# **41. SYSLOG**

## **SYSLOG OVERVIEW**

* SYSLOG is an **industry-standard protocol** for message logging.
* On **network devices**, SYSLOG can be used to **log events**, such as:
  + Changes in **interface status** (UP / DOWN)
  + Changes in **OSPF neighbor status** (UP / DOWN)
  + **System restarts**
  + Other significant network events
* Messages can be **displayed in the CLI**, **saved in the device’s RAM**, or **sent to an external SYSLOG server**.
* Logs are essential for **troubleshooting issues**, **examining incident causes**, and **monitoring system health**.
* **SYSLOG and SNMP** are complementary tools for **monitoring and troubleshooting** devices, but they serve different purposes.

## **SYSLOG MESSAGE FORMAT**

**Format:** seq: timestamp: %facility-severity-MNEMONIC: description

💡 **Note:** These two fields may or may not be displayed, depending on the device’s configuration.

* **seq** – A sequence number indicating the order of messages.
* **timestamp** – A timestamp indicating when the message was generated.
* **facility** – Identifies which process on the device generated the message.
* **severity** – A numerical value indicating the severity of the event.

### **SYSLOG Severity Levels (RFC Standard)**

| **Level** | **Keyword** | **Description** |
| --- | --- | --- |
| 0 | Emergency | System is unusable |
| 1 | Alert | Immediate action required |
| 2 | Critical | Critical condition |
| 3 | Error | Error condition |
| 4 | Warning | Warning condition |
| 5 | Notice | Normal but significant event |
| 6 | Informational | Informational messages |
| 7 | Debug | Debugging messages |

💡 **Mnemonic for memorization:** (E)very (A)wesome (C)isco (E)ngineer (W)ill (N)eed (I)ce cream (D)aily

* **MNEMONIC** – A short code indicating what happened.
* **description** – Detailed information about the event being reported.

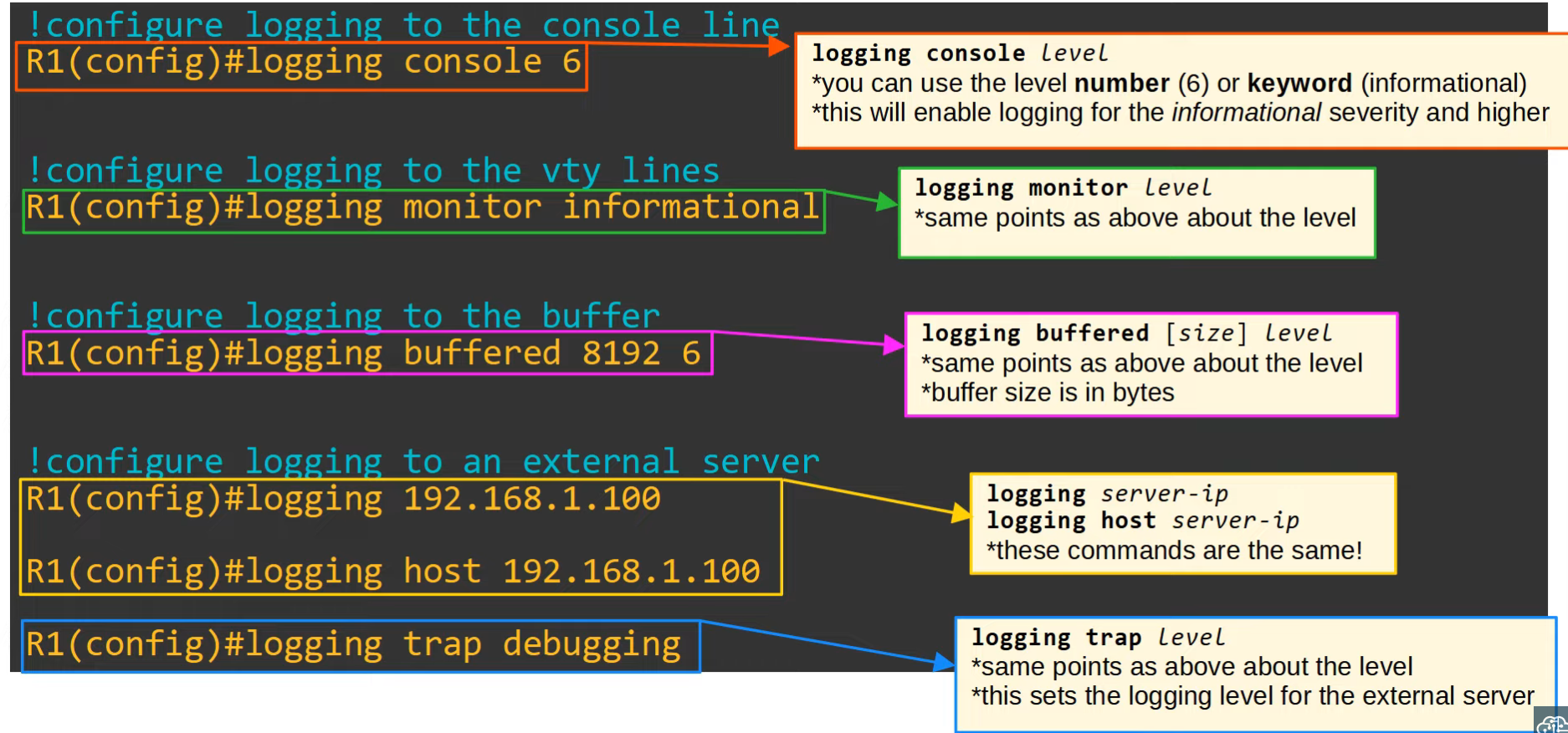
## **SYSLOG LOGGING LOCATIONS**

SYSLOG messages can be stored in different locations:

* **Console Line:**
  + Messages are displayed in the CLI when connected via the **console port**.
  + **By default, all messages (Levels 0-7) are displayed**.
* **Buffer:**
  + Messages are stored in **RAM**.
  + **By default, all messages (Levels 0-7) are stored**.
* **VTY Lines:**
  + Messages are displayed when connected via **Telnet/SSH**.
  + **Disabled by default**.
* **External Server:**
  + Messages are sent to an external **SYSLOG server** for central logging.

**SYSLOG servers listen for messages on UDP port 514.**

**Good to Know:**

****

## **SYSLOG CONFIGURATION**

* **Logging Level:** Works **from the chosen level upward** to Level 0 (Emergency).
* **Severity Level Keywords:** You can specify severity levels using keywords from the severity table.

### **Terminal Monitor**

* Even if logging monitor level is enabled, **SYSLOG messages will not be displayed** when connected via Telnet/SSH.

To display messages, use:  
 R1# terminal monitor

* This command must be used **each time** you connect via Telnet or SSH.

### **Logging Synchronous**

* By default, logging messages **interrupt CLI commands**, causing messy output.

To prevent this, enable **logging synchronous**:  
R1(config)# line console 0

R1(config-line)# logging synchronous

* This ensures that a **new line is printed** if a message interrupts your typing.

### **Service Timestamps & Sequence Numbers**

**Enable timestamps:** R1(config)# service timestamps log datetime

**Enable sequence numbers:** R1(config)# service sequence-numbers

## **SYSLOG vs. SNMP**

Both SYSLOG and SNMP are used for **monitoring and troubleshooting**, but they have different functionalities:

### **SYSLOG**

* Used for **message logging**.
* Logs events based on **facility and severity levels**.
* Helps in **system management, analysis, and troubleshooting**.
* Messages are **pushed** from devices to the server.
* **Limitations:** The server **cannot** actively pull information from devices or modify variables.

### **SNMP**

* Used for **retrieving and organizing device information**.
* Can monitor:
  + **IP addresses**
  + **Interface status**
  + **Temperature, CPU usage, etc.**
* **SNMP servers can:**
  + **Get** – Query information from devices.
  + **Set** – Modify device variables remotely.