Syslog

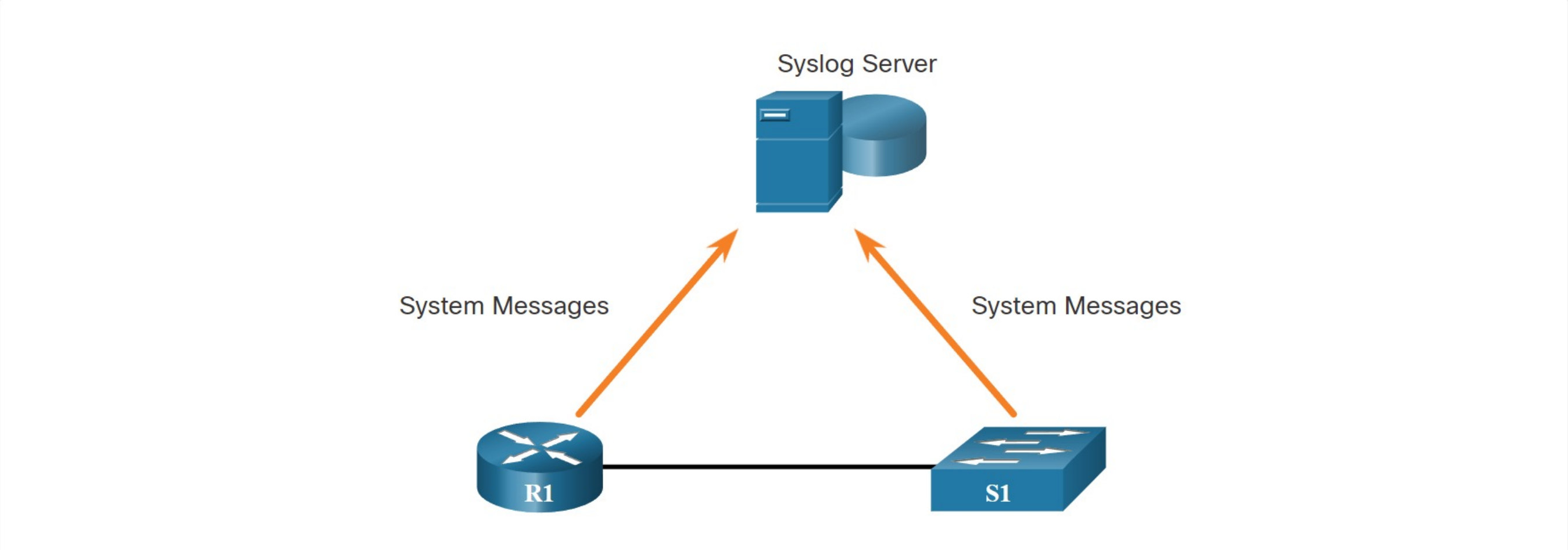
10.5.1

Introduction to Syslog

Like a Check Engine light on your car dashboard, the components in your network can tell you if there is something wrong. The syslog protocol was designed to ensure that you can receive and understand these messages. When certain events occur on a network, networking devices have trusted mechanisms to notify the administrator with detailed system messages. These messages can be either non-critical or significant. Network administrators have a variety of options for storing, interpreting, and displaying these messages. They can also be alerted to those messages that could have the greatest impact on the network infrastructure.

The most common method of accessing system messages is to use a protocol called syslog.

Syslog is a term used to describe a standard. It is also used to describe the protocol developed for that standard. The syslog protocol was developed for UNIX systems in the 1980s but was first documented as RFC 3164 by IETF in 2001. Syslog uses UDP port 514 to send event notification messages across IP networks to event message collectors, as shown in the figure.



Many networking devices support syslog, including: routers, switches, application servers, firewalls, and other network appliances. The syslog protocol allows networking devices to send their system messages across the network to syslog servers.

There are several different syslog server software packages for Windows and UNIX. Many of them are freeware.

The syslog logging service provides three primary functions, as follows:

- The ability to gather logging information for monitoring and troubleshooting
- The ability to select the type of logging information that is captured
- The ability to specify the destinations of captured syslog messages

10.5.2

Syslog Operation

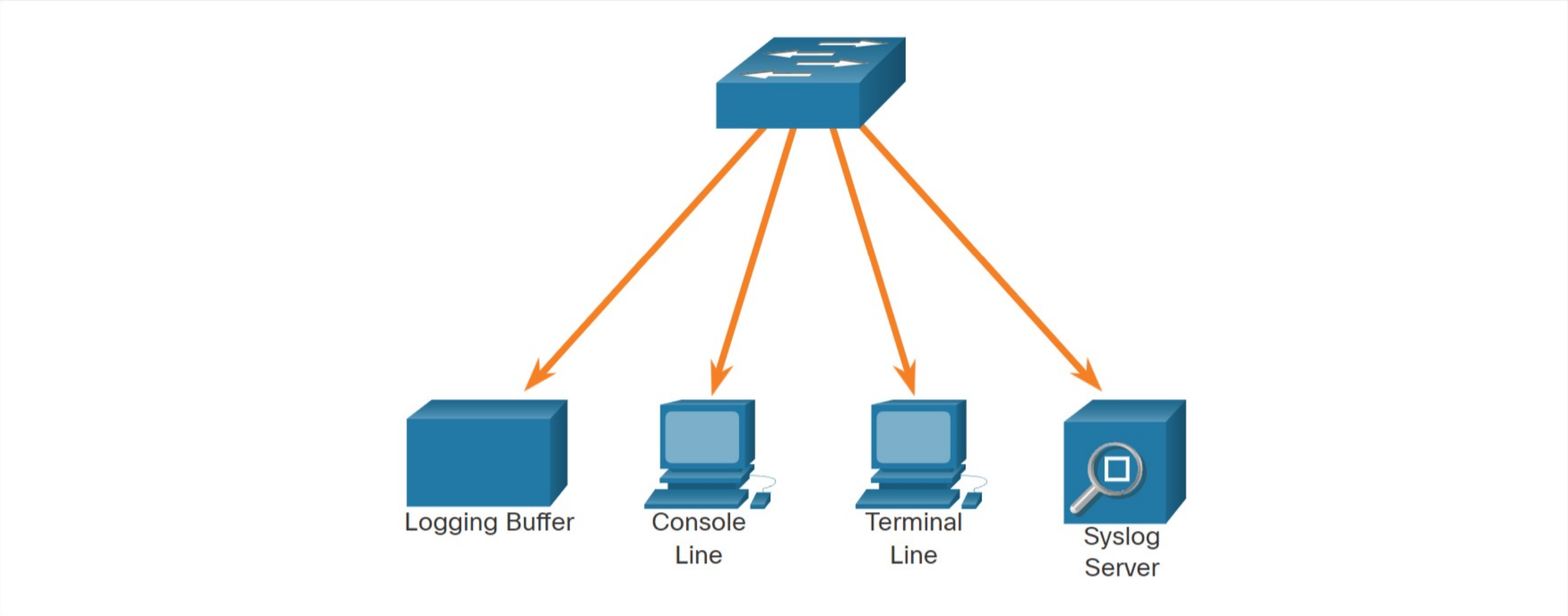
On Cisco network devices, the syslog protocol starts by sending system messages and **debug** output to a local logging process that is internal to the device. How the logging process manages these messages and outputs is based on device configurations. For example, syslog messages may be sent across the network to an external syslog server. These messages can be retrieved without needing to access the actual device. Log messages and outputs stored on the external server can be pulled into various reports for easier reading.

Alternatively, syslog messages may be sent to an internal buffer. Messages sent to the internal buffer are only viewable through the CLI of the device.

Finally, the network administrator may specify that only certain types of system messages be sent to various destinations. For example, the device may be configured to forward all system messages to an external syslog server. However, debug-level messages are forwarded to the internal buffer and are only accessible by the administrator from the CLI.

As shown in the figure, popular destinations for syslog messages include the following:

- Logging buffer (RAM inside a router or switch)
- Console line
- Terminal line
- Syslog server



It is possible to remotely monitor system messages by viewing the logs on a syslog server, or by accessing the device through Telnet, SSH, or through the console port.

10.5.3

Syslog Message Format

Cisco devices produce syslog messages as a result of network events. Every syslog message contains a severity level and a facility.

The smaller numerical levels are the more critical syslog alarms. The severity level of the messages can be set to control where each type of message is displayed (i.e. on the console or the other destinations). The complete list of syslog levels is shown in the table.

Severity Name	Severity Level	Explanation
Emergency	Level 0	System Unusable
Alert	Level 1	Immediate Action Needed
Critical	Level 2	Critical Condition
Error	Level 3	Error Condition
Warning	Level 4	Warning Condition
Notification	Level 5	Normal, but Significant Condition
Informational	Level 6	Informational Message
Debugging	Level 7	Debugging Message

Each syslog level has its own meaning:

- **Warning Level 4 - Emergency Level 0**: These messages are error messages about software or hardware malfunctions; these types of messages mean that the functionality of the device is affected. The severity of the issue determines the actual syslog level applied.
- **Notification Level 5**: This notifications level is for normal, but significant events. For example, interface up or down transitions, and system restart messages are displayed at the notifications level.
- **Informational Level 6**: This is a normal information message that does not affect device functionality. For example, when a Cisco device is booting, you might see the following informational message: %LICENSE-6-EULA_ACCEPT_ALL: The Right to Use End User License Agreement is accepted.
- **Debugging Level 7**: This level indicates that the messages are output generated from issuing various **debug** commands.

10.5.4

Syslog Facilities

In addition to specifying the severity, syslog messages also contain information on the facility. Syslog facilities are service identifiers that identify and categorize system state data for error and event message reporting. The logging facility options that are available are specific to the networking device. For example, Cisco 2960 Series switches running Cisco IOS Release 15.0(2) and Cisco 1941 routers running Cisco IOS Release 15.2(4) support 24 facility options that are categorized into 12 facility types.

Some common syslog message facility codes reported on Cisco IOS routers include:

- **IF** - Identifies that the syslog message was generated by an interface.
- **IP** - Identifies that the syslog message was generated by IP.
- **OSPF** - Identifies that the syslog message was generated by the OSPF routing protocol.
- **SYS** - Identifies that the syslog message was generated by the device operating system.
- **IPSEC** - Identifies that the syslog message was generated by the IP Security encryption protocol.

By default, the format of syslog messages on the Cisco IOS Software is as follows:

```
%facility-severity-MNEMONIC: description
```

For example, sample output on a Cisco switch for an EtherChannel link changing state to up is:

```
%LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

Here the facility is LINK and the severity level is 3, with a MNEMONIC of UPDOWN.

The most common messages are link up and down messages, and messages that a device produces when it exits from configuration mode. If ACL logging is configured, the device generates syslog messages when packets match a parameter condition.

10.5.5

Configure Syslog Timestamp

By default, log messages are not timestamped. In the example, the R1 GigabitEthernet 0/0/0 interface is shutdown. The message logged to the console does not identify when the interface state was changed. Log messages should be timestamped so that when they are sent to another destination, such as a Syslog server, there is record of when the message was generated.

Use the command **service timestamps log datetime** to force logged events to display the date and time. As shown in the command output, when the R1 GigabitEthernet 0/0/0 interface is reactivated, the log messages now contain the date and time.

```
R1# configure terminal
R1(config)# interface g0/0/0
R1(config-if)# shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to down
R1(config-if)# exit
R1(config)# service timestamps log datetime
R1(config)# interface g0/0/0
R1(config-if)# no shutdown
*Mar  1 11:52:42: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to down
*Mar  1 11:52:45: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
*Mar  1 11:52:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
changed state to up
R1(config-if)#
```

Note: When using the **datetime** keyword, the clock on the networking device must be set, either manually or through NTP, as previously discussed.

10.5.6

Check Your Understanding - Syslog Operation

Refer to the following syslog output to answer the questions.

```
*Jun 12 17:46:01.619: %IFMGR-7-NO_IFINDEX_FILE: Unable to open nvram:/ifIndex-table No such file or directory
```

1. **Refer to the syslog output.** What security level generated the message?

○ Error
○ Informational
○ Warning
● Debugging

2. **Refer to the syslog output.** What is the mnemonic for this syslog message?

○ IFMGR
○ Unable to open nvram
● NO_IFINDEX_FILE
○ ifIndex-table

3. **Refer to the syslog output.** What is the syslog reporting facility?

● IFMGR
○ NO_IFINDEX_FILE
○ IFMGR-7
○ ifIndex-table

Check

Show Me

Reset

10.4 SNMP

10.6 Router and Switch File Maintenance