COMP 189: Homework #3

Assigned Jan 27, 2022
Due Feb 4, 2022

59 points total

Instructions: *For each problem, show all your work (required for credit). For answers requiring written answers, while no more than five or six sentences are expected, sufficient justification must be given for any position, opinion, or perspective taken.*

Submission Instructions: *submit your solutions in PDF format through MyCourses Assignments.*

Technical Exercises

1. IP Addresses (8 pts)

1. How many distinct IPv4 addresses exist? Show your calculations.

There is 2^32 address = 4,294,967,296unique addresses

IPV4 is a 32-bit address, meaning 32 placeholders for 1 or 0:
00000000 00000000 00000000 00000000 (represented as 000.000.000.000)

Each 000 ranges from 0 to 255 (i.e. 256 different numbers) since it consists of 8-bit values.
Hence there are 2^32 or 256^4

2. An ambitious McGill student devises a new IP address that has the following format: A.B.C.D.E.F.G.H – where each letter corresponds to a 4 bit value
   a. What range of values can each position take on?

The format for each letter would be represented in bits as: 0000 0000 0000 0000 0000 0000 0000 0000. Where each value has a range of 0 to 1 (i.e. 0000 to 1111).
The range of numbers between 0000 and 1111 is 16 and there are 8 letters (i.e. 32 bits) meaning there are 16^8 values.

   b. How many IP addresses exist in this new system?

Like mentioned above there are 16 possible values for 8 letters. In other words, 16^8 which is 4,294,967,296 unique IP addresses which is the same number as IPV4.

   c. Is this new IP system better than IPv4? Why or why not?

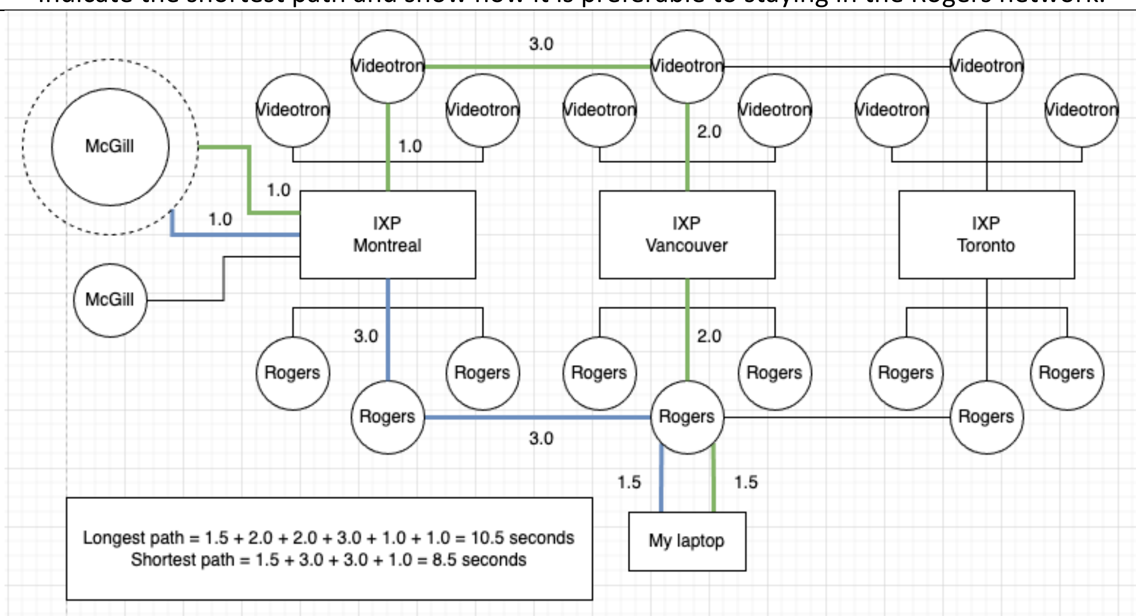
This new system is not better than IPV4 mainly because they identify the same number of devices. Both can uniquely identify 2^32 devices/networks.

We could also argue that in some sense IPV4 is better because it contains five classes: A, B, C, D and E, where these classes have a specific range of IP addresses which dictate the number of devices you can have on your network. Whereas the new system does not have these classes. But this argument is only under the assumption from the explanation that the new IP system does not also have these classes to distinguish different devices/networks.

2. Shortest Routing Paths (10 pts)

Diagram an IXP-POP network (as drawn in class) with the following properties.

- IXPs are represented as squares, POPs are represented as circles, direct wired connections are represented as lines.
- Three IXPs (Vancouver, Toronto, and Montreal)
- A Rogers network with three POPs around each city and a connection into each IXP
- A Videotron network with three POPs around each city and a connection into all three IXPs.
- A McGill network, two POPs (really just routers) – with a connection into the Montreal IXP.
- Your laptop in Vancouver on the Rogers network
- The McGill webserver (at McGill)
- Your laptop is accessing the McGill website and it is using a path that goes through the Videotron network because that's the fastest path.
- Add time labels to each edge in your network that produce this fastest path.
- Indicate the shortest path and show how it is preferable to staying in the Rogers network.

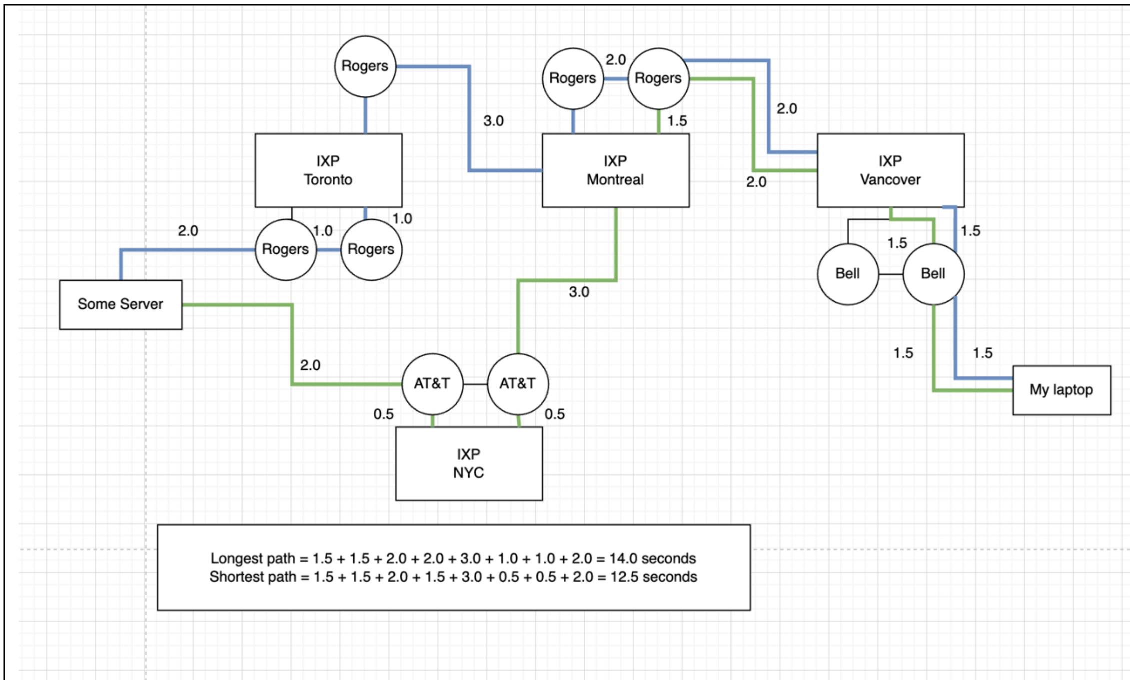


Here we denote the blue line as the shortest path and the green line as the longest path. It's more preferable to stay on the Rogers network because it takes less time to get to the same destination and does not need to cross through a different POP (Rogers to Videotron).

3. Domestic Routes (13 pts)

You are the Chief Technical Officer (CTO) of Canada (this position actually exists) and are tasked with implementing a new "Domestic Routing" initiative – which aims to keep Canadian internet traffic more safe from the snooping view of other countries. The idea is that, if a packet originates in Canada and is bound for a machine in Canada, it can only transit Canadian networks.

1. Using real cities, diagram an IXP-POP network (using conventions from the previous question) in which (a) there is a package originating and ending in Canada, (b) there is a viable path using only Canadian networks, and (c) the fastest path uses a United States (government or corporate) network. Show the path and justify why this path would be taken.
2. Assuming the existence of IXPs and domestic-owned networks, in terms of connectivity, what is the *minimum* condition for implementing the domestic routing initiative?
3. In words, describe the new packet routing policy you'll need to implement in IXPs across Canada to achieve the domestic routing initiative.



1. The shortest path is depicted by the green lines which is the path going through the US networks. The reason this one is preferred is because it because it takes less time to get to the same destination.
2. Canadian ISP and POPS would need to be able to determine if the packets are being sent to a foreign IXP/ISP and not allow it to be sent and instead reroute it to Canadian ISP and POPS that run through Canadian IXPs only.
3. To implement this new packet routing policy, Network admins have to specify in the packet routing policy, to only allow Canadian IP address through as well as ensure that the destination IP of the packet is not international but domestic. If it the packet is being routed to a foreign network, it would not send it and reroute it through another domestic device.

4. Internet Distance (10 pts)

On the internet, distance is measured by how long it takes for your information to get to servers. In this problem, you'll use the command-line command *ping* to determine your relative distance from various places on the internet. In this problem, the time refers to the minimum time reported by ping.

1. Find three university websites, X, Y, and Z
   - Measure your distance from them in physical distance.
   - Measured your distance from them in ping time.

   Give the host names (e.g., www.mcgill.ca) and distances (both physical and ping). In a scatter plot, plot physical distance (x-axis) against ping distance (y-axis). Include the output of your ping command to show your work.

X = McGill University

```
PING www.mcgill.ca (132.216.177.160): 56 data bytes
64 bytes from 132.216.177.160: icmp_seq=0 ttl=244 time=23.071 ms
64 bytes from 132.216.177.160: icmp_seq=1 ttl=244 time=13.572 ms
64 bytes from 132.216.177.160: icmp_seq=2 ttl=244 time=15.477 ms
64 bytes from 132.216.177.160: icmp_seq=3 ttl=244 time=13.110 ms
64 bytes from 132.216.177.160: icmp_seq=4 ttl=244 time=13.529 ms
64 bytes from 132.216.177.160: icmp_seq=5 ttl=244 time=10.413 ms
64 bytes from 132.216.177.160: icmp_seq=6 ttl=244 time=14.582 ms
64 bytes from 132.216.177.160: icmp_seq=7 ttl=244 time=26.134 ms
64 bytes from 132.216.177.160: icmp_seq=8 ttl=244 time=15.781 ms
64 bytes from 132.216.177.160: icmp_seq=9 ttl=244 time=13.734 ms

--- www.mcgill.ca ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 10.413/15.940/26.134/4.601 ms
```

Avg time = 15.9403ms, Distance = 8.55km

Y = University of Toronto

```
PING d3oxxpqksdxu7j.cloudfront.net (54.230.51.6): 56 data byte
64 bytes from 54.230.51.6: icmp_seq=0 ttl=244 time=13.947 ms
64 bytes from 54.230.51.6: icmp_seq=1 ttl=244 time=12.131 ms
64 bytes from 54.230.51.6: icmp_seq=2 ttl=244 time=11.096 ms
64 bytes from 54.230.51.6: icmp_seq=3 ttl=244 time=13.793 ms
64 bytes from 54.230.51.6: icmp_seq=4 ttl=244 time=9.731 ms
64 bytes from 54.230.51.6: icmp_seq=5 ttl=244 time=16.808 ms
64 bytes from 54.230.51.6: icmp_seq=6 ttl=244 time=10.131 ms
64 bytes from 54.230.51.6: icmp_seq=7 ttl=244 time=12.209 ms
64 bytes from 54.230.51.6: icmp_seq=8 ttl=244 time=11.094 ms
64 bytes from 54.230.51.6: icmp_seq=9 ttl=244 time=17.065 ms

--- d3oxxpqksdxu7j.cloudfront.net ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 9.731/12.800/17.065/2.444 ms
```

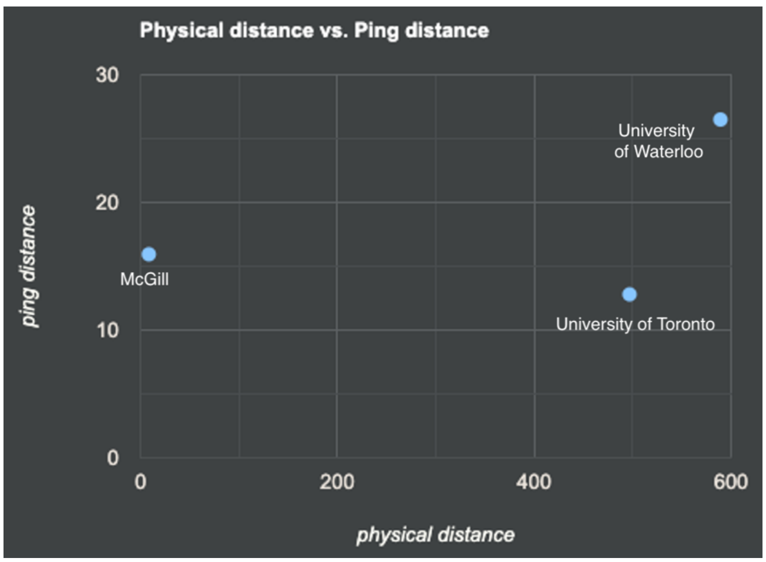
Avg time = 12.8005ms, Distance = 496.86km

Z = Waterloo University

```
PING www-onprem.uwaterloo.ca (129.97.208.23): 56 data bytes
64 bytes from 129.97.208.23: icmp_seq=0 ttl=242 time=34.272 ms
64 bytes from 129.97.208.23: icmp_seq=1 ttl=242 time=25.106 ms
64 bytes from 129.97.208.23: icmp_seq=2 ttl=242 time=33.200 ms
64 bytes from 129.97.208.23: icmp_seq=3 ttl=242 time=24.265 ms
64 bytes from 129.97.208.23: icmp_seq=4 ttl=242 time=25.727 ms
64 bytes from 129.97.208.23: icmp_seq=5 ttl=242 time=25.632 ms
64 bytes from 129.97.208.23: icmp_seq=6 ttl=242 time=22.783 ms
64 bytes from 129.97.208.23: icmp_seq=7 ttl=242 time=25.540 ms
64 bytes from 129.97.208.23: icmp_seq=8 ttl=242 time=25.399 ms
64 bytes from 129.97.208.23: icmp_seq=9 ttl=242 time=23.015 ms

--- www-onprem.uwaterloo.ca ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 22.783/26.494/34.272/3.764 ms
```

Avg time = 26.4939ms, Distance = 589.20km



2. Explain the relationship (or lack there of) you see between physical distance and ping time in your plot.

In this case, there is a lack of relationship between physical distance and ping time as we can see from the scatterplot. This is because the internet distance is a measurement for how fast it takes a packet to reach from the source to the destination. There are many things that can influence the time it takes for example traffic which makes the packet take longer to reach its distance. So even though the distance might be shorter, it might take longer for the ping.

5. Network paths (8 pts)

These are three servers that live inside McGill data centers:

- mammoth.cs.mcgill.ca
- falcon.cs.mcgill.ca
- mail.cs.mcgill.ca

Two of these servers are hosted in the same data center. From inside the McGill network (you will likely need to be physically on campus for this to work), use traceroute to find the two that sit side-by-side in the network. Give evidence to support your claims.

Discussion

1. Rerouting internet traffic (5 pts)

Here is one article covering a case of curious rerouting of massive internet traffic.

How China swallowed 15% of 'Net traffic for 18 minutes | Ars Technica

Find two more events like there where the culprits were different countries (so you'll find one for country X and one for country Y). Give the culprit, the timeframe of the disruption, a link to the article, and a 1-2 sentence summary.

X = Turkey
Y = Taiwan

Culprit: Turkey, Timeframe: a couple hours in the morning on Christmas Eve. Early in December 2004, TTNET (AS9121), a Turkish ISP by accident rerouted well over 100,000 internet routes to all their own transit providers. This caused a large number of internet users to be unable to access some chunks of the internet for at least a few hours since most of the traffic from major websites were being rerouted to TTNET. Link [HERE]

Culprit: Taiwan, Timeframe: May 8th for about three to four minutes. On May 8th, traffic going through a public DNS run by the Taiwanese network information center (TWNIC) rerouted to an entity in Brazil for a few minutes for unknown reasons.

2. Rerouting punishment (5 pts)

Should organizations be punished when erroneous configurations reroute substantial portions of internet traffic? Why or why not? Incorporate routing concepts from class in your justification.

I believe they should be punished for rerouting a big portion of internet traffic.

First because it involves Intellectual Property rules where even though domain names are not protected by the intellectual property law, the names that it makes up might.

There is also the fact that when a business' fills out for a trademark, they are obliged to register for a domain name. If a domain is rerouted like that case with Iran with pornographic website, or Pakistan with YouTube, this could cost them a lot of money in loss of ads for example.

Also, many companies especially those that run businesses online (financial companies, hedge funds, e-businesses, etc) now depend heavily on internet and real-time data and having the internet go down could have massive side effects on them. We could also argue that this is a similar case to how some company's services might go down for some time where other companies depend on that service heavily, for example, when one of Amazon's AWS servers shut down for a few hours (US-east1). Amazon's AWS service received a punishment in the form of impacting their "up-time" which likely reduced from 99.999% to 99.99%. It was not a monetary punishment but more of a "trust" punishment which could lead to many other issues within the company. Even if this was an accident, they still received a punishment because this is not something that should happen.