**Boris Jurosevic**

**CS 2705**

**Network Trouble Shooting Lab**

Pull up a command prompt. Click start->all programs->accessories->command prompt and ping the following sites what IP addresses do you get and what is the average round trip time.

Enter: ping <address>

|  |  |  |
| --- | --- | --- |
|  | IP Address | Average round trip in milli-seconds |
| [www.lego.com](http://www.lego.com) | 171.20.34.151 | 172 ms |
| [www.majong.com](http://www.majong.com) | 208.87.35.103 | 79 ms |
| [www.google.com](http://www.google.com) | 208.117.232.120 | 35 ms |
| [www.facebook.com](http://www.facebook.com) | 31.13.75.17 | 41 ms |
| [www.walmart.com](http://www.walmart.com) | 184.51.49.194 | 21 ms |

Why would PING function be useful in troubleshooting a network problem? What are the limitations of PING?

Ping operates over the ICMP protocol (using ICMP Echo Request and Echo response) to attempt to contact a host given some kind of unique identifier (hostname, domain, IP, etc.). If it is successful, it will return a reply from that IP address; if it is unsuccessful, it will inform you that the “destination could not be reached.” Why is this useful? Suppose you are trying to determine why you are unable to access the company’s remote email server through “Outlook.” The problem could stem from a number of issues, including:

The computer is not properly configured for the internal network (media problems, TCP/IP configuration issues, router is down, etc.). The Internet connection is down. There is an issue in connecting to the email server at the Application or Connection layers (maybe he is connecting to the wrong port, NAT issues, email server is rejecting connections).The remote host is down or is unavailable in general (IP connection issues.

One of the primary ping limitations is that it is, at its heart, an ICMP Echo based tool. What does that mean? Well, ICMP stands for Internet Control Message Protocol. This differs significantly from TCP or UDP since it is not typically used to transmit data directly. It is used for diagnostic, control or error reporting and are processed both by the sender and receiver as a special case, outside of normal IP processing. This has several reasons, performance and security. It makes these packets easier to manage and filter and harder to use to compromise the security and integrity of the systems involved in the transaction (with one notable exception covered below). As a result, ping results can be inconsistent – meaning that sometimes it works and sometimes it does not. A common security filter on internet facing systems is to ‘drop’ ICMP based requests (like ping), so it will look like the site or system is not responding at all on the other end of the request.

Now use trace route to find the hops and time it takes to get to the following websites. It should be noted that the command in Linux is TRACEROUTE but in Windows it is TRACERT. An example of the command you enter at the command prompt for this exercise would be: TRACERT www.weber.edu

Enter: tracert <address>

|  |  |  |
| --- | --- | --- |
|  | # of hops | Time |
| [www.lego.com](http://www.lego.com) | 30 | 169 ms,169 ms,167 ms |
| [www.majong.com](http://www.majong.com) | 30 | 72 ms, 89 ms, 71 ms |
| [www.google.com](http://www.google.com) | 30 | 30 ms, 34 ms , 22 ms |
| [www.facebook.com](http://www.facebook.com) | 30 | 47 ms,40 ms,56 ms |
| [www.walmart.com](http://www.walmart.com) | 30 | 30 ms,27 ms,23 ms |

Why would trace route be helpful to you in troubleshooting a network problem? How would this information differ from what you would get if you did PING?

Trace route would be helpful in troubleshooting because it would determine whether routing problems exist on the network. Trace route can be used to determine which path IP packets are taking to get from your computer to the remote computer. Trace route shouldn't be used on a network without routers. It is not really useful unless there are at least two routers in the network. The Internet has thousands (dare we say millions?) of routers so trace route is perfect for the Internet. Trace route was designed to reveal when network failures such as routing loops and black holes occur and shows roughly where those failures exist.

The main difference is Ping is a quick and easy way to tell you if the destination server is online and estimates how long it takes to send ands receive data to the destination. Trace route tells you the exact route you take to reach the server from your computer (ISP) and how long each hop takes.

We will not switch from a command line trace route to a graphical trace route. This site is hosted on a server outside of your location. It does a trace route from the server to you and a second trace route from the server to the desired destination. It gives you a nice interface to see where it is going. Now go to: <http://www.yougetsignal.com/tools/visual-tracert/>

And do a proxy trace route of the following addresses.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | # of Hops | Time | Miles traveled | Final Geographic location |
| [www.lego.com](http://www.lego.com) | 33 | 30.9 sec | 17,923 | Billund, Denmark |
| [www.majong.com](http://www.majong.com) | 24 | 27.1 | 11,012 | Nassau, Bahamas |
| [www.google.com](http://www.google.com) | 20 | 21 sec | 4,302 | Mountain View, CA, USA |
| [www.facebook.com](http://www.facebook.com) | 18 | 23.8 | 5,972 | Unkown location,  www.facebook.com |
| [www.walmart.com](http://www.walmart.com) | 20 | 23.3 | 3,292 | Unkown location,  akamaitechnologies.com |

Why are the numbers of hops different when comparing trace route and proxy trace? What are your thoughts of the visual pattern of where the signals went around the country and world?

It different because the visual tracert tool displays the path Internet packets traverse to reach a specified destination. The tool works by identifying the IP addresses of each hop along the way to the destination network address.

I thought that this was the most interesting out of the three that we did. I think all three things that we did in this lab has their different meaning and how important they are, but what I found most interesting about visual tracert tool is that it displays geographic location visually.