COMP 431 — INTERNET SERVICES & PROTOCOLS

Spring 2020

(Optional) Extra-Credit Homework, Jan 30

Due: 10:30 am, March 17

Investigations into the Structure and Performance of the Internet

In this assignment you will perform some simple experiments using tools called *ping* and *traceroute* in an attempt to understand the structure and performance of the Internet. *ping* and *traceroute* are network probing utilities that exist on both UNIX and Windows. *ping* is a program that sends a 1-packet IP datagram to a remote host and requests the host to return the datagram to the sender. The *ping* program measures the time it takes for the datagram to be delivered to the remote host and then be returned to the sender. This time is commonly referred to as the "round-trip time" between the sender and receiver. *traceroute* is a more complex tool. Briefly, it discovers and reports the names of the routers along the path between a source and a destination (it "traces the route"), as well as reports on the round-trip-times between the source and each router on the path. A brief tutorial on the use of each tool is included below.

The experiments you will perform will consist of a series of "ping trials" to a remote host. In each experiment you will first determine the route from your local computer to a remote host using *traceroute*. Once you have the route you are to ping each router along the path from the local machine to the remote host 60 times in one minute and record the average delay and loss rates seen. You are to repeat the ping experiments 5 times during a single weekday. The 5 time periods are early morning (7-9am), mid-morning (10am-12pm), mid-afternoon (2-5pm), evening (6-8pm), and night (10pm-6am). During each of these time periods you are to run 1 ping trial to each router on the path to your remote host. Once you have gathered your data, make a series of plots and tables that show the how the delay and loss rates change over time. In addition, write text that describes and explains your data.

You are to perform three series of identical experiments. One experiment should be to a major university on the West coast (*e.g.*, UC Berkeley, UCLA, USC, University of Washington, *etc.*), one should be to your favorite (non-local) web site (to the server that hosts your favorite web site), and one to an institution in Europe or Asia. You can include more sites in your experiments if you like but you must include at least one of each of these three classes of sites.

In this optional, extra-credit assignment, you will work in groups of 3 (feel free to use piazza to find group-mates).

Submission: Ultimately, you are to video record a presentation using slides, upload the recording on youtube, and submit on Gradescope a link to it (along with the names of the 3 students who have worked on the assignment). Your presentation should describe the experiments you performed, the data you gathered (in the form of plots or tables), and any interesting anomalies you observe or conclusions you are able to draw from the data.

30% of the grade is reserved for interesting observations, analysis, or conclusions you make over and above simply presenting the experimental data --- the remaining 70% will be assigned based on the correctness of your experiments, and how informatively you present the data gathered. Be creative and curious!

Remember to present your data in the most succinct manner possible; in general, plots convey the point much more effectively than tables. Make sure you label all plots and indicate the units of what you're plotting.

A Quick Primer on *ping* and *traceroute*

Ping on UNIX

The syntax for the ping command on UNIX is:

```
/bin/ping [-c count] [-s packetsize] host
```

As per the UNIX convention, the parameter options in square brackets ("[ ]") are optional. (There are lots of additional parameters to ping — read the on-line man page for details; here we just list the most useful ones.) The parameters are:

`unt`	The number of times to ping the host (pinging once per second).
`cket_size`	The size of the ping packet to send (in bytes).
	The host name (or IP address) of the host to ping.

For example, if we ping the main Web server for Duke (*www.duke.edu*) 5 times with 50 byte packets we get the following:

```
(classroom) 118> ping -c 5 -s 50 www.duke.edu
PING webhost-lb-01.oit.duke.edu (152.3.189.3) 50(78) bytes of data.
58 bytes from WEBHOST-LB-01.oit.duke.edu (152.3.189.3): icmp_seq=0 ttl=252 time=2.48 ms
58 bytes from WEBHOST-LB-01.oit.duke.edu (152.3.189.3): icmp_seq=1 ttl=252 time=3.65 ms
58 bytes from WEBHOST-LB-01.oit.duke.edu (152.3.189.3): icmp_seq=2 ttl=252 time=2.46 ms
58 bytes from WEBHOST-LB-01.oit.duke.edu (152.3.189.3): icmp_seq=3 ttl=252 time=2.46 ms
58 bytes from WEBHOST-LB-01.oit.duke.edu (152.3.189.3): icmp_seq=4 ttl=252 time=2.47 ms

--- webhost-lb-01.oit.duke.edu ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 2.463/2.707/3.656/0.475 ms, pipe 2
```

First *ping* echos the name and IP address of the machine to be pinged, the IP address of the pinging machine, and the message size. *ping* then reports the results of each of the 5 pings. Note that the messages received are 58 bytes and not 50. The additional 8 bytes are because of protocol headers (which again will be explained later in the course). *ping* then reports the fully qualified name and IP address of the machine that responded to the ping, namely *webhost-lb-01.oit.duke.edu*. Note that the name of the machine responding, *webhost-lb-01.oit.duke.edu*, is different from what we specified on the command line. This is because when *ping* attempts to resolve the domain name *www.duke.edu*, it learns that *www.duke.edu* is a synonym for the machine *webhost-lb-01.oit.duke.edu* (we'll study the problem of name assignment and name resolution later in the course). Next, *ping* reports a sequence number indicating which ping message this is in response to ("icmp_seq=#"). If a ping message is lost there will be a gap in the sequence numbers (*i.e.*, if ping *k* is lost, you won't see a ping report with icmp_seq=*k*). The next field reports the time-to-live value of the response ("ttl=251"). This field can be ignored for this assignment. Finally *ping* reports how long it took the ping message to be delivered to the destination and for the response to return ("time=*x*"). After the 5 summary lines, it reports a summary of the exchange including the number of messages sent, received, and lost as well as the min, average, and maximum round-trip times.

Ping on a PC

The format of the command on the PC is slightly different:

```
ping [-n count] [-l packet_size] host
```

but it works the same way:

```
$ ping -n 5 -l 1000 www.duke.edu

Pinging webhost-lb-01.oit.duke.edu [152.3.189.3] with 1000 bytes of data:
```

```
Reply from 152.3.189.3: bytes=1000 time=3ms TTL=251
Reply from 152.3.189.3: bytes=1000 time=3ms TTL=251
Reply from 152.3.189.3: bytes=1000 time=3ms TTL=251
Reply from 152.3.189.3: bytes=1000 time=3ms TTL=251
Reply from 152.3.189.3: bytes=1000 time=2ms TTL=251

Ping statistics for 152.3.189.3:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum =  3ms, Average = 2ms
```

Once again there is a summary of the command request, though in a different format. After the replies are received, a summary is again reported with the same information as the UNIX version.

On the PC, running the ping command with only a host is the same as running "*ping -n 4 host*"; you get 4 summary lines.

Traceroute on UNIX

The *traceroute* command just takes a hostname (or IP address) as an argument:

```
/bin/traceroute host
```

traceroute probes routers along the path from the local machine to the host with a message that is similar to a ping. Each router will be "pinged" 3 times. *traceroute* reports the series of routers that are encountered along the path from source to destination and the statistics about the time it takes to reach each of these gateways. For example, a traceroute to *www.duke.edu* results in the following trace:

```
comp431sp19:~$ traceroute www.duke.edu
traceroute to www.duke.edu (152.3.72.197), 30 hops max, 60 byte packets
1  fluffy-v23.net.unc.edu (152.2.31.1)  0.471 ms 0.585 ms 0.567 ms
2  core-p-v1554.net.unc.edu (152.19.253.89)  18.957 ms 18.953 ms 19.230 ms
3  border-p-v1213.net.unc.edu (152.2.255.65)  1.186 ms 1.430 ms 1.795 ms
4  ws-gw-to-uncphillips.ncren.net (128.109.1.89)  5.016 ms 4.979 ms 4.923 ms
5  duke-nc1-edge-to-ws-gw.ncren.net (128.109.1.214)  8.836 ms 8.823 ms 8.923 ms
6  * * *
7  * * *
8  * * *
9  * * *
10  152.3.72.254 (152.3.72.254)  10.837 ms 10.665 ms 10.630 ms
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  fitz-ltm-01-ex.oit.duke.edu (152.3.72.251)  585.652 ms !H 585.645 ms !H *
```

This trace shows that there are 22 routers ("hops") traversed when data is transmitted from the local UNIX host to *www.duke.edu*. The first two lines of output simply reports the machine to contact and some other information that is unimportant for now. The line beginning "1" is information about the first gateway reached. This is the router *fluffy-v23.net.unc.edu*, with IP address *152.2.31.1*. The three time values listed on line 1 are the amount of time it took to reach *fluffy-v23* on each of the 3 attempts to probe the route.

The other routers along the way to Duke were three UNC machines (core-p-v1554.net.unc.edu, border-p-v1213.net.unc.edu, border-p-v1213.net.unc.edu) and two North Carolina Research and Education Network (NCREN) machines (ws-gw-to-uncphillips.ncren.net, duke-nc1-edge-to-ws-gw.ncren.net). 10th hope was through the IP address 152.3.72.254 which belongs to a machine at Duke and the final hop is through fitz-ltm-01-ex.oit.duke.edu.

When you use *traceroute* it is highly likely that errors will be encountered. Common errors include lost probe messages and an inability to determine the name of a router or gateway. In the former case, if probe messages are lost or if the host was unreachable, asterisks will be printed in place of a time value (*e.g.*, instead of printing three time values. If traceroute is unable to determine the name of a router or gateway you will see a series of "*'s" for the name of the host---we observed such hops on lines 6 to 9 and 11 to 21. This may indicate that either the probe is failing or that the network administrators do not wish to report any statistics for that gateway. It is recommended that you study the on-line UNIX man page for *traceroute* to completely understand the program's output.

Traceroute on a PC

The *traceroute* command on the PC has a different name (to conform to the archaic MSDOS "8.3" filename format) but basically works the same way:

```
C:\Users\IEUser>tracert www.duke.edu

Tracing route to duke.edu [152.3.72.197]
over a maximum of 30 hops:

 1   <1 ms    <1 ms <1 ms  192.168.226.2
 2    1 ms  <1 ms <1 ms  fluffy-v23.net.unc.edu [152.2.31.1]
 3    1 ms   1 ms 1 ms  core-p-v1554.net.unc.edu [152.19.253.89]
 4    1 ms   1 ms 1 ms  border-p-v1213.net.unc.edu [152.2.255.65]
 5    5 ms   4 ms 5 ms  ws-gw-to-uncphillips.ncren.net [128.109.1.89]
 6    8 ms   8 ms 8 ms  duke-nc1-edge-to-ws-gw.ncren.net [128.109.1.214]
 7    *   * *     Request timed out.
 8    *   * *     Request timed out.
 9    *   * *     Request timed out.
10     * *        * Request timed out.
11    11 ms  10 ms 10 ms  152.3.72.254
12    11 ms  10 ms 12 ms  152.3.72.197

Trace complete.
```

The summary lines simply list the time required for each probe first and then list the hostname and IP address. Note that the PC version doesn't report precise times, instead reporting times like 1 *ms*, less than 10 *ms*, or 80 *ms*.