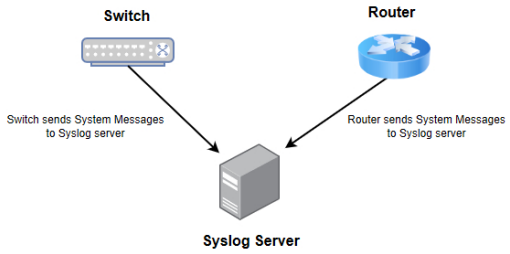
Syslog

Actions on many devices generate events that are logged locally for analysis, such as shutdowns, start-ups, processes, and connections. When you have a large number of devices, it becomes impractical to review these locally. System Logging Protocol (Syslog) is a standard protocol used to convey event or system log notification messages to a designated server, known as a Syslog server. The Syslog server centralizes data collection from various devices for analysis, review, and intervention. The Syslog protocol is outlined by RFC 5424.

The protocol can be enabled on most network equipment such as switches, routers and firewalls, and even endpoint devices. Syslog is available on Unix and Linux based systems and many web servers. Windows systems use their own by default as opposed to Syslog (Windows Event Manager – we'll cover this in the next lesson), these can also be forwarded to a central server, via third-party utilities or other configurations using the Syslog protocol.

Syslog uses **UDP 514** by default; TCP **514** can be used for more reliability; however, certain stricter security standards require that logs are securely transferred, so **TCP 6514** is used as a de facto standard, although not official. Take note that Syslog does not offer authentication or encryption built-in, so it may be susceptible to attacks.



Complete network monitoring requires using multiple tools. Syslog is an important pillar in network monitoring because it ensures that events occurring without a dramatic effect do not fall through the cracks. Best practice is to use a software that combines all the tools to always have an overview of what is happening in the network.

SYSLOG MESSAGES

A Syslog message is made of three components; a Priority Value (PRI), a Header, and a Message. We will explain these three parts below.

Priority Value (PRI)

The Priority Value is derived from both the **Facility Code** and the **Severity Level.** We can use the simple equation to calculate PRI:

```
(facility code * 8) + Severity value = PRI.
```

Below are the Facility Code and Severity Level tables.

Facility Code

Number	Facility description
0	Kernel messages
1	User-level messages
2	Mail system

2	Mail System
3	System Daemons
4	Security/Authorization Messages
5	Messages generated by syslog
6	Line Printer Subsystem
7	Network News Subsystem
8	UUCP Subsystem
9	Clock Daemon
10	Security/Authorization Messages
11	FTP Daemon
12	NTP Subsystem
13	Log Audit
14	Log Alert
15	Clock Daemon
16 - 23	Local Use 0 - 7

Severity Levels

Value	Severity	Keyword	Description	Condition
0	Emergency	`emerg`	System is unusable	A panic condition.
1	Alert	`alert`	Action must be taken immediately	A condition that should be corrected immediately, such as a corrupted system database.
2	Critical	`crit`	Critical conditions	Hard device errors.
3	Error	`err`	Error conditions	
4	Warning	`warning`	Warning conditions	
5	Notice	`notice`	Normal but significant conditions	Conditions that are not error conditions, but that may require special handling.
6	Informational	`info`	Informational messages	
7	Debug	`debug`	Debug-level messages	Messages that contain information normally of use only when debugging a program.

Header

This contains identifying information, such as; Timestamp, Hostname, Application name, Message ID. This is useful for understanding where the system message has come from.

Message

This could be simple readable text or only machine-readable. The content of the message is not defined by the protocol only the format is. Each message sent to the Syslog server has two labels associated with it that make the message easier to handle. The first label describes the function (facility) of the application that generated it. For example, mail servers typically log using the **mail** facility. The second label specifies the severity level. After these two labels, the action in specified. The action is usually a filename in the **/var/log** directory tree, in which the messages will be stored.

Previous Topic
Mark Complete
Next Topic
Back to Lesson