Lab 2 - Enterprise Networking
Izz Irfan Mohd Fauzi
mohdfau2@illinois.edu

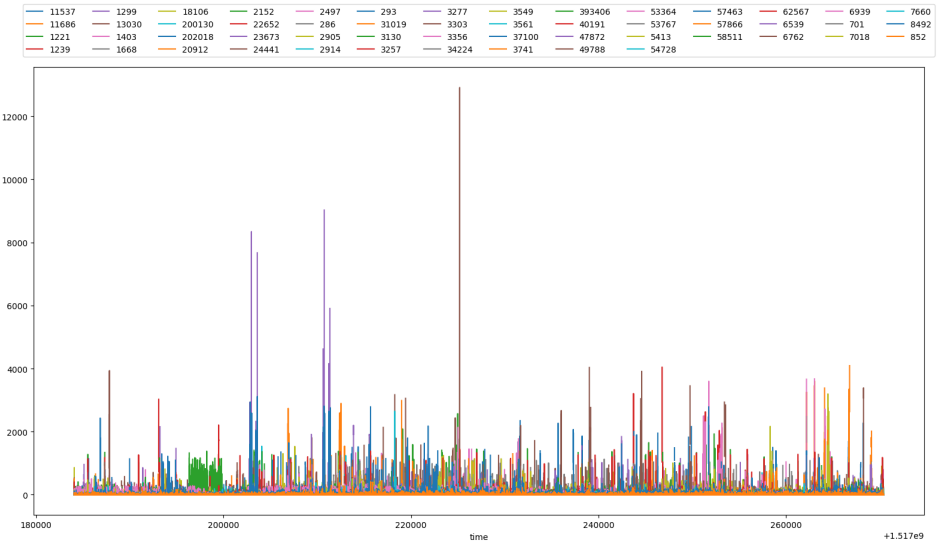
Part 1

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 ignore parentsrecurse 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?

From the data that we got, the most unstable routes would have the highest advertisement an AS makes for it prefixes. From this data we observe that AS 3130 was found to advertise the most.

A bad router could cost a high levels of routing instability places a larger demand on a router's CPU, which can lead to problems in memory consumption and queuing of packet processing. The frequency and size of BGP routing updates can consume a significant amount of resources within the router, causing increasing levels of packet loss and delay. A good router must be able to forward traffic at wire speed, while managing topology changes to routes not currently in use.

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). Yes, you will have a lot of lines in your plot - this is ok! 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?



The best methodology of picking the best AS is to choose the one that doesn't have spikes in the BGP update because we do not want to update too frequently

3. Level 3 Communications (AS 3549) provides two feeds. Suppose you are peered with both of them. Are they doing consistent export (consistent export was described in lecture - consult slides or ask staff if you need clarification)? (Hint: "sort -u" and "diff" may provide a simple way to solve this problem)

Consistent export - the AS-es are advertising the same set of prefixes at all peering points

When we checked two of the feed on the AS 3549, we saw that there was 22,609 number of prefixes out of the total 119,637 that is advertise. The number of prefixes only consist up to 18% which is not good.

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.

The AS's advertising the highest number of prefixes are 3130 (152,185 advertisements), 3549 (119,099 advertisements), 1403 (89,547 advertisements). Yes they could aggregate.

Example:

A,147.28.7.1,3130,99.196.115.0/24
A,147.28.7.1,3130,99.196.114.0/24
A,147.28.7.2,3130,99.193.237.0/24 A,147.28.7.2,3130,99.193.236.0/24
A,147.28.7.2,3130,98.145.125.0/24 A,147.28.7.2,3130,98.145.124.0/24

5. Do you see any ASes advertising bogons? How would you protect your network against those? (Hint: go to bgp.he.net and search for a few ASes)

A bogon is an bogus IP address from the bogon space, which is a set of IP addresses not yet officially assigned to any entity by the Internet Assigned Number Authority (IANA) or a regional Internet registration institute. An example of AS 3549 advertises bogons:

Prefix	Type
208.77.166.9/24	unallocated IPv4
192.84.24.0/24	unallocated IPv4
67.28.48.0/24	unallocated IPv4

A way to protect our network from bogons is to manage a list of possible bogons that you're aware of. Online communities maintains an update of list of bogons, we could start from there as well. Also we could write a script that create all possibility of bogon addresses. Example: address that ends with 0. 10.0.0.0/8, 192.168.0.0/8, 168.121.0.0/8

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 (e.g. How fast should your router's CPU be?) - hint, consider # updates per second you'd need to process (b) your TCAM needs (i.e. How large your TCAM will be? Consider the routing table size). Keep in mind overflows/overload are really bad (why?) - so would you add headroom? How much?

Update per days/Seconds in a day = ~ 366 update/sec

Estimation TCAM space is for 3 million because number of unique prefixes in CAM is about a million and we put a little overhead into it too = ~ 8GB

I would use global trends and Mohrs law to estimate the headroom of data. We need to constanly check every now and then to get a better estimation of our requirement.

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.

To do this we will just block all the IP addresses that is associated with Facebook.

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?

It is hard to know where does the traffic flow. That being said, it is really unsafe as it is totally random based on network congestion and speed. That being said, the government could lease a proprietary network path buy paying some fiber vendors to get a special path to avoid the packet being intercepted by an unknown assailant.

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

We found that AS 11537 had the least withdrawals (6235) out of all the AS's. But 6235 are still a lot of withdrawals! We found this intriguing, and it gives us a sense of how dynamic the internet really is. AS 1403 had 125224 withdrawals, which is significantly

more than AS 11537. AS 1403 is probably a lot more dynamic with a lot of traffic flowing through it, or maybe just a bigger network than AS 11537 having much more routes (and hence withdrawals) to advertise. This way, we could possibly infer the size of an AS's network based on its advertisements and withdrawals.

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

To find out more about AS 46479, we could use the whois command:

whois -h whois.cymru.com "-v AS46479"

Warning: RIPE flags used with a traditional server.

AS | CC | Registry | Allocated | AS Name

46479 | US | arin | 2008-09-30 | HIGHLANDSWIRELESS-PRIMARY-ASN - Pyramid.Net, US

We could do a simple google to get in touch with HIGHLANDS Wireless and get their contact there

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.

One possible route to get to Instagram (AS 6250) from UIUC (AS 38):

1225 | 38 | -1 3561 | 1225 | -1 ---------- 3561 | 6250 | -1

AS 1225 is a provider for UIUC (AS 38). AS 3561 is a provider for AS 6250 and AS 1225.

AS 3561

/\

AS 1225 AS 6250

/

UIUC

Part 2:

1. From a machine within UIUC, perform a traceroute to a machine at IBM. Give the IP address of the first hop router (that is not in UIUC or a University of Illinois-owned AS) which connects to UIUC.

First Hop Router: 38.104.99.41

traceroute to ibm.com (129.42.38.10), 64 hops max, 52 byte packets
1 10.192.0.2 (10.192.0.2) 2.268 ms 2.698 ms 2.380 ms
2 172.20.48.97 (172.20.48.97) 2.259 ms 2.687 ms 1.894 ms
3 t-exiti2.gw.uiuc.edu (130.126.0.166) 2.092 ms 20.541 ms 20.341 ms

4 t-fw2.gw.uiuc.edu (130.126.0.138) 2.227 ms 2.692 ms 2.118 ms

5 t-exite2.gw.uiuc.edu (130.126.0.189) 3.025 ms 2.930 ms 3.220 ms

6 t-dmzb.gw.uiuc.edu (130.126.0.206) 2.987 ms 3.538 ms 2.997 ms
7 ur2rtr-uiuc.ex.ui-iccn.org (72.36.127.5) 3.191 ms 2.805 ms 3.282 ms

8 72.36.126.233 (72.36.126.233) 3.587 ms 3.284 ms 4.138 ms

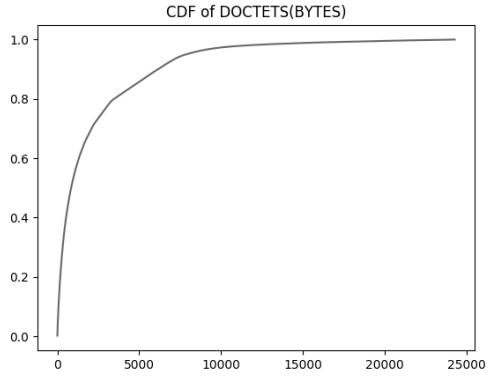
9 t-710rtr.ix.ui-iccn.org (72.36.127.85) 6.507 ms 6.550 ms 5.622 ms
10 72.36.127.206 (72.36.127.206) 5.669 ms 5.835 ms 5.534 ms
11 te0-0-1-3.nr11.b002329-6.ord01.atlas.cogentco.com (38.104.99.41) 6.380 ms 5.773 ms 6.113 ms

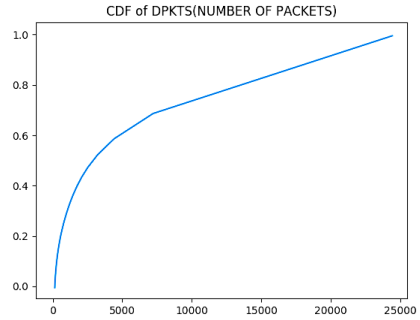
12 te0-4-07.agr22.ord01.atlas.cogentco.com (154.24.35.153) 6.577 ms

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

It is easy to know the BitTorrent traffic, we just count the number of network traffic that has a source or destination part that resides on port 6881 – 6999. Why do we need to do both source and destination? It is because BitTorrent is P2P. Our final value of total traffic that is from those ports are 850. Divide it total traffic we can know the fraction of traffic. 850/24269 = 3.52

3. Plot a CDF of flow lengths flow lengths measured in number of bytes per connection, and again in terms of number of packets per connection.





Code :

```
doctets_sum = data['doctets'].sum()
doctets = data['doctets'].apply(lambda x: float(x)/doctets_sum)
plt.plot(doctets.sort_values(ascending=False).reset_index(drop=True).cumsum())
plt.title('CDF of DOCTETS(BYTES)')
plt.show()
dpkts_sum = data['dpkts'].sum()
dpkts = data['dpkts'].apply(lambda x: float(x)/dpkts_sum)
plt.plot(dpkts.sort_values(ascending=False).reset_index(drop=True).cumsum())
plt.title('CDF of DPKTS(NUMBER OF PACKETS)')
plt.show()
```

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"

From AS 480

131.225.0.0	1020	AS 293	ESNET – Esnet, US
137.138.0.0	412	AS 559	SWITCH Peering request: (peering@switch), CH
142.150.0.0	227	AS 6509	CANARIE-NTN – Canarie Inc, CA
193.40.0.0	226	AS 3221	EENET-AS,EE
129.132.0.0	207	AS 559	SWITCH peering request: (peering@switch),CH

5. What are the top five /16s owned by Abilene-connected institutions which send traffic to AS 680?

To AS 480

128.2.0.0	32	AS 11537	ABILENE – Internet2, US
128.163.0.0	44	AS 11537	ABILENE – Internet2, US
128.42.0.0	68	AS 11537	ABILENE – Internet2, US
152.2.0.0	85	AS 11537	ABILENE – Internet2, US
130.14.0.0	119	AS 11537	ABILENE – Internet2, US

Part 3

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 2119 2001? Also, what is the rate (how many hosts are infected per second on average) at which the infected machine attempted to infect remote hosts?

   Round 1: 704 machines (From 18:20:00 to 18:20:43 -- 43 seconds)

   Round 2: 1615 machines (From 18:21:04 to 18:22:50 -- 106 seconds)

   Therefore, total Infections of both round: (704 + 1615) = 2319
   Average number of hosts infected per second = 2319 / (43 + 106) ~ 15 hosts

2. **Find the first TCP SYNsyn sent to a host (any host) in the trace CRed.07-19-01.dump. How long did it take to receive an SYN-ACKack?**

2001-07-21 18:20:00.740075 192.168.1.1 192.168.1.105TCP 58 → 80 [SYN] Seq=0 Win=512 Len=0 MSS=1460

2001-07-21 18:20:00.750075 192.168.1.105192.168.1.1 TCP 60 8282 [ACK] Seq=1 Ack=2921 Win=17520 Len=0

The ACK is sent almost immediately. ~1ms

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, How many hosts are infected per second (average)?~~ At which rate does the infected machine send packets to the Whitehouse's web server?**

   Infection rate = 298 / 9 = 33.1 packet/sec

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?**

On July 31st, it looks like the worm has stopped infecting other hosts. There are no streams of [SYN]'s sent from 192.168.1.105. It is definitely not performing DDoS or infecting hosts at the same rate it did previously, and has almost died down. We guess that people probably figured out what was going on after the infections on the 19th and 21st July and fixed their firewalls/networks.

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

We believe the Code Red worm is transferred to 192.168.1.105 via a web-request from 192.168.1.1.

Based on our assumption, we could say that it is downloaded from a webpage. Hence we could monitor port 80 traffic of the computer.

Countermeasures against a virus or worm include:

- Updating the computers software
- Put a filter on BGP or set up iptables to disallow user to download stuff from the internet while only allow for specific IP
- Disconnect computer with the internet

4a. Testing connectivity with *ping*

1. Using ping, study the latency between where you are currently, and pavlovmedia.com (nationwide ISP headquartered in Champaign) (or google.com). Run ping for a while and study how latency changes over time. What do you observe?

PING pavlovmedia.com (66.209.200.43) 56(84) bytes of data.
64 bytes from pavlovmedia.com (66.209.200.43): icmp_seq=1 ttl=128 time=25.3 ms 64 bytes from pavlovmedia.com (66.209.200.43): icmp_seq=2 ttl=128 time=23.8 ms 64 bytes from pavlovmedia.com (66.209.200.43): icmp_seq=3 ttl=128 time=22.4 ms 64 bytes from pavlovmedia.com (66.209.200.43): icmp_seq=4 ttl=128 time=20.6 ms ...
--- pavlovmedia.com ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 99414ms
rtt min/avg/max/mdev = 19.824/21.785/32.125/1.899 ms

As you can observe above, the latency change through time. This is because we are using wireless so there will be some fluctuation in network on top of the latency in fiber optic lines.

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?

(a)

PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=128 time=3.57 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=128 time=3.86 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=128 time=5.35 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=128 time=4.87 ms
...
--- 10.0.0.1 ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 99253ms rtt min/avg/max/mdev = 2.961/4.350/16.260/1.638 ms

Ping from computer to gateway generated high fluctuation represented by the difference between minimum and maximum. However, over time those average out by showing a small deviation. Should expect consistent timing between computer to gateway, however, test was done through wireless on a busy building complex causing the signal to vary in intensity. Latency very close to Pavlov.

(b)

PING www.d.tsinghua.edu.cn (166.111.4.100) 56(84) bytes of data.
64 bytes from www.tsinghua.edu.cn (166.111.4.100): icmp_seq=1 ttl=128 time=240 ms 64 bytes from www.tsinghua.edu.cn (166.111.4.100): icmp_seq=2 ttl=128 time=244 ms 64 bytes from www.tsinghua.edu.cn (166.111.4.100): icmp_seq=3 ttl=128 time=238 ms 64 bytes from www.tsinghua.edu.cn (166.111.4.100): icmp_seq=4 ttl=128 time=236 ms ...
--- www.d.tsinghua.edu.cn ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 99313ms
rtt min/avg/max/mdev = 235.254/243.589/512.505/36.079 ms

Since we are pinging at a very long distance, it is expected that the ping will be in the range of the hundreds. This is because light can only travel at the speed of light hence it is the hardware limitation of fiber optics.

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

The replies stop but the program does not stop running. This is because the program is sending still trying to send ping request. Once connections is restored the ping request goes through and the message will appear again.

4c. Querying DNS with *dig*

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

Dig to facebook.com:

; <<>> DiG 9.10.6 <<>> facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32775
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096 ;; QUESTION SECTION: ;facebook.com.

;; ANSWER SECTION: facebook.com.

;; AUTHORITY SECTION: facebook.com. facebook.com.

;; ADDITIONAL SECTION: a.ns.facebook.com. b.ns.facebook.com. a.ns.facebook.com. b.ns.facebook.com.

IN A 242 IN A

165 IN NS 165 IN NS

630 IN A
630 IN A
165 IN AAAA 165 IN AAAA

157.240.2.35

a.ns.facebook.com. b.ns.facebook.com.

69.171.239.12
69.171.255.12 2a03:2880:fffe:c:face:b00c::35 2a03:2880:ffff:c:face:b00c::35

;; Query time: 4 msec
;; SERVER: 130.126.2.131#53(130.126.2.131) ;; WHEN: Sat Sep 29 22:08:25 CDT 2018
;; MSG SIZE rcvd: 180

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?

IP address returned from https://toolbox.googleapps.com/apps/dig/#A/:

⇒ facebook.com. 271 IN A 31.13.65.36

A different IP address is returned. This could be because you might connect to different Facebook addresses based on where you're connecting from. When I dig to facebook.com from my computer, I'm connecting to Facebook from a different IP than https://toolbox.googleapps.com/apps/dig/#A/.

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?

Dig to www.facebook.com

; <<>> DiG 9.10.6 <<>> www.facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48813
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096 ;; QUESTION SECTION: ;www.facebook.com.

;; ANSWER SECTION: www.facebook.com. 678 star-mini.c10r.facebook.com. 34

star-mini.c10r.facebook.com. 157.240.2.35

a.ns.c10r.facebook.com. b.ns.c10r.facebook.com.

69.171.239.11
69.171.255.11 2a03:2880:fffe:b:face:b00c::99 2a03:2880:ffff:b:face:b00c::99

;; AUTHORITY SECTION: c10r.facebook.com. c10r.facebook.com.

;; ADDITIONAL SECTION: a.ns.c10r.facebook.com. b.ns.c10r.facebook.com. a.ns.c10r.facebook.com. b.ns.c10r.facebook.com.

672 672

672
672
672

672

;; Query time: 4 msec
;; SERVER: 130.126.2.131#53(130.126.2.131) ;; WHEN: Sat Sep 29 22:16:32 CDT 2018
;; MSG SIZE rcvd: 213

We believe that facebook.com and www.facebook.com have the same IP address. Most big websites created another DNS that get rid of the www because people tend to forget to write it up. Canonical name or CNAME is used to records alias of one name to another. It allow multiple DNS webpages name to point to one DNS entry

4d. Checking interface properties with *ifconfig*

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 (MAC) Address:
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500

ether f4:0f:24:30:44:28

inet6 fe80::cc:62e9:726a:a60a%en0 prefixlen 64 secured scopeid 0x6 inet 10.195.46.226 netmask 0xfffc0000 broadcast 10.195.255.255 nd6 options=201<PERFORMNUD,DAD>

media: autoselect status: active

Layer 3 (IP) Address: 10.195.46.226

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

Traffic log for these interfaces:

en0 1500 <Link#6> f4:0f:24:30:44:28 1058764 0 598476 0 0 en0 1500 divyams-mac fe80:6::cc:62e9:7 1058764 - 598476 - - en0 1500 10.192/14 wirelessprv-10- 1058764 - 598476 - -

Traffic Received: 1058764 bytes Traffic Sent: 598476 bytes

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

Hurricane Maria: Summary of communication status - and lack of

Hurricane Maria struck Dominica and Puerto Rico In September 2017. The hurricane causes the whole LibertyPR's network to be down in the whole country. This problem is unprecedented because it is involving mother nature rather than human actions/errors. LibertyPR infrastructure was wiped out by a hurricane. From main fiber connections to Cable headends was down. Theft was also followed after due to the lack of governance in times of disaster. LibertyPR pledge that they would provide WiFi hotspot for limited hours to alleviate the situation.

I believe network engineer do not usually take account of these kind of stuff when trying to design a network topology. I believe with better implementation of infrastructure which could withstand weather could probably be installed. Ideally fiber wire is planted approximately 5-10 feet below the ground. We need to plant it deeper to ensure that natural disaster would not affect it but it will come in a higher cost. During times of emergency, it is important that we have connections with the internet because it will speed up the rescue efforts with better communication.

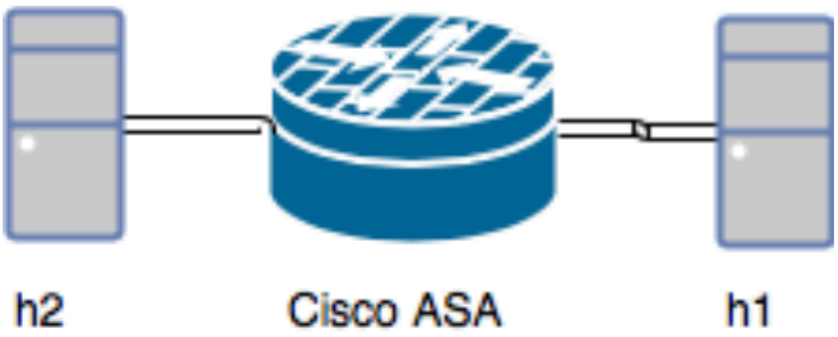
Contact info, AS4766 Korea Telecom

Igor's network has been blocked off by Korea Telecom (AS4766). Korea Telecom probably did this by configuring their border routers to filter out IP addresses from Igor's network. We can't be sure if this is accidental or Korea Telecom actually intended to do this.

Our guess is that Korea Telecom is doing this by using a ip as-path access-list on their border routers? Maybe there is something on their websites being hosted on their network that they don't want Igor's users to see? This could also be issues within Korea Telecom's eBGP and iBGP being incorrectly configured.

I couldn't find any responses to Igor's thread, but if there are a other unrelated AS's complaining about Korea Telecom, then it is most likely to be a technical issue rather than an intentional blacklist.

Part 6: Configure a Cisco ASA



Code for Part 6:

!
interface GigabitEthernet1/4
nameif h2

security-level 100
ip address 192.168.2.1 255.255.255.0

!
interface GigabitEthernet1/5
nameif h1
security-level 50
ip address 192.168.3.1 255.255.255.0

!

IPERF from Server (Listening)

Accepted connection from 192.168.3.2, port 52962
[5] local 192.168.2.2 port 80 connected to 192.168.3.2 port 52963 [ID] Interval Transfer Bandwidth
[5] 0.00-1.00 sec 99.6 MBytes 835 Mbits/sec

[5] 1.00-2.00 sec 92.5 MBytes 776 Mbits/sec
[5] 2.00-3.00 sec 98.3 MBytes 825 Mbits/sec
[5] 3.00-4.00 sec 97.1 MBytes 814 Mbits/sec
[5] 4.00-5.00 sec 95.2 MBytes 798 Mbits/sec
[5] 5.00-6.00 sec 94.4 MBytes 792 Mbits/sec
[5] 6.00-7.00 sec 87.2 MBytes 731 Mbits/sec
[5] 7.00-8.00 sec 88.2 MBytes 740 Mbits/sec

[5] 8.00-9.00 sec 92.8 MBytes 778 Mbits/sec
[5] 9.00-10.00 sec 87.4 MBytes 733 Mbits/sec [5] 10.00-10.03 sec 2.79 MBytes 768 Mbits/sec

IPerf from Client (TCP 80)

4] local 192.168.3.2 port 52963 connected to 192.168.2.2 port 80
[ID] Interval Transfer Bandwidth
[4] 0.00-1.01 sec 100 MBytes 835 Mbits/sec
[4] 1.01-2.00 sec 94.2 MBytes 796 Mbits/sec
[4] 2.00-3.00 sec 98.2 MBytes 825 Mbits/sec
[4] 3.00-4.00 sec 97.6 MBytes 818 Mbits/sec
[4] 4.00-5.00 sec 95.2 MBytes 800 Mbits/sec
[4] 5.00-6.00 sec 94.2 MBytes 791 Mbits/sec
[4] 6.00-7.00 sec 85.4 MBytes 716 Mbits/sec

[4] 7.00-8.00 sec 90.2 MBytes 757 Mbits/sec [4] 8.00-9.00 sec 92.2 MBytes 772 Mbits/sec [4] 9.00-10.00 sec 87.6 MBytes 736 Mbits/sec ----------

[ID] Interval Transfer Bandwidth
[4] 0.00-10.00 sec 936 MBytes 785 Mbits/sec [4] 0.00-10.00 sec 935 MBytes 785 Mbits/sec
iperf Done.