Welcome and Course Introduction

- Jeremy's IT Lab provides a free, complete course for the CCNA.
- Viewers are encouraged to subscribe, like, comment, and share the lecture to help spread the free series.

Lecture Topic: Syslog

- This lecture covers **Syslog**.
- Syslog is a protocol used to keep logs of various events that happen on the device.
- **Examples of logged events:**
  - Interfaces going up or down
  - OSPF neighbor relationships going up or down
- Log messages can be shown in real-time in the CLI of the device to inform you of important events as they occur.
- Log messages can also be stored in the device or on an external server and examined later.
- These logs are very important, so understanding Syslog is essential for network admins and engineers.

Exam Relevance

- Syslog is mentioned in **exam topic 4.5**.
- Exam topic 4.5 requires you to be able to describe the use of syslog features including **facilities** and **levels**.

Lecture Agenda

- First: a brief overview of Syslog and how it works.

- Then: the Syslog message format.
  - Syslog messages have a standard format, and it's important to know the format so you can read and understand Syslog messages.
- Then: the various Syslog facilities and severity levels.
  - The terms "facility" and "severity" are mentioned in the exam topics list, so they are covered in this lecture.
- Then: some basic Syslog configurations.
  - Like SNMP, Syslog configuration is not mentioned in the exam topics, but hands-on practice is still important.
- The lecture ends with a bonus practice question from Boson Software's ExSim for CCNA, described as the best practice exams for the CCNA.

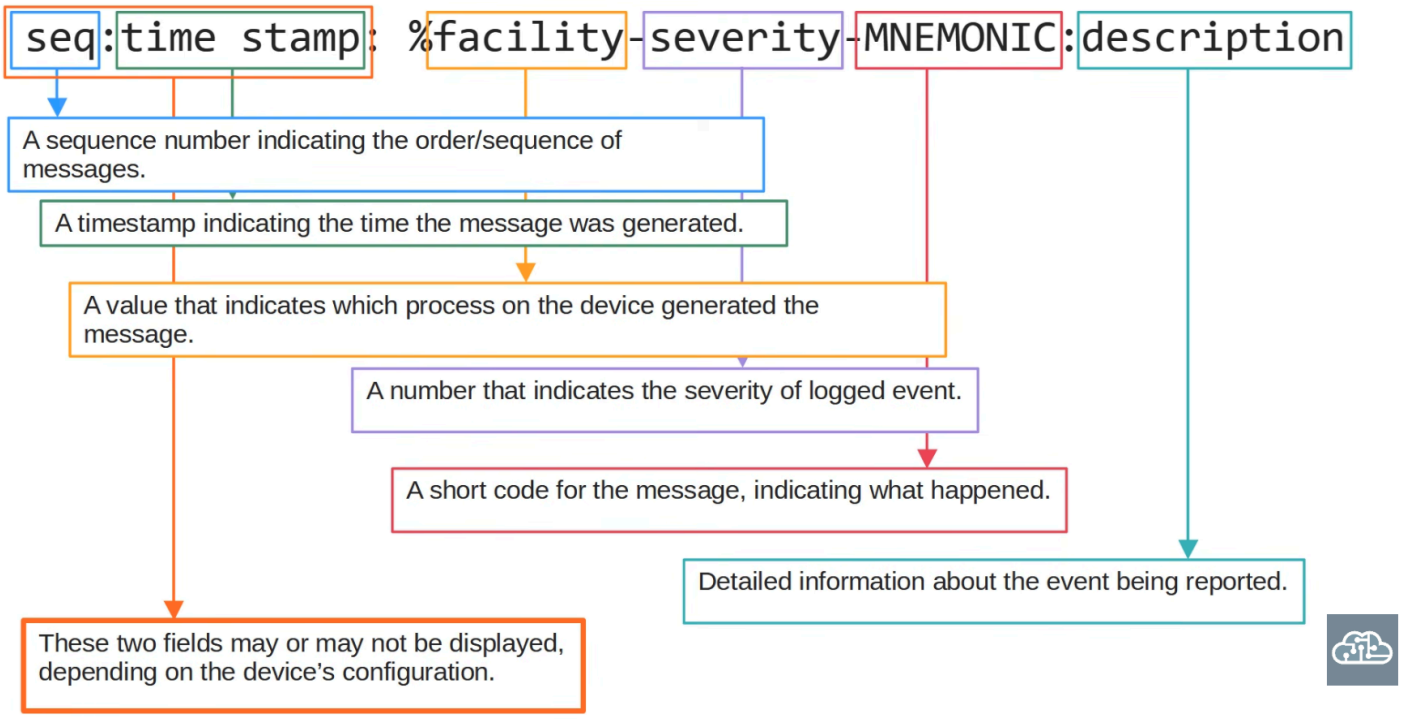
Quick Overview of Syslog

- 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
  - Changes in OSPF neighbor status
  - Neighbor status in other routing protocols like EIGRP and BGP
  - System restarts
- Tons of different events can be logged, so the professor does not try to list them all.
- The messages can be displayed in the CLI as you configure the device, 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
```

- **Example:** The professor used NO SHUTDOWN to enable a router interface. Two Syslog messages were displayed, indicating that the interface state has changed to UP.
    - The professor notes that students have likely seen these messages when configuring devices in Packet Tracer.
- Logs are essential when troubleshooting issues and examining the cause of incidents.
- Syslog and SNMP are both used for monitoring and troubleshooting devices.
    - They are complementary to each other, but their functionalities are quite different.
- After covering Syslog in this lecture, the professor will give a brief summary of how Syslog and SNMP are different at the end.

Syslog Message Format



- There are fields you can expect to see in a standard Syslog message.
- First, there is a **sequence number** indicating the order, the sequence, of the log messages.

- **timestamp** indicating at what time the message was generated.
    - Timestamps are particularly important, especially when comparing the logs of different devices.
    - Assuming both devices have accurate time thanks to NTP, you can use these timestamps to compare when different events occurred on different devices.
    - Note: these two fields, the sequence number and timestamp, may or may not be displayed, depending on the device's configuration.
    - Sequence numbers are often not used; however, timestamps are very important and the professor highly recommends including them in Syslog messages.
- **facility** — a value that indicates which process on the device generated this message.
    - **Example:** If OSPF generated the message when an OSPF neighbor came up, OSPF would be displayed in this field.
- **severity** — indicates the severity of the event.
    - Some messages are just informational, simply letting you know that something happened.
    - Other messages indicate something much more serious that might need to be dealt with immediately.
    - There are 8 severity levels, and you'll need to know them all for the exam.
- **mnemonic** — a short code for the message that indicates what happened.
    - **Example:** If the facility is OSPF, this mnemonic might be a code indicating that the message is about OSPF neighbor adjacencies.
    - **Example:** If the facility is LINK, it might be a code indicating that the message is about an interface going up or down.
- Finally, there is the **description** — the detailed information about the event being reported, about what actually happened.

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

- These levels indicate how serious, how severe, the event is.
    - **Example:** Something like a serious hardware failure is more severe than an OSPF neighbor moving to the FULL state.
- 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 identifying the level.
- Each level has a brief description, taken directly from the official RFC for Syslog.

The 8 severity levels, from most severe to least severe:

- **Level 0 — Emergency:** events which render the system unusable.
- **Level 1 — Alert:** events for which action must be taken immediately.
    - These are also very serious events.
- **Level 2 — Critical:** the description is simply 'critical conditions'.
- **Level 3 — Error:** same description style as critical and warning.
- **Level 4 — Warning:** same description style as critical and error.

- **Level 5 — Notice:** used for messages representing a 'normal but significant condition'.
  - In the official RFC for Syslog, the keyword for level 5 is 'Notice'.
  - In the CLI of Cisco IOS, the name is Notification.
  - Make sure you know both names: Notice and Notification for level 5.
- **Level 6 — Informational.**
- **Level 7 — Debugging:** the least severe level.
  - These are the least severe messages.

Vendor Interpretation of Severity Levels

- The RFC doesn't give detailed definitions about exactly what events fit into each severity level.
- Each vendor will interpret these levels differently.
- **Quote from the RFC:** "Because severities are very subjective, a relay or collector (basically that means a Syslog server) should not assume that all originators have the same definition of severity."
  - This is from RFC 5424, The Syslog Protocol, which is free to read online.
  - **Example:** You shouldn't expect a Cisco router's 'Warning' level to be exactly the same as a Juniper router's 'Warning' level, for example.
  - Each vendor may interpret each level differently.

Memorization for the CCNA Exam

- For the CCNA exam, make sure you have memorized the levels and keywords.
  - **Example:** You should know that level 1 is Alert, and Informational is level 6.
- **Mnemonic to remember the levels:** Every Awesome Cisco Engineer Will Need Ice cream Daily.

Examples of Syslog Messages

- The professor presents several examples of Syslog messages and emphasizes the importance of being able to identify each part of the message.

- **Example 1: Interface state change**

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

  - First, there is the timestamp, indicating the month, date, hours, minutes, seconds, and milliseconds.
  - Notice that there is no sequence number before the timestamp.
  - As mentioned earlier, the sequence number and timestamp fields may or may not be displayed, depending on the device's configuration.
  - The facility is LINK.
  - The severity is 3.
  - The mnemonic is UPDOWN, which tells us the message is about an interface going up or down.
  - The description tells us exactly what happened: Interface gigabitethernet0/0 changed state to up.
  - Make sure you're able to identify each part of this message.
    - If asked what the facility of this Syslog message is, you should be able to answer 'LINK'.
    - If asked about the severity, you should be able to answer '3' or 'error', depending on the options.
  - Judging by the exam topics list, those seem like the kind of question you can expect on the exam.

- **Example 2: OSPF neighbor moving to the FULL state**

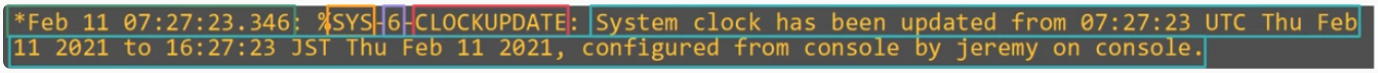
```
*Feb 11 05:04:39.606: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on GigabitEthernet0/0 from
LOADING to FULL, Loading Done
```

  - The facility is OSPF.
  - IOS declares this a level 5, notification level, message.
  - The mnemonic is A D J C H G, adjacency change.

- **Example 3: Configuration message with sequence numbers enabled**

  - For this example, the professor turned on the sequence numbers so you can see what it looks like.
  - The facility is SYS for system.
  - The severity is 5 again — remember the keywords for level 5: 'notice' or 'notification'.
  - The mnemonic is CONFIG_I.
  - The description is 'configured from console by jeremy on console.'
  - You get messages like this when you exit global config mode and return to privileged exec mode.

- **Example 4: Timezone change**



  - This time the professor changed the timezone from UTC to JST and this message was displayed.
  - The facility is SYS.
  - The severity is 6.
  - The keyword for level 6 is 'informational'.
  - The mnemonic is CLOCKUPDATE.

- Once again, make sure you can identify each part of a Syslog message — it's stated directly in the exam topics list.

Overview of Syslog Message Locations

- Soon we'll take a look at how to configure Syslog in the CLI, but before that, here's an overview of the different locations Syslog messages can be sent to.

- **First location: the console line**
  - Syslog messages will be displayed when connected to the device via the console port.
  - By default, all messages, from level 0 through level 7, are displayed when connected to the CLI via the device's console port.
  - **Example:** In Packet Tracer, when you click on a device and go to the CLI tab, it operates as if you're connected via the console port of the device. That's why Syslog messages are displayed when configuring devices in Packet Tracer via the CLI tab.
- **Next location: the VTY lines**
  - Syslog messages will be displayed in the CLI when connected to the device via Telnet or SSH.
  - Telnet and SSH will be covered in a later lecture. They are protocols used to connect to a device over a network, without being directly connected to the device's console port.
  - Logging to the VTY lines is disabled by default, so Syslog messages will not be displayed if you're connecting to the device via Telnet or SSH.
  - **Example:** If you shutdown an interface, no message will be displayed.
- **Next location: the 'buffer' of the device**
  - Syslog messages will be saved to RAM.
  - By default, all messages, from level 0 to level 7, will be displayed in the buffer.
  - You can view the messages in the buffer with the `show logging` command. We'll take a look at that command in the lab lecture.

Verification:

```
show logging
```

- **Another location: an external server**
  - You can also configure the device to send Syslog messages to an external server.
  - This is very useful, especially in large networks, but also in small networks.
  - Having a central server for the Syslog messages makes network management easier and makes it easier to compare the logs of multiple devices.
  - By the way, Syslog servers will listen for Syslog messages on UDP port 514. So, if a device sends a Syslog message to a Syslog server, the destination port will be UDP 514. Remember that!

Basic Syslog Configurations

- The professor provides basic Syslog configuration commands for each location.
- Note: in all of these commands, you can specify either the number or the keyword of the level.
- Note: specifying a level does not only enable messages of that level; it enables logging for that severity and higher (numerically lower levels).

- **Configuring logging to the console line**

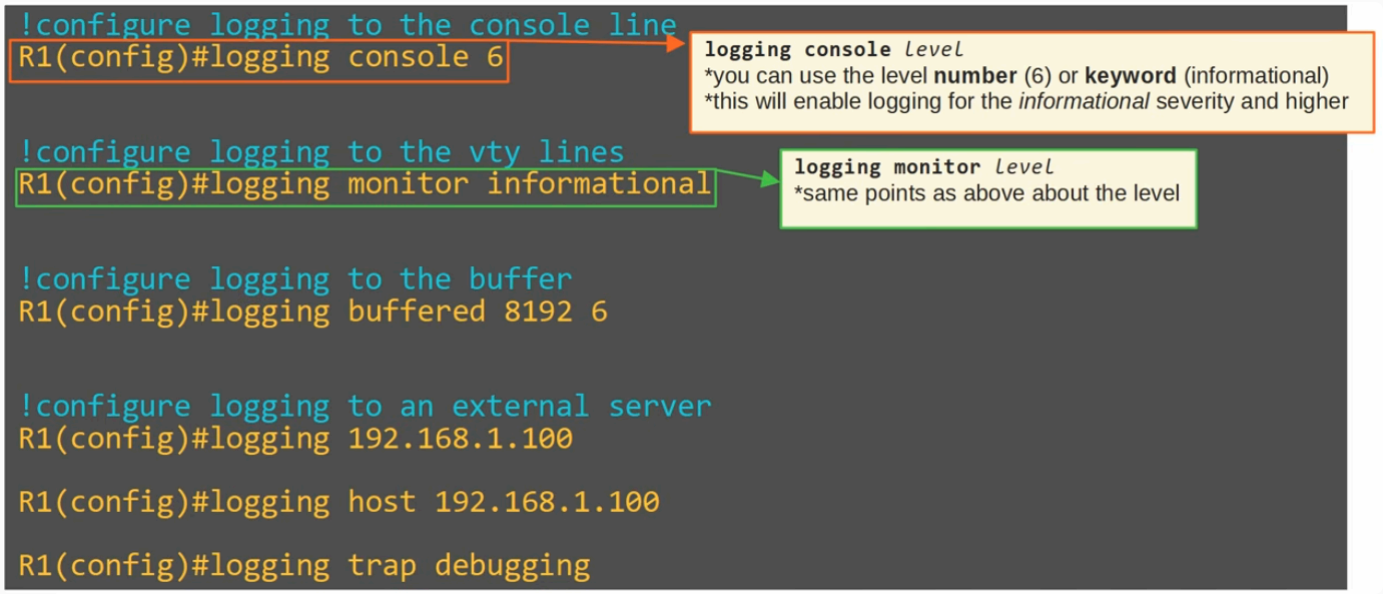
```
!configure logging to the console line
R1(config)#logging console 6


!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

  - This is enabled by default, but here's how you configure it.
  - The command is `logging console`, followed by the level.
  - The professor specified 6, but could have used the keyword INFORMATIONAL instead.
  - This enables logging for informational severity and higher, so informational to emergency, which includes levels 6, 5, 4, 3, 2, 1, and 0.
  - Note: by default the console logs all messages, including level 7, debugging, so setting the level to 6 actually slightly restricts the messages that will be displayed via the console.

```
R1(config)# logging console 6
```

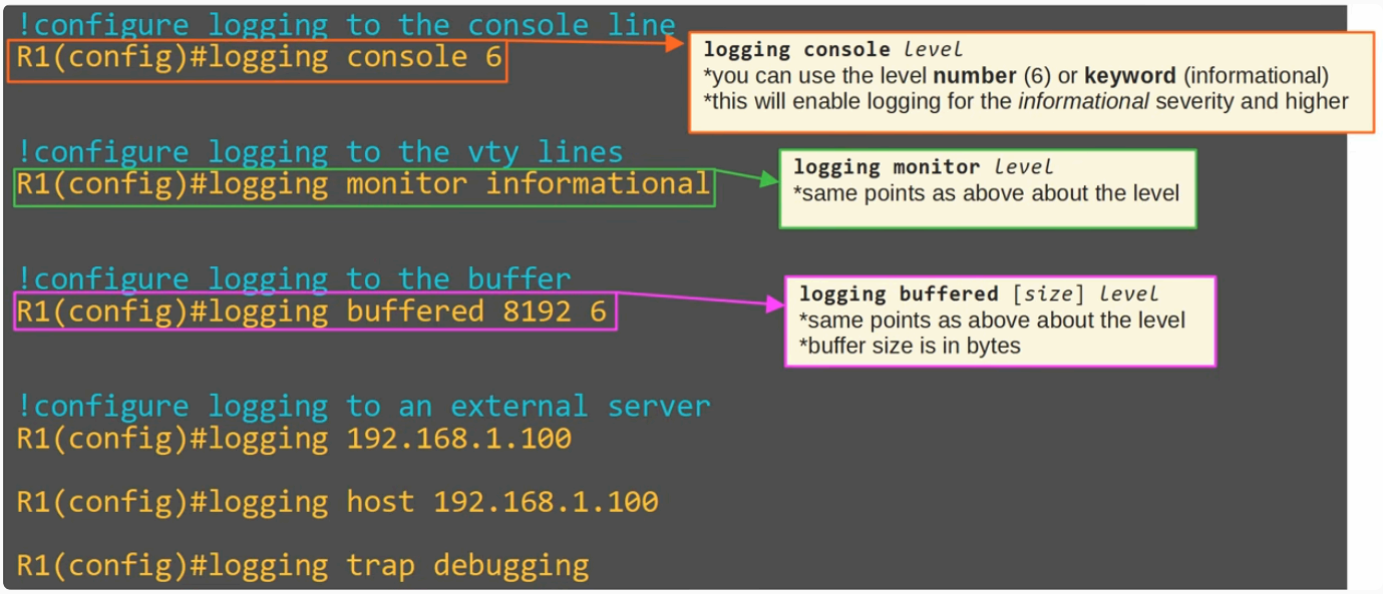
- **Configuring logging to the VTY lines**



  - The command is `logging monitor`, followed by the level.
  - Just like above, you can specify the level number or keyword; this time the professor used the keyword of INFORMATIONAL instead of the level, 6.

```
R1(config)# logging monitor informational
```

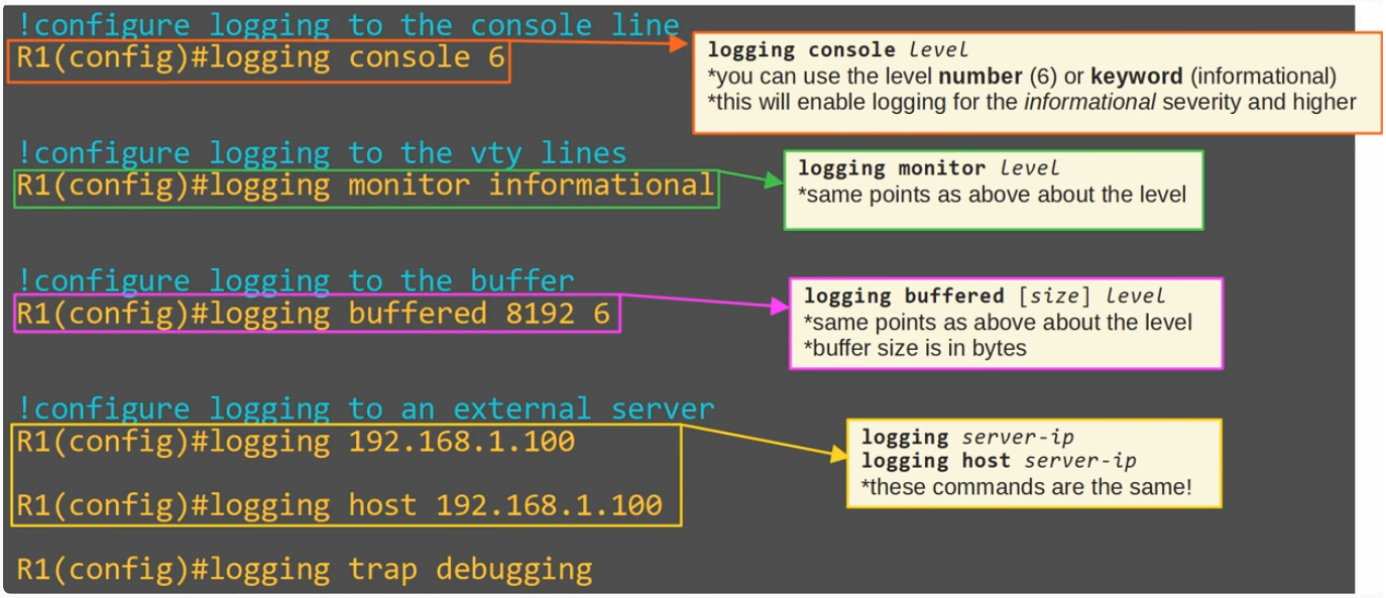
- **Configuring logging to the buffer**



  - The command is `logging buffered`, followed by the size of the buffer in bytes and the level.
  - The size is optional; if you don't specify it, the device will use its default size.
  - Note: be careful not to set the buffer size too large, because that can take system memory away from other essential operations.
  - To repeat, to specify the logging level you can use either the number or the keyword, and it enables logging for not only level 6 but also levels 5, 4, 3, 2, 1, and 0.

```
R1(config)# logging buffered 4096 6
```

- **Configuring logging to an external server**

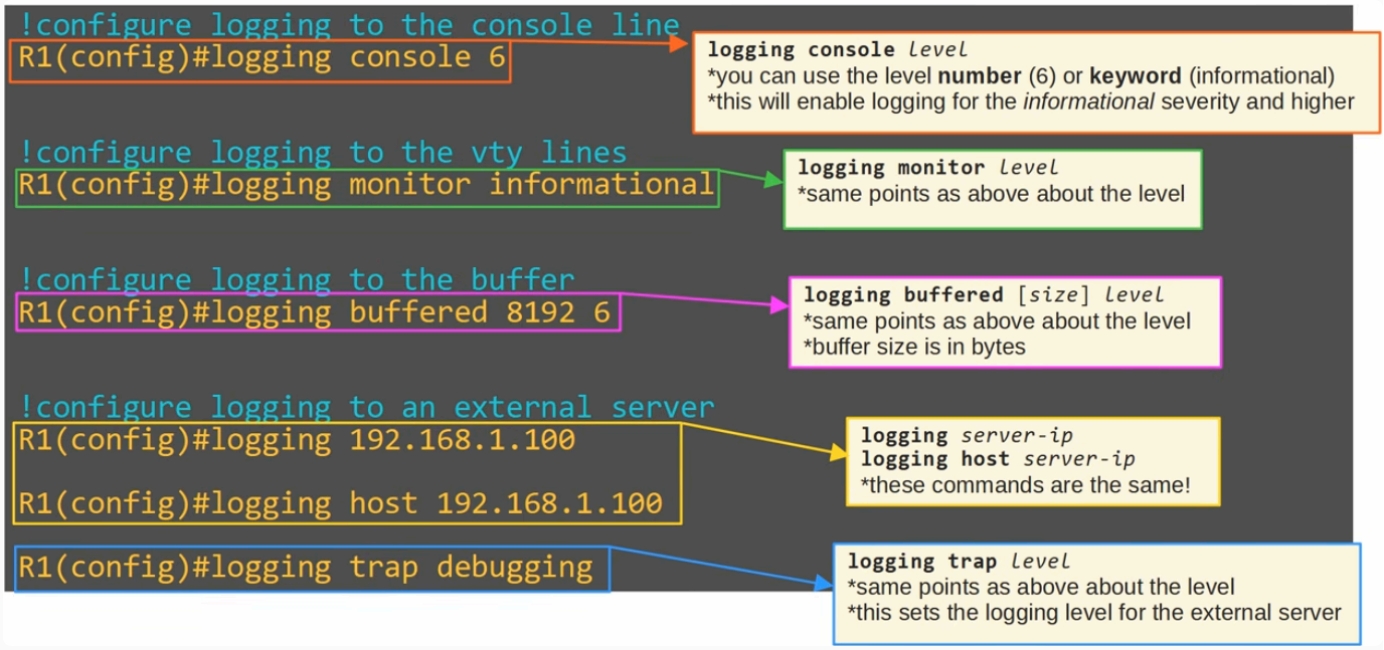


  - The command is `logging`, followed by the server IP, or `logging host`, followed by the server IP.
  - The commands are the same; you can use whichever.

```
R1(config)# logging 192.168.1.100
```

```
R1(config)# logging host 192.168.1.100
```

- **Configuring the level of messages sent to the external server**



  - To configure the levels of messages sent to the external server, you need to use a different command: `logging trap`, followed by the level.
  - The professor specified DEBUGGING, but once again could have used the level number of 7 instead.
  - This enables logging of all levels, not just 7 but also 6, 5, 4, 3, 2, 1, and 0.

```
R1(config)# logging trap debugging
```

- That's how you enable Syslog logging to different locations and specify which levels of messages should be displayed.
- Because Syslog configuration isn't specified in the exam topics, you probably don't have to memorize these commands for the exam.
- However, the professor will include flashcards for them, and you can get some practice with them in the following lab lecture.

Terminal Monitor Command

- Even if `logging monitor` is enabled, by default Syslog messages will not be displayed when connected via Telnet or SSH.
- You need another command, too.

```
R1#terminal monitor
```

- For the messages to be displayed, you must use `terminal monitor`, from privileged exec mode.
- This command must be used every time you connect to the device via Telnet or SSH.
- **Example:** If you connect via SSH and use the `terminal monitor` command, Syslog messages will be displayed as you configure the device.
- However, after you log out, that 'session' is finished and the `terminal monitor` command is no longer effective.
- To display Syslog messages in the CLI when you connect again next time, you'll need to use the `terminal monitor` command again.
- The professor will demonstrate this in the lab lecture.

```
R1# terminal monitor
```

Logging Synchronous Command

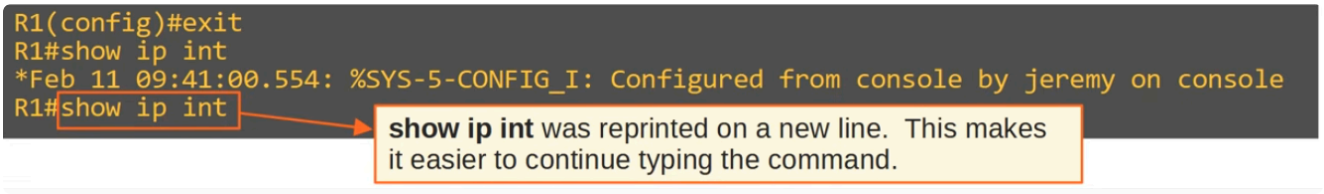
```
R1(config)#exit
R1#show ip in
*Feb 11 09:38:41.607: %SYS-5-CONFIG_I: Configured from console by jeremy on
consoleterface brief
```

- This next command isn't essential, but very convenient.
- By default, logging messages displayed in the CLI while you are in the middle of typing a command will result in the command and the log message being mixed together.

- **Example:** The professor was typing `show ip in`, and a log message was displayed. He continued typing the command, and the command continued right after the log message.
    - The professor changed the color of the command to make it easier to see, but when this actually happens in the CLI it can be hard to see where the Syslog message ends and where the command continues.
- To prevent this, you should use the `logging synchronous` command on the appropriate line.
- The professor will talk more about 'line' configuration in the Telnet and SSH lecture.

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

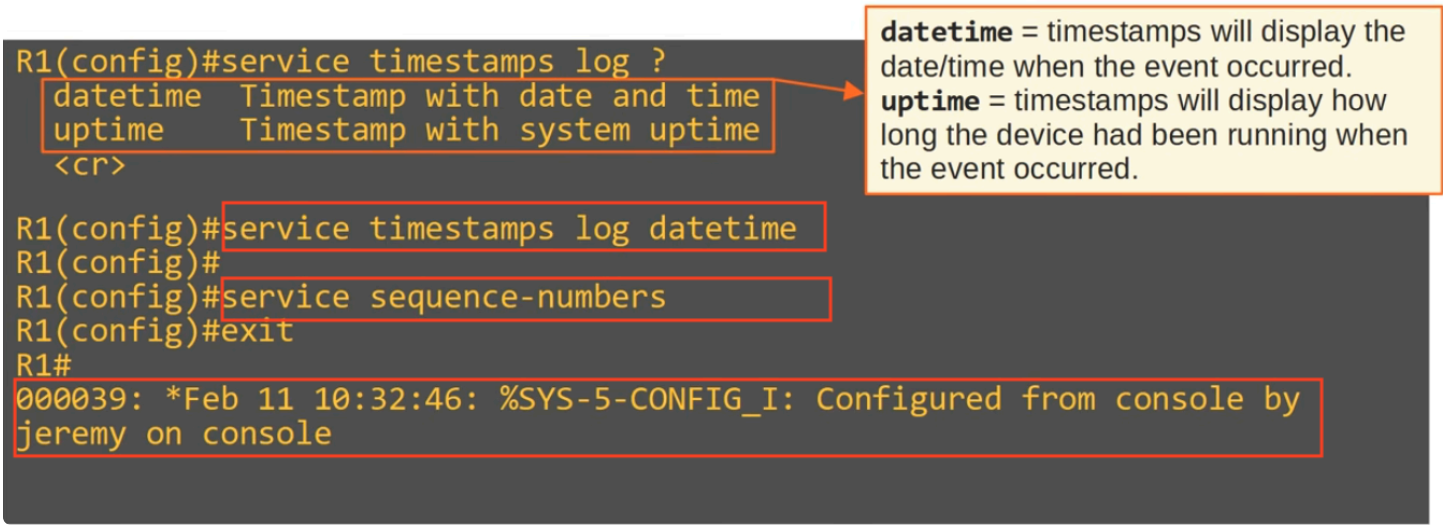
- **Example:** Here's how you can enter the console line, `line console 0`, and then configure `logging synchronous`.
    - This will cause a new line to be printed if your typing is interrupted by a message.



    - **Example:** The professor typed `show ip int`, a log message was displayed, and then `show ip int` was reprinted on a new line.
        - This makes it easier to continue typing the command.
- This is a nice command to know and a command the professor usually uses when doing labs. It just makes things easier to see.

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

Service Timestamps and Service Sequence-Numbers Commands



- The last two commands the professor wants to show are `service timestamps` and `service sequence-numbers`.
- This is how you control whether or not the timestamps and sequence numbers will be displayed in Syslog messages.
- To enable timestamps for Syslog messages, use `service timestamps log`, followed either by DATETIME or UPTIME.
  - If you specify DATETIME, timestamps will display the actual date and time when the event occurred.
  - If you specify UPTIME, timestamps won't display the date and time; they will display how long the device had been running when the event occurred.
  - DATETIME is usually the preferred option, so that's what the professor chose.
- Then the professor enabled sequence numbers with the `service sequence-numbers` command.

```
R1(config)# service timestamps log datetime
```

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

- **Example:** After the professor exited global config mode, the Syslog message displayed had both a sequence number and a timestamp.
- The professor thinks it's a good idea to always enable timestamps, although personally he doesn't find sequence numbers particularly useful, so he prefers to keep them disabled.

Syslog Commands — Quick Reference

```
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
```

Command	What it does
`logging console severity`	Sets which severity levels appear on the **console connection**.
`logging monitor severity`	Sets which severity levels appear on **VTY/SSH/Telnet sessions**.
`logging buffered [size] severity`	Stores log messages in the router's **RAM buffer**.
`logging server-ip`	Specifies the **Syslog server IP address** where logs are sent.
`logging host server-ip`	Same purpose: specifies the **Syslog server** that receives logs.
`logging trap severity`	Sets which severity levels are **sent to the Syslog server**.
`terminal monitor`	Makes Syslog messages appear in your current **SSH/Telnet session**.
`logging synchronous`	Prevents log messages from **interrupting commands you're typing**.
`service timestamps log datetime`	Adds the **date and time** to log messages.
`service timestamps log uptime`	Adds how long the device has been **running** to log messages.
`service sequence-numbers`	Adds a **sequence number** to each log message so you can track their order.

Comparison of Syslog and SNMP

- Syslog and SNMP are both used for monitoring and troubleshooting of devices.
- They are complementary, but their functionalities are different.
- **Syslog:**
  - Used for message logging.
  - Events that occur within the system are categorized based on facility and severity and logged, both within the device and likely to an external Syslog server.
  - Used for system management, analysis, and troubleshooting.
  - **Big difference:** Messages are sent from the devices to the server, but the server can't actively pull information from the devices, like an SNMP Get message, or modify variables on the devices, like an SNMP Set message.
- **SNMP:**
  - Used to retrieve and organize information about the SNMP managed devices.
  - Things like IP addresses, current interface status, device temperature, CPU usage, etc. are stored as variables and organized within the MIB.
  - SNMP servers can use Get to query the clients and Set to modify variables on the clients.
- Syslog and SNMP are used together to facilitate network device management, and you need to be familiar with both of them for the test.

Review of Syslog

- Before the quiz, the professor provides a review of what was covered in the lecture.
- First, a brief overview of Syslog: it's an industry standard protocol for logging events that occur on devices.
- The professor introduced the Syslog message format, as well as facilities and severity levels.
  - Make sure you know all of those severity level numbers and names.
  - Make sure you can identify the different parts of a Syslog message.

- Finally, the professor showed some basic Syslog configurations.
    - You probably won't be asked about Syslog configuration on the exam.
    - However, the hands-on practice in Packet Tracer will be very helpful.
- Make sure to watch until the end of the quiz for a bonus practice question from Boson Software's ExSim, the best practice exams for the CCNA, and the ones the professor used to prepare for his exams.
