Lab – Tracing a Route

Objectives

Part 1: Verifying Network Connectivity Using Ping

Part 2: Tracing a Route to a Remote Server Using Traceroute

Part 3: 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

Using an Internet connection, you will use two route tracing utilities to examine the Internet pathway to destination networks. First, you will verify connectivity to a website. Second, you will use the **traceroute** utility on the Linux command line. Third, you will use a web-based traceroute tool (http://www.monitis.com/traceroute/).

Required Resources

- CyberOps Workstation VM
- Internet access

Part 1: Verifying Network Connectivity Using Ping

To trace the route to a distant network, the VM must have a working connection to the Internet.

a. Start the CyberOps Workstation VM. Log into the VM with the following credentials:

   Username: **analyst**

   Password: **cyberops**

b. Open a terminal window in the VM to ping a remote server, such as www.cisco.com.

```
[analyst@secOps ~]$ ping -c 4 www.cisco.com
PING e2867.dsca.akamaiedge.net (184.24.123.103) 56(84) bytes of data.
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com
(184.24.123.103): icmp_seq=1 ttl=59 time=13.0 ms
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com
(184.24.123.103): icmp_seq=2 ttl=59 time=12.5 ms
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com
(184.24.123.103): icmp_seq=3 ttl=59 time=14.9 ms
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com
(184.24.123.103): icmp_seq=4 ttl=59 time=11.9 ms

--- e2867.dsca.akamaiedge.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 11.976/13.143/14.967/1.132 ms
```

c. The first output line displays the Fully Qualified Domain Name (FQDN) e2867.dsca.akamaiedge.net. This is followed by the IP address 184.24.123.103. Cisco hosts the same web content on different servers throughout the world (known as mirrors). Therefore, depending upon where you are geographically, the FQDN and the IP address will be different.

   Four pings were sent and a reply was received from each ping. Because each ping received a response, there was 0% packet loss. On average, it took 3005 ms (3005 milliseconds) for the packets to cross the network. A millisecond is 1/1,000th of a second. Your results will likely be different.

Part 2: Tracing a Route to a Remote Server Using Traceroute

Now that basic reachability has been verified by using the ping tool, it is helpful to look more closely at each network segment that is crossed.

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 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 decimal 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.

a. At the terminal prompt, type **traceroute www.cisco.com**.

```
[analyst@secOps ~]$ traceroute www.cisco.com
traceroute to www.cisco.com (184.24.123.103), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  6.527 ms  6.783 ms  6.826 ms
 2  10.39.176.1 (10.39.176.1)  27.748 ms  27.533 ms  27.480 ms
 3  100.127.65.250 (100.127.65.250)  27.864 ms  28.570 ms  28.566 ms
 4  70.169.73.196 (70.169.73.196)  29.063 ms  35.025 ms  33.976 ms
 5  fed1bbrj01.xe110.0.rd.sd.cox.net (68.1.0.155)  39.101 ms  39.120 ms
39.108 ms
 6  a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103)
38.004 ms  13.583 ms  13.612 ms
```

b. If you would like to save the traceroute output to a text file for later review, use the right carat (>) and the desired filename to save the output in the present directory. In this example, the traceroute output is saved in the /home/analyst/cisco-traceroute.txt file.

```
[analyst@secOps ~]$ traceroute www.cisco.com > cisco-traceroute.txt
```

You can now enter the **cat cisco-traceroute.txt** command to view the output of the trace stored in the text file.

c. Perform and save the traceroute results for one of the following websites. These are the Regional Internet Registry (RIR) websites located in different parts of the world:

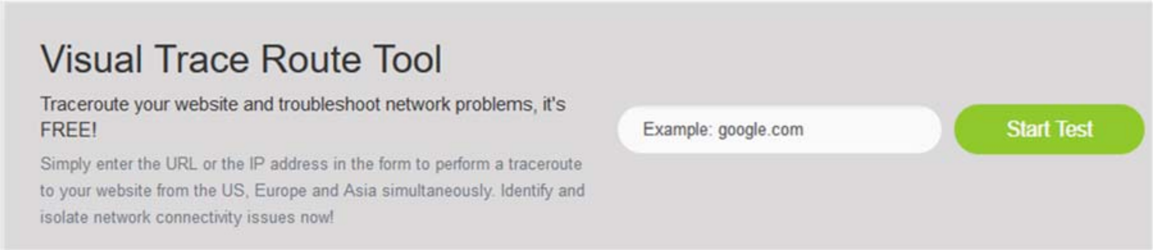
Africa:	**www.afrinic.net**
Australia:	**www.apnic.net**
Europe:	**www.ripe.net**
South America:	**www.lacnic.net**

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

Part 3: Trace a Route to a Remote Server Using Web-Based Traceroute Tool

a. Open a web browser in the VM and navigate to http://www.monitis.com/traceroute/.

b. Enter any website you wish to replace **Example: google.com** and press **Start Test**.



Visual Trace Route Tool

Traceroute your website and troubleshoot network problems, it's FREE!

Simply enter the URL or the IP address in the form to perform a traceroute to your website from the US, Europe and Asia simultaneously. Identify and isolate network connectivity issues now!

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

____

____

Reflection

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.)

____

© Cisco and/or its affiliates. All rights reserved. Cisco Confidential