

Protocol Information

A standard for message logging that allows applications and systems to send log messages to a centralized location for storage, analysis, and monitoring. Syslog uses **UDP port 514!**

Syslog Message Format

seq no: timestamp: %facility-severity-MNEMONIC: description

This is the the standard format for syslog messages, often used in **Cisco devices**

Breakdown of the Syslog message format

seq no	represents the sequence number
timestamp	the date and time of the event
facility	represents what the log message is referring to
severity	severity code in the range 0 to 7
MNEMONIC	short code for the message
description	brief description of the event

Syslog Severity Levels

Severity	Description	Numerical code
Emergency	System is unusable	0
Alert	Action must be taken immediately	1
Critical	Critical conditions	2
Error	Error conditions	3
Warning	Warning conditions	4
Notice	Normal but significant condition	5
Informational	Informational messages	6
Debug	Debug-level messages	7

Example of message generated by a Cisco router

```
*Mar 28 12:12:12.312: %LINEPROTO-5-UPDOWN: Line
protocol on Interface GigabitEthernet0/1, changed
state to down
```

References and Further reading

RFC 5424
Configuring Syslog

Syslog Message Facilities

Numerical code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslogd
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 (note 2)
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

Calculation of Priority

*Priority = Facility*8 + Severity**

For example, a kernel message (Facility=0) with a Severity of Emergency (Severity=0) would have a Priority value of 0.



