Exercise 7—BGP, Autonomous Systems and the Internet

Name: ________________________ SUNET ID: ________________________@stanford.edu
Please write your SUNET ID clearly.

Background
In this exercise, you are going to peek into a portion of the Internet's routing table. Recall that the Internet predominantly consists of interconnected Autonomous Systems (ASes). The goal of this exercise is to show you the wealth of tools at your disposal to query and understand the AS-level connectivity, by taking a peek at historical and live BGP activity on the Internet.

Warmup: Finding information about an IP address.
There are a number of worldwide Internet registries that allocate IP addresses to customers. America's Internet registry is called ARIN (American Registry for Internet Numbers) and Asia-Pacific has APNIC. These registries offer authoritative "whois" services so you can quickly find out who owns an IP address and the IP address block it is a part of.

Log into myth, and using the whois command shown below, answer the following questions.

    myth> whois -h whois.arin.net 8.8.8.8

1. Who owns the IP address 8.8.8.8? ________________________

2. Which IP address block is 8.8.8.8 part of? _____________ / ___

3. Who owns other addresses in the 8.0.0.0/8 subnet? _____________

Finding the AS's on the path taken by a packet.
The Internet registry whois servers also give information about autonomous system an IP address belongs to. Traceroute can query the whois servers to return the AS numbers.

Log into a myth machine, and run "traceroute -A google.com". The "-A" option causes traceroute to query an Internet registry and return the hop's AS number. Now, answer the following questions:

1. What is/are Stanford's AS number(s)? ________________________

2. What is/are Google's AS number(s)? ________________________

3. There is one other organization on the path between Stanford and Google. What is it, and what is its AS number?
    ________________________. Its AS number is ____________.

Finding prefixes announced by an AS.
After routing registries allocate an AS number and prefixes to an organization, the routers will start
connecting to other AS's and start announcing the prefixes. Many large ISPs collect and share information about routes they learned on their websites. We will be using Hurricane Electric's BGP website: http://bgp.he.net

1. List all IPv4 prefixes announced by Stanford University (AS32) (Visit:http://bgp.he.net/AS32)

__________________________________________________________

2. List all /8 IPv4 blocks announced by MIT:

__________________________________________________________

**Route Collectors.**
So far, you've mostly queried static AS and prefix information that may not be up to date. To get a more up-to-date view, we can query "Looking Glass" (lg) servers which are operated by many ISPs to give a read-only public view of their routing tables. We will be looking at the routing tables on the following servers:

- route-views.routeviews.org (A Cisco router at University of Oregon)
- route-server.gblx.net (Global Crossing was a tier 1 ISP; it was acquired by Level 3 in 2011)

Log into one of the route servers: If prompted for a password, read the instructions from the route server – it will give you one.

telnet route-views.routeviews.org

Now, run the following command to get a path to Google's public DNS server, and look at the output:

route-views> show ip bgp 8.8.8.8

Answer the following questions:
1. How many AS paths are available from University of Oregon to Google? _______

2. For the chosen path, where is the first transit AS from the University of Oregon to Google geographically located?

___________________________________________________________

3. Does Google peer with Univ. of Oregon? (Circle the right answer): YES | NO

Now log into Level 3's route server, and answer the following questions:

1. How many AS paths are available from Level 3 AS to Google? _______

2. What is the maximum AS path length from Level 3 to Google? _______
3. Does Google peer with Level 3? (Circle the right answer): YES | NO

**Historical Records.**  
RIPE is a regional Internet registry for Europe, Middle East and Central Asia. RIPE has a number of route collectors worldwide which passively peer with hundreds of networks worldwide and gives access to historical BGP updates. For this exercise, we will be using the BGPlay tool at:  
[https://stat.ripe.net/widget/bgplay](https://stat.ripe.net/widget/bgplay)

Visit the above page and type in the prefix 208.65.153.0/24 into the textbox that says "Reload the widget by entering a resource here". The website will prompt for a date range. We will travel back in time to see announcements for this prefix on a particular date. Select the following dates as shown below (Feb 24th–25th of 2008) and click "done":

![Image of date selection](image)

After you click "done", click the green circular tick button and wait for the widget to show the data. The website will popup and show that the prefix was announced by **more than one AS**.

1. Which AS's announce 208.65.153.0/24? ___________ and ___________

2. Which organizations own the above AS's? __________________________
   and __________________________

3. How long does it take for the newly announced changes to stabilize?
Approximately ____________ minutes

4. How many minutes does it take for the AS that actually owns the prefix to start re-announcing paths to the same prefix?

Approximately ________________ minutes

5. How long does it take for the other AS to reroute most of the paths back to itself?

Approximately ________________ minutes

**Another historical event**
Reload the BGPlay website and enter 46.53.0.0/17 into the widget, and view the routing activity from 29th November 2012 to 30th November 2012. You should see a number of routing events for this prefix during this time interval:

Click anywhere to the left of the blue-colored "spike" you see in the widget (the selected time is the red line in the figure above). You should see connectivity between a number of AS's and the AS's that announce the prefix 46.53.0.0/17. Now, click anywhere to the right of the spike.

1. Roughly how many paths do you see from neighboring AS's to the two AS's that announce the prefix 46.53.0.0/17 after the spike of updates?

________________________

2. Which organization owns the above prefix? ____________________

3. What do you think happened?

__________________________________________