Lab 2: Enterprise Networking

PART 1: Debugging exterior routing with BGP Updates

Please investigate and answer the following questions in your report:

1.Pretend you are an AS directly peered with vantage point 12.0.1.63. Process all updates for this vantage point for the day of January 29, 2018 (all updates for that day, not just one snapshot file - consider using wget and check out the "-A" flag and how to make wget ignore robots.txt and recurse just one level). Which routes (to prefixes) are the most unstable? What is going on with those routes, why are they unstable, what do you observe?

Commands :

wget -r -e robots=off --wait 1 -A updates.20180129.*.bz2 http://archive.routeviews.org/bgpdata/2018.01/UPDATES/

for f in ../UPDATES/updates.20180129.*; do ./bgpdump -M $f -O output.txt; done.
awk '/12.0.1.63/ && /W/' output.txt | sort -rnk5 | head -10

```
root@b317c63c8ac5:/home/lab2/archive.routeviews.org/bgpdata/2018.01/ripencc-bgpdump-99da8741c8c8# awk '/12.0.1.63/ && /W/' output.txt | sort -rnk5 | head -10
BGP4MP|01/29/18 00:14:58|W|12.0.1.63|7018|193.0.132.0/22
BGP4MP|01/29/18 00:14:52|W|12.0.1.63|7018|209.177.171.0/24
BGP4MP|01/29/18 00:14:47|W|12.0.1.63|7018|66.146.74.0/24
BGP4MP|01/29/18 00:14:47|W|12.0.1.63|7018|66.146.31.0/24
BGP4MP|01/29/18 00:14:47|W|12.0.1.63|7018|66.146.14.0/24
BGP4MP|01/29/18 00:14:41|W|12.0.1.63|7018|199.245.187.0/24
BGP4MP|01/29/18 00:14:41|W|12.0.1.63|7018|198.148.151.0/24
BGP4MP|01/29/18 00:14:24|W|12.0.1.63|7018|93.181.192.0/19
BGP4MP|01/29/18 00:14:23|W|12.0.1.63|7018|93.181.192.0/19
BGP4MP|01/29/18 00:14:22|W|12.0.1.63|7018|209.177.171.0/24
```

awk '/12.0.1.63/ && /193.0.132.0\/'/22/ && /W/' output.txt |head -30

```
root@b317c63c8ac5:/home/lab2/archive.routeviews.org/bgpdata/2018.01/ripencc-bgpdump-99da8741c8c8# awk '/12.0.1.63/ && /193.0.132.0\/'/22/ && /W/' output.txt |head -30
BGP4MP|01/29/18 00:01:04|W|12.0.1.63|7018|193.0.132.0/22
BGP4MP|01/29/18 00:01:13|W|12.0.1.63|7018|193.0.132.0/22
BGP4MP|01/29/18 00:02:15|W|12.0.1.63|7018|193.0.132.0/22
BGP4MP|01/29/18 00:02:19|W|12.0.1.63|7018|193.0.132.0/22
BGP4MP|01/29/18 00:03:15|W|12.0.1.63|7018|193.0.132.0/22
BGP4MP|01/29/18 00:04:01|W|12.0.1.63|7018|193.0.132.0/22
BGP4MP|01/29/18 00:04:55|W|12.0.1.63|7018|193.0.132.0/22
BGP4MP|01/29/18 00:06:15|W|12.0.1.63|7018|193.0.132.0/22
BGP4MP|01/29/18 00:07:21|W|12.0.1.63|7018|193.0.132.0/22
BGP4MP|01/29/18 00:08:01|W|12.0.1.63|7018|193.0.132.0/22
BGP4MP|01/29/18 00:09:02|W|12.0.1.63|7018|193.0.132.0/22
BGP4MP|01/29/18 00:09:54|W|12.0.1.63|7018|193.0.132.0/22
BGP4MP|01/29/18 00:10:07|W|12.0.1.63|7018|193.0.132.0/22
BGP4MP|01/29/18 00:11:01|W|12.0.1.63|7018|193.0.132.0/22
BGP4MP|01/29/18 00:12:01|W|12.0.1.63|7018|193.0.132.0/22
```

BGP4MP|01/29/18 00:13:11|W|12.0.1.63|7018|193.0.132.0/22
BGP4MP|01/29/18 00:13:54|W|12.0.1.63|7018|193.0.132.0/22
BGP4MP|01/29/18 00:14:58|W|12.0.1.63|7018|193.0.132.0/22

awk '/12.0.1.63/ && /\'/'24/' output.txt |head -30

root@b317c63c8ac5:/home/lab2/archive.routeviews.org/bgpdata/2018.01/ripencc-bgpdump-99da8741c8c8# awk '/12.0.1.63/ && /\'/'24/' output.txt |head -30

BGP4MP|01/29/18 00:00:58|A|12.0.1.63|7018|93.175.149.0/24|7018 1299 29075 12654|IGP

BGP4MP|01/29/18 00:00:58|A|12.0.1.63|7018|84.205.69.0/24|7018 3257 13237 12654|IGP

BGP4MP|01/29/18 00:00:58|A|12.0.1.63|7018|84.205.74.0/24|7018 3257 12637 12654|IGP

BGP4MP|01/29/18 00:00:58|A|12.0.1.63|7018|84.205.70.0/24|7018 2497 12654|IGP

BGP4MP|01/29/18 00:00:59|A|12.0.1.63|7018|84.205.68.0/24|7018 6830 513 513 12654|IGP

BGP4MP|01/29/18 00:00:59|A|12.0.1.63|7018|202.56.215.0/24|7018 6762 9498 24560|IGP

BGP4MP|01/29/18 00:00:59|A|12.0.1.63|7018|84.205.71.0/24|7018 1299 47872 12654|IGP

BGP4MP|01/29/18 00:00:59|A|12.0.1.63|7018|84.205.65.0/24|7018 2914 12654|IGP

BGP4MP|01/29/18 00:00:59|A|12.0.1.63|7018|84.205.65.0/24|7018 2914 12654|IGP

BGP4MP|01/29/18 00:00:59|W|12.0.1.63|7018|173.227.3.0/24

BGP4MP|01/29/18 00:00:59|W|12.0.1.63|7018|174.137.46.0/24

BGP4MP|01/29/18 00:00:59|A|12.0.1.63|7018|66.146.14.0/24|7018 3356 11841 11123 11123 11123|IGP

BGP4MP|01/29/18 00:00:59|A|12.0.1.63|7018|66.146.31.0/24|7018 3356 11841 11123 11123 11123|IGP

BGP4MP|01/29/18 00:00:59|A|12.0.1.63|7018|209.177.171.0/24|7018 3356 18465|IGP

BGP4MP|01/29/18 00:00:59|A|12.0.1.63|7018|66.146.74.0/24|7018 3356 11841 11123 11123|IGP

BGP4MP|01/29/18 00:01:00|A|12.0.1.63|7018|174.137.46.0/24|7018 3356 3549 19893 21880|IGP

BGP4MP|01/29/18 00:01:00|A|12.0.1.63|7018|173.227.3.0/24|7018 3356 3549 21817 14589 40036|IGP

BGP4MP|01/29/18 00:01:00|A|12.0.1.63|7018|84.205.82.0/24|7018 6453 37271 12654|IGP

BGP4MP|01/29/18 00:01:00|A|12.0.1.63|7018|103.253.149.0/24|7018 6453 4755 132768|IGP

BGP4MP|01/29/18 00:01:00|A|12.0.1.63|7018|103.253.150.0/24|7018 6453 4755 132768|IGP

BGP4MP|01/29/18 00:01:00|A|12.0.1.63|7018|103.253.148.0/24|7018 6453 4755 132768|IGP

BGP4MP|01/29/18 00:01:00|A|12.0.1.63|7018|150.107.95.0/24|7018 6453 4755 132768|IGP

BGP4MP|01/29/18 00:01:00|W|12.0.1.63|7018|103.253.149.0/24

BGP4MP|01/29/18 00:01:00|W|12.0.1.63|7018|103.253.150.0/24

BGP4MP|01/29/18 00:01:00|W|12.0.1.63|7018|103.253.148.0/24

BGP4MP|01/29/18 00:01:00|W|12.0.1.63|7018|150.107.95.0/24

BGP4MP|01/29/18 00:01:00|A|12.0.1.63|7018|174.137.46.0/24|7018 2914 19893 21880|IGP

BGP4MP|01/29/18 00:01:00|A|12.0.1.63|7018|209.177.171.0/24|7018 3356 18465|IGP

BGP4MP|01/29/18 00:01:00|A|12.0.1.63|7018|173.227.3.0/24|7018 3356 3549 21817 14589 40036|IGP

BGP4MP|01/29/18 00:01:00|A|12.0.1.63|7018|66.146.14.0/24|7018 3356 11841 11123 11123 11123|IGP

The most unstable route is 193.0.132.0/22 , it fails for 18 times. For prefix, the most unstable routes are /24, which accounts for 7 times in the top 10 unstable routes. We could infer from the data that the ip address with prefix 24 has a high risk to fail with 12.0.1.63 which might also be prefix 24. It also has a high frequency when it communicate IGPs, not more than 10 IGP communication it will fail at least one time.

2. Now pretend you are an AS directly peered with all vantage points. Plot the number of updates per minute you receive from each peer (have a line chart, with one line per vantage point, and one data point on each line per minute - x axis is minutes, y axis is # of updates in that minute -- consider using a map data structure). Include the plot in your report. What do you observe? If you were going to choose a peer to purchase service from, which would you choose?

Commands:

cut -d "|" -f 2 output.txt | sort | uniq -c > output1.txt

nano output1.txt | wc -l

843

awk '{sum+=$1;}END{print sum}' da14 > o14

I make 843 roughly into 14 groups and each one represents one minute updates. At first the updates are huge and after that, it tends to be slow. If I'm going to choose a peer to purchase, I will purchase the ones in group o7 because it has the least updates and in that case, the cost and failure are minimized.

ump-99da8741c8c8/group_data# cat o1

32758

root@b317c63c8ac5:/home/lab2/archive.routeviews.org/bgpdata/2018.01/ripencc-bgpd

ump-99da8741c8c8/group_data# cat o2

9802

root@b317c63c8ac5:/home/lab2/archive.routeviews.org/bgpdata/2018.01/ripencc-bgpd

ump-99da8741c8c8/group_data# cat o3

10023

root@b317c63c8ac5:/home/lab2/archive.routeviews.org/bgpdata/2018.01/ripencc-bgpd

ump-99da8741c8c8/group_data# cat o4

12361

root@b317c63c8ac5:/home/lab2/archive.routeviews.org/bgpdata/2018.01/ripencc-bgpd

ump-99da8741c8c8/group_data# cat o5

15252

root@b317c63c8ac5:/home/lab2/archive.routeviews.org/bgpdata/2018.01/ripencc-bgpd

ump-99da8741c8c8/group_data# cat o6

8386

root@b317c63c8ac5:/home/lab2/archive.routeviews.org/bgpdata/2018.01/ripencc-bgpd

ump-99da8741c8c8/group_data# cat o7

9900

root@b317c63c8ac5:/home/lab2/archive.routeviews.org/bgpdata/2018.01/ripencc-bgpd

ump-99da8741c8c8/group_data# cat o8

9726

root@b317c63c8ac5:/home/lab2/archive.routeviews.org/bgpdata/2018.01/ripencc-bgpd

ump-99da8741c8c8/group_data# cat o9

17304

root@b317c63c8ac5:/home/lab2/archive.routeviews.org/bgpdata/2018.01/ripencc-bgpd

ump-99da8741c8c8/group_data# cat o10

17137

root@b317c63c8ac5:/home/lab2/archive.routeviews.org/bgpdata/2018.01/ripencc-bgpd

ump-99da8741c8c8/group_data# cat o11

14607

root@b317c63c8ac5:/home/lab2/archive.routeviews.org/bgpdata/2018.01/ripencc-bgpd

ump-99da8741c8c8/group_data# cat o12

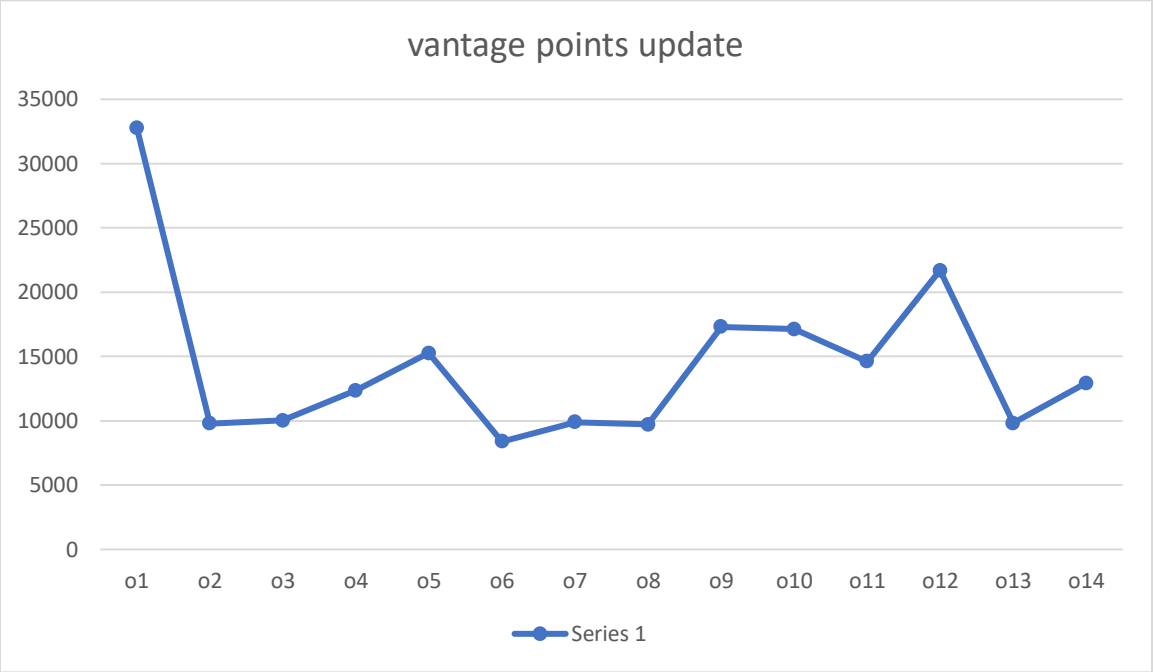
21678

root@b317c63c8ac5:/home/lab2/archive.routeviews.org/bgpdata/2018.01/ripencc-bgpdump-99da8741c8c8/group_data# cat o13

9814

root@b317c63c8ac5:/home/lab2/archive.routeviews.org/bgpdata/2018.01/ripencc-bgpdump-99da8741c8c8/group_data# cat o14

12937



3. Level 3 Communications (AS 3549)AT&T provides two feeds. Suppose you are peered with both of them. Are they doing consistent export? (Hint: "sort -u" may provide a simple way to solve this problem)

Command:

awk '/3549/' output.txt | sort -rnk5 | head -20

root@b317c63c8ac5:/home/lab2/archive.routeviews.org/bgpdata/2018.01/ripencc-bgpdump-99da8741c8c8# awk '/3549/' output.txt | sort -rnk5 | head -20

BGP4MP|01/29/18 00:01:01|A|4.69.184.193|3356|139.138.101.0/24|3356 3549 395325 395325 395325 395325 395325 395325 395325 395325 395325 395325 395325|IGP

BGP4MP|01/29/18 00:13:24|A|67.17.82.114|3549|154.73.60.0/24|3549 3356 16637 327769|IGP

BGP4MP|01/29/18 00:13:05|A|208.51.134.246|3549|154.73.60.0/24|3549 3356 16637 327769|IGP

BGP4MP|01/29/18 00:13:05|A|208.51.134.246|3549|154.73.60.0/24|3549 3356 16637 327769|IGP

BGP4MP|01/29/18 00:13:05|A|208.51.134.246|3549|154.73.60.0/24|3549 3356 16637 327769|IGP

BGP4MP|01/29/18 00:13:24|A|67.17.82.114|3549|160.19.248.0/22|3549 3356 4230 266566 266172|IGP

BGP4MP|01/29/18 00:13:16|A|208.51.134.246|3549|160.19.249.0/24|3549 3356 4230 266566 266172|IGP

BGP4MP|01/29/18 00:13:16|A|208.51.134.246|3549|160.19.248.0/24|3549 3356 4230 266566 266172|IGP

BGP4MP|01/29/18 00:13:16|A|208.51.134.246|3549|160.19.248.0/22|3549 3356 4230 266566 266172|IGP

BGP4MP|01/29/18 00:13:03|A|208.51.134.246|3549|160.19.249.0/24|3549 3356 4230 266566 266172|IGP

BGP4MP|01/29/18 00:13:03|A|208.51.134.246|3549|160.19.248.0/24|3549 3356 4230 266566 266172|IGP

BGP4MP|01/29/18 00:13:03|A|208.51.134.246|3549|160.19.248.0/22|3549 3356 4230 266566 266172|IGP

BGP4MP|01/29/18 00:13:02|A|208.51.134.246|3549|160.19.249.0/24|3549 3356 4230 266566 266172|IGP

BGP4MP|01/29/18 00:13:02|A|208.51.134.246|3549|160.19.248.0/24|3549 3356 4230 266566 266172|IGP

BGP4MP|01/29/18 00:13:02|A|208.51.134.246|3549|160.19.248.0/22|3549 3356 4230 266566 266172|IGP

BGP4MP|01/29/18 00:12:53|A|67.17.82.114|3549|160.19.249.0/24|3549 3356 4230 266566 266172|IGP

BGP4MP|01/29/18 00:12:53|A|67.17.82.114|3549|160.19.248.0/24|3549 3356 4230 266566 266172|IGP

BGP4MP|01/29/18 00:12:53|A|67.17.82.114|3549|160.19.248.0/22|3549 3356 4230 266566 266172|IGP

BGP4MP|01/29/18 00:12:37|A|208.51.134.246|3549|160.19.249.0/24|3549 3356 4230 266566 266172|IGP

BGP4MP|01/29/18 00:12:37|A|208.51.134.246|3549|160.19.249.0/24|3549 3356 4230 266566 266172|IGP

From the time slot , we can infer that the time is not consistent although they did get the export continuous.

4. Let's find some ASes that are not doing a good job. Find the top ASes that are advertising the most prefixes. Could they aggregate? Give an example.

Command:

awk '/W/' output.txt | sort -rnk6 | head -20

root@b317c63c8ac5:/home/lab2/archive.routeviews.org/bgpdata/2018.01/ripencc-bgpdump-99da8741c8c8# awk '/W/' output.txt | sort -rnk6 | head -20

BGP4MP|01/29/18 00:15:00|W|203.181.248.168|7660|59.99.0.0/20

BGP4MP|01/29/18 00:15:00|W|203.181.248.168|7660|59.89.0.0/20

BGP4MP|01/29/18 00:14:59|W|64.71.137.241|6939|209.177.171.0/24

BGP4MP|01/29/18 00:14:59|W|202.73.40.45|18106|193.0.132.0/22

BGP4MP|01/29/18 00:14:59|W|202.73.40.45|18106|193.0.132.0/22

BGP4MP|01/29/18 00:14:59|W|147.28.7.2|3130|193.0.132.0/22

BGP4MP|01/29/18 00:14:59|W|144.228.241.130|1239|61.155.155.0/24

BGP4MP|01/29/18 00:14:59|W|144.228.241.130|1239|189.113.11.0/24

BGP4MP|01/29/18 00:14:59|W|144.228.241.130|1239|182.53.195.0/24

BGP4MP|01/29/18 00:14:59|W|103.247.3.45|58511|209.177.171.0/24

BGP4MP|01/29/18 00:14:58|W|91.218.184.60|49788|193.0.132.0/22

BGP4MP|01/29/18 00:14:58|W|192.241.164.4|62567|193.0.132.0/22

BGP4MP|01/29/18 00:14:58|W|162.251.163.2|53767|103.242.164.0/22

BGP4MP|01/29/18 00:14:58|W|162.251.163.2|53767|103.198.184.0/24

BGP4MP|01/29/18 00:14:58|W|162.243.188.2|393406|193.0.132.0/22

BGP4MP|01/29/18 00:14:58|W|147.28.7.1|3130|103.242.164.0/22

BGP4MP|01/29/18 00:14:58|W|134.222.87.1|286|200.62.56.0/23

BGP4MP|01/29/18 00:14:58|W|129.250.1.71|2914|193.0.132.0/22

BGP4MP|01/29/18 00:14:58|W|12.0.1.63|7018|193.0.132.0/22

BGP4MP|01/29/18 00:14:57|W|137.39.3.55|701|212.80.30.0/24

Most of them are /24, /22 and they have a tendency to become even bad based on the numbers appear in each minute. Here are only 20 lists but it can become worse if lists 100 or more than that.

5. Do you see any ASes advertising bogons? How would you protect your network against those?

Yes. There might be at least one kind of bogons. One is that with INCOMPETE end instead of IGP. We ignore that IP address invalid here. We should design a filter to filter the IP address which has the ending “INCOMPETE”. The one ended with repeated IP address is also not good, and we probably need to remove and make it unique.

6. Suppose you are an enterprise that has traditionally done default routing. But you are getting bigger and now want to participate in BGP. Do some performance analysis on these updates to get a sense of (a) your CPU needs - hint, consider # updates per second you'd need to process (b) your TCAM needs. Keep in mind overflows/overload are really bad (why?) - so would you add headroom? How much?

Most of the data are 1000 – 2000 per minute and 16 times – 33 times per second, so I suggest to do the average and put the needs to be 25HZ.

7. Now suppose you are an employee that has access to the BGP routers at your company. You don't like Facebook and want to take them offline. How would you do it? Note Facebook is a distributed service.

Aimed at the AS instead of the IP address, it would be better since the ip address by Facebook could be a lot but the AS is limited by them and we could filter by their AS numbers.

8. Now suppose you are the US Department of Defense. You send a lot of traffic to US Kadena Air Force Base, Japan. Does that traffic go through networks owned by any other foreign countries that might be considered adversaries of the United States, and that might want to snoop on that data?

Definitely, as the adversaries of the United States, they would snoop on that data. They could attack protocol like BGP when vantage points are sending packets from USA.

9. Think of something else interesting to analyze in this data - analyze it, and report what you find.

We have :

1. Different time slots analyze

2. Aim at a specific vantage point

3. Find out its error ips etc

4. Aim at a specific AS and do its ip address analyze

5. Analyze the withdraw status and the normal status

We could do IGP ip address analyze.

1. Here I could pick up a time slot randomly

2. I pick up the vantage point randomly

3. Then find out its IGP ip address, draw the connect graph

4. Do the same thing with the IGP ips each for about three levels

5. Finally, I get a graph which represents a social connection for those ips.

From the graph, I find the IGP and BGP connects a lot and we could use short-path first or other algorithms to calculated the efficient way for (peer to peer) or (customer to producer) communications

10. Suppose you find out that AS 46479 is the source of a lot of problems. How would you get in touch with them?

Just as I illustrated in the Q9 : use a graph idea here from the point AS 46479. Get its related ip address and then do the analyze of them. The other idea here is to use "awk" etc to find out all the data which has AS 46479 and then do the analyze of those data.

11. In addition to inferring the Internet's AS-level topology, it is also useful to infer the way that traffic flows over that topology. The manner in which an AS advertises a route in the Internet can very commonly be classified into one of several categories: (a) *provider-customer* relationships, where a customer pays a provider money (typically) for service. In this case, the provider advertises all routes it receives to the customer, and advertises all routes from the customer to all its neighbors. (b) *peer-peer* relationships, where two ASes agree to peer out of their own mutual benefit, and typically no money is exchanged. ASes almost always advertise all their routes from customers to peers. However, they almost always prevent provider/peer routes from being advertised to other provider/peers.

Instead of performing this inference yourself, we will provide a file containing these relationships for you: http://www.cs.illinois.edu/~caesar/courses/cs436/19980501.as-rel.txt.bz2.

This file was originally downloaded from http://www.caida.org/data/active/as-relationships/, and contains an AS-level graph annotated with inter-ISP relationships. The format of the file is explained in comments at the start of the file; 0 means the ASes are peers, -1 means the first AS is a provider of the second.

Suppose an IP packet is sent from a computer in UIUC (AS 38) to Instagram (hosted by AWS, AS 6250). Using this file, name one possible sequence of ASes it may traverse.

Command:

root@b317c63c8ac5:/home/lab2# bzip2 -d 19980501.as-rel.txt.bz2

root@b317c63c8ac5:/home/lab2# ls

19980501.as-rel.txt archive.routeviews.org

AS38 => AS6250 : find out one possible sequence

AS38

38|293|0

38|1224|-1

38|3967|0

AS6250 => No data

AS6251 => 6251|52|-1

AS6259 => 6259|2015|-1

It might find out AS6251 instead of AS6250, usually find out the nearest points if the target points are not available.

293|6251|0

293|6259|0

Also Consider for the profit :

Thus, it might do : AS38 – AS293 - AS6251 --(AS6250)

AS38 => AS1224 => no data

AS38 – AS3967 => many branches (might be one could maxium profit)

PART 2: Characterizing traffic aggregates with Netflow

Please investigate and answer the following questions in your report:

1. From a machine within UIUC, perform a traceroute to a machine at IBM. Give the IP address of the Abilene router which connects to UIUC. This is the router where the flow trace file was collected.

UIUC : 130.126.52.0/24 => Using ipconfig or google
http://www.ispinfo.net/isp/130.126.52.html
IBM : 129.42.54.189

Command:

grep "130.126.*" netflowOutput.txt

root@b317c63c8ac5:/home/lab2# grep "130.126.*" netflowOutput.txt
1132964110,0,2710918988,62.40.96.65,1,1500,2710865696,2710865696,0,0,132.199.1.211,130.126.81.15,62.40.103.252,78,40,80,1073,6,0,16,16,16,680,11537
1132964315,0,2711123954,62.40.96.65,5,236,2711086697,2711097697,0,0,129.13.73.33,130.126.243.129,62.40.103.252,78,40,1396,13769,6,0,16,16,16,680,11537
1132964865,0,2711674039,62.40.96.65,1,40,2711626698,2711626698,0,0,141.55.121.91,130.126.52.226,62.40.103.252,78,40,2599,4178,6,0,16,13,16,680,11537

Next hop : 62.40.103.252

Traceroute to IBM :

Command:

traceroute IBM.com

root@b317c63c8ac5:/home/lab2# traceroute IBM.com
traceroute to IBM.com (129.42.38.10), 30 hops max, 60 byte packets
 1 172.17.0.1 (172.17.0.1) 0.088 ms 0.037 ms 0.120 ms
 2 192.168.0.1 (192.168.0.1) 97.688 ms 97.698 ms 97.816 ms
 3 mr-urb-180-1.dmisinetworks.net (66.253.180.1) 99.278 ms 99.639 ms 99.241 ms
 4 host-181-129.pavcmi.corp.pavlovmedia.com (66.253.181.129) 99.736 ms 99.945 ms 100.023 ms
 5 host-0-148.cmi.clients.pavlovmedia.com (216.171.0.148) 100.151 ms 100.230 ms 99.081 ms

6 te0-0-1-2-3538.edge1.inind1.pavlovmedia.net (173.230.125.80) 101.416 ms 25.632 ms 26.864 ms

7 te0-0-1-1.nr11.b021117-0.ind01.atlas.cogentco.com (38.104.214.129) 26.672 ms 112.321 ms 112.251 ms

8 154.24.38.21 (154.24.38.21) 82.792 ms 112.092 ms 112.177 ms

9 be3180.ccr41.ord01.atlas.cogentco.com (154.54.45.170) 112.214 ms 112.098 ms 112.105 ms

10 be2765.ccr41.ord03.atlas.cogentco.com (154.54.45.18) 113.742 ms
be2766.ccr41.ord03.atlas.cogentco.com (154.54.46.178) 113.750 ms
be2765.ccr41.ord03.atlas.cogentco.com (154.54.45.18) 113.677 ms

11 * * *

12 4.69.208.197 (4.69.208.197) 375.633 ms 375.540 ms 325.216 ms

13 ATT-CORPORA.edge5.Denver1.Level3.net (4.53.6.66) 325.124 ms 325.089 ms 325.060 ms

2. What fraction of traffic is BitTorrent traffic (ports 6881-6999), and what fraction is web request (port 80) traffic?

Command:

grep "6[8-9][8-9][0-9]" netflowOutput.txt | head -30

root@b317c63c8ac5:/home/lab2# grep "6[8-9][8-9][0-9]" netflowOutput.txt | head -30

1132964100,0,2710908967,62.40.96.65,1,137,2710816817,2710816817,0,0,134.96.3.126,194.249.29.6,62.40.96.56,78,48,1092,36881,6,0,24,16,16,680,2107

1132964100,0,2710908967,62.40.96.65,3,4500,2710835717,2710864038,0,0,165.91.212.126,153.19.205.47,62.40.96.64,40,42,4286,6881,6,0,16,16,16,11537,8501

1132964100,0,2710908967,62.40.96.65,2,2600,2710823199,2710868818,0,0,131.247.12.127,149.170.58.235,62.40.96.64,40,42,4302,2494,6,0,16,16,16,11537,786

1132964100,0,2710908967,62.40.96.65,2,1552,2710868818,2710871054,0,0,143.107.122.134,148.81.187.119,62.40.96.64,40,42,3719,673,6,0,16,16,16,11537,8501

1132964100,0,2710908967,62.40.96.65,2,3000,2710835817,2710846696,0,0,130.18.161.135,144.32.41.78,62.40.96.64,40,42,6881,54630,6,0,16,16,16,11537,786

1132964100,0,2710908967,62.40.96.65,1,100,2710867819,2710867819,0,0,131.188.23.138,143.50.221.143,62.40.96.56,78,48,26881,3326,6,0,24,16,16,680,1853

1132964100,0,2710908967,62.40.96.65,2,104,2710869818,2710872819,0,0,128.61.32.143,129.206.196.27,62.40.105.0,40,78,2304,7957,6,0,16,19,16,11537,680

1132964100,0,2710908967,62.40.96.65,5,7100,2710860696,2710868818,0,0,128.163.2.145,141.53.194.251,62.40.105.0,40,78,1999,11173,6,0,16,16,13,11537,680

1132964105,0,2710913977,62.40.96.65,1,40,2710817818,2710817818,0,0,130.85.70.158,150.140.186.149,62.40.96.80,40,53,6882,1341,6,0,16,16,16,11537,5408

1132964105,0,2710913977,62.40.96.65,5,7100,2710830036,2710869501,0,0,131.96.156.160,193.136.77.126,62.40.96.60,40,43,6881,15166,6,0,16,16,15,11537,1930

1132964105,0,2710913977,62.40.96.65,4,5517,2710817501,2710873039,0,0,161.253.48.161,195.134.100.136,62.40.96.80,40,53,3041,6881,6,0,24,18,18,11537,5408

1132964105,0,2710913977,62.40.96.65,1,40,2710869818,2710869818,0,0,129.143.9.168,145.97.39.155,62.40.96.64,78,42,1504,80,6,0,16,16,21,680,1103

1132964105,0,2710913977,62.40.96.65,1,40,2710861500,2710861500,0,0,200.18.98.175,141.2.66.47,62.40.105.0,40,78,2821,6881,6,0,16,20,16,11537,680

1132964105,0,2710913977,62.40.96.65,2,546,2710863500,2710869818,0,0,134.102.71.180,143.50.218.240,62.40.96.56,78,48,3014,8767,17,0,0,16,16,680,1853

1132964110,0,2710918988,62.40.96.65,1,52,2710849038,2710849038,0,0,141.44.152.195,195.209.66.146,62.40.96.64,78,42,2622,16881,6,0,16,15,19,680,5568

1132964110,0,2710918988,62.40.96.65,6,9000,2710851696,2710868818,0,0,141.14.16.205,193.171.43.250,62.40.96.56,78,48,3902,3965,6,16,16,16,15,680,1853

1132964110,0,2710918988,62.40.96.65,8,9140,2710826038,2710869818,0,0,128.61.5.210,129.215.37.45,62.40.96.64,40,42,6881,1701,6,0,16,19,16,11537,786

1132964110,0,2710918988,62.40.96.65,2,3000,2710853039,2710872501,0,0,128.61.5.210,195.111.75.162,62.40.96.56,40,48,6881,59436,6,0,16,19,16,11537,1955

1132964110,0,2710918988,62.40.96.65,1,40,2710838699,2710838699,0,0,139.18.2.216,144.82.100.140,62.40.96.64,78,42,56897,80,6,0,16,15,16,680,786

1132964110,0,2710918988,62.40.96.65,1,40,2710839500,2710839500,0,0,139.30.17.218,130.232.133.194,62.40.96.64,78,42,16897,4564,6,0,16,16,16,680,2603

1132964115,0,2710923998,62.40.96.65,2,3000,2710859500,2710861696,0,0,137.226.34.232,156.18.37.70,62.40.96.60,78,43,16881,4836,6,0,16,16,16,680,2200

1132964115,0,2710923998,62.40.96.65,1,1157,2710824500,2710824500,0,0,137.226.34.232,156.18.37.70,62.40.96.60,78,43,16881,4836,6,0,24,16,16,680,2200

1132964115,0,2710923998,62.40.96.65,5,6052,2710826838,2710873696,0,0,137.226.34.232,193.144.12.130,62.40.96.60,78,43,16881,36525,6,0,16,16,14,680,766

1132964115,0,2710923998,62.40.96.65,1,1179,2710838500,2710838500,0,0,137.226.34.232,193.144.12.130,62.40.96.60,78,43,16881,36525,6,0,24,16,14,680,766

1132964115,0,2710923998,62.40.96.65,2,3000,2710830044,2710853038,0,0,137.226.34.232,212.51.212.205,62.40.96.64,78,42,16881,3830,6,0,16,16,20,680,8501

1132964115,0,2710923998,62.40.96.65,1,1500,2710835039,2710835039,0,0,128.192.189.232,62.108.167.9,62.40.96.64,40,42,3836,6999,6,80,24,16,20,11537,8501

1132964115,0,2710923998,62.40.96.65,3,3040,2710860818,2710868696,0,0,128.143.24.237,164.8.221.161,62.40.96.56,40,48,2476,16881,6,96,16,16,16,11537,2107

1132964115,0,2710923998,62.40.96.65,2,2432,2710816502,2710836500,0,0,128.143.24.237,164.8.221.161,62.40.96.56,40,48,2476,16881,6,96,24,16,16,11537,2107

1132964115,0,2710923998,62.40.96.65,1,52,2710853696,2710853696,0,0,130.75.181.238,195.178.72.147,62.40.96.56,78,48,6881,1638,6,0,16,16,19,680,2852

1132964115,0,2710923998,62.40.96.65,2,3000,2710844039,2710858065,0,0,134.76.214.238,129.173.193.123,62.40.96.56,78,48,3399,6883,6,0,16,16,16,680,6509

We could find 78,42 is most common I/O , so that the fraction should be around : I/O = 2 .

Command:

grep "80" netflowOutput.txt

root@b317c63c8ac5:/home/lab2# grep "80" netflowOutput.txt

1132964995,0,271180 4078,62.40.96.65,1,1500,2711731821,2711731821,0,0,150.144.30.108,195.113.97.230,62.40.96.56,40,48,80,49270,6,0,16,16,16,6509,2852

1132964995,0,271180 4078,62.40.96.65,1,964,2711734507,2711734507,0,0,150.144.30.108,195.113.97.230,62.40.96.56,40,48,80,49271,6,0,16,16,16,6509,2852

1132964995,0,271180 4078,62.40.96.65,1,1500,2711734507,2711734507,0,0,150.144.30.108,195.113.97.230,62.40.96.56,40,48,80,49272,6,0,16,16,16,6509,2852

1132964995,0,271180 4078,62.40.96.65,1,1500,2711738821,2711738821,0,0,128.143.100.108,193.52.24.125,62.40.96.60,40,43,27008,55913,6,96,24,16,16,11537,2200

1132964995,0,271180 4078,62.40.96.65,1,52,2711765821,2711765821,0,0,152.1.40.109,160.75.100.14,62.40.96.80,40,53,35958,443,6,0,16,16,16,11537,8517

1132964995,0,271180 4078,62.40.96.65,1,1284,2711741699,2711741699,0,0,134.130.58.109,137.205.34.41,62.40.96.64,78,42,3077,3549,6,0,24,16,16,680,786

1132964995,0,271180 4078,62.40.96.65,1,1420,2711747709,2711747709,0,0,130.14.29.110,134.102.40.14,62.40.105.0,40,78,80,38587,6,0,16,16,16,11537,680

1132964995,0,271180 4078,62.40.96.65,1,52,2711738821,2711738821,0,0,130.14.29.110,134.226.152.146,62.40.96.64,40,42,80,41688,6,0,16,16,16,11537,1213

1132964995,0,271180 4078,62.40.96.65,1,1420,2711742055,2711742055,0,0,130.14.29.110,132.187.22.163,62.40.105.0,40,78,80,21813,6,0,16,16,16,11537,680

1132964995,0,2711804078,62.40.96.65,1,1420,2711751822,2711751822,0,0,130.14.29.110,13

2.187.22.163,62.40.105.0,40,78,80,21825,6,0,16,16,16,11537,680

1132964995,0,2711804078,62.40.96.65,1,1420,2711752506,2711752506,0,0,130.14.29.110,13

2.187.22.163,62.40.105.0,40,78,80,21826,6,0,16,16,16,11537,680

1132964995,0,2711804078,62.40.96.65,1,1420,2711755699,2711755699,0,0,130.14.29.110,13

2.187.22.163,62.40.105.0,40,78,80,21830,6,0,16,16,16,11537,680

1132964995,0,2711804078,62.40.96.65,1,1420,2711765821,2711765821,0,0,130.14.29.110,13

2.187.22.163,62.40.105.0,40,78,80,21840,6,0,16,16,16,11537,680

The most common I/O is 40,78 so that I/O = 0.5

3. Plot a CDF of flow lengths measured in number of bytes per connection, and again in terms of number of packets per connection.
4. What are the top five /16's owned by Abilene-connected institutions to which AS 680 sends traffic? Use whois to give the ASCII names of the companies/entities which own these prefixes. e.g., whois -h whois.cymru.com "-v AS10000"

Command :

grep "680" netflowOutput.txt | head -30

root@b317c63c8ac5:/home/lab2# grep "680" netflowOutput.txt | head -30

1132964100,0,2710908967,62.40.96.65,1,71,2710859500,2710859500,0,0,141.74.254.123,193

.170.92.31,62.40.96.56,78,48,21,2653,6,0,24,15,15,680,1853

1132964100,0,2710908967,62.40.96.65,1,1332,2710856697,2710856697,0,0,141.74.254.123,1

93.170.92.31,62.40.96.56,78,48,25465,2655,6,0,16,15,15,680,1853

1132964100,0,2710908967,62.40.96.65,2,212,2710831500,2710850702,0,0,141.74.254.123,19

3.170.92.31,62.40.96.56,78,48,21,3975,6,0,24,15,15,680,1853

1132964100,0,2710908967,62.40.96.65,1,1332,2710841818,2710841818,0,0,141.74.254.123,1

93.170.92.31,62.40.96.56,78,48,24466,2447,6,0,16,15,15,680,1853

1132964100,0,2710908967,62.40.96.65,1,52,2710862818,2710862818,0,0,141.74.254.123,193
.170.92.31,62.40.96.56,78,48,25913,1946,6,0,17,15,15,680,1853
1132964100,0,2710908967,62.40.96.65,1,71,2710848500,2710848500,0,0,141.74.254.123,193
.170.92.31,62.40.96.56,78,48,21,2790,6,0,24,15,15,680,1853
1132964100,0,2710908967,62.40.96.65,1,52,2710831500,2710831500,0,0,141.74.254.123,193
.170.92.31,62.40.96.56,78,48,21,2029,6,0,16,15,15,680,1853
1132964100,0,2710908967,62.40.96.65,1,52,2710845038,2710845038,0,0,141.74.254.123,193
.170.92.31,62.40.96.56,78,48,21,4087,6,0,16,15,15,680,1853
1132964100,0,2710908967,62.40.96.65,1,125,2710860501,2710860501,0,0,141.74.254.123,19
3.170.92.31,62.40.96.56,78,48,21,4087,6,0,24,15,15,680,1853
1132964100,0,2710908967,62.40.96.65,1,68,2710852500,2710852500,0,0,141.74.254.123,132
.239.152.71,62.40.103.252,78,40,21,56347,6,0,24,15,16,680,11537
1132964100,0,2710908967,62.40.96.65,1,52,2710843818,2710843818,0,0,141.74.254.123,148
.81.117.136,62.40.96.64,78,42,21,55028,6,0,17,15,16,680,8501
1132964100,0,2710908967,62.40.96.65,1,48,2710819038,2710819038,0,0,139.30.8.125,142.1
03.71.246,62.40.96.56,78,48,1433,11656,6,0,18,16,16,680,6509
1132964100,0,2710908967,62.40.96.65,1,40,2710837818,2710837818,0,0,193.174.27.125,35.
8.142.3,62.40.103.252,78,40,2914,9000,6,0,16,15,8,680,11537
1132964100,0,2710908967,62.40.96.65,1,48,2710844818,2710844818,0,0,129.206.84.125,147
.83.157.37,62.40.96.60,78,43,3035,1022,6,0,2,16,16,680,766
1132964100,0,2710908967,62.40.96.65,1,48,2710844818,2710844818,0,0,129.206.84.125,147
.83.156.47,62.40.96.60,78,43,2790,1022,6,0,2,16,16,680,766
1132964100,0,2710908967,62.40.96.65,1,40,2710848038,2710848038,0,0,129.206.84.125,147
.83.39.56,62.40.96.60,78,43,1477,3389,6,0,16,16,16,680,766
1132964100,0,2710908967,62.40.96.65,1,48,2710854696,2710854696,0,0,129.206.84.125,147
.83.161.59,62.40.96.60,78,43,4078,1022,6,0,2,16,16,680,766
1132964100,0,2710908967,62.40.96.65,1,48,2710822703,2710822703,0,0,129.206.84.125,147
.83.147.120,62.40.96.60,78,43,4236,1022,6,0,2,16,16,680,766
1132964100,0,2710908967,62.40.96.65,1,48,2710869696,2710869696,0,0,129.206.84.125,147
.83.165.133,62.40.96.60,78,43,1504,1022,6,0,2,16,16,680,766

1132964100,0,2710908967,62.40.96.65,1,48,2710843500,2710843500,0,0,129.206.84.125,147
.83.155.160,62.40.96.60,78,43,2648,1022,6,0,2,16,16,680,766
1132964100,0,2710908967,62.40.96.65,1,48,2710832818,2710832818,0,0,129.206.84.125,147
.83.152.171,62.40.96.60,78,43,1893,1022,6,0,2,16,16,680,766
1132964100,0,2710908967,62.40.96.65,1,48,2710820500,2710820500,0,0,129.206.84.125,147
.83.146.173,62.40.96.60,78,43,4033,1022,6,0,2,16,16,680,766
1132964100,0,2710908967,62.40.96.65,1,48,2710822703,2710822703,0,0,129.206.84.125,147
.83.148.200,62.40.96.60,78,43,4598,1022,6,0,2,16,16,680,766
1132964100,0,2710908967,62.40.96.65,1,48,2710862039,2710862039,0,0,129.206.84.125,147
.83.162.227,62.40.96.60,78,43,4720,1022,6,0,2,16,16,680,766
1132964100,0,2710908967,62.40.96.65,1,48,2710836039,2710836039,0,0,129.206.84.125,147
.83.153.245,62.40.96.60,78,43,2223,1022,6,0,2,16,16,680,766
1132964100,0,2710908967,62.40.96.65,1,48,2710860500,2710860500,0,0,129.206.84.125,147
.83.161.254,62.40.96.60,78,43,4275,1022,6,0,2,16,16,680,766
1132964100,0,2710908967,62.40.96.65,1,52,2710823199,2710823199,0,0,139.18.191.125,129
.173.192.86,62.40.96.56,78,48,1250,15267,6,0,16,15,16,680,6509
1132964100,0,2710908967,62.40.96.65,1,60,2710846818,2710846818,0,0,128.237.235.125,14
1.3.12.13,62.40.105.0,40,78,54225,110,6,0,2,16,16,11537,680
1132964100,0,2710908967,62.40.96.65,1,137,2710816817,2710816817,0,0,134.96.3.126,194.
249.29.6,62.40.96.56,78,48,1092,36881,6,0,24,16,16,680,2107
1132964100,0,2710908967,62.40.96.65,1,49,2710838700,2710838700,0,0,134.102.69.126,140
.180.161.218,62.40.103.252,78,40,4090,12426,6,0,24,16,18,680,11537

Top 5 with 16s AS are :

6,0,24,15,16,680,11537
6,0,17,15,16,680,8501
6,0,18,16,16,680,6509
6,0,2,16,16,680,766
6,0,24,16,16,680,2107

root@b317c63c8ac5:/home/lab2# whois -h whois.cymru.com "-v AS11537"

Warning: RIPE flags used with a traditional server.

AS | CC | Registry | Allocated | AS Name

11537 | US | arin | 1998-09-23 | ABILENE - Internet2, US

root@b317c63c8ac5:/home/lab2# whois -h whois.cymru.com "-v AS8501"

Warning: RIPE flags used with a traditional server.

AS | CC | Registry | Allocated | AS Name

8501 | PL | ripencc | 1997-10-10 | PIONIER-AS PIONIER, National Research and Education Network in Poland, PL

root@b317c63c8ac5:/home/lab2# whois -h whois.cymru.com "-v AS6509"

Warning: RIPE flags used with a traditional server.

AS | CC | Registry | Allocated | AS Name

6509 | CA | arin | 1996-05-10 | CANARIE-NTN - Canarie Inc, CA

root@b317c63c8ac5:/home/lab2# whois -h whois.cymru.com "-v AS766"

Warning: RIPE flags used with a traditional server.

AS | CC | Registry | Allocated | AS Name

766 | ES | ripencc | 1993-09-01 | REDIRIS RedIRIS Autonomous System, ES

root@b317c63c8ac5:/home/lab2# whois -h whois.cymru.com "-v AS2107"

Warning: RIPE flags used with a traditional server.

AS | CC | Registry | Allocated | AS Name

2107 | SI | ripencc | 1992-11-06 | ARNES-NET Academic and Research Network of Slovenia, SI

Top 5 with 16s AS names:

6,0,24,15,16,680,11537 => ABILENE - Internet2, US

6,0,17,15,16,680,8501 => PIONIER-AS PIONIER, National Research and Education Network in Poland, PL

6,0,18,16,16,680,6509 => CANARIE-NTN - Canarie Inc, CA

6,0,2,16,16,680,766 => REDIRIS RedIRIS Autonomous System, ES

6,0,24,16,16,680,2107 => ARNES-NET Academic and Research Network of Slovenia, SI

5. What are the top five /16s owned by Abilene-connected institutions which send traffic to UIUC?

UIUC ip address : (https://answers.uillinois.edu/illinois/page.php?id=47572)

72.36.64.0/18 ; 128.174.0.0/16 ; 130.126.0.0/16 ; 192.17.0.0/16

Use ip 192.17.0.0/16 for example :

root@b317c63c8ac5:/home/lab2# grep "192.17.*" netflowOutput.txt

1132964125,0,2710933902,62.40.96.65,1,54,2710904501,2710904501,0,0,192.17.24.4,233.4.200.18,0.0.0.0,40,0,10002,10002,17,0,0,16,0,11537,0

1132964145,0,2710953940,62.40.96.65,1,40,2710894501,2710894501,0,0,141.14.215.78,192.172.226.77,62.40.103.252,78,40,47544,80,6,0,17,16,24,680,11537

1132964225,0,2711033997,62.40.96.65,1,52,2710942819,2710942819,0,0,132.252.152.194,192.17.239.250,62.40.103.252,78,40,35726,2128,6,0,17,16,16,680,11537

1132964265,0,2711073970,62.40.96.65,1,687,2711038039,2711038039,0,0,130.75.87.83,192.17.239.250,62.40.103.252,78,40,5850,5850,17,0,0,16,16,680,11537

1132964365,0,2711173952,62.40.96.65,1,56,2711118039,2711118039,0,0,62.40.105.2,192.172.226.24,62.40.103.252,78,40,0,0,1,192,0,30,24,20965,11537

1132964365,0,2711173952,62.40.96.65,1,54,2711173502,2711173502,0,0,192.17.24.4,233.4.200.18,0.0.0.0,40,0,10002,10002,17,0,0,16,0,11537,0

1132964385,0,2711193990,62.40.96.65,1,40,2711164819,2711164819,0,0,139.18.2.81,192.17
1.153.207,62.40.96.64,78,42,2995,80,6,0,16,15,18,680,786
1132964405,0,2711214021,62.40.96.65,1,40,2711129039,2711129039,0,0,128.192.177.219,1
37.224.239.184,62.40.96.64,40,42,2056,12691,6,80,16,16,16,11537,1103
1132964485,0,2711293971,62.40.96.65,1,388,2711287039,2711287039,0,0,132.187.230.1,192
.17.239.250,62.40.103.252,78,40,8089,8089,17,0,0,16,16,680,11537
1132964485,0,2711293971,62.40.96.65,1,54,2711273040,2711273040,0,0,192.17.24.4,233.4.
200.18,0.0.0.0,40,0,10002,10002,17,0,0,16,0,11537,0
1132964530,0,2711339051,62.40.96.65,1,56,2711261820,2711261820,0,0,141.30.1.254,192.1
72.226.24,62.40.103.252,78,40,0,0,1,0,0,16,24,680,11537
1132964545,0,2711353976,62.40.96.65,2,108,2711298698,2711317819,0,0,192.17.24.4,233.4
.200.18,0.0.0.0,40,0,10002,10002,17,0,0,16,0,11537,0
1132964560,0,2711369004,62.40.96.65,1,52,2711346819,2711346819,0,0,134.106.38.46,142.
150.192.177,62.40.96.56,78,48,40183,22,6,0,16,14,16,680,6509
1132964585,0,2711394039,62.40.96.65,1,84,2711324503,2711324503,0,0,132.252.152.193,19
2.17.239.250,62.40.103.252,78,40,0,0,1,0,0,16,16,680,11537
1132964615,0,2711424018,62.40.96.65,1,68,2711393040,2711393040,0,0,134.106.38.46,142.
150.192.177,62.40.96.56,78,48,41099,22,6,0,24,14,16,680,6509
1132964625,0,2711434039,62.40.96.65,1,60,2711413039,2711413039,0,0,141.14.215.78,192.
172.226.77,62.40.103.252,78,40,48003,80,6,0,2,16,24,680,11537
1132964645,0,2711454371,62.40.96.65,1,59,2711395697,2711395697,0,0,134.2.205.228,192.
17.239.251,62.40.103.252,78,40,32824,5722,17,0,0,16,16,680,11537
1132964690,0,2711499039,62.40.96.65,1,40,2711451504,2711451504,0,0,141.55.121.91,128.
192.177.219,62.40.103.252,78,40,2237,16725,6,0,16,13,16,680,11537
1132964705,0,2711514040,62.40.96.65,1,60,2711461504,2711461504,0,0,141.76.120.196,192
.17.111.210,62.40.103.252,78,40,44882,21209,6,0,2,16,16,680,11537
1132964710,0,2711519041,62.40.96.65,4,5200,2711438050,2711449820,0,0,128.192.177.219
,141.55.121.91,62.40.105.0,40,78,16725,2237,6,80,16,16,13,11537,680
1132964765,0,2711574190,62.40.96.65,1,1300,2711505698,2711505698,0,0,128.192.177.219
,141.55.121.91,62.40.105.0,40,78,16725,2237,6,80,16,16,13,11537,680

1132964795,0,2711604032,62.40.96.65,1,52,2711568698,2711568698,0,0,134.106.38.46,142.150.192.177,62.40.96.56,78,48,44622,22,6,0,17,14,16,680,6509

1132964795,0,2711604032,62.40.96.65,1,348,2711566719,2711566719,0,0,134.106.38.46,142.150.192.177,62.40.96.56,78,48,44622,22,6,0,24,14,16,680,6509

1132964845,0,2711654030,62.40.96.65,2,108,2711635506,2711652699,0,0,192.17.24.4,233.4.200.18,0.0.0.0,40,0,10002,10002,17,0,0,16,0,11537,0

1132964905,0,2711714034,62.40.96.65,1,54,2711697821,2711697821,0,0,192.17.24.4,233.4.200.18,0.0.0.0,40,0,10002,10002,17,0,0,16,0,11537,0

1132964905,0,2711714034,62.40.96.65,1,89,2711655505,2711655505,0,0,139.19.142.4,192.17.239.250,62.40.103.252,78,40,12000,47837,6,0,24,15,16,680,11537

1132964910,0,2711719039,62.40.96.65,1,48,2711694698,2711694698,0,0,207.157.90.11,192.171.128.89,62.40.96.64,40,42,34394,445,6,0,2,18,18,11537,786

1132964950,0,2711759085,62.40.96.65,1,52,2711689698,2711689698,0,0,134.2.205.228,192.17.239.250,62.40.103.252,78,40,59990,3128,6,0,16,16,16,680,11537

1132964965,0,2711774039,62.40.96.65,1,54,2711749040,2711749040,0,0,192.17.24.4,233.4.200.18,0.0.0.0,40,0,10002,10002,17,0,0,16,0,11537,0

1132964970,0,2711779039,62.40.96.65,1,48,2711771039,2711771039,0,0,207.157.90.11,192.171.129.170,62.40.96.64,40,42,36330,445,6,0,2,18,18,11537,786

TOP five 16s owners who send packets to UIUC

6,0,17,16,16,680,11537 => ABILENE - Internet2, US

6,0,16,14,16,680,6509 => CANARIE-NTN - Canarie Inc, CA

6,80,16,16,16,11537,1103 => SURFNET-NL SURFnet, The Netherlands,NL

6,80,16,16,13,11537,680 => ARNES-NET Academic and Research Network of Slovenia, SI

6,0,16,16,16,680,559 =>SWITCH Peering requests: (peering@switch.ch), CH

PART 3: Analyzing packet-level traffic with tcpdump

Please investigate and answer the following questions in your report:

1.Next, we will use tcpdump to analyze the contents of an existing trace. Download http://www.cs.illinois.edu/~caesar/courses/cs436/CodeRedTraces.tgz. This file contains a trace of a small network infected by the Code Red worm. More details about the trace are given at http://www.bofh.sh/CodeRed/index.html. You can display the contents of a trace by executing a command similar to *tcpdump -n -r CRed.07-19-01.dump*. The Code Red worm's behavior is divided into stages: after initially infecting a machine, it first attempts to infect other machines for a period of 20 days. How many remote hosts did the infected machine (192.168.1.105) attempt to infect on July 19 2001? Also, what is the *rate* at which the infected machine attempted to infect remote hosts?

The answer is 2711 and command is following:

```
root@b317c63c8ac5:/home/lab2/CRED# tcpdump -n -r CRed.07-19-01.dump | awk
'/192.168.1.105/' > test.txt
root@b317c63c8ac5:/home/lab2/CRED# cut -d ">" -f 1 test.txt  > test1.txt
root@b317c63c8ac5:/home/lab2/CRED# cat test1.txt | awk '/192.168.1.105/' | sort | uniq -c |
wc -l
2711
```

We could plot each minute by the following, but here to calculate the average :
RATE = 2711 / (2H + 10 MIN) = 2711 / (130 MIN) = 2 times/ min

```
root@b317c63c8ac5:/home/lab2/CRED# cat test1.txt | awk '/192.168.1.105/' | sort | uniq -c >
test
root@b317c63c8ac5:/home/lab2/CRED# cut -d "." -f 1 test  > test2.txt
root@b317c63c8ac5:/home/lab2/CRED# cat test2.txt | sort | uniq -c | wc -l
38
root@b317c63c8ac5:/home/lab2/CRED# cat test2.txt | sort | uniq -c
     17       1 23:20:00
     87       1 23:20:01
     88       1 23:20:03
     12       1 23:20:04
     88       1 23:20:09
     12       1 23:20:10
      2       1 23:20:19
    100       1 23:20:22
    100       1 23:20:25
    100       1 23:20:31
    100       1 23:20:43
    100       1 23:20:46
    100       1 23:20:52
    100       1 23:21:04
    100       1 23:21:07
    100       1 23:21:13
    100       1 23:21:25
    100       1 23:21:28
    100       1 23:21:34
    100       1 23:21:46
    100       1 23:21:49
    100       1 23:21:55
     97       1 23:22:07
      3       1 23:22:08
```

98 1 23:22:10

3 1 23:22:11

97 1 23:22:16

5 1 23:22:17

49 1 23:22:28

51 1 23:22:29

47 1 23:22:31

53 1 23:22:32

40 1 23:22:37

60 1 23:22:38

100 1 23:22:50

100 1 23:22:53

100 1 23:22:59

2 2 23:22:10

2.Find the first TCP syn sent to a remote host in the trace CRed.07-19-01.dump. How long did it take to receive an ack?

We have the figure in the previous question, the first TCP time is 23:20:19.200075 and it takes 23:20:19.440075 - 23:20:19.200075 = 0.22s to receive an ack.

23:20:19.200075 IP 192.168.1.222.1782 > 192.168.1.105.80: Flags [P.], seq 2157693313:2157693573, ack 1462304593, win 17408, length 260: HTTP: GET / HTTP/1.1[!http]

23:20:19.210075 IP 192.168.1.105.80 > 192.168.1.222.1782: Flags [P.], seq 1:1425, ack 260, win 16621, length 1424: HTTP: HTTP/1.1 200 O[!http]

23:20:19.240075 IP 192.168.1.222.1782 > 192.168.1.105.80: Flags [P.], seq 260:651, ack 1425, win 17520, length 391: HTTP: GET /pagerror.[!http]

23:20:19.240075 IP 192.168.1.105.80 > 192.168.1.222.1782: Flags [P.], seq 1425:1565, ack 651, win 16230, length 140: HTTP: HTTP/1.1 304 N[!http]

23:20:19.440075 IP 192.168.1.222.1782 > 192.168.1.105.80: Flags [.], ack 1565, win 17380, length 0

3.20 days after infection, the Code Red worm begins to DDoS the Whitehouse's web server (198.137.240.91). On July 21 2001, what is the rate at which the infected machine sent packets to the Whitehouse's web server?

We could plot each minute by the following, but here to calculate the average :
RATE = 300 / (9 MIN) = 300 / (9 MIN) = 33 times/ min

root@b317c63c8ac5:/home/lab2/CRED# cat data1 | awk'/198.137.240.91/' >data1_2

root@b317c63c8ac5:/home/lab2/CRED# cat data1_2 | sort | uniq -u | wc -l

300

21:51:57.830075 IP 192.168.1.1 > 192.168.1.105: ICMP redirect 198.137.240.91 to host 192.168.1.254, length 76

21:52:06.930075 IP 192.168.1.105.1324 > 198.137.240.91.80: Flags [S], seq 1202412454, win 16384, options [mss 1460,nop,nop,sackOK], length 0

4.On July 30, 2001, what do you observe about the worm's behavior? Is it performing DDoS or infecting hosts at the same rate it did previously?

It aims at specific host and do the ARP request back and forth. Thus, it might be DDoS attack.

root@b317c63c8ac5:/home/lab2/CRED# tcpdump -n -r CRed.07-30-01.dump > f1

23:58:43.690075 IP 192.168.1.1.8283 > 192.168.1.105.80: Flags [S], seq 3262085028, win 512, options [mss 1460], length 0

23:58:43.690075 ARP, Request who-has 192.168.1.1 tell 192.168.1.105, length 46

23:58:43.690075 ARP, Reply 192.168.1.1 is-at 00:a0:24:8a:fc:71, length 28

23:58:43.690075 IP 192.168.1.105.80 > 192.168.1.1.8283: Flags [S.], seq 808403467, ack 3262085029, win 17520, options [mss 1460], length 0

23:58:43.690075 IP 192.168.1.1.8283 > 192.168.1.105.80: Flags [.], ack 1, win 32120, length 0

23:58:43.690075 IP 192.168.1.1.8283 > 192.168.1.105.80: Flags [.], seq 1:1461, ack 1, win 32120, length 1460: HTTP: GET /default.i[!http]

23:58:43.690075 IP 192.168.1.1.8283 > 192.168.1.105.80: Flags [.], seq 1461:2921, ack 1, win 32120, length 1460: HTTP

23:58:43.700075 IP 192.168.1.105.80 > 192.168.1.1.8283: Flags [.], ack 2921, win 17520, length 0

23:58:43.700075 IP 192.168.1.1.8283 > 192.168.1.105.80: Flags [P.], seq 2921:4040, ack 1, win 32120, length 1119: HTTP

23:58:43.880075 IP 192.168.1.105.80 > 192.168.1.1.8283: Flags [.], ack 4040, win 16401, length 0

23:58:44.990075 IP 192.168.1.105.80 > 192.168.1.1.8283: Flags [P.], seq 1:5, ack 4040, win 16401, length 4: HTTP: GET [!http]

23:58:45.010075 IP 192.168.1.1.8283 > 192.168.1.105.80: Flags [.], ack 5, win 32120, length 0

23:58:48.050075 IP 192.168.1.1.8283 > 192.168.1.105.80: Flags [F.], seq 4040, ack 5, win 32120, length 0

23:58:48.050075 IP 192.168.1.105.80 > 192.168.1.1.8283: Flags [.], ack 4041, win 16401, length 0

23:58:54.070075 IP 192.168.1.105.138 > 192.168.1.255.138: NBT UDP PACKET(138)

5.If you wanted to protect your machine from being infected by Code Red, what sort of filters might you install in your firewall?

As the analysis before, the worm will perform DDoS or unlimited Hosts attack. We should filter in DDoS and Hosts separately. For Hosts : we design filter for packets control such as TCP/UDP, BGP, find out the abnormal SYP and ACK events and filter them. For DDoS : we could do Packets analysis , storage analysis to monitor whether there is a huge amount increase of our packets or data storage in our system. Design the filter to refuse that once the abnormal events are continuing.

PART 4: Analyzing reachability with packet probing and querying

4a. Testing connectivity with *ping*

Ping is a networking utility used to test reachability and latency. It works by sending ICMP messages to a particular IP address. The receiver, if running a proper implementation of ICMP, will reply back to the source.

Please perform the following steps, and answer the corresponding questions in your report:

1. Using ping, study the latency between where you are currently, and www.illinos.edu. Run ping for a while and study how latency changes over time. What do you observe?

Now it timeout request, but it should display the normal in daytime.

Bob:~ zyx$ ping www.illinois.edu

PING illinois.edu (192.17.13.36): 56 data bytes

Request timeout for icmp_seq 0

Request timeout for icmp_seq 1

Request timeout for icmp_seq 2

Request timeout for icmp_seq 3

Request timeout for icmp_seq 4

Request timeout for icmp_seq 5

Request timeout for icmp_seq 6

Request timeout for icmp_seq 7

Request timeout for icmp_seq 8

Request timeout for icmp_seq 9

Request timeout for icmp_seq 10

Request timeout for icmp_seq 11

Request timeout for icmp_seq 12

Request timeout for icmp_seq 13

Request timeout for icmp_seq 14

Request timeout for icmp_seq 15

Request timeout for icmp_seq 16

Request timeout for icmp_seq 17

2.Next, run ping to test latency to (a) an interface on the same physical LAN as yourself (b) an interface on www.tsinghua.edu.cn. Compare the average latency you find to what you discovered in the question above. What do you observe?

My ip address in 66.253.180.51;

Bob:~ zyx$ ping 66.253.180.51

PING 66.253.180.51 (66.253.180.51): 56 data bytes

64 bytes from 66.253.180.51: icmp_seq=0 ttl=64 time=1.341 ms

64 bytes from 66.253.180.51: icmp_seq=1 ttl=64 time=1.022 ms

64 bytes from 66.253.180.51: icmp_seq=2 ttl=64 time=1.164 ms

64 bytes from 66.253.180.51: icmp_seq=3 ttl=64 time=1.119 ms

64 bytes from 66.253.180.51: icmp_seq=4 ttl=64 time=2.609 ms

64 bytes from 66.253.180.51: icmp_seq=5 ttl=64 time=1.617 ms

64 bytes from 66.253.180.51: icmp_seq=6 ttl=64 time=3.425 ms

64 bytes from 66.253.180.51: icmp_seq=7 ttl=64 time=2.580 ms

Bob:~ zyx$ ping localhost

PING localhost (127.0.0.1): 56 data bytes

Request timeout for icmp_seq 0

Request timeout for icmp_seq 1

Request timeout for icmp_seq 2

Request timeout for icmp_seq 3

Request timeout for icmp_seq 4

Bob:~ zyx$ ping www.tsinghua.edu.cn

PING www.d.tsinghua.edu.cn (166.111.4.100): 56 data bytes

64 bytes from 166.111.4.100: icmp_seq=0 ttl=231 time=226.427 ms

64 bytes from 166.111.4.100: icmp_seq=1 ttl=231 time=233.728 ms

64 bytes from 166.111.4.100: icmp_seq=2 ttl=231 time=257.142 ms

64 bytes from 166.111.4.100: icmp_seq=3 ttl=231 time=213.776 ms

64 bytes from 166.111.4.100: icmp_seq=4 ttl=231 time=223.528 ms

64 bytes from 166.111.4.100: icmp_seq=5 ttl=231 time=242.095 ms

64 bytes from 166.111.4.100: icmp_seq=6 ttl=231 time=225.067 ms

64 bytes from 166.111.4.100: icmp_seq=7 ttl=231 time=219.342 ms

64 bytes from 166.111.4.100: icmp_seq=8 ttl=231 time=237.420 ms

64 bytes from 166.111.4.100: icmp_seq=9 ttl=231 time=216.990 ms

64 bytes from 166.111.4.100: icmp_seq=10 ttl=231 time=214.587 ms

64 bytes from 166.111.4.100: icmp_seq=11 ttl=231 time=237.598 ms

64 bytes from 166.111.4.100: icmp_seq=12 ttl=231 time=215.547 ms

64 bytes from 166.111.4.100: icmp_seq=13 ttl=231 time=216.212 ms

The time to receive the send packet in myself is much shorter than ping to www.illinois.edu.

The time to receive the send packet in www.tsinghua.edu.cn is much longer than ping to www. illinois.edu.

3.Disconnect yourself from the network while you are running ping. What happens? Connect to the network. What happens?

Disconnect the network : the ICMP packets are not send successfully and no route can be found to the host; When connect again : the ICMP packets are restored to normal status and we could see the time slot for sending and receiving.

ping: sendto: No route to host

ping: sendto: No route to host

Request timeout for icmp_seq 434

ping: sendto: No route to host

Request timeout for icmp_seq 435

ping: sendto: No route to host

Request timeout for icmp_seq 436

ping: sendto: No route to host

Request timeout for icmp_seq 437

ping: sendto: No route to host

Request timeout for icmp_seq 438

64 bytes from 66.253.180.51: icmp_seq=509 ttl=64 time=1.259 ms

64 bytes from 66.253.180.51: icmp_seq=510 ttl=64 time=2.416 ms

64 bytes from 66.253.180.51: icmp_seq=511 ttl=64 time=5.676 ms

64 bytes from 66.253.180.51: icmp_seq=512 ttl=64 time=1.015 ms

4b. Studying IP-layer reachability using *traceroute*

Traceroute is a networking utility used to discover the IP-layer path between a pair of interfaces. It is also based on ICMP, but uses a clever trick - it repeatedly sends packets with increasing TTLs -- intermediate routers, upon TTL expiry, send an ICMP message back to the source. In so doing, traceroute can discover the set of IP-layer hops along the path to the provided destination.

Please perform the following steps, and answer the corresponding questions in your report. Please perform the following steps:

1. Run traceroute to www.cs.illinois.edu from your current location. Then run it to government.ru. Which ISPs does your packet traverse? Can you figure out some cities that your path traverses? For the latter, which link is probably the trans-atlantic (or trans-pacific) link?

Localhost => mr-urb-180-1.dmisinetworks.net => host-181-129.pavcmi.corp.pavlovmedia.com => …(3-13) => cpanel.engr.illinois.edu

Cities are in UIUC.

Bob:~ zyx$ traceroute www.cs.illinois.edu

traceroute to cpanel.engr.illinois.edu (192.17.90.136), 64 hops max, 52 byte packets

1 192.168.0.1 (192.168.0.1) 2.001 ms 3.238 ms 2.101 ms

2 mr-urb-180-1.dmisinetworks.net (66.253.180.1) 2.415 ms 3.729 ms 2.087 ms

3 host-181-129.pavcmi.corp.pavlovmedia.com (66.253.181.129) 3.033 ms 4.015 ms 3.601 ms

4 be1-3526.edge1.ilcmi1.pavlovmedia.net (173.230.125.56) 3.293 ms 6.074 ms 3.890 ms

5 te0-0-1-2-3538.edge1.inind1.pavlovmedia.net (173.230.125.80) 9.217 ms 9.700 ms 6.935 ms

6 uiuc-customer.pavlovmedia.net (216.171.30.118) 7.343 ms 6.450 ms 6.949 ms

7 iccn-ur2rtr-uiuc2.gw.uiuc.edu (72.36.127.6) 10.142 ms 7.398 ms 6.566 ms

8 t-exite2.gw.uiuc.edu (130.126.0.205) 9.678 ms 6.465 ms 6.743 ms

9 t-fw2.gw.uiuc.edu (130.126.0.190) 7.274 ms 11.459 ms 63.112 ms

10 t-exiti1.gw.uiuc.edu (130.126.0.133) 8.874 ms 11.626 ms 9.552 ms

11 130.126.0.241 (130.126.0.241) 8.331 ms 8.539 ms 8.827 ms

12 172.20.24.6 (172.20.24.6) 9.982 ms 9.096 ms 8.356 ms

13 172.20.25.246 (172.20.25.246) 10.861 ms
172.20.25.250 (172.20.25.250) 12.177 ms 7.663 ms

14 cpanel.engr.illinois.edu (192.17.90.136) 7.872 ms 8.459 ms 8.346 ms

Localhost => mr-urb-180-1.dmisinetworks.net => host-181-129.pavcmi.corp.pavlovmedia.com => …(3-17) => be2845.rcr22.fra06.atlas.cogentco.com => ..

Cities from UIUC to atlas and trans-Atlantic link

Bob:~ zyx$ traceroute government.ru

traceroute: Warning: government.ru has multiple addresses; using 95.173.136.163

traceroute to government.ru (95.173.136.163), 64 hops max, 52 byte packets

1 192.168.0.1 (192.168.0.1) 4.895 ms 0.944 ms 0.888 ms

2 mr-urb-180-1.dmisinetworks.net (66.253.180.1) 3.648 ms 3.539 ms 2.295 ms

3 host-181-129.pavcmi.corp.pavlovmedia.com (66.253.181.129) 2.785 ms 3.721 ms 7.755 ms

4 host-0-148.cmi.clients.pavlovmedia.com (216.171.0.148) 3.292 ms 4.723 ms 3.531 ms

5 te0-0-1-2-3538.edge1.inind1.pavlovmedia.net (173.230.125.80) 8.533 ms 6.758 ms 7.224 ms

6 te0-0-1-1.nr11.b021117-0.ind01.atlas.cogentco.com (38.104.214.129) 10.822 ms 10.749 ms 7.516 ms

7 154.24.38.25 (154.24.38.25) 7.265 ms
154.24.38.21 (154.24.38.21) 8.358 ms
154.24.38.25 (154.24.38.25) 11.010 ms
8 be3330.rcr21.cmh02.atlas.cogentco.com (154.54.1.78) 11.550 ms 10.996 ms 17.951 ms
9 be2732.ccr21.cle04.atlas.cogentco.com (154.54.40.250) 15.481 ms 14.645 ms
be2733.ccr22.cle04.atlas.cogentco.com (154.54.41.54) 13.850 ms
10 be2994.ccr32.yyz02.atlas.cogentco.com (154.54.31.234) 26.676 ms 20.888 ms
be2993.ccr31.yyz02.atlas.cogentco.com (154.54.31.226) 20.548 ms
11 be3260.ccr22.ymq01.atlas.cogentco.com (154.54.42.90) 28.247 ms 29.187 ms 32.343 ms
12 be3043.ccr22.lpl01.atlas.cogentco.com (154.54.44.165) 97.676 ms
be3042.ccr21.lpl01.atlas.cogentco.com (154.54.44.161) 97.835 ms 101.063 ms
13 be2182.ccr41.ams03.atlas.cogentco.com (154.54.77.245) 114.994 ms 115.631 ms
be2183.ccr42.ams03.atlas.cogentco.com (154.54.58.70) 112.346 ms
14 be2814.ccr42.fra03.atlas.cogentco.com (130.117.0.142) 115.187 ms
be2813.ccr41.fra03.atlas.cogentco.com (130.117.0.122) 130.914 ms
be2814.ccr42.fra03.atlas.cogentco.com (130.117.0.142) 115.625 ms
15 be2845.rcr22.fra06.atlas.cogentco.com (154.54.56.190) 132.366 ms 114.215 ms
be2846.rcr22.fra06.atlas.cogentco.com (154.54.37.30) 113.641 ms
16 rostelecom.demarc.cogentco.com (149.11.20.138) 114.617 ms 114.049 ms 114.173 ms
17 213.59.212.123 (213.59.212.123) 161.905 ms 166.929 ms

2. Perform a traceroute to www.youtube.com. Use Cogent's Looking glass (http://www.cogentco.com/en/network/looking-glass) from Paris, France to the same two sites above.

traceroute to www.youtube.com:

Bob:~ zyx$ traceroute www.youtube.com

traceroute: Warning: www.youtube.com has multiple addresses; using 172.217.9.78

traceroute to youtube-ui.l.google.com (172.217.9.78), 64 hops max, 52 byte packets

1 192.168.0.1 (192.168.0.1) 1.796 ms 0.980 ms 0.830 ms

2 mr-urb-180-1.dmisinetworks.net (66.253.180.1) 2.281 ms 2.321 ms 1.717 ms

3 host-181-129.pavcmi.corp.pavlovmedia.com (66.253.181.129) 7.536 ms 4.530 ms 2.691 ms

4 host-0-148.cmi.clients.pavlovmedia.com (216.171.0.148) 8.107 ms 5.673 ms 6.485 ms

5 te0-0-1-2-3523.edge1.ilord1.pavlovmedia.net (173.230.125.50) 8.086 ms 9.197 ms 5.565 ms

6 173.230.125.23 (173.230.125.23) 17.464 ms 8.126 ms 6.191 ms

7 74.125.50.220 (74.125.50.220) 8.130 ms 8.811 ms 6.178 ms

8 * 108.170.243.193 (108.170.243.193) 11.428 ms *

9 72.14.239.123 (72.14.239.123) 7.061 ms 5.887 ms 9.825 ms

10 ord38s09-in-f14.1e100.net (172.217.9.78) 9.567 ms 7.743 ms 8.612 ms

```
traceroute to government.ru (95.173.136.163), 30 hops max, 60
byte packets
 1  gi0-7-0-18.5.agr22.par01.atlas.cogentco.com (130.117.254.73)
0.715 ms  0.720 ms
 2  be2097.ccr41.par01.atlas.cogentco.com (130.117.49.78)  0.890
ms be2108.ccr42.par01.atlas.cogentco.com (130.117.50.134)  0.817
ms
 3  be2799.ccr41.fra03.atlas.cogentco.com (154.54.58.233)
10.069 ms be2800.ccr42.fra03.atlas.cogentco.com (154.54.58.237)
9.990 ms
 4  be2846.rcr22.fra06.atlas.cogentco.com (154.54.37.30)  10.467
ms  10.476 ms
 5  rostelecom.demarc.cogentco.com (149.11.20.138)  10.356 ms
rostelecom.demarc.cogentco.com (149.11.20.238)  10.797 ms
 6  213.59.212.117 (213.59.212.117)  49.845 ms 213.59.212.229
(213.59.212.229)  51.099 ms
 7  188.128.72.2 (188.128.72.2)  61.335 ms 46.61.162.26
(46.61.162.26)  60.860 ms
 8  95.173.133.147 (95.173.133.147)  53.693 ms *


traceroute to www.youtube.com (216.58.208.174), 30 hops max, 60
byte packets
 1  gi0-7-0-18.5.agr22.par01.atlas.cogentco.com (130.117.254.73)
0.571 ms  0.631 ms
 2  be2108.ccr42.par01.atlas.cogentco.com (130.117.50.134)
0.722 ms  0.818 ms
```

```
 3  be3183.ccr31.par04.atlas.cogentco.com (154.54.38.66)  0.740
ms  1.237 ms
 4  tata.par04.atlas.cogentco.com (130.117.15.70)  0.976 ms
0.785 ms
 5  72.14.212.77 (72.14.212.77)  8.620 ms  8.638 ms
 6  108.170.244.241 (108.170.244.241)  8.909 ms  8.921 ms
 7  108.170.233.114 (108.170.233.114)  8.966 ms 108.170.238.162
(108.170.238.162)  8.976 ms
 8  108.170.234.252 (108.170.234.252)  32.204 ms  32.173 ms
 9  209.85.143.66 (209.85.143.66)  8.638 ms 64.233.175.112
(64.233.175.112)  8.542 ms
10  * 108.170.246.129 (108.170.246.129)  8.562 ms
11  216.239.46.39 (216.239.46.39)  8.567 ms 216.239.46.29
(216.239.46.29)  8.589 ms
12  lhr25s09-in-f174.1e100.net (216.58.208.174)  8.512 ms  8.470
ms
```

4c. Querying DNS with *dig*

dig is a tool that can query the Domain Name System (DNS) to obtain the domain name associated with an IP address or vice versa.

Please perform the following steps, and answer the corresponding questions in your reportPlease perform the following steps:

1.Use dig on your computer to find out the IP address of facebook.com.

Bob:~ zyx$ dig facebook.com

facebook.com. 280 IN A 157.240.19.35

2.Use https://toolbox.googleapps.com/apps/dig/#A/ to find out the IP address of facebook.com. Why might this return a different answer?

```
;ANSWER
facebook.com. 36 IN A 31.13.65.36
```

The facebook.com might have multiply servers ; The techniques to dig is different between from website and from Linux command setting; The communication protocols are different since we don’t set up a protocol here.

3.Use dig to lookup www.facebook.com (instead of facebook.com -- add a "www" in front). Dig returns different information this time. What is the explanation of what is being returned? What is a CNAME record?

www.facebook.com. 2385 IN CNAME star-mini.c10r.facebook.com.

star-mini.c10r.facebook.com. 43 IN A 157.240.19.35

```
;ANSWER
www.facebook.com. 1831 IN CNAME star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com. 59 IN A 157.240.22.35
```

This time the ip address are in the same range 157.240.* and it's because we use the same protocol (http) for communications.

4d. Checking interface properties with *ifconfig*

ifconfig is a command-line utility which prints and configures information about interfaces configured on your computer. Please use ifconfig to find out (and answer the corresponding questions in your report):

1.What are the layer 3 and layer 2 addresses of the interface your computer uses to send traffic to the public Internet?

Layer 2 : ether 32:00:15:8d:20:00

layer 3: inet 192.168.0.100 netmask 0xffffff00 broadcast 192.168.0.255

2.How much traffic has been sent and received on that interface?

```
Bob:~ zyx$ ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 32:00:15:8d:20:00
        inet6 fe80::cc1:396a:807b:b9ad%en0 prefixlen 64 secured scopeid 0x5
        inet 192.168.0.100 netmask 0xffffff00 broadcast 192.168.0.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
          status: active
```

mtu = 1500 which means the the size of the largest network layer protocol data unit that can be communicated in a single network transaction is 1500 ,all the traffic is below 1500 in eno.

PART 5: Putting it all together: Dealing with real problems

1.Attacks from poneytelecom.edu. What exactly is the problem? If you were Dovid, how would you protect your network from these attacks?

Dovid complained that the attacks might from poneytelecom.eu and many other people have faced the same problems, however, there are no clues for their attacks. If I were him, I would first do DDoS firewall and check my storage and internet connections because it is much serious attack than others types. Then, do the normal types of firewall settings. Finally, ask the institutions to monitor their behaviors and if it's bad then use the legal laws to deal with them.

2.Spectrum prefix hijacks. What exactly is the problem? What is Christopher Morrow's hypothesis about what is going on? What does "pure transit" mean?

Christopher complained that the disorder usage of the Internet might from someone and he could reach to the google.com. Thus, he sends the email to find out the reasons and to see whether others have the same problems. He thinks it's hijacking a few of the prefixes by someone. Pure transit mean no originated prefixes and it might be the one which causes the problems and it sends the spams and takes lots of resources to cause the service out of work.

3.Packet loss through Level 3 in Southern California? Also see the followup here. What exactly is Greg's hypothesis? How do his results back that up? What do you think is going on? And how would you work around the problem to get better service to your customers if you were Greg?

Greg thinks that the loss of the packets are from the Level 3 Los Angeles and Cogent peering and not from the same Level 3 LA (LosAngeles1) nodes to Cogent to Texas. He did many ping tests towards the specific routes and find out whether there are some packets loss in that routes. I think he is right and since there are no loss of packets in the mainly routes, which points out the packets must be somewhere else and peering are mostly likely to be that. First of all, I would like to do much tests in different time slots and using more techniques such the BGP and Traceroute etc. Trying to make it more accurate. What's more, try to get their network topology and test all the nodes in there network. Finally, find out the most likely one and discuss whether there are some nodes which can't be detected easily.

4. Contact info, AS4766 Korea Telecom. What does Igor think happened to his network? How specifically could Korea Telecom have done that (what specifically would they configure)? Describe how could be due to a misconfiguration (what sort of mistake could Korea Telecom have made?) And also describe why this might be intentional (what sort of reasons might Korea Telecom have to block Igor's network?

Igor thinks that NOC seems to have blacklisted his complete AS (198252) and they are not responding to e-mail and his customers are complaining so much. Korea Telecom will first investigate the reasons and if that's true, they would like to find out network connections and let Igor connect. If no, they would like to tell Igor what causes the disconnection and ask Igor to deal with that. If it's the mistake, NOC might take Igor to a different institution which they want to block for a long time. I think the most likely thing is their firewall, and Igor might have sent too much traffic them at one time and some behaviors are not normal so that they are in the block list.

5.Companies using public IP space owned by others for internal routing. What is Robert talking about? Why might this be bad practice? Why might it be good practice? Later down that thread, what is Harald Koch talking about?

Robert thinks large enterprises using non RFC1918 IP space that other entities are assigned by ARIN for internal routing and lots of Private Ip address space had been used up. But from Harald Koch, the good practice is that the company will have spare ip address to use and no worry for losing all of them overlapping. He gives many IP6 examples with NATs from his previous employers to illustrate why the company do that, which he thinks might not be a bad thing.

6. Hurricane Maria: Summary of communication status - and lack of . What problems did Hurricane Maria cause to networks? How did operators deal with these problems? How would you make your network resilient to these problems?

Hurricane Maria cause the cell service and Wi-Fi problems. The fact is seems there are massive amounts of supplies sitting in San Juan and that they can't get truck drivers to deliver them. The operators can't deliver the fibers and cables on time and the crash of many network still exist. Using normal network checking methods to find out whether there is a bad connection and fixed that. Using ping first to ping some test points and then do physical inspection from firewall to the VPS.

7. Pick another email thread from the NANOG archives: https://mailman.nanog.org/pipermail/nanog/ that describes a problem you find interesting. Then do the same thing, describe the problem and how you would solve it.

https://mailman.nanog.org/pipermail/nanog/2018-March/094467.html

Amazon peering problem happened sometime. Mike can't connect to peering at amazon.com. and he want to find out someone who have similarly problem and help him out. I would like to see this problem is kind of common to people when they did some business to big companies and they finally can't connect due to some causes. I even can't get into the website to amazon aws sometime and feel like annoyed when my EC2 is stilling running. First of all, I contact the aws and to see what's happening. Mike might also do that. What's more, I'd like to see whether we could solve it by using ping or dig tools to that website and see our connections whether it's in good conditions. Finally, we might want to set up a different machine or operating system to connect again.

Post-Mortem/Wishlist

1. In the code-red problem, the problem asks for the first outside host but no outside hosts in the trace. it then says the first host period, but the first host that replies replies after zero time. Would be nice to make problem more interesting. Better yet can we get a more recent trace?

   Yes. I think it's better to get a more recent trace than first. For that, it's hard to go back and find out the first one in terminal and also it's meaningful to do some analysis to the most recent trace.

2. Change Kadena to some other foreign site. Maybe identify some ISP in kadena and let them know that's the isp.

   No clue for this one, I think both are good for me.