following example records the logs in the extended flash space, with the file name of **syslog.txt**, file size of 128 KB, and log level of 6.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging file flash:syslog
```

Notifications

If the length of a configured log file name exceeds 20 characters, for example, 21 characters, an error is prompted.

```
%Error: The file length must not be longer then 20, Current file length 21.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 logging file numbers

Function

Run the **logging file numbers** command to configure the number of system log files that are written into the extended flash space.

Run the **no** form of this command to remove this configuration and restore the default configuration.

The default number of system log files is **16**.

Syntax

logging file numbers *file-numbers*

no logging file numbers

Parameter Description

file-numbers: Number of log files. The value range is from 2 to 16.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The system will not delete the generated log files after the number of log files is modified. Therefore, to save the extended flash space, you need to manually delete the log files generated in the system (before deletion, you can transfer the log files to an external server through TFTP). For example, 16 log files will be created by default after the function of writing logs into log files is enabled. If the device has generated 16 log files and if you want to change the number of log files to 2, new logs are overridden or overwritten in the log files with the index of 0 and 1 by turns. The existing log files with the index of 2 to 16 are retained. You can manually delete them.

Examples

The following example sets the number of log files to 8.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging file numbers 8
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 logging flash flush

Function

Run the **logging flash flush** command to immediately write logs in the system buffer into the flash space.

Syntax

logging flash flush

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- The **logging flash flush** command takes effect once after it configures the function above. Upon the configuration, logs in the buffer will be immediately written into the flash space.
- After the function is enabled to write logs into the flash space, the logs generated in the device will be saved in the log buffer of the system temporarily. They are not written into the flash space unless the buffer is fully occupied or the timer expires. But this command allows you to immediately write them into the flash space.

Examples

The following example immediately writes the logs in the system buffer into the flash space.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging flash flush
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **dir** (basic configuration/file system management command)

1.14 logging flash interval

Function

Run the **logging flash interval** command to configure the interval at which you write system logs into the extended flash space.

Run the **no** form of this command to remove this configuration and restore the default configuration.

Logs are written into the flash space at an interval of 3600s by default.

Syntax

logging flash interval *log-write-flash-interval*

no logging flash interval

Parameter Description

log-write-flash-interval: Interval at which you write logs into the flash space in seconds. The value range is from 1 to 51840.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To prevent the system from writing logs into the flash space frequently, do not set the interval to a small value .

Examples

The following example sets the interval at which you write logs into the flash space to 5 min.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging flash interval 300
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 logging filter direction

Function

Run the **logging filter direction** command to filter the logs sent to a direction.

Run the **no** form of this command to remove this configuration.

Logs sent to all the directions are filtered by default, namely, **all** is set.

Syntax

logging filter direction { **all** | **buffer** | **file** | **server** | **terminal** }

no logging filter direction { **all** | **buffer** | **file** | **server** | **terminal** }

Parameter Description

all: Filters the logs sent to all the directions (including the directions of the console, virtual type terminal (VTY), log buffer, log file, and log server).

buffer: Filters the logs sent to the log buffer (the logs displayed by the **show logging** command).

file: Filters the logs sent to log files.

server: Filters the logs sent to the log server.

terminal: Filters the logs sent to the console and VTY terminal, including telnet and Secure Shell (SSH).

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- To filter the logs in all the directions (including the directions of the console, VTY terminal, log buffer, log file, and log server) after they match filtering rules, configure the **all** keyword.
- When you filter the logs sent to a specific direction only, for example, the filtered logs are not sent to the terminal interface but must be written into log files or sent to a log server, you only need to configure the command to filter the logs sent to the terminal.

Examples

The following example filters the logs sent to the terminal, including the console and VTY terminal.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging filter direction terminal
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 logging filter type

Function

Run the **logging filter type** command to configure the log filtering type.

Run the **no** form of this command to restore the log filtering type.

The default filtering type is **filter-only**.

Syntax

logging filter type { **contains-only** | **filter-only** }

no logging filter type

Parameter Description

contains-only: Displays only the logs that contain keywords specified in the filtering rules.

filter-only: Filters and displays the logs that contain keywords specified in the filtering rules.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- Too many logs from one module may result in spamming on the terminal CLI. If you do not care about them, you can apply **filter-only** on the device to filter such logs.
- To display some logs only, you can apply **contains-only** on the device to display only the logs that match filtering rules on the terminal. Then, you can check whether any event occurs.
- If the filtering direction and filtering type instead of filtering rules are configured, the configurations do not take effect, that is, logs are not filtered.
- The **filter-only** and **contains-only** filtering types are mutually exclusive, that is, you can configure only one filtering type at a time.

Examples

The following example sets the log filtering type to **contains-only**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging filter type contains-only
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 logging filter rule

Function

Run the **logging filter rule** command to configure the log filtering rule.

Run the **no** form of this command to remove this configuration.

No log filtering rule is configured by default, that is, logs are not filtered.

Syntax

logging filter rule { **exact-match module** *module-name* **mnemonic** *mnemonic-name* **level** *inform-level* | **single-match** { **level** *inform-level* | **mnemonic** *mnemonic-name* | **module** *module-name* } }

no logging filter rule { **exact-match module** *module-name* **mnemonic** *mnemonic-name* **level** *inform-level* | **single-match** { **level** *inform-level* | **mnemonic** *mnemonic-name* | **module** *module-name* } }

Parameter Description

exact-match: Configures exact matching.

single-match: Configures single matching.

module *module-name*: Specifies the name of the module whose logs need to be filtered.

mnemonic *mnemonic-name*: Specifies the mnemonic name of the logs to be filtered.

level *inform-level*: Specifies the level of the logs to be filtered.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- To filter a specific log, use the **exact-match** rule. You must specify the specific module name, mnemonic name, and log level.
- To filter some types of logs, use the **single-match** rule. You must specify the module name, log level, or mnemonic name.
- If the same module name, mnemonic name, or log level is configured in both the **single-match** and **exact-match** rules, the **single-match** rule prevails over the **exact-match** rule.

Examples

The following example sets the log filtering rule to **exact-match**, module name to **LOGIN**, log level to **5**, and mnemonic to **LOGOUT**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging filter rule exact-match module LOGIN mnemonic LOGOUT
level 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 logging life-time level

Function

Run the **logging life-time level** command to configure the storage time of log files in the extended flash space.

Run the **no** form of this command to remove this configuration.

No storage time is configured by default. The storage time depends on the size of the configured log files.

Syntax

logging life-time level *inform-level life-time-days*

no logging life-time level *level*

Parameter Description

inform-level: Log level. The value range is from 0 to 7.

life-time-days: Number of storage days for log files in days. The value range is from 7 to 365.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- Because the sizes of extended flash space and the importance of logs at various levels are different, you are advised to configure different storage days for logs of various levels.
- When the time-based log storage function is enabled, the original log storage function based on file size becomes invalid, and the log files are stored in the **syslog/** directory of the extended flash space.

Examples

The following example sets the storage time of the logs of level 6 to 10 days.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging life-time level 6 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 logging monitor

Function

Run the **logging monitor** command to configure the level of logs that are displayed in the window of the monitor terminal.

Run the **no** form of this command to prohibit the window of the monitor terminal from printing log packets.

The default level of logs that are displayed in the window of the monitor terminal is **7** (debugging information).

Syntax

logging monitor [*severity-level*]

no logging monitor

Parameter Description

severity-level: Severity level of a log packet. The level can be a level name or a digit. For details about the severity levels of logs, see 1.3 Table 1-1.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To display logs in the VTY window, run the **terminal monitor** command. The **logging monitor** command is used to define the level of logs that are displayed in the VTY window. For details about the severity levels of logs, see 1.3 Table 1-1.

Examples

The following example sets the level of logs that are displayed in the VTY window to 6.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging monitor informational
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 logging on

Function

Run the **logging on** command to allow the display of logs on different devices.

Run the **no** form of this command to disable the log display.

Logs are allowed to be displayed on different devices by default.

Syntax

logging on

no logging on

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Logs can be displayed in the console window and VTY window, or recorded in different devices, including the memory buffer, extended flash space, and syslog server. If the logging function is disabled, only the logs with a severity level lower than 1 are displayed or recorded.

Examples

The following example disables the logging function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no logging on
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 logging policy

Function

Run the **logging policy** command to configure a level-based log reporting policy.

Run the **no** form of this command to remove a level-based log reporting policy. No level-based log reporting policy is configured by default.

Syntax

logging policy module *module-name* [**not-lesser-than**] *policy-level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }

no logging policy module *module-name* [**not-lesser-than**] *policy-level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }

no logging policy

Parameter Description

module-name: Module name of a level-based log reporting policy.

not-lesser-than: Configures log filtering rules for a level-based log reporting policy. When this parameter is specified, the logs of a specified level or higher are sent to the specified destination, and the other logs are filtered. When this option is not specified, the logs of a specified level or lower are sent to the specified destination, and the other logs are filtered.

policy-level: Level of logs, for which a level-based log reporting policy needs to be configured.

all: Applies the level-based log reporting policy to the logs sent in all the directions.

server: Applies the level-based log reporting policy to the logs sent to the log server only.

file: Applies the level-based log reporting policy to the logs sent to log files only.

console: Applies the level-based log reporting policy to the logs sent to the console only.

monitor: Applies the level-based log reporting policy to the logs sent to the remote terminal only.

buffer: Applies the level-based log reporting sent to the logs saved in the buffer only.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example outputs logs of level 5 or higher generated by the SYS module to the console only, but logs of level 3 or lower by the SYS module to the buffer only.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging policy module SYS not-lesser-than 5 direction console
Hostname(config)# logging policy module SYS 3 direction buffer
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 logging rate-limit

Function

Run the **logging rate-limit** command to enable logging rate limiting to limit the logs that are output per second.

Run the **no** form of this command to disable the logging rate limiting.

Logging rate limiting is disabled by default.

Syntax

logging rate-limit { *number* | **all** *number* | **console** { *number* | **all** *number* } } [**except** [*severity-level*]]

no logging rate-limit

Parameter Description

number: Number of logs that are processed per second. The value range is from 1 to 10000.

all: Configures rate limit for all the logs, including those of levels 0 to 7.

console: Configures the maximum number of logs that are displayed on the console per second.

except: Applies no rate limit to the logs of the specified severity level or lower. The default severity level is error (level 3), that is, no rate limit is applied to the logs of level 3 or lower.

severity-level: Severity level of logs. A smaller value indicates a higher severity level. The value range is from 0 to 7.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to prevent the output of massive logs.

Examples

The following example sets the maximum number of logs of all levels (including debugging information) that are processed per second to 10 but does not control logs of the warning level and higher.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging rate-limit all 10 except warnings
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 logging rd on

Function

Run the **logging rd on** command to enable log redirection in a virtual switching unit (VSU) environment, to redirect the logs of the slave or standby device to the active device.

Run the **no** form of this command to disable log redirection.

Log redirection is enabled by default.

Syntax

logging rd on

no logging rd on

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example disables log redirection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no logging rd on
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 logging rd rate-limit

Function

Run the **logging rd rate-limit** command to enable log redirection rate limiting in a VSU environment to limit the logs that are redirected from the slave or standby device to the active device per second.

Run the **no** form of this command to disable log redirection rate limiting.

The log redirection limits the maximum number of logs to be redirected per second to **200** by default.

Syntax

logging rd rate-limit *number* [**except** [*severity-level*]]

no logging rd rate-limit

Parameter Description

number: Maximum number of logs that are redirected per second. The value range is from 1 to 10000.

except: Applies no rate limit to the logs of the specified severity level or lower. The default severity level is error (level 3), that is, no rate limit is applied to the logs of level 3 or lower.

severity-level: Severity level of logs. A smaller value indicates a higher severity level. The value range is from 0 to 7.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to prevent the redirection of massive logs from the slave or standby device to the active device.

Examples

The following example sets the maximum number of all logs (including debugging information) that are redirected from the slave or standby device to the active device per second to 10 but does not control logs of the warning level and higher.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging rd rate-limit 10 except warnings
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 logging server

Function

Run the **logging server** command to configure a syslog server for receiving logs.

Run the **no** form of this command to remove this configuration.

Run the **no logging server udp-port** command to restore the default configuration.

No syslog server is configured by default.

Syntax

logging server [**oob**] { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**via** *mgmt-name*] [**udp-prot** *port-number*] [**vrf** *vrf-name*] [**facility** *facility-type*] [**level** *inform-level*]

no logging server [**oob**] { *hostname* | *ipv4-address* [**vrf** *vrf-name*] | **ipv6** *ipv6-address* } [**via** *mgmt-name*]

no logging server { *hostname* | *ipv4-address* [**vrf** *vrf-name*] | **ipv6** *ipv6-address* } [**via** *mgmt-name*] **udp-prot**

Parameter Description

oob: Specifies out-of-band communication for the log server (sending logs to the log server through the MGMT interface). This option is available only when the device has an MGMT interface.

hostname: Domain name of the syslog server that receives logs.

ipv4-address: IPv4 address of the syslog server that receives logs.

vrf *vrf-name*: Specifies the name of the VRF instance connected to the syslog server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the syslog server that receives logs.

via *mgmt-name*: Specifies the MGMT port used by the syslog server when the **oob** option is contained in the command.

udp-port *port-number*: Specifies the port number of the syslog server. The value range is from 1 to 65535, and the default value is **514**.

facility *facility-type*: Facility value of logs that are received by the syslog server. If the RFC5424 log format is disabled, the default facility value for logs sent to the server is **local7 (23)**. If the RFC5424 log format is enabled, such default facility value is **local0 (16)**.

level *inform-level*: Level of logs that are received by the syslog server. The value range is from 0 to 7. The default level of logs sent to the log server is information (level 6). The severity level can be a level name or a digit.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- Up to five syslog servers are configured on one device. The logs on the device are sent to all the configured syslog servers at the same time.
- In this command, the **via** parameter is available only when the **oob** parameter is configured. But the **vrf** parameter is unavailable.
- The IPv6 server does not support **vrf** or **oob**.

Examples

The following example configures a syslog server with IP address10.1.1.100 and port 8099.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging server 202.101.11.1 udp-port 8099
```

The following example configures a syslog server with IPv6 address AAAA:BBBB::FFFF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging server ipv6 AAAA:BBBB::FFFF
```

Notifications

When more than five syslog servers are already configured on the device, the following notification will be displayed:

```
You can't configure more than 5 syslog servers!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 logging source interface

Function

Run the **logging source interface** command to set the source interface for log packets.

Run the **no** form of this command to remove this configuration.

No log source address is configured, and the source IP address of the log packets sent to the server is the IP address of the interface that sends the packets by default.

Syntax

logging source [**interface**] *interface-type interface-number*

no logging source [**interface**]

Parameter Description

interface-type: Interface type.

interface-number: Interface number.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

By default, the source IP address of log packets sent to the syslog server is the IP address of the interface that sends the packets. To track and manage log packets, the administrator runs this command to set the source IP address of all log packets to the IP address of an interface. Thus, the administrator can identify the device that sends the log packets based on the unique IP address. If this source interface is not configured on the device or no IP address is configured for the source interface, the source IP address of the log packets is still the IP address of the interface that sends the packets.

Examples

The following example sets the source IP address of system log packets to the address of interface Loopback 0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging source interface loopback 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 logging source ip

Function

Run the **logging source ip** command to configure the source IPv4 address for log packets.

Run the **no** form of this command to remove this configuration.

No source IPv4 address is configured for log packets by default.

Syntax

logging source ip *ipv4-address*

no logging source ip

Parameter Description

ipv4-address: Source IPv4 address of log packets sent to the IPv4 syslog server.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

By default, the source IPv4 address of log packets sent to the syslog server is the IPv4 address of the interface that sends the packets. To track and manage log packets, the administrator runs this command to set the source IPv4 address of all log packets to a fixed IPv4 address. Thus, the administrator can identify the device that sends the log packets based on the unique IPv4 address. If this IPv4 address is not configured on the device, the source IPv4 address of the log packets is still the IPv4 address of the interface that sends the packets.

Examples

The following example sets the source IP address of system log packets to 192.168.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging source ip 192.168.1.1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 logging source ipv6

Function

Run the **logging source ipv6** command to configure the source IPv6 address for log packets.

Run the **no** form of this command to remove this configuration.

No source IPv6 address is configured for log packets by default.

Syntax

logging source ipv6 *ipv6-address*

no logging source ipv6

Parameter Description

ipv6-address: Source IPv6 address of log packets sent to the IPv6 syslog server.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

By default, the source IPv6 address of log packets sent to the syslog server is the IPv6 address of the interface that sends the packets. To track and manage log packets, the administrator runs this command to set the source IPv6 address of all log packets to a fixed IPv6 address. Thus, the administrator can identify the device that sends the log packets based on the unique IPv6 address. If this IPv6 address is not configured on the device, the source IPv6 address of the log packets is still the IPv6 address of the interface that sends the packets.

Examples

The following example sets the source IPv6 address of system log packets to 1::1/64.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging source ipv6 1::1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.29 logging statistic enable

Function

Run the **logging statistic enable** command to enable periodical log reporting.

Run the **no** form of this command to disable periodical log reporting.

Periodical log reporting is disabled by default.

Syntax

logging statistic enable

no logging statistic enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is used to enable periodical log reporting, the system outputs a series of performance statistics at an interval so that the log server can monitor the system performance.

Examples

The following example enables periodical log reporting.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging statistic enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.30 logging statistic mnemonic interval

Function

Run the **logging statistic mnemonic interval** command to configure the interval of periodical log reporting.

Run the **no** form of this command to restore the default configuration.

The interval of periodical logging is 15 min by default.

Syntax

logging statistic mnemonic *mnemonic* **interval** *logging-statistic-interval*

no logging statistic mnemonic *mnemonic*

Parameter Description

mnemonic: Mnemonic string for periodical log reporting, used to identify a statistical object of system performance.

logging-statistic-interval: Interval of periodical log reporting in minutes. The value range is 0, 15, 30, 60, and 120, where **0** indicates disabling periodical log reporting for the statistical object.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the interval of periodical log reporting for statistical object MATCH to 30 min.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging statistic mnemonic MATCH interval 30
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.31 logging statistic terminal

Function

Run the **logging statistic terminal** command to enable periodical log reporting (system performance statistics logs) to the console and the remote terminal.

Run the **no** form of this command to disable this feature.

Periodical log reporting to the console and remote terminal is disabled by default.

Syntax

logging statistic terminal

no logging statistic terminal

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables periodical log reporting to the console and remote terminal.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging statistic terminal
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.32 logging synchronous

Function

Run the **logging synchronous** command to enable the synchronization of user input and log output to prevent interruption of user input.

Run the **no** form of this command to disable this feature.

The synchronization of user input and log output is disabled by default.

Syntax

logging synchronous

no logging synchronous

Parameter Description

N/A

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

Run this command to enable the synchronization of user input and log output to prevent interruption of user input. If the port UP-DOWN log is displayed during input of the **configure terminal** command, the input command is output again:

```
Hostname# configure terminal
Oct  9 23:40:55 %LINK-CHANGED: Interface GigabitEthernet 0/1, changed state to
down
Oct  9 23:40:55 %LINEPROTO-UPDOWN: Line protocol on Interface GigabitEthernet
0/1, changed state to DOWN
```

Examples

The following example enables the synchronization of user input and log output on the console.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line console 0
Hostname(config-line)# logging synchronous
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.33 logging trap

Function

Run the **logging trap** command to configure the severity level of logs that are sent to the syslog server.

Run the **no** form of this command to disable the function of sending log packets to the syslog server.

The default severity level of logs sent to the syslog server is **6** (informational message).

Syntax

logging trap [*severity-level*]

no logging trap

Parameter Description

severity-level: Severity level of logs. The range is from 0 to 7. The severity level can be a level name or a digit.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- To send logs to the syslog server, first configure the **logging server** command, and then use the **logging trap** command to specify the severity level of the logs to be sent. For details about the severity levels of logs, see 1.3 Table 1-1.
- When the device independently configures the severity level of logs to be received by the log server, the severity level configured separately for the log server prevails.

Examples

The following example sets the severity level of logs sent to syslog server 202.101.11.22 to 6.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging server 202.101.11.22
Hostname(config)# logging trap informational
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.34 logging userinfo

Function

Run the **logging userinfo** command to enable user login/logout logging.

Run the **no** form of this command to disable user login/logout logging.

User login/logout logging is disabled by default.

Syntax

logging userinfo

no logging userinfo

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After user login/logout logging enabled, a log will prompt the device administrator when a user connects to the device. The log format is as follows:

```
Mar 22 14:05:45 %LOGIN-LOGIN_SUCCESS: User login from vty0 (192.168.23.68) OK.
```

Examples

The following example enables user login/logout logging.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging user-info
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.35 logging userinfo command-log

Function

Run the **logging userinfo command-log** command to enable user operation logging.

Run the **no** form of this command to disable user operation logging.

User operation logging is disabled by default.

Syntax

logging userinfo command-log

no logging userinfo command-log

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- After user operation logging is enabled, a log will be displayed to prompt the device administrator when a user modifies device configurations. The log format is as follows:

```
Mar 22 14:10:40 %CLI-EXEC_CMD: Configured from vty0 (192.168.23.68) command-log: logging server 192.168.23.68.
```

- If the 5424 log format is configured using the **service log-format rfc5424** command, you need to configure the **logging delay-send terminal** command before you output the operation logs to the terminal (because delayed log reporting is registered for the operation logs).

Examples

The following example enables user operation logging.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging userinfo command-log
The security log has been recorded, this command does not need to be opened.
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.36 logging performance switch

Function

Run the **logging performance switch** command to enable performance log output.

Run the **no** form of this command to disable performance log output.

Performance log output is disabled by default.

Syntax

logging performance switch

no logging performance switch

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When performance log output is enabled, the log output through the performance logging interface is transmitted through the performance log channel (that is, the logs are sent to the log server only; this mechanism usually does not need to be configured, and it is designed for the service that outputs many logs to the server rapidly).

Examples

The following example enables performance log output.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging performance switch
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.37 service log-format rfc5424

Function

Run the **service log-format rfc5424** command to switch to the RFC5424 log format.

Run the **no** form of this command to switch to the original log format.

The default syslog format is **RFC3164**.

Syntax

service log-format rfc5424

no service log-format rfc5424

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- After the system is switched to the RFC5424 log format, the **service sequence-numbers**, **service sysname**, **service timestamps**, **service private-syslog**, and **service standard-syslog** commands that are applicable to the original log format fail and are hidden.
- When the system is switched to the original log format, the **logging delay-send**, **logging policy**, and **logging statistic** commands that are applicable to the RFC5424 log format fail and are hidden.
- Before and after log format switching, the output of the **show logging** and **show logging config** commands changes.

Examples

The following example sets the log format to RFC5424.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# service log-format rfc5424
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.38 show logging

Function

Run the **show logging** command to display the log parameter configurations and log statistics as well as the log packets in the memory buffer. Log packets are displayed based on the timestamp from earliest to latest.

Syntax

show logging

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the log parameter configurations and log statistics as well as the log packets in the memory buffer when the RFC5424 log format is not enabled.

```
Hostname> enable
Hostname# show logging
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
```

```
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 15242 message lines logged,0 fail
    logging to  202.101.11.22
    logging to  192.168.200.112
Log Buffer (Total 131072 Bytes): have written 1336,
015487: *Sep 19 02:46:13: Hostname %LINK-UPDOWN: Interface FastEthernet 0/24,
changed state to up.
015488: *Sep 19 02:46:13: Hostname %LINEPROTO-UPDOWN: Line protocol on Interface
FastEthernet 0/24, changed state to up.
015489: *Sep 19 02:46:26: Hostname %LINK-UPDOWN: Interface FastEthernet 0/24,
changed state to down.
015490: *Sep 19 02:46:26: Hostname %LINEPROTO-UPDOWN: Line protocol on Interface
FastEthernet 0/24, changed state to down.
015491: *Sep 19 02:46:28: Hostname %LINK-UPDOWN: Interface FastEthernet 0/24,
changed state to up.
015492: *Sep 19 02:46:28: Hostname %LINEPROTO-UPDOWN: Line protocol on Interface
FastEthernet 0/24, changed state to up.
```

Table 1-1Output Fields of the show logging Command with the RFC5424 Log Format Disabled

Field	Description
Syslog logging	Logging function ● "enabled" is displayed when the function is enabled. ● "disabled" is displayed when the function is disabled.
Console logging	Level of the logs displayed on the console as well as log statistics
Monitor logging	Level of the logs displayed in the VTY window as well as log statistics
Buffer logging	Level of the logs recorded in the memory buffer as well as log statistics
Standard format	Standard log format
Timestamp debug messages	Timestamp format of debugging information
Timestamp log messages	Timestamp format of logs
Sequence-number log messages	Sequence number function
Sysname log messages	Whether to enable the function of adding a system name to logs
Count log messages	Log statistics collection
Trap logging	Level of the logs sent to the syslog server as well as log statistics
Log Buffer	Log packets recorded in the memory buffer

The following example displays the log parameter configurations and log statistics as well as the log packets in the memory buffer when the RFC5424 log format is enabled.

```
Hostname> enable
Hostname# show logging
Syslog logging: enabled
  Console logging: level debugging, 4740 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 4745 messages logged
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:3, Current send
index:3, Cycle:10 seconds
Count log messages: enable
  Trap logging: level informational, 2641 message lines logged,4155 fail
    logging to  192.168.23.89
    logging to  2000::1
  Delay-send logging: 2641 message lines logged
    logging to  192.168.23.89  by tftp
Log Buffer (Total 4096 Bytes): have written 4096, Overwritten 3292
<135>1 2013-07-24T12:19:33.130290Z Hostname - 7 - Please config the IP address
for capwap.
<132>1 2013-07-24T12:20:02.80313Z Hostname CAPWAP 4 NO_IP_ADDR - No ip address
for capwap.
<135>1 2013-07-24T12:20:02.80343Z Hostname - 7 - Please config the IP address for
capwap.
<132>1 2013-07-24T12:20:32.250265Z Hostname CAPWAP 4 NO_IP_ADDR - No ip address
for capwap.
<134>1 2013-07-24T12:29:33.410123Z Hostname SYS 6 SHELL_LOGIN [USER@4881 name=""
type="" from="console"] user login success.
<134>1 2013-07-24T12:29:34.343763Z Hostname SYS 6 SHELL_CMD [USER@4881 name=""]
[CMD@4881 task="rl_con" cmd="enable"]
```

Table 1-2Output Fields of the show logging Command with the RFC5424 Log Format Enabled

Field	Description
Syslog logging	Logging function ● "enabled" is displayed when the function is enabled. ● "disabled" is displayed when the function is disabled.
Console logging	Level of the logs displayed on the console as well as log statistics
Monitor logging	Level of the logs displayed in the VTY window as well as log statistics
Buffer logging	Level of the logs recorded in the memory buffer as well as log statistics
Count log messages	Log statistics function
Statistic log messages	Function of periodical log reporting

Field	Description
Statistic log messages to terminal	Whether to enable periodical log reporting to the console and remote terminal
Delay-send file name	Name of the file that buffers delayed log reporting on the local device, currently written file index, and the interval of delayed log reporting
Trap logging	Level of the logs sent to the syslog server as well as log statistics
Delay-send logging	Address of the server for delayed log reporting, reporting mode, and statistics
Log Buffer	Log packets recorded in the memory buffer

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.39 show logging config

Function

Run the **show logging config** command to display the log parameter configurations and log statistics.

Syntax

show logging config

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the log configurations when the RFC5424 log format is not enabled.

```
Hostname> enable
Hostname# show logging config
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 15242 message lines logged,0 fail
    logging to  202.101.11.22
    logging to  192.168.200.112
```

Table 1-1Output Fields of the show logging config Command with the RFC5424 Log Format Disabled

Field	Description
Syslog logging	Logging function ● "enabled" is displayed when the function is enabled. ● "disabled" is displayed when the function is disabled.
Console logging	Level of the logs displayed on the console as well as log statistics
Monitor logging	Level of the logs displayed in the VTY window as well as log statistics
Buffer logging	Level of the logs recorded in the memory buffer as well as log statistics
Standard format	Standard log format
Timestamp debug messages	Timestamp format of debugging information
Timestamp log messages	Timestamp format of logs
Sequence-number log messages	Sequence number function
Sysname log messages	Whether to enable the function of adding a system name to logs
Count log messages	Log statistics function
Trap logging	Level of the logs sent to the syslog server as well as log statistics

The following example displays the log configurations when the RFC5424 log format is enabled.

```
Hostname> enable
Hostname# show logging
Syslog logging: enabled
```

```
  Console logging: level debugging, 4740 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 4745 messages logged
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:3, Current send
index:3, Cycle:10 seconds
Count log messages: enable
  Trap logging: level informational, 2641 message lines logged,4155 fail
    logging to  192.168.23.89
    logging to  2000::1
  Delay-send logging: 2641 message lines logged
    logging to  192.168.23.89  by tftp
```

Table 1-2Output Fields of the show logging config Command with the RFC5424 Log Format Enabled

Field	Description
Syslog logging	Logging function ● "enabled" is displayed when the function is enabled. ● "disabled" is displayed when the function is disabled.
Console logging	Level of the logs displayed on the console as well as log statistics
Monitor logging	Level of the logs displayed in the VTY window as well as log statistics
Buffer logging	Level of the logs recorded in the memory buffer as well as log statistics
Count log messages	Log statistics function
Statistic log messages	Whether to enable periodical log reporting
Statistic log messages to terminal	Whether to enable periodical log reporting to the console and remote terminal
Delay-send file name	Name of the file that buffers delayed log reporting on the local device, currently written file index, and the interval of delayed log reporting
Trap logging	Level of the logs sent to the syslog server as well as log statistics
Delay-send logging	Address of the server for delayed log reporting, reporting mode, and statistics

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.40 show logging count

Function

Run the **show logging count** command to display the number of times logs are generated by each module and the last generation time.

Syntax

show logging count

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the statistics on logs generated by each module in the system.

```
Hostname> enable
Hostname# show logging count
Module Name   Message Name Sev Occur      Last Time
==================================================SYS           CONFIG_I
5   1         Jul 6 10:29:57
--------------SYS       TOTAL      1
```

Table 1-1 Output Fields of the show logging count Command

Field	Description
Module Name	Log module name
Message Name	Log mnemonic name
Sev	Log level

Field	Description
Occur	Number of log entries of this type counted since the execution of the logging count command
Last Time	Last time that a log of this type is generated

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.41 show logging reverse

Function

Run the **show logging reverse** command to display the log parameter configurations and log statistics as well as the log packets in the memory buffer. Log messages are displayed based on the timestamp from latest to earliest.

Syntax

show logging reverse [**timestamp** *YY/MM/DD hh:mm:ss*]

Parameter Description

timestamp: Configures the timestamp, that is, the end time of the logs to be queried.

YY: Year in the timestamp.

MM: Month in the timestamp.

DD: Day in the timestamp.

hh:mm:ss: Hour, minute, and second in the timestamp.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

- This command is used to display the log parameter configurations and log statistics as well as the log packets in the memory buffer. Log messages are displayed based on the timestamp from latest to earliest.

- The command is also used to display the logs from the current time to the input time. The log packets are displayed based on the timestamp from latest to earliest.

Examples

The following example displays log packets based on the timestamp from latest to earliest when the RFC5424 log format is not enabled.

```
Hostname> enable
Hostname# show logging reverse
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 15242 message lines logged,0 fail
    logging to  202.101.11.22
    logging to  192.168.200.112
Log Buffer (Total 131072 Bytes): have written 1336,
015492: *Sep 19 02:46:28: Hostname %LINEPROTO-UPDOWN: Line protocol on Interface
FastEthernet 0/24, changed state to up.
015491: *Sep 19 02:46:28: Hostname %LINK-UPDOWN: Interface FastEthernet 0/24,
changed state to up.
015490: *Sep 19 02:46:26: Hostname %LINEPROTO-UPDOWN: Line protocol on Interface
FastEthernet 0/24, changed state to down.
015489: *Sep 19 02:46:26: Hostname %LINK-UPDOWN: Interface FastEthernet 0/24,
changed state to down.
015488: *Sep 19 02:46:13: Hostname %LINEPROTO-UPDOWN: Line protocol on Interface
FastEthernet 0/24, changed state to up.
015487: *Sep 19 02:46:13: Hostname %LINK-UPDOWN: Interface FastEthernet 0/24,
changed state to up.
```

Table 1-1Output Fields of the show logging reverse Command with the RFC5424 Log Format Disabled

Field	Description
Syslog logging	Logging function ● "enabled" is displayed when the function is enabled. ● "disabled" is displayed when the function is disabled.
Console logging	Level of the logs displayed on the console as well as log statistics
Monitor logging	Level of the logs displayed in the VTY window as well as log statistics
Buffer logging	Level of the logs recorded in the memory buffer as well as log statistics

Field	Description
Standard format	Standard log format
Timestamp debug messages	Timestamp format of debugging information
Timestamp log messages	Timestamp format of logs
Sequence-number log messages	Sequence number function
Sysname log messages	Whether to enable the function of adding a system name to logs
Count log messages	Log statistics collection
Trap logging	Level of the logs sent to the syslog server as well as log statistics
Log Buffer	Log packets recorded in the memory buffer

The following example displays log packets based on the timestamp from latest to earliest when the RFC5424 log format is enabled.

```
Hostname> enable
Hostname# show logging reverse
Syslog logging: enabled
  Console logging: level debugging, 4740 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 4745 messages logged
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:3, Current send
index:3, Cycle:10 seconds
Count log messages: enable
  Trap logging: level informational, 2641 message lines logged,4155 fail
    logging to  192.168.23.89
    logging to  2000::1
  Delay-send logging: 2641 message lines logged
    logging to  192.168.23.89  by tftp
Log Buffer (Total 4096 Bytes): have written 4096, Overwritten 3292
<134>1 2013-07-24T12:29:34.343763Z Hostname SYS 6 SHELL_CMD [USER@4881 name=""]
[CMD@4881 task="rl_con" cmd="enable"]
<134>1 2013-07-24T12:29:33.410123Z Hostname SYS 6 SHELL_LOGIN [USER@4881 name=""
type="" from="console"] user login success.
<132>1 2013-07-24T12:20:32.250265Z Hostname CAPWAP 4 NO_IP_ADDR - No ip address
for capwap.
<135>1 2013-07-24T12:20:02.80343Z Hostname - 7 - Please config the IP address for
capwap.
<132>1 2013-07-24T12:20:02.80313Z Hostname CAPWAP 4 NO_IP_ADDR - No ip address
for capwap.
```

```
<135>1 2013-07-24T12:19:33.130290Z Hostname - 7 - Please config the IP address
for capwap.
```

Table 1-2Output Fields of the show logging reverse Command with the RFC5424 Log Format Enabled

Field	Description
Syslog logging	Logging function ● "enabled" is displayed when the function is enabled. ● "disabled" is displayed when the function is disabled.
Console logging	Level of the logs displayed on the console as well as log statistics
Monitor logging	Level of the logs displayed in the VTY window as well as log statistics
Buffer logging	Level of the logs recorded in the memory buffer as well as log statistics
Count log messages	Log statistics- function
Statistic log messages	Whether to enable periodical log reporting
Statistic log messages to terminal	Whether to enable periodical log reporting to the console and remote terminal
Delay-send file name	Name of the file that buffers delayed log reporting on the local device, currently written file index, and the interval of delayed log reporting
Trap logging	Level of the logs sent to the syslog server as well as log statistics
Delay-send logging	Address of the server for delayed log reporting, reporting mode, and statistics
Log Buffer	Log packets recorded in the memory buffer

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.42 terminal monitor

Function

Run the **terminal monitor** command to enable log display in the window of the current monitor terminal.

Run the **terminal no monitor** command to disable this feature.

Log display in the window of the current monitor terminal is disabled by default.

Syntax

terminal monitor

terminal no monitor

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is only used to configure a temporary attribute for the current VTY terminal. The temporary attribute is not stored permanently. After the VTY terminal session ends, the system will adopt the default configuration, and the temporary attribute will fail. This command is also run on the console but does not take effect.

Examples

The following example enables log display in the current VTY window.

```
Hostname> enable
Hostname# terminal monitor
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A