

Lab – Troubleshooting Internet Connectivity

Objectives

In this lab, you will learn how to troubleshoot network connectivity using the following command utilities and software tools. Route tracing utilities allow a user to determine the path or route a packet takes as well as the delay across an IP network. Several tools exist to perform this function.

- Test Network Connectivity Using Ping
- Trace a Route to a Remote Server Using Windows Tracer
- Trace a Route to a Remote Server Using Web-Based and Software Tools
- Compare Traceroute Results

Tracert

Traceroute is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from source to destination. Tracert will show the IP addresses of all routers it the packet traversed along the way to its final destination. Traceroute also records the time taken between each hop traversed during its route to the destination.

Tracert is typically executed at the command line as:

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

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.

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.

Due to the “meshed” nature of the interconnected networks that comprise the Internet, two traceroutes between the same source and destination conducted some time apart may produce different results. Routers will periodically update their routing tables. When a router goes missing, it is removed from the routing table, and the best path is recalculated.

Command-line-based route tracing tools come embedded with the operating system to include Windows, MAC, Linux, routers, and switches.

Mapping Network Connectivity

In this lab, you will use an Internet connection and different route tracing utilities to examine the path a packet would take to reach a destination network. This lab requires Internet access and access to the command line.

In this first part of the lab, you will use the Windows embedded tracert utility. Next, you will use a web-based traceroute tool. To trace the route to a distant network, the PC used must have a working connection to the Internet. The first tool we will use is ping. Ping is a tool used to test whether a host is reachable. Packets of information are sent to the remote host with instructions to reply.


Your local PC measures whether a response is received to each packet, and how long it takes for those packets to cross the network. The name ping comes from active sonar technology in which a pulse of sound is sent underwater and bounced off of terrain or other ships.

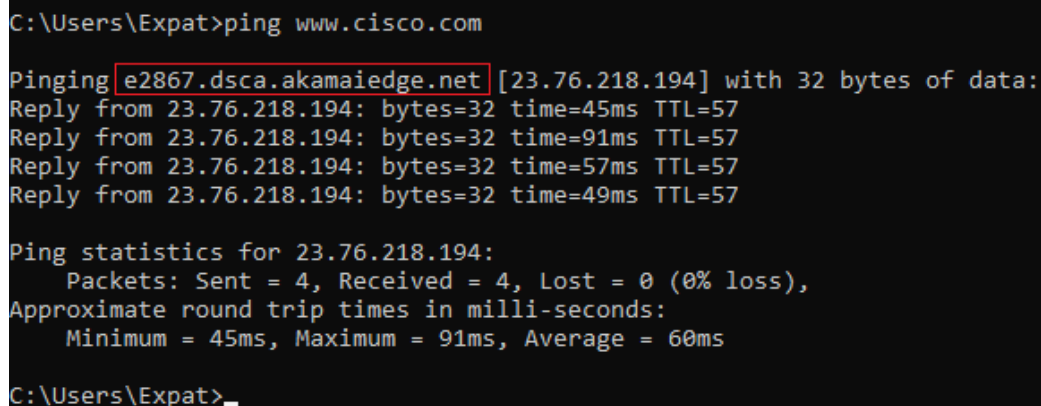
From your PC, click the Windows Start icon, type **cmd** in the Search programs and files box, and then press Enter.

At the command-line prompt, type:

```
ping www.cisco.com.
```

The first output line displays the Fully Qualified Domain Name (FQDN) e2867.dscb.akamaiedge.net. This is followed by the IP address 23.76.218.194. Cisco hosts the same web content on different servers throughout the world (known as mirrors). Therefore, depending upon where you are in the world, the FQDN and the IP address will be different.

 Command Prompt



```
C:\Users\Expat>ping www.cisco.com

Pinging e2867.dscb.akamaiedge.net [23.76.218.194] with 32 bytes of data:
Reply from 23.76.218.194: bytes=32 time=45ms TTL=57
Reply from 23.76.218.194: bytes=32 time=91ms TTL=57
Reply from 23.76.218.194: bytes=32 time=57ms TTL=57
Reply from 23.76.218.194: bytes=32 time=49ms TTL=57

Ping statistics for 23.76.218.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 45ms, Maximum = 91ms, Average = 60ms

C:\Users\Expat>_
```

If you got the same results or something similar with your PING attempt, you have Internet connectivity.

Four pings were sent, and a reply was received from each ping. Because each ping was responded to, there was 0% packet loss. On average, it took 60 ms (64 milliseconds) for the packets to cross the network. A millisecond is 1/1,000 of a second.

```
Ping statistics for 23.76.218.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 45ms, Maximum = 91ms, Average = 60ms
```

Streaming video and online games are two applications that suffer when there is packet loss or a slow network connection. A more accurate determination of an Internet connection speed can be determined by sending 100 pings, instead of the default 4.

Here are the output results for our 100-PING test:

```
Ping statistics for 23.76.218.194:
    Packets: Sent = 100, Received = 99, Lost = 1 (1% loss),
Approximate round trip times in milli-seconds:
    Minimum = 44ms, Maximum = 77ms, Average = 49ms
```

We can extend our networking testing by attempting to PING Regional Internet Registry (RIR) websites located in different parts of the world:

For Africa:

```
C:\> ping www.afrinic.net
```

```
C:\Users\Expat>ping www.afrinic.net

Pinging www.afrinic.net [196.216.2.6] with 32 bytes of data:
Reply from 196.216.2.6: bytes=32 time=415ms TTL=48
Reply from 196.216.2.6: bytes=32 time=400ms TTL=48
Reply from 196.216.2.6: bytes=32 time=396ms TTL=48
Reply from 196.216.2.6: bytes=32 time=400ms TTL=48

Ping statistics for 196.216.2.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 396ms, Maximum = 415ms, Average = 402ms

C:\Users\Expat>
```

For Australia:

```
C:\> ping www.apnic.net
```

```
C:\Users\Expat>ping www.apnic.net

Pinging www.apnic.net.cdn.cloudflare.net [104.18.235.68] with 32 bytes of data:
Reply from 104.18.235.68: bytes=32 time=24ms TTL=56
Reply from 104.18.235.68: bytes=32 time=25ms TTL=56
Reply from 104.18.235.68: bytes=32 time=26ms TTL=56
Reply from 104.18.235.68: bytes=32 time=30ms TTL=56

Ping statistics for 104.18.235.68:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 24ms, Maximum = 30ms, Average = 26ms

C:\Users\Expat>
```

For Europe:

```
C:\> ping www.ripe.net
```

```
C:\Users\Expat>ping www.ripe.net

Pinging www.ripe.net [193.0.6.139] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 193.0.6.139:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

The 'request timed out' means that either the site is down or ICMP packets requests are being blocked. If we open a web browser and visit the website using the given URL, we see that the site is up and running.

For South America:

```
C:\> ping www.lacnic.net
```

```
Pinging www.lacnic.net [200.3.14.184] with 32 bytes of data:
Reply from 200.3.14.184: bytes=32 time=382ms TTL=52
Reply from 200.3.14.184: bytes=32 time=384ms TTL=52
Reply from 200.3.14.184: bytes=32 time=389ms TTL=52
Reply from 200.3.14.184: bytes=32 time=425ms TTL=52

Ping statistics for 200.3.14.184:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 382ms, Maximum = 425ms, Average = 395ms

C:\Users\Expat>
```

All these pings were run from a computer located in the U.S.

Using Tracert to trace a Route to a Remote Server

We have verified basic connectivity using the PING tool. We can now look more closely at each network segment crossed using the tracert tool.

At the command prompt, type **tracert www.cisco.com**.

```
C:\Users\Expat>tracert www.cisco.com.

Tracing route to e2867.dsca.akamaiedge.net [104.111.164.146]
over a maximum of 30 hops:

  0  2 ms  2 ms  3 ms  192.168.0.1
  1  *      *      *      Request timed out.
  2  11 ms  30 ms  11 ms  172.31.103.5
  3  28 ms  12 ms  13 ms  130.105.255.11
  4  23 ms  14 ms  14 ms  130.105.255.10
  5  30 ms  46 ms  34 ms  114.108.194.73
  6  36 ms  30 ms  37 ms  130.105.0.24
  7  *      *      *      Request timed out.
  8  57 ms  56 ms  48 ms  a104-111-164-146.deploy.static.akamaitechnologies.com [104.111.164.146]

Trace complete.

C:\Users\Expat>
```

Type **tracert www.afrinic.net**

```
C:\Users\Expat>tracert www.afrinic.net

Tracing route to www.afrinic.net [196.216.2.6]
over a maximum of 30 hops:

 1    8 ms    2 ms    2 ms  192.168.0.1
 2    *      *      *      Request timed out.
 3   10 ms   10 ms   10 ms  172.31.103.5
 4    9 ms   12 ms   35 ms  130.105.255.11
 5   10 ms   11 ms   23 ms  130.105.255.10
 6   28 ms   27 ms   57 ms  114.108.194.73
 7   31 ms   42 ms   34 ms  130.105.0.18
 8   59 ms   48 ms   49 ms  v235.core1.hkg1.he.net [74.82.46.37]
 9   90 ms  131 ms  157 ms  100ge2-1.core1.sin1.he.net [184.105.222.102]
10  235 ms  222 ms  221 ms  100ge11-1.core1.mrs1.he.net [184.105.65.14]
11  272 ms  229 ms  232 ms  100ge4-2.core1.par2.he.net [184.105.222.21]
12  256 ms  239 ms  259 ms  100ge11-1.core1.lon2.he.net [184.105.223.253]
13  426 ms  406 ms  403 ms  10ge11-14.core1.jnb1.he.net [184.104.192.114]
14  400 ms  404 ms  410 ms  afrinic.jinx.net.za [196.223.14.60]
15  401 ms  400 ms  416 ms  tun0.br02.iso.afrinic.net [196.192.114.48]
16  402 ms  414 ms  419 ms  www.afrinic.net [196.216.2.6]

Trace complete.
```

Type `tracert www.lacnic.net`

```
C:\Users\Expat>tracert www.lacnic.net

Tracing route to www.lacnic.net [200.3.14.184]
over a maximum of 30 hops:

 1    2 ms    6 ms    2 ms  192.168.0.1
 2    *      *      *      Request timed out.
 3   17 ms   10 ms   18 ms  172.31.103.5
 4   17 ms   17 ms   21 ms  130.105.255.11
 5   27 ms   11 ms   32 ms  130.105.255.10
 6   28 ms   42 ms   51 ms  114.108.194.73
 7   34 ms   42 ms   41 ms  130.105.0.18
 8   51 ms   60 ms   67 ms  v235.core1.hkg1.he.net [74.82.46.37]
 9  139 ms  111 ms  105 ms  100ge10-1.core1.tyo1.he.net [184.105.64.130]
10  187 ms  189 ms  206 ms  100ge11-1.core1.sea1.he.net [184.105.213.117]
11  210 ms  214 ms  211 ms  100ge1-2.core1.msp1.he.net [184.104.194.22]
12  223 ms  224 ms  224 ms  100ge13-1.core2.chi1.he.net [184.105.223.177]
13  252 ms  241 ms  236 ms  100ge16-1.core1.nyc4.he.net [184.105.223.162]
14  438 ms  389 ms  354 ms  e0-35.core3.sao1.he.net [184.104.195.22]
15  346 ms  380 ms  348 ms  as28001.saopaulo.sp.ix.br [187.16.216.61]
16  357 ms  349 ms  355 ms  200.3.12.41
17  345 ms  359 ms  363 ms  200.3.12.34
18  373 ms  354 ms  345 ms  www.lacnic.net [200.3.14.184]

Trace complete.
```

Interpreting tracert outputs.

Routes traced can go through many hops and any number of 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 numbers, rather than words, routers are uniquely identified using IP addresses (numbers with the format x.x.x.x). The tracert tool shows you what path through the network a packet of information takes to reach its final destination. The tracert tool also gives you an idea of how fast traffic is going on each segment of the network. Three packets are sent to each router in the path, and the return time is measured in milliseconds. Now use this information to analyze the tracert results to www.cisco.com. Below is the entire traceroute:

To summarize, Internet traffic starts at your PC and travels through the home router. It then connects to the ISP and travels through its network until it arrives at the final destination.

This is a relatively unusual example in which there is only one ISP involved from start to finish. It is typical to have two or more ISP involved, as displayed in the following examples.

Using Web-Based and Software Tools

Use a web-based traceroute tool.

Use <https://www.ultratools.com/tools/traceRoute> to trace the route to the following three websites:

www.cisco.com
www.afrinic.net
www.lacnic.net.

In the next example, I have inputted the URL for www.ally.com and annotated that I want a maximum of 32 hops. From the Traceroute results, we are given the IP address of the router for each hop. If we click on the IP address, we will be taken to the domain registrar information for that router, where it is located and who owns the device.

I see that the 4th hop is located in Germany with an IP address of 173.205.39.229. If I click on the IP address, I will be shown the whois information for this device.

IP Traceroute Tool

Traceroute checks the route packets take to the specified host from the UltraTools server.

Enter a host name or IP address, and Maximum Hops:

<input type="text" value="www.ally.com"/>	<input type="text" value="32"/>	<input type="button" value="Go »"/>
---	---------------------------------	-------------------------------------

Related Tools: [Looking Glass](#) [Ping](#) [Ping-IPv6](#) [Traceroute-IPv6](#) [DNS Traversal](#)

Traceroute Information

Hop number:	1
Connected to:	assc-ultrafw-vlan2598.dc10.neustar.com (10.176.98.1)
Roundtrip times:	1.782 ms 1.633 ms 1.526 ms
Hop number:	2
Connected to:	ashlfns02-vlan102.dc10.neustar.com (10.176.2.3)
Roundtrip times:	1.433 ms 1.764 ms 1.837 ms
Hop number:	3
Roundtrip times:	Timed out.
Hop number:	4
Connected to:	et-0-0-43-3.cr2-was1.ip4.gtt.net (173.205.39.229)
Roundtrip times:	4.021 ms 4.304 ms 3.285 ms
Country:	germany
Hop number:	5
Connected to:	98.124.182.234 (98.124.182.234)
Roundtrip times:	11.962 ms 11.951 ms 11.933 ms
Country:	united states

Whois Information

Go »

Related Tools: [DNS Traversal](#) [Traceroute](#) [Vector Trace](#) [Ping](#) [WHOIS Lookup](#)

Source:	whois.arin.net
IP Address:	173.205.39.229
Name:	TINET-TINET
Handle:	NET-173-205-36-0-1
Registration Date:	3/14/16
Range:	173.205.36.0-173.205.39.255
Customer:	Tinet GmbH
Customer Handle:	C06066273
Address:	Hugenottenallee 167
City:	Neu-Isenburg
State/Province:	
Postal Code:	63263
Country:	Germany
Name Servers:	

Summary –

This lab, as so many implications, it's hard to cover them all. We get the troubleshooting part, but what about trying to find where an unsolicited email originated from? By looking at the HTML of the email, we can see the sender's IP address, so we can use these same tools to see what path the email took to get to your mailbox by just doing a reverse lookup.

The big takeaway for this lab is to remember that the Internet is a MESH topology. It's built this way for redundancy. Today you will be given one set of results using tracert. If a router in the results goes down overnight, the next day, you would be shown a different tracert result because the path for the packet had to be rerouted.