JEREMY'S IT LAB

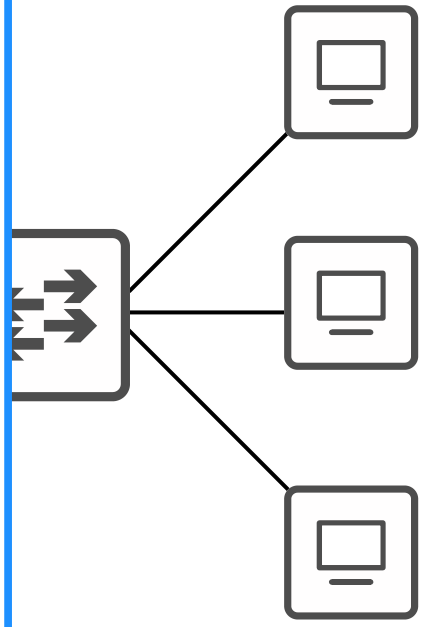
CCNA Day 41

Syslog

1.0 Network Fundamentals	20%
2.0 Network Access	20%
3.0 IP Connectivity	25%
4.0 IP Services	10%

4.1 Configure and verify inside source NAT using static and pools
4.2 Configure and verify NTP operating in a client and server mode
4.3 Explain the role of DHCP and DNS within the network
4.4 Explain the function of SNMP in network operations
4.5 Describe the use of syslog features including facilities and levels
4.6 Configure and verify DHCP client and relay
4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping
4.8 Configure network devices for remote access using SSH
4.9 Describe the capabilities and function of TFTP/FTP in the network

5.0 Security Fundamentals	15%
6.0 Automation and Programmability	10%



Things we'll cover

- Syslog overview
- Syslog message format
- Syslog facilities and severity levels
- Syslog configuration

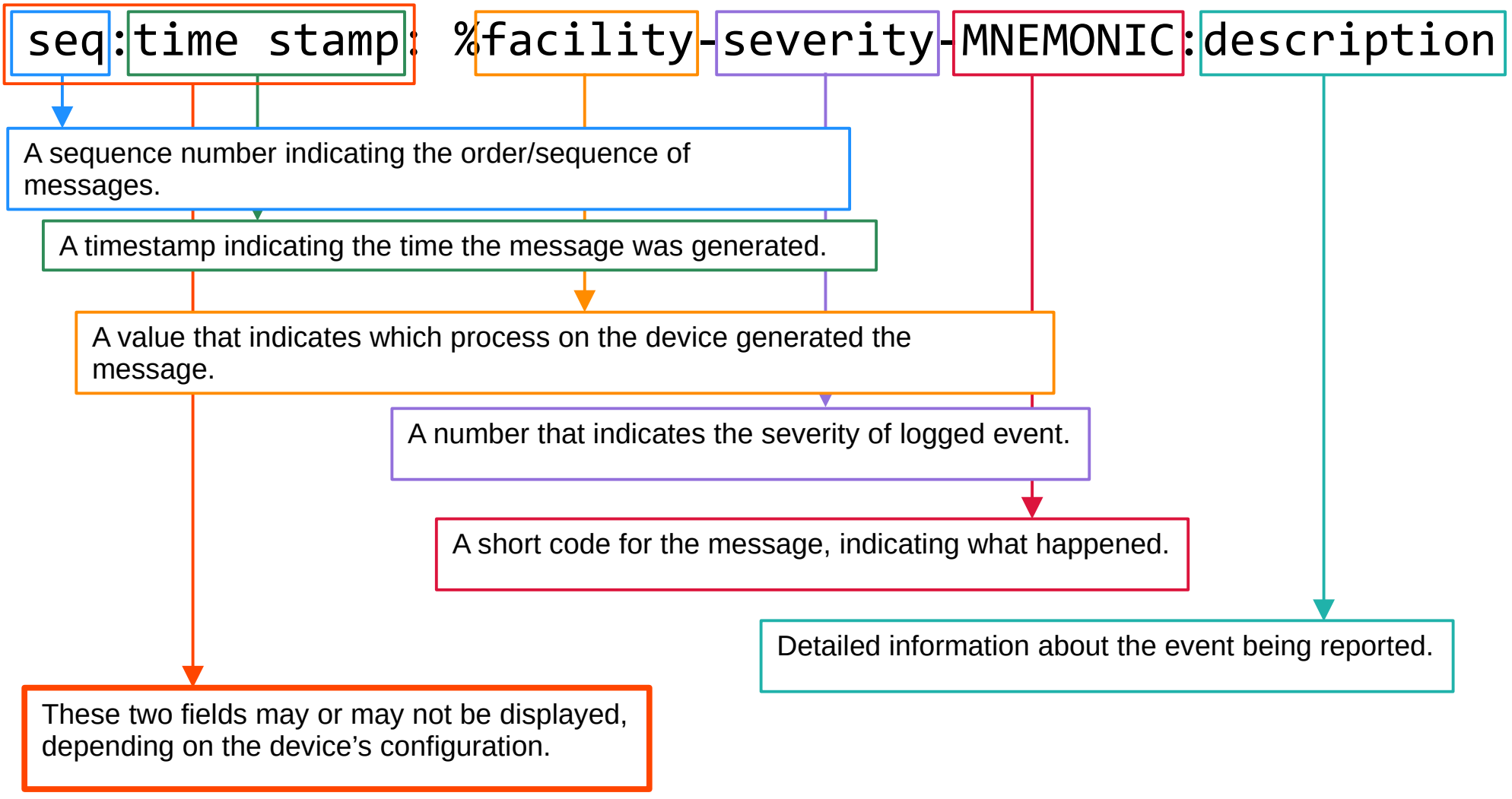
Syslog

- 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, etc.
- The messages can be displayed in the CLI, saved in the device's RAM, or sent to an external Syslog server.

```
R1(config)#int g0/0
R1(config-if)#no shutdown
R1(config-if)#
*Feb 11 03:02:55.304: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Feb 11 03:02:56.305: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
```

- 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



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

Every **A**wesome **C**isco **E**ngineer **W**ill **N**eed **I**ce cream **D**aily

Syslog Message Examples

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

```
*Feb 11 03:02:55.304: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
```

```
*Feb 11 05:04:39.606: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on GigabitEthernet0/0 from
LOADING to FULL, Loading Done
```

```
000043: *Feb 11 05:06:43.331: %SYS-5-CONFIG_I: Configured from console by jeremy on console
```

```
*Feb 11 07:27:23.346: %SYS-6-CLOCKUPDATE: System clock has been updated from 07:27:23 UTC Thu Feb
11 2021 to 16:27:23 JST Thu Feb 11 2021, configured from console by jeremy on console.
```

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 – level 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.

- **Buffer:** Syslog messages will be saved to RAM. By default, all messages (level 0 – level 7) are displayed.
  → You can view the messages with **`show logging`**.

- **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**. Remember that port number!

Syslog Configuration

```
!configure logging to the console line
R1(config)#logging console 6

!configure logging to the vty lines
R1(config)#logging monitor informational

!configure logging to the buffer
R1(config)#logging buffered 8192 6

!configure logging to an external server
R1(config)#logging 192.168.1.100

R1(config)#logging host 192.168.1.100

R1(config)#logging trap debugging
```

logging console *level*
*you can use the level **number** (6) or **keyword** (informational)
*this will enable logging for the *informational* severity and higher

logging monitor *level*
*same points as above about the level

logging buffered [*size*] *level*
*same points as above about the level
*buffer size is in bytes

logging *server-ip*
logging host *server-ip*
*these commands are the same!

logging trap *level*
*same points as above about the level
*this sets the logging level for the external server

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
```

- This 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 the **logging synchronous** on the appropriate *line*.
(I will talk more about 'line' configuration in the Telnet/SSH video!)

```
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
```

show ip int was reprinted on a new line. This makes it easier to continue typing the command.

service timestamps / service sequence-numbers

```
R1(config)#service timestamps log ?
  datetime  Timestamp with date and time
  uptime    Timestamp with system uptime
  <cr>

R1(config)#service timestamps log datetime
R1(config)#
R1(config)#service sequence-numbers
R1(config)#exit
R1#
000039: *Feb 11 10:32:46: %SYS-5-CONFIG_I: Configured from console by
jeremy on console
```

datetime = timestamps will display the date/time when the event occurred.
uptime = timestamps will display how long the device had been running when the event occurred.

Syslog Command Summary

```
R1(config)# logging console severity

R1(config)# logging monitor severity

R1(config)# logging buffered [size] severity

R1(config)# logging server-ip

R1(config)# logging host server-ip

R1(config)# logging trap severity

R1# terminal monitor

R1(config-line)# logging synchronous

R1(config)# service timestamps log [datetime | uptime]

R1(config)# service sequence-numbers
```

Syslog vs SNMP

- Syslog and SNMP are both used for monitoring and troubleshooting of devices. They are complementary, but their functionalities are different.

- **Syslog** is 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** is 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.

Things we covered

- Syslog overview
- Syslog message format
- Syslog facilities and severity levels
- Syslog configuration

Quiz 1

What is the severity level of the following Syslog message?

```
*Feb 11 09:41:00.554: %SYS-5-CONFIG_I: Configured from console by jeremy on console
```

a) System

b) Informational

c) Notification

d) Warning

e) Alert

f) Debugging

g) Config

Quiz 2

What is the severity level of the following Syslog message?

```
*Feb 11 03:02:55.304: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
```

a) Emergency

b) Error

c) Notification

d) Notice

e) Critical

f) Notice

g) Warning

Quiz 3

Which of the following locations are Syslog messages sent to by default, without any specific Syslog configuration? (select two)

a) External Syslog server

b) Console line

c) Buffer

d) VTY lines

Quiz 4

You issue the **logging buffered 6** command on R1. Syslog messages of which severity levels will be saved to the logging buffer?

a) All Syslog messages

b) Severity 6 and 7

c) Severity 0 to 6

d) Severity 6 only

Quiz 5

Which of the following Syslog message fields might not be displayed, depending on the device's configuration? (select two)

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

a) seq

b) facility

c) severity

d) time stamp