Project #2

CIS 427 – Fall 2018
Prof. John P. Baugh, Ph.D.

Points: ___________________ / 100
Due: November 9, 2018 at 11:59 p.m.

Introduction

In this assignment you will get a chance to experiment with two very useful and widely-used network diagnostic tools, `traceroute` and `ping`, to expose you to some of the interesting quirks in network routing and packet round trip times.

Before you proceed with the assignment, read the related documents of these tools carefully and make sure that you understand how they work. Keep in mind that some of the following tasks involve measurements during an entire week, so you need to start working on this as early as possible.

Routing measurements

As the name implies, `traceroute` essentially allows you to trace the entire route from your machine to a remote machine. The remote machine can be specified either as a name or as an IP address.

We include a sample output of an execution of `traceroute` and explain the salient features. The command in a Windows system:

```
>tracert www.yahoo.com
```

tries to determine the path from the source machine to `www.yahoo.com`. (Note that the command should be **`traceroute www.yahoo.com,`** if you do it in a Linux/UNIX system). The machine encountered on the path after the first hop is `fob.net.umd.umich.edu [141.215.80.1]`, the next is `i-cw-elb.net.umd.umich.edu [141.215.2.33]`, and so on. In all, it takes 15 hops to reach `p13.www.dcn.yahoo.com`.

```
C:\Documents and Settings\jinhua>tracert www.yahoo.com

Tracing route to www.yahoo.akadns.net [216.109.118.71]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  fob.net.umd.umich.edu [141.215.80.1]
  2    <1 ms    <1 ms    <1 ms  i-cw-elb.net.umd.umich.edu [141.215.2.33]
  3    <1 ms    <1 ms    <1 ms  141.215.2.130
  4     1 ms     1 ms    <1 ms  i-merit.net.umd.umich.edu [141.215.2.2]
  5    12 ms    12 ms    13 ms  198.108.22.165
  6    24 ms    12 ms    12 ms  g1.ba21.b002281-1.ord01.atlas.cogentco.com [66.28.21.233]
  7    16 ms    15 ms    13 ms  p12-0.core02.ord01.atlas.cogentco.com [154.54.2.241]
  8    82 ms    38 ms    39 ms  p6-0.core02.jfk02.atlas.cogentco.com [66.28.4.85]
  9    54 ms    40 ms    40 ms  p14-0.core01.phl01.atlas.cogentco.com [66.28.4.2]
 10    51 ms    43 ms    44 ms  p4-0.core01.dca01.atlas.cogentco.com [66.28.4.17]
 11     47 ms     45 ms     45 ms  p2-0.core01.iad01.atlas.cogentco.com [154.54.2.202]
 12     45 ms     47 ms     46 ms  yahoo.iad01.atlas.cogentco.com [154.54.10.2]
 13     52 ms     47 ms     45 ms  ae1.p400.msr1.dcn.yahoo.com [216.115.96.181]
 14     48 ms     47 ms     50 ms  ge5-2.bas1-m.dcn.yahoo.com [216.109.120.151]
 15     45 ms     46 ms     78 ms  p8.www.dcn.yahoo.com [216.109.118.71]

Trace complete.
```

In this part of the assignment, you will monitor the routing stability of the Internet using traceroute. ***Choose 5 destination hosts (`targets'). If you work in a pair, you will need 10 targets.*** The targets should be distributed around the world.

Please do not monitor hosts of the .MIL domain. They may come for you in your sleep and your family will never see you again.

In addition, you should avoid routers and hosts that disable or don’t support ICMP functions (e.g.,with a lot of timeout responses).

1. Using traceroute (from a local machine), monitor and record the routing path to each target for an entire week. You should perform about 2 measurements every day, for a total of at least 10 measurements per target for the duration of the week.
2. Some host names may be dynamically mapped to a number of geographically dispersed servers (e.g., www.cnn.com). Therefore, after you learn the IP address of a host name, you need use the IP address instead of the host name (e.g. tracert 23.235.40.73).
3. For which targets do you observe the same routing path in all measurements? For which targets do you observe several different paths? Comment on the **stability** of the routes that you have monitored.
4. For the paths that do tend to change, what is the nature of the routing change (e.g., differences in the number of hops, differences in the network providers that traffic goes through, differences in the exact router interfaces that traffic goes through)? *Hint: To identify the Autonomous System Number or ISP for each router, you can use the command “whois -h whois.arin.net ASN” or “whois -h radb.ra.net IPaddr” or visit http://www.arin.net/whois/ for more information.*
5. For a path that is not stable, attempt to (roughly) estimate how often does the route change. You may need to perform more frequent measurements to those targets.

Loss and Round-Trip Time (RTT) measurements

The ping utility is one of the more useful utilities for testing a network. The ping utility works by sending a short message of type echo-request to a host using a network protocol called **ICMP**, the **Internet Control Message Protocol**. A host that supports ICMP (and most do) and receives an echo-request message simply replies by sending a short ICMP message of type echo-response back to the originating host.

The following is a sample output of an execution of `ping`:

```
C:\Documents and Settings\jinhua>ping –n 14 sina.com.cn
```

```
Pinging sina.com.cn [202.106.184.200] with 32 bytes of data:

Reply from 202.106.184.200: bytes=32 time=255ms TTL=237
Reply from 202.106.184.200: bytes=32 time=256ms TTL=237
Reply from 202.106.184.200: bytes=32 time=254ms TTL=237
Reply from 202.106.184.200: bytes=32 time=262ms TTL=237
Request timed out.
Reply from 202.106.184.200: bytes=32 time=251ms TTL=237
Reply from 202.106.184.200: bytes=32 time=252ms TTL=237
Reply from 202.106.184.200: bytes=32 time=253ms TTL=237
Reply from 202.106.184.200: bytes=32 time=298ms TTL=237
Reply from 202.106.184.200: bytes=32 time=265ms TTL=237
Reply from 202.106.184.200: bytes=32 time=254ms TTL=237
Reply from 202.106.184.200: bytes=32 time=267ms TTL=237
Reply from 202.106.184.200: bytes=32 time=258ms TTL=237

Ping statistics for 202.106.184.200:
    Packets: Sent = 14, Received = 12, Lost = 2 (14% loss),
Approximate round trip times in milli-seconds:
    Minimum = 251ms, Maximum = 298ms, Average = 260ms
```

In this part of the assignment, you will monitor the loss and delay performance characteristics of some Internet paths using ping. You can use the same set of targets as in the previous part of the assignment. It is better, however, to choose targets that do not experience frequent routing changes.

1. As in the previous part of the assignment, measure the loss rate and RTTs for each target for the duration of a week. You should perform about 2 measurements every day, for a total of about 10 measurements per target for the duration of the week. Each measurement should send **120 echo requests** by using the *`-n count`* (number of echo requests to send) option.
2. Use the previous measurements to classify your targets as `loss free', `minor losses' (0 < loss rate < 5%), `significant losses' (5% < loss rate <10%), and `major losses' (loss rate > 10%). Does this classification remain the same throughout the week for each target?
3. Measure the minimum/maximum/mean RTT for each target.
4. Plot the loss rate and RTTs for each target as a function of time. Do you observe any significant changes between different times-of-day or days-of-week?

Deliverables

Write an experiment report (approximately 10-20 pages) that describes your methodology and results. Avoid verbose discussion of the results. Additional results, insight, and analysis of the results, however, are *strongly* encouraged. In general, your report should include the following components:

- Abstract (summary)
- Introduction (background and hypothesis)
- Methodology
- Results
- Conclusions

- What did you learn?

Please submit **the report and all your DATA files (plain text)** as a single zip file to the Canvas under the appropriate folder.