Syslog is a standard for sending and receiving notification messages–in a particular format–from various network devices. The messages include time stamps, event messages, severity, host IP addresses, diagnostics and more. In terms of its built-in severity level, it can communicate a range between level 0, an Emergency, level 5, a Warning, System Unstable, critical and level 6 and 7 which are Informational and Debugging.

Moreover, Syslog is open-ended. Syslog was designed to monitor network devices and systems to send out notification messages if there are any issues their functionality–it also sends out alerts for pre-defined events and monitors suspicious activity via the change log/event log of participating network devices.

The Syslog protocol is defined in RFC 3164. The messages are sent across IP networks to the event message collectors or syslog servers. Syslog uses the User Datagram Protocol (UDP), port 514, to communicate. Although, syslog servers do not send back an acknowledgment of receipt of the messages. Since 2009, syslog has been standardized by the IETF in RFC 5424.

All network devices such as routers, servers, firewalls, etc. create or prompt logs about statuses and the events that occur. For a small system tracking these logs is not a problem, the problem arises when we are dealing with big systems where tracking all these logs and information becomes challenging. To overcome this problem we use Syslog with a logging server known as Syslog server (such as Kiwi Syslog server, Graylog, Solarwind Syslog server, etc.).

A Syslog server allows us to send the log information of all our network devices to one centralized place. The log messages are sent on UDP port 514 to the Syslog server. From here we can search, manage and archive all of the log information.

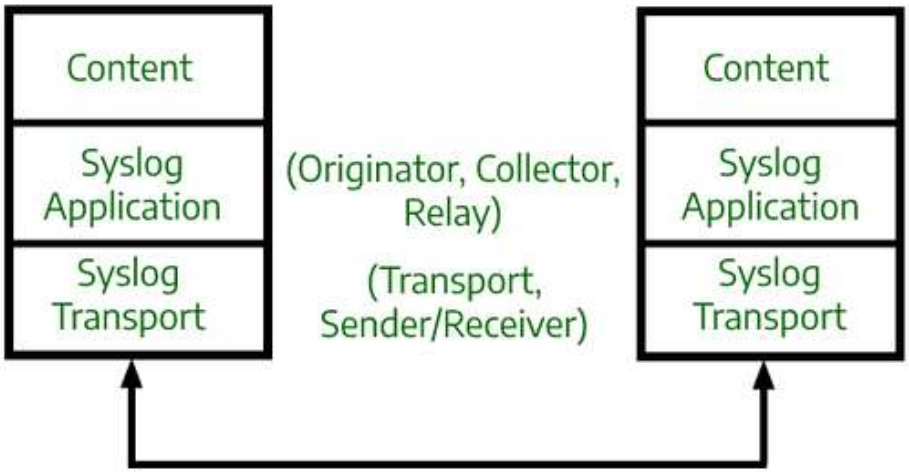
A wide variety of devices supports the Syslog protocol hence, it can be used to log various types of events like logs from a web server, a router, etc.

What is Syslog?

Syslog is a standard protocol for message logging that computer systems use to send event logs to a Syslog server for storage. On network devices, Syslog can be used to log events such as changes in interface status, system restarts, etc. A lot of different types of events can be logged. Logs are essential when troubleshooting issues, examining the cause of incidents, etc.

Working :
Syslog standard defines three layers i.e., the Syslog transport layer, Syslog application layer, and Syslog content layer.

1. **Syslog content layer –**
   It is the actual data contained in the event message. It contains some informational elements such as the facility codes and severity levels.
2. **Syslog Application layer –**
   This layer generates, interprets, routes, and stores the message.
3. **Syslog Transport layer –**
   This layer transmits the message over a network.



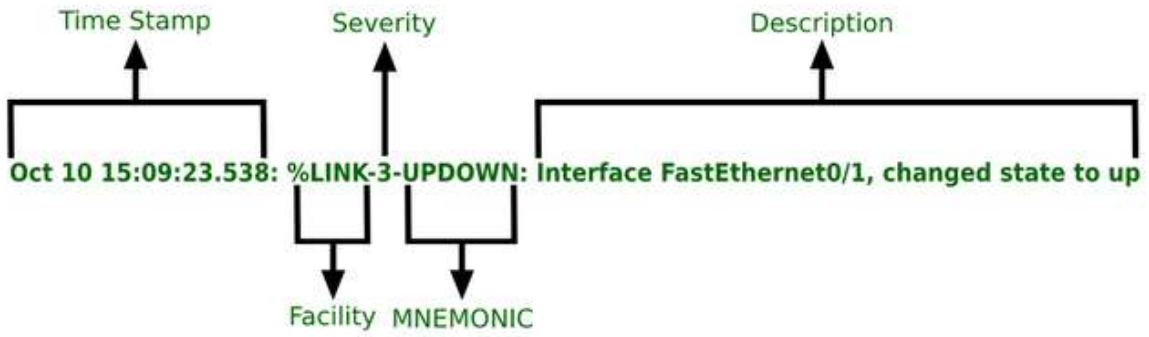
Syslog Layers

Syslog message format :
`seq:timestamp: %facility-severity-MNEMONIC:description`

seq may or may not be shown in the actual Syslog message.

1. **seq –** A sequence number indicating the sequence/order of a message.
2. **timestamp –** A timestamp indicates at what time the message was generated.
3. **facility –** A value that indicates which process on the device generated this message.
4. **severity –** A number that indicates the severity of the logged event. There are 8 severity levels.
5. **MNEMONIC –** A shortcode for the message, indicating what happened.

6. **description –** Detailed information about the event being reported.



Example of Syslog Message Format

This is a log message that can be seen while configuring routers and switches.

Syslog facility Codes :

Code	Keyword	Description
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth	security/authorization messages
5	syslog	messages generated internally by Syslog

6	lpr	line printer subsystem
7	news	network news subsystem
8	uucp	UUCP subsystem
9	cron	clock daemon
10	authpriv	security/authorization messages
11	ftp	FTP daemon
12	ntp	NTP subsystem
13	security	log audit
14	console	log alert
15	solaris-cron	clock daemon
16-23	local	local use 0-7 (local0-7)

At the bottom we have codes from 16-23 for local use, these are generally used for network devices.

Syslog Severity levels :

This is important because if we don't have severity values it would send all the log messages to the server altogether which is not recommended as it would clog the server. With the help of the severity level, we can choose which messages are sent based on their severity.

Level	Keyword	Description
0	Emergency	System is unusable

1	Alert	Action must be taken immediately
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant condition(Notifications)
6	Informational	Informational messages
7	Debugging	Debug-level messages

There are 8 severity levels, each severity level has a number, 0 being the most severe and 7 being the least severe. Each level also has a keyword, which is a name that identifies the severity level. Then there is a brief description of the severity level.

1. Level 0, emergency, events that render the system unusable.
2. Level 1, alert, is for events for which action must be taken immediately. So, these are also very urgent/serious events.
3. Level 2 is called critical, and the description is simply ‘critical conditions’. Same
4. Level 3, error.
5. Level 4, warning.
6. Level 5, notice/notification, is used for messages representing a ‘normal but significant condition’.
7. Level 6 is ‘Informational’, and then finally
8. Level 7, is Debugging. These are the least severe messages.

Syslog server :
Syslog servers are used to collect Syslog messages from multiple sources into a single location. A Syslog server can be a physical server or a virtual machine. Few components make it possible for Syslog servers to receive, store and interpret the messages.

1. **Syslog listener –**
   Syslog listener allows the server to receive messages sent over the network by gathering Syslog data sent over port 514 of UDP as UDP messages are not acknowledged or unreliable, hence some

network devices might send Syslog data through TCP to ensure message delivery.

2. **Database –**
   As large networks generate a lot of Syslog data they need to be able to store the Syslog data for quick retrieval and easy reference.
3. **Automation and Filtering –**
   It is hard to find specific log entries in a large amount of data. A Syslog server allows you to collect as well as filter the logs.

Need of logs :

1. Log information is very important and helpful when we are troubleshooting problems. For example – Let’s say some users report a network outage as it happened in recent Facebook, WhatsApp, and Instagram outage, then we can just go through all the log information to see if there were any issues.
2. Another benefit of storing log information in a central place is data retention.
3. It can provide transient information which is needed to return the system prior status after a failure.