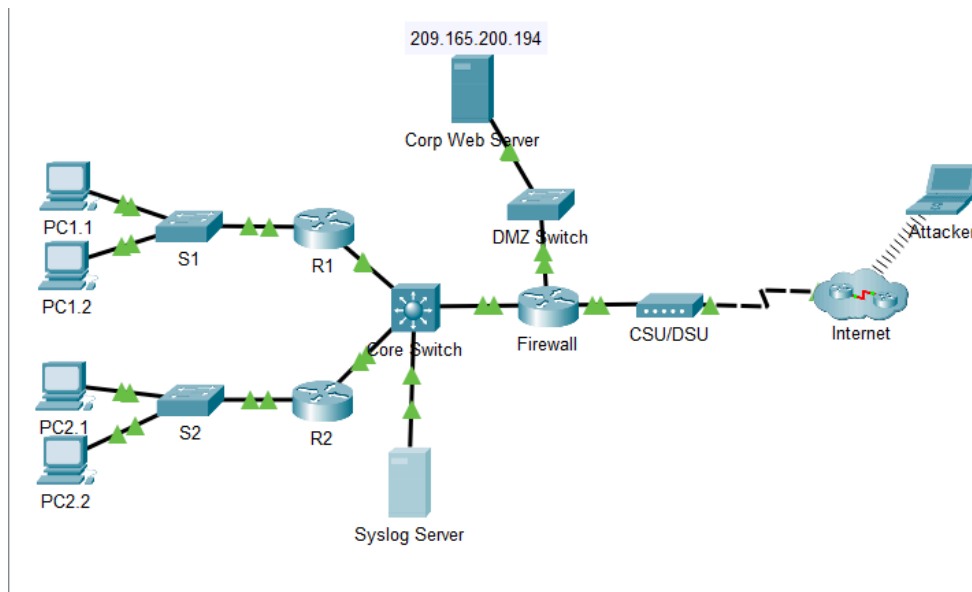


# Logging from Multiple Sources

## Background / Scenario

In this activity, you will use Packet Tracer to view network data generated by syslog, AAA, and NetFlow.



## Part 1: View Log Entries with Syslog

### Step 1: The syslog Server

Packet Tracer supports basic syslog operations and can be used for demonstration. The syslog server collects the log entries and allows them to be read.

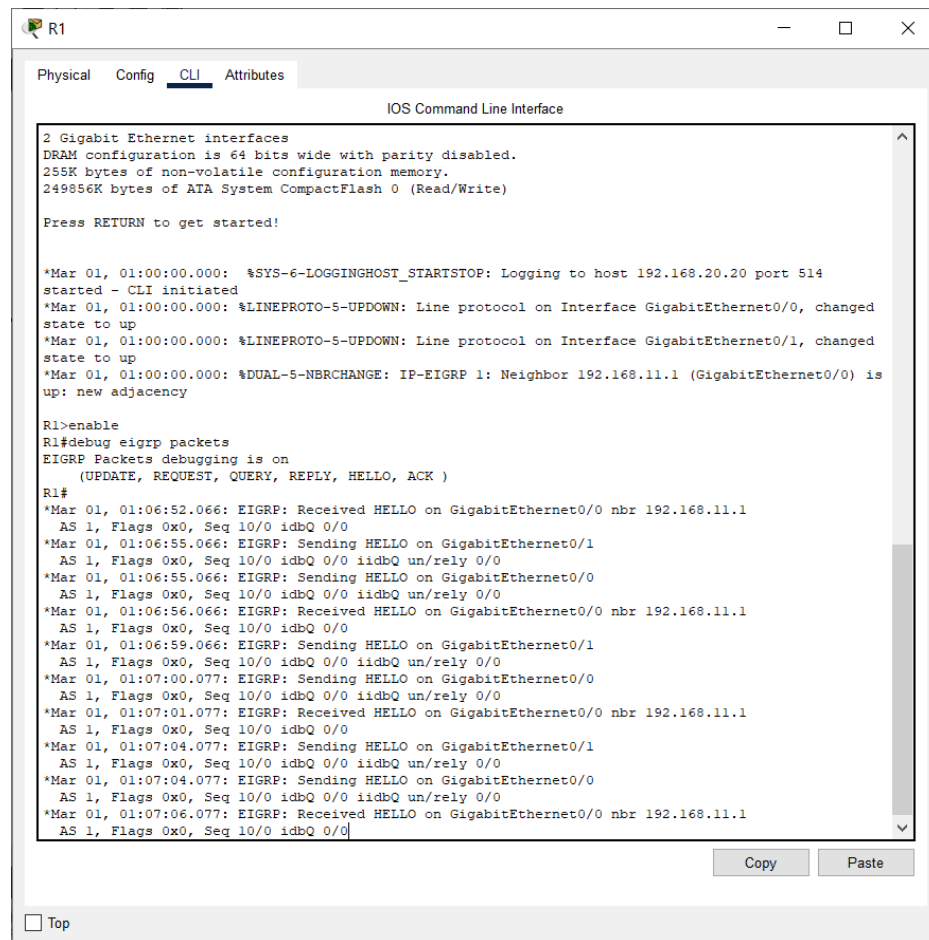
Log entries are categorized by seven severity levels. Lower levels represent more serious events. The levels are: emergencies **(0)**, **alerts (1)**, **critical (2)**, **errors (3)**, **warnings (4)**, **notifications (5)**, **informational (6)**, and **debugging (7)**. Syslog clients can be configured to ship log entries to syslog servers based on the severity level.

- Click the Syslog Server to open its window.
- Select the Services tab and select SYSLOG from the list of services shown on the left.
- Click On to turn on the Syslog service.
- Syslog entries coming from syslog clients will be shown in the window on the right. Currently, there are no entries.

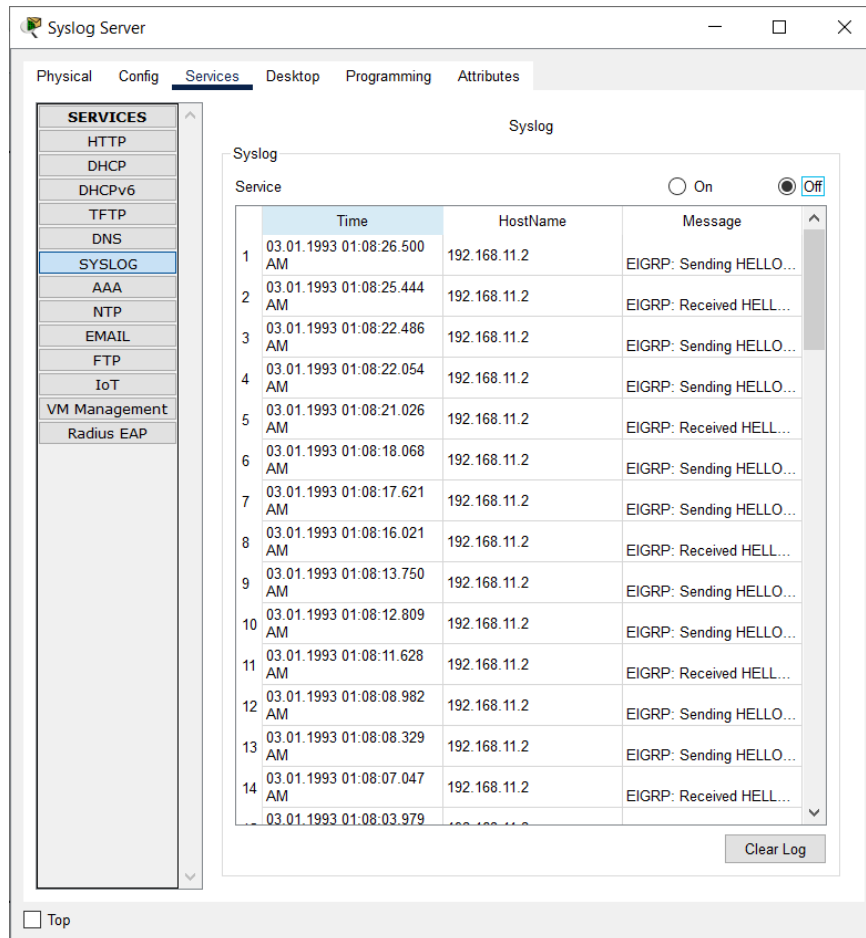
## Step 2: Enable Syslog.

The devices are already configured to send log messages to the syslog server, but Packet Tracer only supports the logging for the debugging severity level with syslog. Because of that, we must generate debug level messages (level 7) so they can be sent to the syslog server.

- Click R1 > CLI tab.
- Press Enter to get a command prompt and enter the command `enable`.
- Enter the command `debug eigrp packets` to enable EIGRP debugging. The command line console will immediately fill with debug messages.



- Return to the Syslog Server window. Verify that log entries appear on the syslog server.
- After a few messages have been logged, click the radio button to turn the syslog service Off.



What is some of the information that is included in the syslog messages that are being displayed by the Syslog Server?

**R: Time:** 03.01.1993 01:08:25.444 AM

**Hostname:** 192.168.11.2

**Message:** EIGRP: Received HELLO on GigabitEthernet0/0 nbr 192.168.11.1 AS 1, Flags 0x0, Seq 10/0 idbQ 0/0

f. Close the R1 device window..

### Step 3: Log User Access

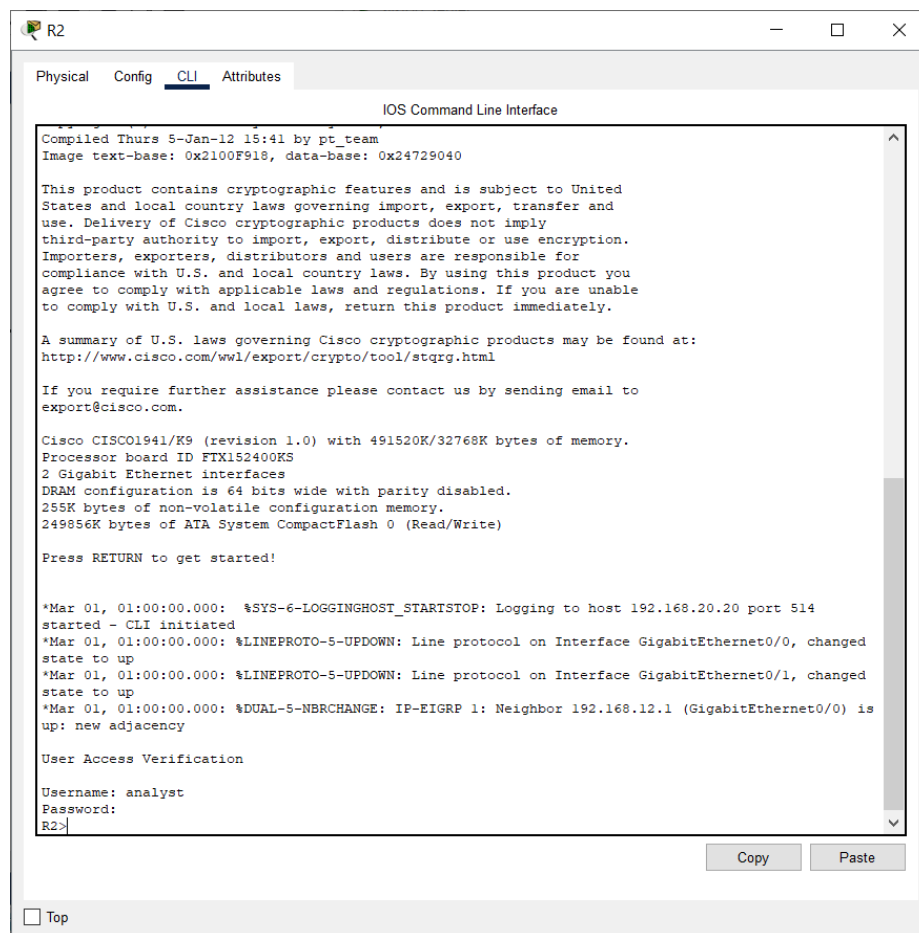
Another important type of log relates to user access. Having records of user logins is crucial for troubleshooting and traffic analysis. Cisco IOS supports Authentication, Authorization and Accounting (AAA). With AAA, it is possible not only to delegate the user validation task to an external server but also to log activities.

TACACS+ is a protocol designed to allow remote authentication through a centralized server.

Packet Tracer offers basic AAA and TACACS+ support. R2 is also configured as a TACACS+ server. R2 will ask the server if that user is valid by verifying username

and password, and grant or deny access based on the response. The server stores user credentials and is also able to log user login transactions. Follow the steps below to login to R2 and display the log entries related to that login:

- a. Click the Syslog Server to open its window.
- b. Select the Desktop tab and select AAA Accounting. Leave this window open.
- c. Click R2 > CLI.
- d. Press Enter to get a command prompt. R2 will ask for username and password before granting access to its CLI. Enter the following user credentials: analyst and cyberops as the username and password, respectively.



The screenshot shows a window titled 'R2' with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the 'IOS Command Line Interface'. The text in the window includes:

```
Compiled Thurs 5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wml/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISC01941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

*Mar 01, 01:00:00.000: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.20.20 port 514
started - CLI initiated
*Mar 01, 01:00:00.000: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to up
*Mar 01, 01:00:00.000: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to up
*Mar 01, 01:00:00.000: %DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.12.1 (GigabitEthernet0/0) is
up: new adjacency

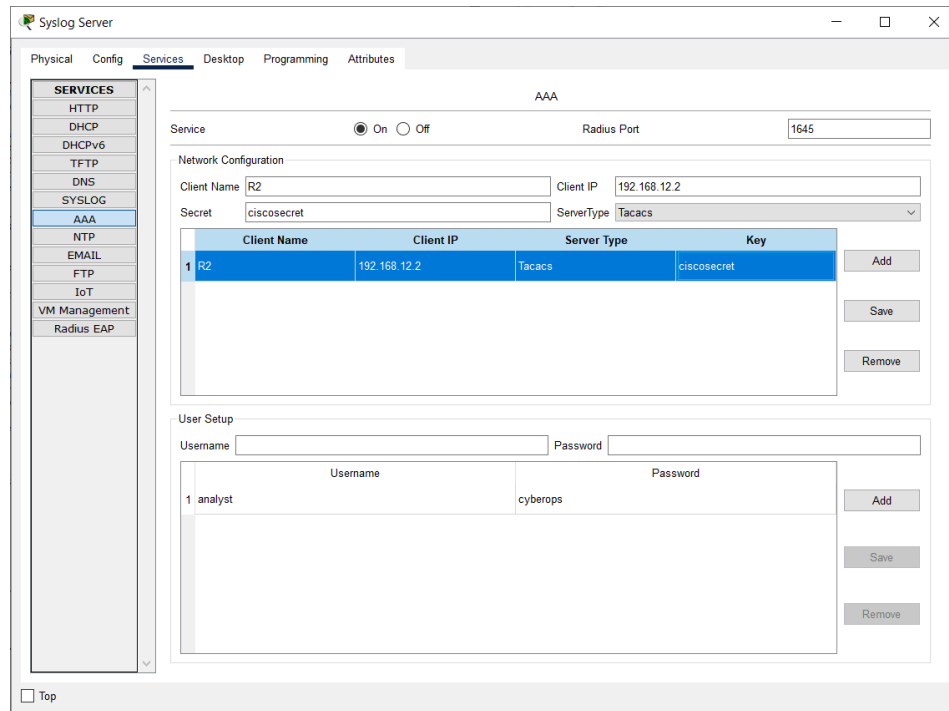
User Access Verification
Username: analyst
Password:
R2>
```

At the bottom of the window, there are 'Copy' and 'Paste' buttons, and a 'Top' button with a checkbox.

- e. Return to the Syslog Server's AAA Accounting Records window.

What information is in the log entry?

*R: The entry contains the username and password used, R2's IP address (the device used for the login attempt) and a Start flag. The Start flag indicates that the analyst user logged in at the time shown.*

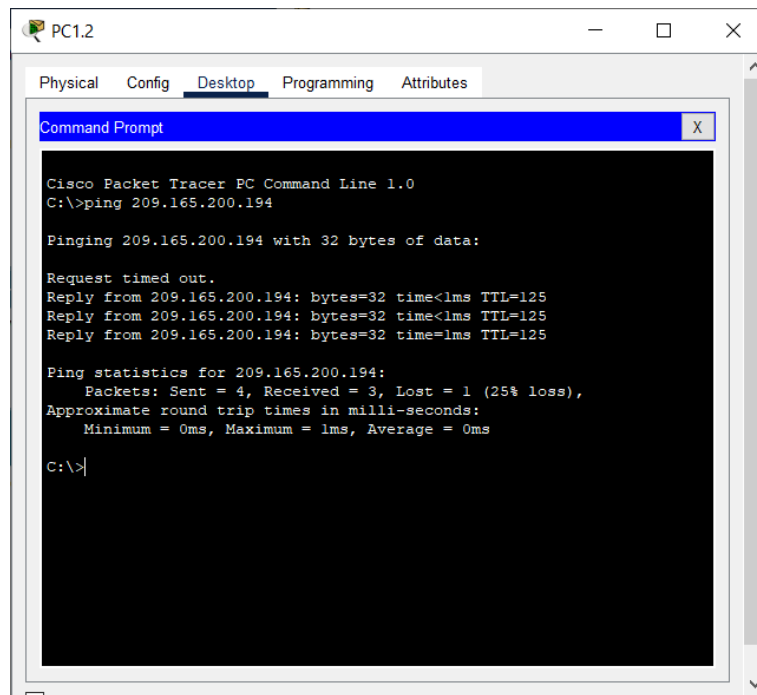


f. On R2, enter the logout command.

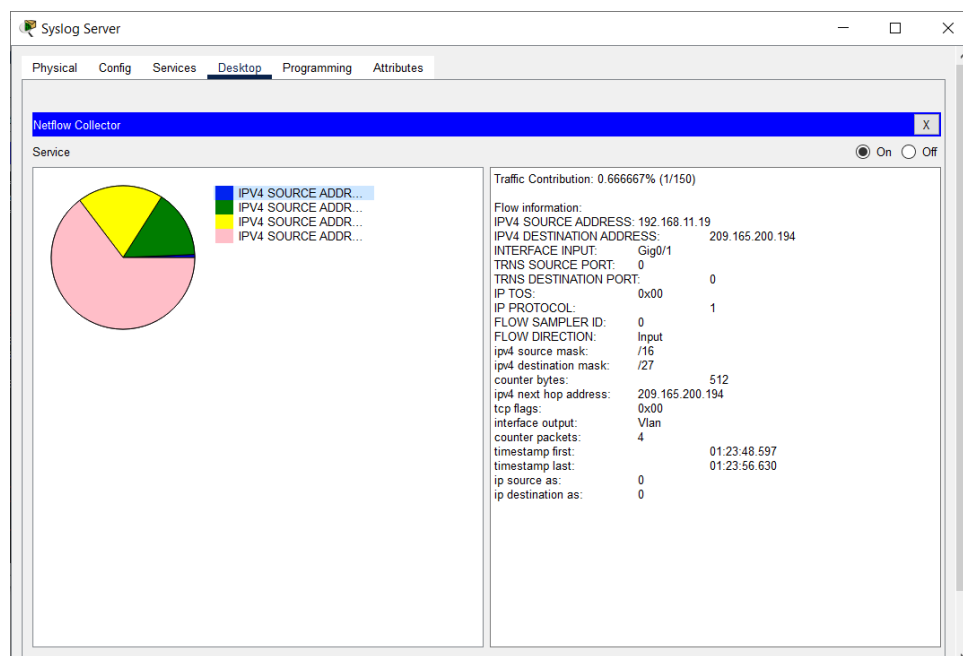
## Part 2: NetFlow and Visualization

In the topology, the Syslog server is also a NetFlow collector. The firewall is configured as a NetFlow exporter.

- Click the Syslog Server to bring up its window. Close the AAA Accounting Records window.
- From the Desktop tab, select Netflow Collector. The NetFlow collector services should be turned on.
- From any PC, ping the Corp Web Server at 209.165.200.194. After a brief delay, the pie chart will update to show the new traffic flow.



Note: The pie charts displayed will vary based on the traffic on the network. Other packet flows, such as EIGRP-related traffic, are being sent between devices. NetFlow is capturing these packets and exporting statistics to the NetFlow Collector. The longer NetFlow is allowed to run on a network, the more traffic statistics will be captured.



# Reflection

While the tools presented in this activity are useful, each one has its own service and may need to run on totally different devices. A better way is to have all the logging information be concentrated under one tool, allowing for easy cross-reference and powerful search capabilities. Security information and event management (SIEM) platforms can gather log files and other information from diverse sources and integrate the information for access by a single tool.