Tuesday, July 29, 2025 1:24 AM

SYSLOG

SYSLOG OVERVIEW

- SYSLOG is an INDUSTRY-STANDARD PROTOCOL for message logging
- On NETWORK DEVICES, SYSLOG can be used to LOG EVENTS
  - Changes in INTERFACE status (UP / DOWN)
  - Changes in OSFP NEIGHBOUR STATUS (UP / DOWN)
  - System Restarts
  - etc…
- The messages can be displayed in the CLI, saved in the DEVICE'S RAM or sent to an external SYSLOG SERVER

- Logs are essential when troubleshooting issues, examining the cause of incidents, etc.
- SYSLOG and SNMP are both used for MONITORING and TROUBLESHOOTING of DEVICES. They are complementary, but their functionalities are different

SYSLOG MESSAGE FORMAT

seq: time stamp: %facility-severity-MNEMONIC:description

💡 These TWO FIELDS may or may not be displayed, depending on the DEVICE'S configuration

seq = A SEQUENCE NUMBER indicating the order / sequence of messages

time stamp = A TIMESTAMP indicating the time the message was generated

facility = A VALUE that indicates which process on the DEVICE generated the message

severity = A NUMBER that indicates the severity of a logged event.

Official RFC for SYSLOG severity levels

💡 LEVELS and KEYWORDS need to be MEMORIZED for the CCNA

Syslog Severity Levels

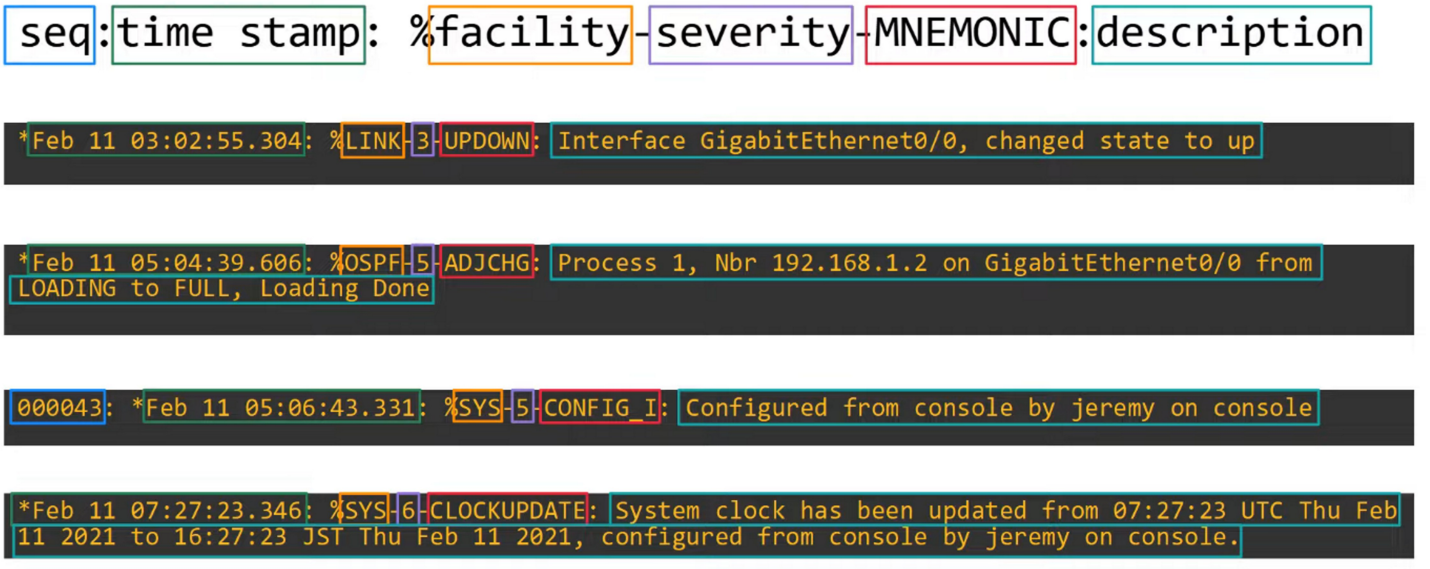
Level	Keyword	Description
0	**Emergency**	System is unusable
1	**Alert**	Action must be taken immediately
2	**Critical**	Critical conditions
3	**Error**	Error conditions
4	**Warning**	Warning conditions
5	**Notice**	Normal but significant condition (**Notification**)
6	**Informational**	Informational messages
7	**Debugging**	Debug-level messages

💡 MEMORIZATION MNEMONIC : (E)very (A)wesome (C)isco (E)ngineer (W)ill (N)eed (I)ce cream (D)aily

MNEMONIC = A SHORT CODE for the message, indicating what happened

description = Detailed information about the EVENT being reported

Syslog Message Examples



SYSLOG LOGGING LOCATIONS

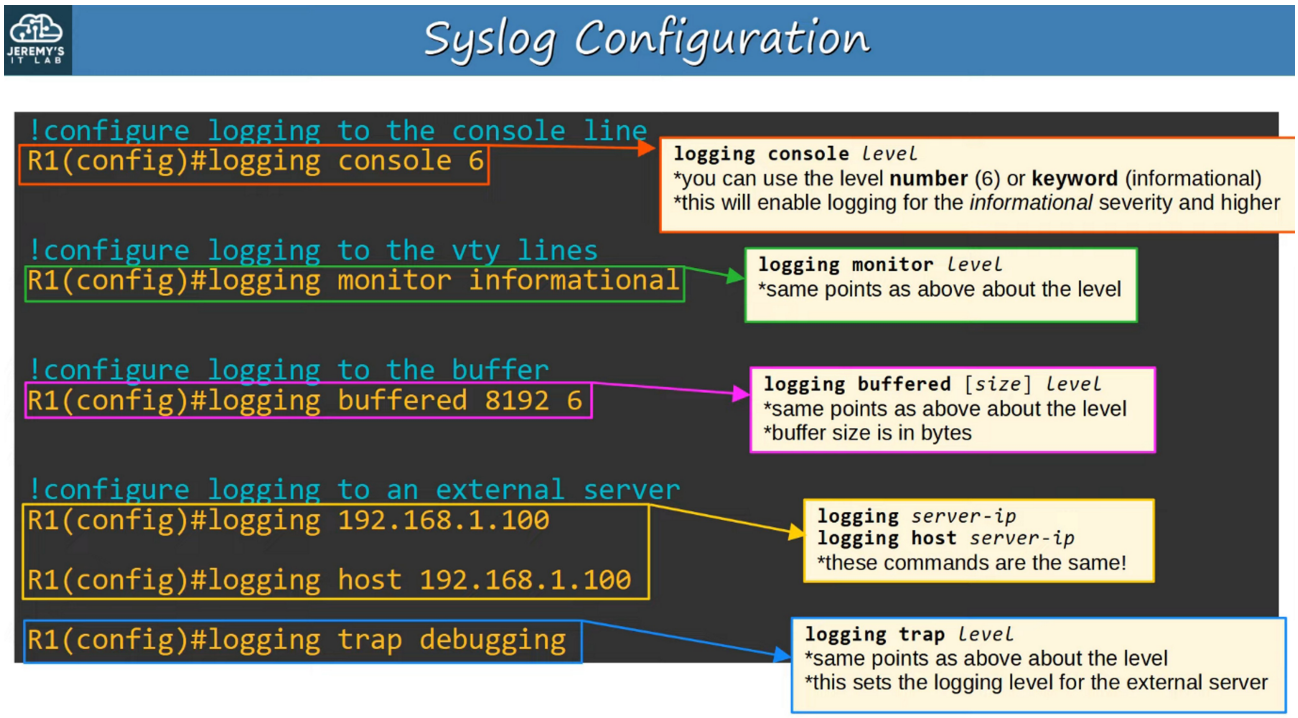
- CONSOLE LINE
  - SYSLOG messages will be displayed in the CLI when connected to the DEVICE via the CONSOLE port. By DEFAULT, all messages (Level 0-7) are displayed
- BUFFER
  - Syslog messages will be saved to RAM. By default, ALL messages (Level 0-7) are displayed
- VTY LINES

- SYSLOG messages will be displayed in the CLI when connected to the DEVICE via Telnet/SSH (coming in a later video). Disabled by default.

- EXTERNAL SERVER
  - You can configure the DEVICE to send SYSLOG messages to an external server

** SYSLOG SERVERS will listen for messages on UDP PORT 514 **

SYSLOG CONFIGURATION



level works from the chosen level and upward toward Level 0 (EMERGENCY)

level or keyword from the Severity Table works when choosing a level

TERMINAL MONITOR

- Even if logging monitor level is enabled, by default SYSLOG messages will not be displayed when connected via Telnet or SSH
- For the messages to be displayed, you must use the following command:
  - R1# terminal monitor
- The command must be used every time you connect to the DEVICE via Telnet or SSH

LOGGING SYNCHRONOUS

- By default, logging messages displayed in the CLI while you are in the middle of typing a command will result in something like this:

```
R1(config)#exit
R1#show ip in
*Feb 11 09:38:41.607: %SYS-5-CONFIG_I: Configured from console by jeremy on
consoleterface brief
```

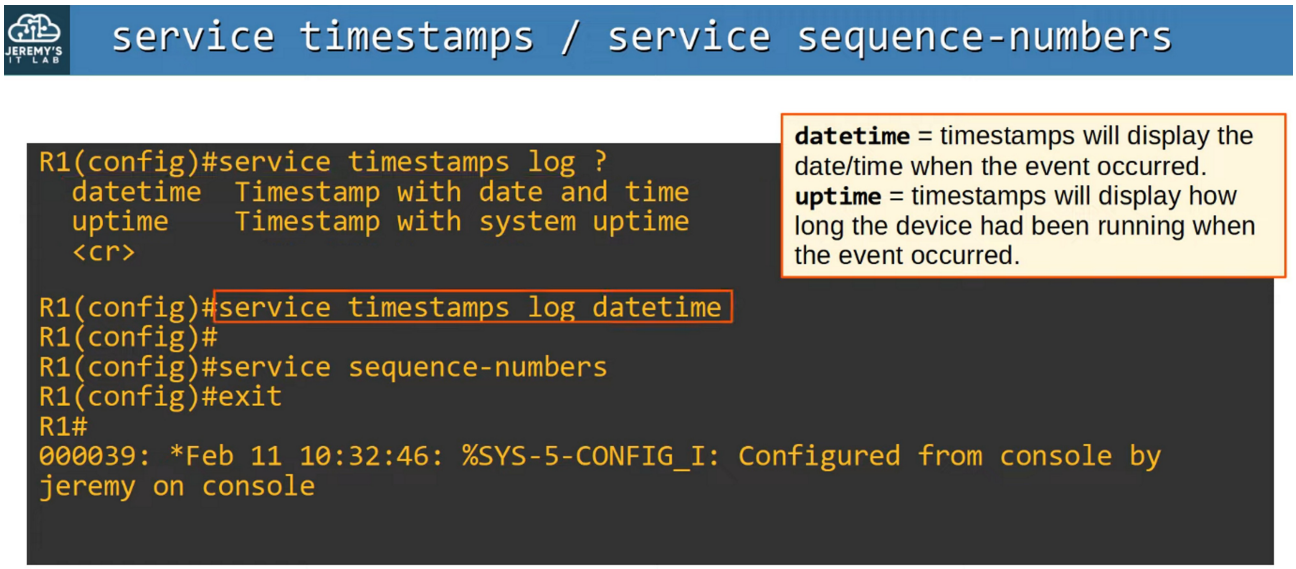
- To prevent this, you should use logging synchronous on the appropriate *line*

```
R1(config)#line console 0
R1(config-line)#logging synchronous
```

- This will cause a new line to be printed if your typing is interrupted by a message

```
R1(config)#exit
R1#show ip int
*Feb 11 09:41:00.554: %SYS-5-CONFIG_I: Configured from console by jeremy on console
R1#show ip int
```

SERVICE TIMESTAMPS and SERVICE SEQUENCE-NUMBERS



SYSLOG versus SNMP

- SYSLOG and SNMP are both used for MONITORING and TROUBLESHOOTING of DEVICES. They are COMPLIMENTARY, but their FUNCTIONALITIES are different.
- SYSLOG
  - Used for MESSAGE LOGGING
  - Events that occur within the system are categorized based on FACILITY / SEVERITY and LOGGED
  - Used for SYSTEM MANAGEMENT, ANALYSIS, and TROUBLESHOOTING
  - Messages are sent from the DEVICES to the SERVER.
    - The SERVER can't actively pull information from the DEVICES (like SNMP 'get') or modify variables (like SNMP 'set')
- SNMP
  - Used to retrieve and organize information about the SNMP managed DEVICES
    - IP ADDRESSES
    - Current INTERFACE status
    - Temperature
    - CPU Usage
    - etc…
  - SNMP SERVERS can use Get to query the CLIENTS and Set to MODIFY variables on the CLIENTS