Contents

1 Configuring Syslog

1.1 Introduction

1.1.1 Overview

If link status change or events such as receiving of exception packets and processing exception occur during the device running, a log packet in a fixed format is generated automatically. A log packet can be added with a timestamp and a sequence number, classified by the log priority, and output to the console, monitor terminal, log server, or other media. Logs are used by administrators to monitor the running status of the device, analyze the network conditions, and locate problems.

1.1.2 Classification of System Logs

System logs fall into two types:

- Common logs
- Debugging logs

Note

To generate debugging logs, you need to enable a debug command. Such logs are used to locate problems, and may be ignored by users.

1.1.3 Levels of System Logs

Eight severity levels are defined for system logs in a descending order, including emergency, alert, critical, error, warning, notification, informational, and debugging, which correspond to eight numerical values from 0 to 7 respectively. A smaller value indicates a higher level. Table 1-1 describes the log levels.

Note

Only logs with a level equal to or higher than the specified level are output. For example, if the level of logs is set to informational (level 6), logs of level 6 or higher are output.

Table 1-1Description of Log Levels

Keyword	Level	Description
emergencies	0	Indicates that 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.

Keyword	Level	Description
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.
emergencies		

1.1.4 Output Direction of System Logs

System logs can be output to the console, monitor, server, buffer, and file. The default level and type of logs vary with the output direction. You can customize filtering rules for different output directions. Table 1-1 describes output directions of system logs.

Table 1-1Description of System Log Output Directions

Name of Output Direction	Default Output Direction	Default Output Level	Description
console	Console	debugging (Level 7)	Outputs logs and debugging information.
monitor	Monitor terminal	debugging (Level 7)	Outputs logs and debugging information to facilitate remote maintenance.
server	Log server	informational (Level 6)	Outputs logs and debugging information.
buffer	Log buffer	debugging (Level 7)	Outputs logs and debugging information. The log buffer is used to store system logs during the device running.
file	Log file	informational (Level 6)	Outputs logs and debugging information, and periodically writes logs in the log buffer into files.

1.1.5 RFC5424 Log Format

All system logs are in the following format regardless of their output directions:

```
<priority>version timestamp sysname MODULE LEVEL MNEMONIC [structured-data]
description
```

The log format is described below:

<Priority>version timestamp system name module name level mnemonic structured parameter area log content

For example, if you exit the configuration mode, the following log is displayed on the console:

```
<133>1 2013-07-24T12:19:33.130290Z orion_B26Q SYS 5 CONFIG - Configured from
console by console
```

The following details each field:

- priority

  The priority is calculated using the following formula: Facility × 8 + Level. "Level" indicates the log level and "Facility" indicates the facility value. The facility value can be set during log configuration. When the RFC5424 log function is enabled, the default facility value is local0 (16).

- version

  According to RFC5424, the version is always **1**.

- timestamp

  The timestamp records the generation time of a system log to help you check and locate system events. Orion_B26Q devices use the following uniform timestamp format when the RFC5424 logging function is enabled:

  ```
  YYYY-MM-DDTHH:MM:SS.SECFRACZ
  ```

  Table 1-1 describes each parameter.

Table 1-1Description of Timestamp Parameters

Timestamp Parameter	Parameter Name	Description
YYYY	Year	Indicates the year.
MM	Month	Indicates the month in the current year.
DD	Day	Indicates the day in the current month.
T	Separator	A date must end with "T".
HH	Hour	Indicates the hour.
MM	Minute	Indicates the minute.
SS	Second	Indicates the second.
SECFRAC	Millisecond	Indicates the millisecond (1–6 digits).
Z	End mark	Time must end with "Z".

- sysname (system name)

  This field indicates the name of the device that generates a log so that the log server can identify the host of such device.

- MODULE (module name)

  This field indicates the name of the module that generates a log. The value is an upper-case string of 2 to 20 characters, which can contain upper-case letters, digits, and underscores. The **module** field is mandatory for common logs by default, and optional for debugging logs.

- LEVEL (log level)

  Eight system log levels from 0 to 7 are defined. The level of system logs generated by each module is determined during development and cannot be changed.

- MNEMONIC

  This field indicates a summary of the generation of a log. The value is an upper-case string of 4 to 32 characters, which can contain upper-case letters, digits, and underscores. The **mnemonic** field is mandatory for common logs by default, and optional for debugging logs.

- structured-data (structured parameter area)

  This field is introduced to RFC5424, to describe log parameters in a way that helps device parsing. Each log can contain 0 or multiple parameters. If no parameter exists, the placeholder (-) must be used. Each parameter is in the following format:

  ```
  [SD_ID@enterpriseID PARAM-NAME=PARAM-VALUE]
  ```

  Table 1-2 describes each parameter.

Table 1-2Description of Structured Parameters

Structured Parameter	Parameter Name	Description
SD_ID	Name of parameter information	The name of parameter information is capitalized, and must be unique in a log.
@	Separator	"@enterpriseID" is necessary for the customized parameters, but not for parameters defined in RFC5424.
enterpriseID	Enterprise ID	The enterprise ID is maintained by the Internet Assigned Numbers Authority (IANA). The enterprise ID of orion_B26Q devices is 4881. You can query the enterprise ID at the official website of IANA.
PARAM-NAME	Parameter name	The parameter name is capitalized, and must be unique in the structured parameter area of a log.
PARAM-VALUE	Parameter value	The parameter value must be enclosed in double quotation marks. Values of the IP address and MAC address must be capitalized, and values of other parameters are capitalized as required.

- description (log text)

  This field indicates the content of a system log.

1.1.6 System Log Filtering

By default, the logs generated by the system are output in all directions. The device provides the log filtering function, which allows you to filter logs by log output direction, log keyword, and matching rule. When you do not care about some logs or you care about some logs only, use the log filtering function to filter the logs.

- Filtering direction

  Four log filtering directions are defined:

  - **buffer**: Filters the logs sent to the log buffer, that is, the logs displayed by the **show logging** command.
  - **file**: Filters the logs written into logging files.
  - **server**: Filters the logs sent to the log server.
  - **terminal**: Filters the logs sent to the console and monitor terminal (including telnet and SSH).

Note

The four filtering directions can be used either collectively (logs in various directions are filtered) or separately (logs in one direction are filtered).

- Filtering Mode

  Two filtering modes are available:

  - **contains-only**: Indicates that only the logs that contain keywords specified in the filtering rules are output. When you care about some logs only, you can apply the contains-only mode on the device to output only the logs that match the filtering rules on the terminal. Thus, you can check whether any event occurs.
  - **filter-only**: Indicates that the logs that contain keywords specified in the filtering rules are filtered and are not output. Too many logs from a module may result in spamming on the terminal CLI . If you do not care about this type of logs, you can apply the filter-only mode and configure filtering rules to filter such logs.

Note

The two filtering modes are mutually exclusive, that is, you can configure only one filtering mode at a time.

- Filtering Rule

  Two log filtering rules are available:

  - **exact-match**: If exact-match is selected, you must select all the three filtering options (log module, log level, and log mnemonic). To filter a specific log, use the exact-match filtering rule.
  - **single-match**: If single-match is selected, you only need to select one of the three filtering options (log module, log level, and log mnemonic). To filter a specified type of log, use the single-match filtering rule.

Note

If the same module name, log level, or mnemonic is configured in both the single-match and exact-match rules, the single-match rule prevails.

1.1.7 Log Reporting

The log reporting functions falls into level-based reporting, delayed reporting, and periodical reporting, which are described as follows:

- Level-based reporting

You can perform the level-based policy function to send logs of modules and severity levels to different destinations.

For example, you can configure a command to send OSPF module logs of level 4 or lower to the log server, and OSPF module logs of level 5 or higher to local log files.

- Delayed reporting

  Delayed log reporting means that instead of being directly sent to the log server, system logs generated in the system are buffered in the log files in the device and then periodically sent to the log server. Delayed log reporting can be configured to reduce the packet transmission and interaction frequency between the device and the log server. In this way, the performance pressure on the device and the log server and the burden of the intermediate network is reduced.

- Periodical reporting

  Logs about device performance statistics are periodically sent. All timers for periodically sending logs are managed by the syslog module. When a timer expires, the syslog module calls the log processing function registered by each module to display and output the performance statistic logs to the remote syslog server in real time. The server analyzes these logs to evaluate the device performance.

Caution

- To configure log reporting, enable the RFC5424 log format function; otherwise, you cannot configure level-based reporting, delayed reporting, and periodical reporting.
- When the RFC5424 log format is enabled, logs can be output in all directions, and delayed reporting is enabled by default. At the same time, the periodical reporting function is disabled.

1.1.8 Configuring System Log Monitoring

System log monitoring means that the system monitors external connections to the device and records logs.

- After user login/logout logging is enabled, the system records the user's connections to the device. The recorded information includes the login username and source address.
- After user operation logging is enabled, the system records device configuration changes. The recorded information includes the operation username, source address, and operation content.

1.1.9 Protocols and Standards

- RFC 3164: The BSD syslog Protocol
- RFC 5424: The_Syslog_Protocol

1.2 Configuration Task Summary

Syslog configuration includes the following tasks:

(1) Configuring Basic Syslog Features

(2) (Optional) Configuring the System Log Format.

(3) Configuring Log Reporting Configure at least one of the functions.

- Configuring Level-based Log Reporting

- Configuring Delayed Log Reporting
- (Optional) Configuring Periodical Log Reporting

(4) (Optional) Configuring System Log Monitoring

(5) (Optional) Configuring the Output Direction of System Logs. Configure at least one of the output directions.

- Configuring the Output of System Logs to the Console
- Configuring the Output of System Logs to the Monitor Terminal
- Configuring the Function of Writing System Logs into the Memory Buffer
- Configuring the Transmission of System Logs to the Log Server
- Configuring the Function of Writing System Logs into Log Files

(6) (Optional) Configuring System Log Filtering

(7) (Optional) Configuring System Log Redirection

(8) (Optional) Configuring Performance Logging Function

(9) (Optional) Configuring Synchronization of User Input and Log Output

1.3 Configuring Basic Syslog Features

1.3.1 Overview

This section describes how to enable the syslog function so that the system processes logs and users view the logs generated by the device.

1.3.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable logging.

logging on

By default, logging is enabled.

1.4 Configuring the System Log Format

1.4.1 Overview

By configuring system log display, you can adjust the display format of system logs.

1.4.2 Restrictions and Guidelines

- After the RFC5424 log format is enabled, a uniform timestamp format is adopted, and **uptime** and **datetime** are not differentiated.
- In the RFC5424 log format, the timestamp may or may not contain the time zone. Currently, only the timestamp without the time zone is supported.

1. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Set the system log format to the RFC5424 log format.

service log-format rfc5424

1.5 Configuring Log Reporting

1.5.1 Configuration Tasks

The log reporting configuration includes the following tasks. Configure at least one of the tasks.

- Configuring Level-based Log Reporting
- Configuring Delayed Log Reporting
- (Optional) Configuring Periodical Log Reporting

1.5.2 Restrictions and Guidelines

The log reporting function can be configured and takes effect only when the RFC5424 format is enabled.

1.5.3 Configuring Level-based Log Reporting

1. Overview

You can configure a level-based log reporting policy to output logs of different modules and severity levels to different destinations.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Set the system log format to the RFC5424 log format.

service log-format rfc5424

(4) Configure a level-based log reporting policy.

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

No level-based log reporting policy is configured by default.

1.5.4 Configuring Delayed Log Reporting

1. Overview

Delayed log reporting means that, instead of being directly sent to the log server, system logs generated in the system are buffered in the log files in the device and then periodically sent to the log server. Delayed log reporting can be configured for system logs to reduce the message transmission and interaction frequency between the device and the log server. In this way, the performance pressure on the device and the syslog server and the burden of the intermediate network is reduced.

2. Restrictions and Guidelines

- Generally, you are not advised to output logs reported in a delayed manner to the console or remote terminal. Otherwise, many logs reported in a delayed manner are displayed, increasing the burden on the device.
- The configured file name cannot contain any dot (.) because the system automatically adds the index and the file name extension (**.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 the file system of your PC, such as \, /, :, *, ", <, >, and |. For example, the configured file name is **log_server**, the current index is 5, the file size is 1000 bytes, and the source IP address of the device sending 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**.
- If few logs are generated on the device, you are advised to set the interval of delayed log reporting to a large value so that more logs are sent to the remote server at a time.
- By default, the log file sent to the remote server is named **File size_device IP address_index.txt**. If the name of the file for delayed log reporting is modified, the log file sent to the remote server is named **Configured file name prefix_file size_device IP address_index.txt**. The file stored on the local flash space of the device is named **Configured file name prefix_index.txt**. The default file name prefix is **syslog_ftp_server**, the interval for delayed log reporting is 3600s (1 hour), and the log file size is 128 KB.
- The maximum interval for delayed log reporting is 65535s (18 hours). If you set the interval for delayed log reporting to a larger value, the size of logs generated in this period may exceed the file size (128 KB). To prevent loss of logs, the logs are written into a new log file, and the index increases by 1. When the timer expires, all log files buffered in this period are sent to the log server at a time.
- The flash space for buffering local log files on the device is limited. Therefore, up to eight log files are buffered on the device. If more than eight log files are buffered on the device, all the log files generated earlier are sent to the log server at a time.
- You can send logs to the log server through File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP). The addresses of up to five log servers are configured for one device. Either FTP or TFTP is specified for each server.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Set the system log format to the RFC5424 log format.

service log-format rfc5424

(4) Configure delayed log reporting. The following configurations are optional. Configure at least one of them as actually needed.

- Configure delayed log reporting to the console and remote terminal.

  logging delay-send terminal

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

- Configure the name of the file for delayed log reporting.

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

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

- Configure the interval for delayed log reporting.

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

  The interval for delayed log reporting is 3600s (1 hour) by default.

- Configure the server address and reporting mode.

  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** }

  Delayed log reporting is disabled by default.

1.5.5 Configuring Periodical Log Reporting

1. Overview

This section describes how to configure periodical log reporting so that the server can collect all the logs on the device at the same time point.

2. Restrictions and Guidelines

- The interval of periodical log reporting and the function of outputting logs to the console and remote terminal take effect only after periodical log reporting is enabled.
- You are advised to disable the function of outputting periodically reported logs to the console and remote terminal. Otherwise, when the reporting timer expires, many performance statistics logs are displayed, increasing the burden on the device.
- To ensure that the server collects all performance statistics logs from the device at the same time point, the timers of all statistical objects are restarted when you modify the interval of one statistic object.
- The default interval of periodical log reporting is 15 minutes. To enable the server to collect all performance statistics logs from the device at the same time point, you need to set the log reporting interval of different

statistic objects to be a multiple of another interval . Currently, the interval can be set to 0, 15, 30, 60, or 120. Here, **0** indicates that periodical log reporting is disabled.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Set the system log format to the RFC5424 log format.

service log-format rfc5424

(4) Configure periodical log reporting.

logging statistic enable

Periodical log reporting is disabled by default.

(5) (Optional) Configure periodical log reporting to the console and remote terminal.

logging statistic terminal

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

(6) (Optional) Configure the interval for periodical log reporting.

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

The default interval of periodical log reporting is 15 min.

1.6 Configuring System Log Monitoring

1.6.1 Overview

System log monitoring enables the system to monitor the external connections to the device and record logs.

1.6.2 Restrictions and Guidelines

- If both the **logging userinfo** command and the **logging userinfo command-log** command are configured on the device, only the results shown by the **logging userinfo command-log** command are displayed when you run the **show running-config** command.
- The **logging userinfo** command is run in global configuration mode to enable login/logout logging. After this function is configured, the device displays logs when users access the devices through telnet, Secure Shell (SSH), or Hypertext Transfer Protocol (HTTP) so that the administrator monitors the device connection status.
- The **logging userinfo command-log** command is run in global configuration mode to enable user operation logging. After this function is configured, the system displays related logs to notify the administrator of configuration changes.
- User operations are logged when commands are configured and run. By default, the device does not generate operation logs when a user modifies the device configuration. If the 5424 log format is configured, that is, the **service log-format rfc5424** command is configured, you need to configure the **logging delay-send terminal** command so that operation logs are output to the terminal (because delayed log reporting is

registered for operation logs).

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure system log monitoring. The following configurations are all optional. Configure at least one of them as actually needed.

- Enable user login/logout logging.

  logging userinfo

  User login/logout logging is disabled by default.

- Enable user operation logging.

  logging userinfo command-log

  User operation logging is disabled by default.

1.7 Configuring the Output Direction of System Logs

1.7.1 Configuration Tasks

System log output direction configuration includes the following tasks. Configure at least one of the tasks.

- (Optional) Configuring the Output of System Logs to the Console
- (Optional) Configuring the Output of System Logs to the Monitor Terminal
- (Optional) Configuring the Function of Writing System Logs into the Memory Buffer
- (Optional) Configuring the Transmission of System Logs to the Log Server
- (Optional) Configuring the Function of Writing System Logs into Log Files

1.7.2 Configuring the Output of System Logs to the Console

1. Overview

This section describes how to configure the output of system logs to the console so that the device can output logs generated by the system to the console. Then, administrator can monitor the running status of the system.

2. Restrictions and Guidelines

- If too many system logs are generated, you can limit the logging rate to reduce logs output to the console.
- By default, system logging is enabled. You are advised not to disable it. If too many system logs are displayed, you can configure the level of logs to be displayed on different devices to reduce the logs displayed.
- The **logging count** command is run to enable the log statistics function in global configuration mode. After this function is enabled, the system records the number of times logs are generated by each module and

the generation time of the last log.

- The default level of logs that are displayed on the console is debugging (Level 7). You can run the **show logging config** command in privileged EXEC mode to display the level of logs that are displayed on the console.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable log statistics collection.

logging count

Log statistics collection is disabled by default.

(4) (Optional) Configure the level of logs that are output to the console.

logging console [*severity-level*]

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

(5) (Optional) Configure logging rate limiting.

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

Logging rate limiting is disabled by default.

1.7.3 Configuring the Output of System Logs to the Monitor Terminal

1. Overview

This section describes how to configure the output of system logs to the monitor terminal so that the device can output system logs to the remote monitor terminal. Then, the administrator can monitor the running status of the system.

2. Restrictions and Guidelines

- If too many system logs are generated, you can limit the logging rate to reduce logs output to the monitor terminal.
- By default, the current monitor terminal is not allowed to output logs after you remotely connect to the device. You need to manually run the **terminal monitor** command to allow the current monitor terminal to display logs. The **terminal monitor** command is valid only for the current connection. When the terminal reconnects to the device, the default settings of this command are restored**.**

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enable log display on the current monitor terminal.

terminal monitor

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

(3) Enter the global configuration mode.

configure terminal

(4) (Optional) Configure the level of logs to be output to the monitor terminal.

logging monitor [*severity-level*]

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

1.7.4 Configuring the Function of Writing System Logs into the Memory Buffer

1. Overview

This section describes how to configure the function of writing system logs into the memory buffer so that the device can write generated system logs into the memory buffer. Then, the administrator can view recent system logs by running the **show logging** command.

2. Restrictions and Guidelines

- If the buffer is full, earlier logs are overwritten when system logs are written into the memory buffer.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the parameters for the memory buffer, into which logs are to be written.

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

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

1.7.5 Configuring the Transmission of System Logs to the Log Server

1. Overview

This section describes how to configure the device to transmit generated system logs to the log server so that the administrator can monitor device logs on the server.

2. Restrictions and Guidelines

- The log timestamp or sequence number function must be enabled. Otherwise, the logs are not sent to the log server.
- If the device has an MGMT interface and is connected to the log server through the MGMT interface, you must add the **oob** option (indicating that system logs are sent to the log server through the MGMT interface) when configuring the **logging server** command. You can use the **via** parameter only when **oob** is specified in the command. In this case, **/vrf** is unavailable.
- The **logging server** command is used to specify the address of the log server that receives logs. You can specify multiple log servers, and logs are sent simultaneously to all these log servers.
- Up to five log servers are configured for a orion_B26Q product.

- When a domain name is entered to configure a log server, the **logging hostname** command is disabled.
- To track and manage logs, you can use the **logging source interface** 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 logs based on the unique address. If this source interface is not configured or the IP address is not configured for this source interface, the source IP address of log packets is the IP address of the interface that sends the log packets.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the transmission of logs to a specified log server.

(4) **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*] | { *ipv4-address* | **ipv6** *ipv6-address* } [**vrf** *vrf-name*] [**udp-prot** *port-number*] [**facility** *facility-type*] [**level** *inform-level*] }(Optional) Configure the level of logs that are sent to the log server.

logging trap [*severity-level*]

The default level of logs that are sent to the log server is 6 (informational messages).

(5) (Optional) Configure the facility value for logs to be sent to the log server.

logging facility *facility-type*

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

(6) (Optional) Configure the source interface for logs to be sent to the log server.

logging source interface *interface-type interface-number*

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

(7) (Optional) Configure the source address for logs to be sent to the log server.

- Configure an IPv4 source address for the logs to be sent to the log server.

  logging source ip *ipv4-address*

- Configure an IPv6 source address for the logs to be sent to the log server.

  logging source ipv6 *ipv6-address*

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

1.7.6 Configuring the Function of Writing System Logs into Log Files

1. Overview

This section describes how to configure the function of writing system logs into log files so that the device can save generated system logs to the log files for viewing. Logs are saved in a log file buffer before being saved

to the log file. The system writes the content in the log file buffer to the log file at the specified frequency, and you can also save the logs to a log file manually. After the logs are saved, the content in the log file buffer will be cleared. When logs need to be saved, the device automatically generates log files.

2. Restrictions and Guidelines

- System logs are not immediately written into log files. They are first buffered in the memory buffer, and then written into log files either periodically (at an interval of 1 hour by default) or when the buffer is full.
- When no log file is generated and the remaining space of the storage medium is insufficient, the device does not save the newly generated logs to a log file. Therefore, you must regularly clean up the storage space of the storage medium to ensure the log file function.
- The **logging file** command is used to create a log file with a specified file name on a specified file storage device. The file size increases with logs, but cannot exceed the configured value of **max-file-size**. If the value of **max-file-size** is not specified, the default size of a log file is 128 KB.
- After the **logging file** command is configured, the system saves logs to log files. A log file name does not contain any file type extension. The log file name extension is always **txt**, which cannot be changed.
- After this function is configured, logs will be written into log files at an interval of 1 hour. If you have run the **logging file flash:syslog** command, 16 log files are created, such as **syslog.txt**, **syslog_1.txt**, **syslog_2.txt**, …, **syslog_14.txt**, and **syslog_15.txt**. Logs are overwritten into the 16 log files in sequence and cyclically. For example, the system writes logs into **syslog_1.txt** after **syslog.txt** is fully occupied. When **syslog_15.txt** is fully occupied, logs are written into **syslog.txt** again.
- If no extended flash space is available, the **logging file flash** command is automatically hidden and is not configured. If no FLASH2 is available, the **logging file flash2** command is automatically hidden and is not configured. If FLASH2 is available and the **logging file flash** command is configured, logs are recorded in FLASH2.
- The system will not delete the generated log files after the number of log files is modified. Therefore, to save the space of 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 are 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 overwritten into 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 these log files as needed.
- After the time-based log storage is enabled, the system writes logs of the same level that are generated in the same day into the same log file. The log file is named **yyyy-mm-dd_filename_level.txt**, where **yyyy-mm-dd** indicates the absolute time of the day when the logs are generated, **filename** indicates the log file name configured by the **logging file flash** command, and **level** indicates the log level.
- After you specify the storage time for logs of a level, the system will delete the logs once the storage time expires. For better network management, the storage time ranges from 7 days to 365 days.
- If the time-based log storage is not enabled, logs are stored based on the file size to support old configuration commands.
- After the **logging flash flush** command is configured, the logs in the buffer are immediately written into a log file.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the parameters for the log file, into which logs are written.

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

(4) Configure the number of log files.

logging file numbers *file-numbers*

The default number of log files is 16.

(5) Configure the interval for writing logs into log files.

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

By default, logs are written into flash files at an interval of 3600s.

(6) Configure the storage time of logs written into log files.

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

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

(7) Configure the function of immediately writing logs in the buffer into log files.

logging flash flush

1.8 Configuring System Log Filtering

1.8.1 Overview

By default, all the logs generated by the system are displayed on the console or other terminals. By configuring log filtering, the network administrator can filter the generated system logs, select only the required logs to be displayed, or have the logs displayed on a specified terminal.

1.8.2 Restrictions and Guidelines

- Two filtering modes are available: **contains-only** and **filter-only**, which are mutually exclusive. You can configure only one filtering mode at a time.
- Log filtering rules fall into **exact-match** and **single-match**. The **single-match** rule prevails over the **exact-match** rule. If the same module, mnemonic, or information level is configured in both the **single-match** and **exact-match** rules, the logs complying with the **single-match** rule are filtered first.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the log filtering direction. The following configurations are optional. Select at least one of the configurations as actually needed.

- Configure the log filtering direction.

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

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

- Configure the log filtering mode.

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

  The filtering type is set to **filter-only** by default.

(4) Configure the log filtering rule.

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 log filtering rule is configured by default.

1.9 Configuring System Log Redirection

1.9.1 Overview

In a virtual switching unit (VSU) environment, you can configure the system log redirection function to redirect the logs of the slave device to the active device so that the network administrator can manage the logs uniformly.

1.9.2 Restrictions and Guidelines

- The system log redirection function is used in a VSU active-standby environment only, and does not apply to the standalone environment.
- You are advised to run the **logging rd rate-limit** command to limit the rate of the logs redirected to the active device. This is to limit the number of the logs that are redirected from the slave device to the active device per second. This prevents considerable logs on the slave device from burdening the system.
- In a VSU environment, logs on the slave device can be displayed in its console window, redirected to the active device for display in the console or virtual type terminal (VTY) window of the active device, or stored in the memory buffer of the active device, extended flash space or syslog server.
- In a VSU environment composed of box-type devices, after the log redirection function is enabled, logs on the slave or standby device will be redirected to the active device for output, and the role flag string "(*device ID)" will be added to the beginning of each log, to indicate that the log is a redirected log. Assume that four devices form a VSU. The ID of the active device is 1, the ID of the slave device is 2, and the IDs of two standby devices are 3 and 4. No role flag string is added to logs generated by the active device. The role flag string (*2) is added to logs redirected from the slave device to the active device. The role flag strings (*3) and (*4) are added respectively to logs redirected from the two standby devices to the active device.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the log redirection function.

logging rd on

(4) (Optional) Configure the rate limit on redirected logs.

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

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

1.10 Configuring Performance Logging Function

1.10.1 Overview

After the performance logging function is enabled, the logs that are output through the performance logging interface will be transmitted through the performance logging channel.

1.10.2 Restrictions and Guidelines

The performance logging function needs to be configured only when massive logs are displayed on the server within a short period. Only several functional services require this function.

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the performance logging function.

logging performance switch

The performance logging function is disabled by default.

1.11 Configuring Synchronization of User Input and Log Output

1.11.1 Overview

When the synchronization of user input and log output is enabled, even if logs are displayed during user input, the user input information is displayed after display, thereby ensuring the input integrity and continuity.

1.11.2 Restrictions and Guidelines

The **logging synchronous** command is configured in line configuration mode, and on each line that enables this function.

1.11.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Synchronize user input and log output.

logging synchronous

Synchronization of user input and log output is disabled by default.

1.12 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Caution

Running the **clear** commands may lose vital information and thus interrupt services.

Table 1-1Syslog Monitoring

Command	Purpose
clear logging	Clears logs in the memory buffer.
show logging	Displays log statistics and logs in the memory buffer based on the timestamp from earliest to latest.
show logging reverse	Displays log statistics and logs in the memory buffer based on the timestamp from latest to earliest.
show logging config	Displays system log configurations and statistics.
show logging count	Displays log statistics of each module in the system.

1.13 Configuration Examples

1.13.1 Configuring the RFC5424 Log Format

1. Requirements

The network administrator can check system logs to learn about the operation status of the device, better understand and manage the device, or locate problems.

2. Topology

Figure 1-1Topology for RFC5424 Log Format Configuration

3. Notes

- Configure the L3 network reachable between the device and the server.
- Enable logging
- Set the system log format to RFC5424 format.
- Configure log reporting.
  - Configure level-based log reporting.
  - Configure delayed log reporting.
  - Configure periodical log reporting.
- Configure log monitoring.
  - Configure the log statistics collection.
  - Set the rate of outputting system logs to the console to 50 logs per second.
  - Configure the display of logs on the monitor terminal.
- Synchronize user input and log output.
- Enable performance logging.
- Configure log filtering.
  - Set the filtering directions of logs to **terminal** and **server**.
  - Set the log filtering mode to **filter-only**.
  - Set the log filtering rule to **single-match** to filter the logs with a module name containing "SYS".
- Configure the output direction of system logs.
  - Configure the function of writing system logs into a log file named **syslog**.
  - Configure the transmission of system logs to the log server with the IPv4 address of 10.1.1.1.
  - Configure the size of the system logs to be written into the memory buffer to 128 KB (131072 bytes).

4. Procedure

(1) Configure the management IP address for the device.

```
Device> enable
Device# configure terminal
Device(config)#interface vlan 1
Device(config-if-VLAN 1)# ip address 10.1.1.2 255.255.255.0
Device(config-if-VLAN 1)# exit
```

(2) Enable logging

```
Device(config)# logging on
```

(3) Set the system log format to RFC5424 format.

```
Device(config)# service log-format rfc5424
```

(4) Configure log reporting.

Configure delayed log reporting.

```
Device(config)# logging delay-send terminal
Device(config)# logging delay-send interval 7200
Device(config)# logging delay-send file flash:syslog_orion_B26Q
Device(config)# logging delay-send server 192.168.23.12 mode ftp user admin
password admin
```

Configure level-based log reporting.

```
Device(config)# logging policy module SYS not-lesser-than 5 direction console
Device(config)# logging policy module SYS 3 direction buffer
```

Configure periodical log reporting.

```
Device(config)# logging statistic enable
Device(config)# logging statistic terminal
Device(config)# logging statistic mnemonic TUNNEL_STAT interval 30
```

(5) Configure log monitoring.

```
Device(config)# logging userinfo
Device(config)# logging userinfo command-log
```

Configure log statistics collection.

```
Device(config)# logging count
```

Configure the output of system logs to the console.

```
Device(config)# logging console informational
```

Set the rate of outputting system logs to the console to 50 logs per second.

```
Device(config)# logging rate-limit console 50
```

Configure the output of system logs to the monitor terminal.

```
Device(config)# logging monitor informational
Device(config)# line vty 0 4
Device(config-line)# monitor
```

(6) Synchronize user input and log output

```
Device(config-line)# logging synchronous
Device(config-line)# exit
```

(7) Enable performance logging.

```
Device(config)# logging performance switch
```

(8) Configure system log filtering.

Set the filtering directions of logs to **terminal** and **server**.

```
Device(config)# logging filter direction server
Device(config)# logging filter direction terminal
```

Set the log filtering mode to **filter-only**.

```
Device(config)# logging filter type filter-only
```

Set the log filtering rule to **single-match** to filter the logs with a module name containing "SYS".

```
Device(config)# logging filter rule single-match module SYS
```

(9) Configure the output direction of system logs.

Configure the function of writing system logs into a log file named **syslog**.

```
Device(config)# logging file flash:syslog debugging
Device(config)# logging flash interval 600
```

Configure the transmission of system logs to the log server with the IPv4 address of 10.1.1.1.

```
Device(config)# logging server 10.1.1.1
```

Configure the size of the system logs to be written into the memory buffer to 128 KB (131072 bytes).

```
Device(config)# logging buffered 131072 informational
```

5. Verification

(1) Run the **ping** command to check whether the L3 route between the server and the log server is reachable.

```
Device# ping 10.1.1.1
Sending 5, 100-byte ICMP Echoes to 10.1.1.1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms.
```

(2) Run the **show logging config** command to check the configuration result.

```
Device# show logging config
Syslog logging: enabled
  Console logging: level informational, 84 messages logged
  Monitor logging: level informational, 0 messages logged
  Buffer logging: level debugging, 92 messages logged
  File logging: level debugging, 105 messages logged
  File name:syslog.txt, size 128 Kbytes, the 1 file is currently being written
  Statistic log messages: enable
  Statistic log messages to terminal: enable
  Delay-send log messages to terminal: enable
  Delay-send file name:syslog_orion_B26Q, Current write index:0, Current send
index:0, Cycle:7200 seconds
  Count log messages: enable
  Trap logging: level debugging, 84 message lines logged,10 fail
    logging to  10.1.1.100
  Delay-send logging: 0 message lines logged
    logging to  10.1.1.1  by ftp
```

6. Configuration Files

Device configuration file

```
hostname Device
!
service log-format rfc5424
logging filter direction server
logging filter direction terminal
logging filter rule single-match module SYS
logging rate-limit console 50
logging count
```

```
logging userinfo command-log
logging buffered 131072 informational
logging file flash:syslog debugging
logging flash interval 600
logging console informational
logging monitor informational
logging facility local7
logging server 10.1.1.1
logging performance switch
logging policy module SYS not-lesser-than 5 direction console
logging policy module SYS 3 direction buffer
logging statistic enable
logging statistic terminal
logging statistic mnemonic TUNNEL_STAT interval 30
logging delay-send terminal
logging delay-send interval 7200
logging delay-send file flash:syslog_orion_B26Q
logging delay-send server 192.168.23.12 mode ftp user admin password admin
!
interface VLAN 1
 ip address 10.1.1.2 255.255.255.0
!
end
```