5.1.5 Lab - Tracing a Route

> **This lab has been updated for use on NETLAB+.**
> **www.netdevgroup.com**

Objectives

Step 1: Tracing a Route to a Remote Server Using Traceroute

Step 2: Trace a Route to a Remote Server Using Web-Based Traceroute Tool

Background

Tracing a route will list each routing device that a packet crosses as it traverses the network from source to destination. Route tracing is typically executed at the command line as:

```
tracert <destination network name or end device address>
```

(Microsoft Windows systems)

or

```
traceroute <destination network name or end device address>
```

(Unix and similar systems)

The **traceroute** (or **tracert**) tool is often used for network troubleshooting. By showing a list of routers traversed, it allows the user to identify the path taken to reach a particular destination on the network or across internetworks. Each router represents a point where one network connects to another network and through which the data packet was forwarded. The number of routers is known as the number of "hops" the data traveled from source to destination.

The displayed list can help identify data flow problems when trying to access a service such as a website. It can also be useful when performing tasks such as downloading data. If there are multiple websites (mirrors) available for the same data file, one can trace each mirror to get a good idea of which mirror would be the fastest to use.

Two trace routes between the same source and destination conducted some time apart may produce different results. This is due to the "meshed" nature of the interconnected networks that comprise the internet and the Internet Protocols' ability to select different pathways over which to send packets.

Command-line-based route tracing tools are usually embedded with the operating system of the end device.

Scenario

You will use two route tracing utilities to examine the internet pathway to destination networks. First, you will use the **traceroute** utility on the Linux command line. Second, you will use a web-based traceroute tool (https://gsuite.tools/traceroute).

Instructions

Step 1: Tracing a Route to a Remote Server Using Traceroute

Routes traced can go through many hops and a number of different Internet Service Providers (ISPs), depending on the size of your ISP and the location of the source and destination hosts. Each "hop" represents a router. A router is a specialized type of computer used to direct traffic across the internet. Imagine taking an

www.netacad.com

automobile trip across several countries using many highways. At different points in the trip you come to a fork in the road in which you have the option to select from several different highways. Now further imagine that there is a device at each fork in the road that directs you to take the correct highway to your final destination. That is what a router does for packets on a network.

Because computers talk in binary or hexadecimal numbers, rather than words, routers are uniquely identified using IP addresses. The **traceroute** tool shows you what path through the network a packet of information takes to reach its final destination. The **traceroute** tool also gives you an idea of how fast traffic is going on each segment of the network. Packets are sent to each router in the path, and the return time is measured in milliseconds.

To do this, the **traceroute** tool is used. Since the internet is not accessible within the environment, captured files are preloaded onto the virtual machine for review.

a. Launch the **Workstation** VM. Log on to the *Workstation* VM as the `analyst`, using the password `cyberops` and open a **terminal** window.

b. At the command prompt, change to the **/home/analyst/lab.support.files/traceroute_files/** directory.

```
[analyst@secOps ~]$ cd /home/analyst/lab.support.files/traceroute_files/
```

c. Analyze the captured **cisco-traceroute.txt** file using the **cat** command.

```
[analyst@secOps traceroute_files]$ cat cisco-traceroute.txt
```

```
[analyst@secOps traceroute_files]$ cat cisco-traceroute.txt
traceroute to www.cisco.com (23.193.180.155), 30 hops max, 60 byte packets
 1  10.34.0.1 (10.34.0.1)  39.893 ms  81.481 ms  81.486 ms
 2  209.95.50.1.static.midphase.com (209.95.50.1)  83.381 ms  83.383 ms  83.385 ms
 3  173.244.202.21.static.midphase.com (173.244.202.21)  82.023 ms 173.244.223.113.static.midphase.com
(173.244.223.113)  83.370 ms 173.244.202.21.static.midphase.com (173.244.202.21)  82.001 ms
 4  * seatac30-vpn.vpnreactor.com (173.244.202.30)  81.996 ms *
 5  * a23-193-180-155.deploy.static.akamaitechnologies.com (23.193.180.155)  83.343 ms  121.545 ms
```

d. While in the same directory, use the **cat** command to view captured *traceroute* traffic for the following websites with their associated filenames. These are the *Regional Internet Registry* (*RIR*) websites located in different parts of the world:

Africa:	**www.afrinic.net**	**afrnic-traceroute.txt**
Australia:	**www.apnic.net**	**apnic-traceroute.txt**
Europe:	**www.ripe.net**	**ripe-traceroute.txt**
South America:	**www.lacnic.net**	**lacnic-traceroute.txt**

Note: Some of these routers along the route may not respond to traceroute.

Step 2: Trace a Route to a Remote Server Using Web-Based Traceroute Tool

a. Open a web browser on your machine with internet accessibility and navigate to:
https://gsuite.tools/traceroute

b. Enter any website you wish. **Example: www.cisco.com** and press **Trace**.

Review the geographical locations of the responding hops. What did you observe regarding the path?

_____

_____

Reflection Question

How is the traceroute different when going to www.cisco.com or other websites from the terminal (see Part 2) rather than from the online website? (Your results may vary depending upon where you are located geographically, and which ISP is providing connectivity to your school.)

_____

_____