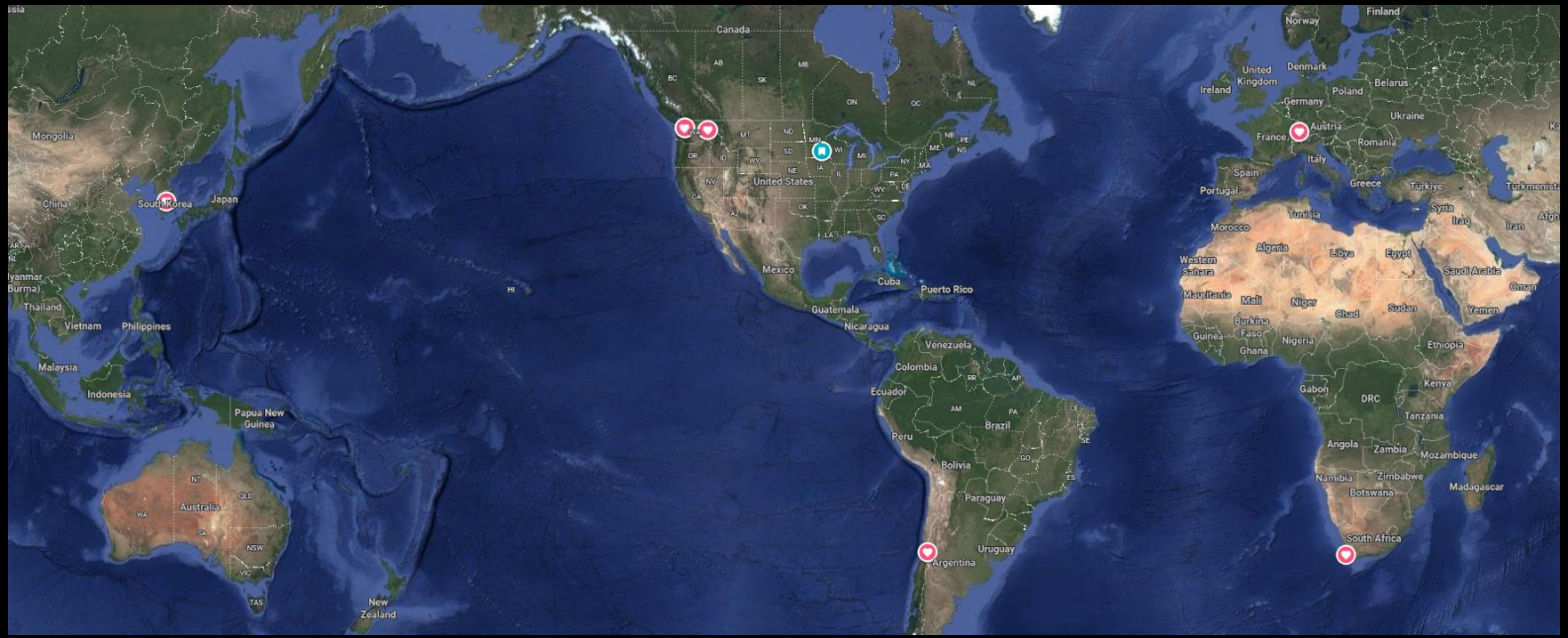
Network Topology

Alden Harcourt

The Mission: Where in the Internet is Carleton?

The Goal: To discover and map the network paths between Carleton College and six diverse destinations across the globe using Traceroute.

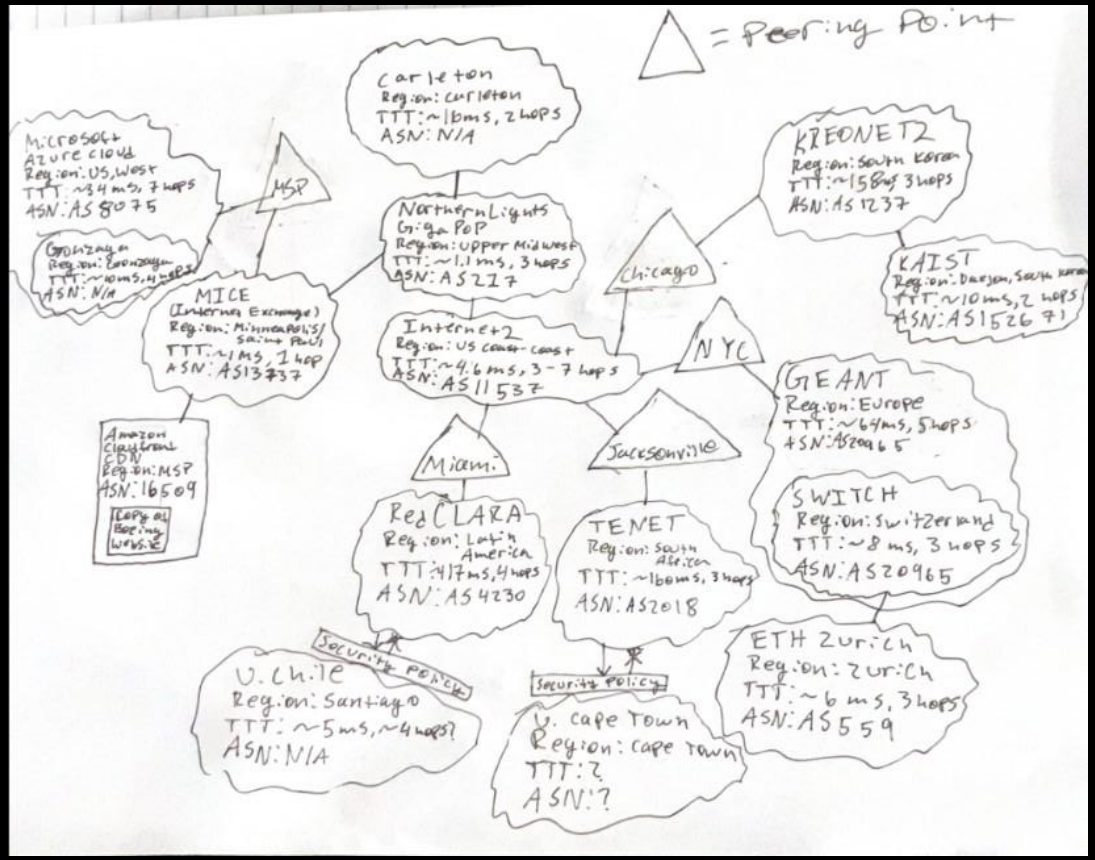


Our Tool: What is Traceroute?

How We See the Path

- Traceroute sends a series of packets to a destination to discover the path they take
- Each router along the way is a hop
- It measure the Round Trip Time (RTT), or latency, in milliseconds, of each hop

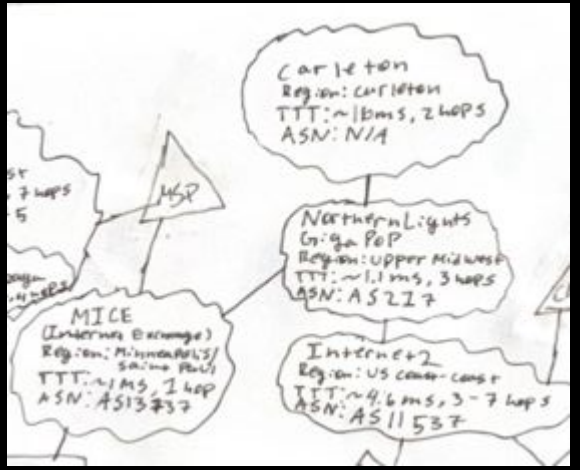
Carleton's Place in the Internet



Carleton’s On-Ramp to the Internet

Carleton has two primary paths to connectivity

- **The Academic Path:** Through the NorthernLights GigaPoP to Internet2, which were used to reach other universities.
- **The Commercial Path:** Through a local internet exchange in Minneapolis (MICE) for commercial sites like Boeing and Gonzaga (hosted in the Microsoft Azure cloud).



Barrier #1: The Content Delivery Network (CDN)

Why is the path to Boeing so short? (5 hops)

- Many large companies place copies of their websites on servers all over the world to make them load faster for a user.
- The trace didn't go to Boeing's headquarters. It went to an amazon server in MSP indicated by the msp in the server name and corroborated by whatismyipaddress.com
- The CDN is a barrier to seeing the true path, but it's what makes the modern web so fast.

```
1    15 ms     5 ms     3 ms  10.133.0.254
2    26 ms    14 ms    10 ms  137.22.198.4
3    21 ms    11 ms     9 ms  telecomb-gr-01-te0-2-0-11-789.northernlights.gigapop.net [146.
4     *        *        *     Request timed out.
5     *        *        *     Request timed out.
6     *        *        *     Request timed out.
7     *        *        *     Request timed out.
8     7 ms    13 ms    10 ms  150.222.205.149
9    21 ms     9 ms    23 ms  server-18-160-181-124.msp50.r.cloudfront.net [18.160.181.124]
```

What is a Peering Point?

- The internet is a network of networks. For data to get from one major network (like Internet2) to another (like KREONET2 in Korea), they must physically connect
- A peering point is a physical location, often a large datacenter, where these massive networks agree to meet and exchange traffic
- Essentially the international departures gate at an airport

The Transatlantic Jump to Europe

- The path to Zurich connects at a peering point in Boston. From there, it travels along a terrestrial fiber line to a coastal Cable Landing Station before crossing the Atlantic via a submarine cable.
- whatismyipaddress.com indicates that the 198.71.45.233 address is in New York, which is unlikely given the latency jump.
- The site also indicates that the 62.40.98.76 address is in Geneva, making it most likely that the 198.71.45 address is on the European side of an underwater cable.
- Therefore, the peering point is most likely the 163.253.2.173 IP address.

```
 50 ms    36 ms  fourhundredge-0-0-0-0.4079.core1.bost2.net.internet2.edu [163.253.2.173]
103 ms   102 ms  198.71.45.233
  *        *     Request timed out.
  *        *     Request timed out.
110 ms   110 ms  ae3-0.mx1.gen.ch.geant.net [62.40.98.76]
```

The Transpacific Jump to Asia

- The path to Asia connects at a peering point in Chicago. From this gateway, data travels overland via a terrestrial fiber backbone to the West Coast, where it enters a submarine cable for the journey to Korea.
- This shows up as one hop because the routers in Chicago and Korea see each other as direct neighbors through the peering point.
- I struggled to find a large institution in East-Asia that didn’t use a CDN. Targeting an FTP (File Transfer Protocol) server bypassed the use of CDNs.
    - CDNs are designed for web traffic, not direct file transfers.

```
 7    19 ms    22 ms    19 ms  fourhundredge-0-0-0-6.4079.core1.star.net.internet2.edu [163.253.2.21]
 8    30 ms    15 ms    17 ms  internet2-kreonet2.chic.kreonet2.net [134.75.108.45]
 9     *        *        *     Request timed out.
10   162 ms   164 ms   163 ms  dj-br1--daej-rtr2kreonet2.net [134.75.103.121]
```

A Southern Connection

1. Trace to UChile travels down the Internet2 network to Jacksonville
2. The data takes one hop to a peering router in Miami
3. The data is handed from Internet2 to RedClara (A Large Latin American Network)
4. Data travels on a submarine cable to Panama

```
13    42 ms    46 ms    42 ms  fourhundredge-0-0-0-6.4079.core1.jack.net.internet2.edu [163.253.1.5]
14    47 ms    47 ms    48 ms  i2-mia.redclara.net [200.0.207.9]
15   161 ms   160 ms   159 ms  mia-pty.redclara.net [200.0.204.30]
```

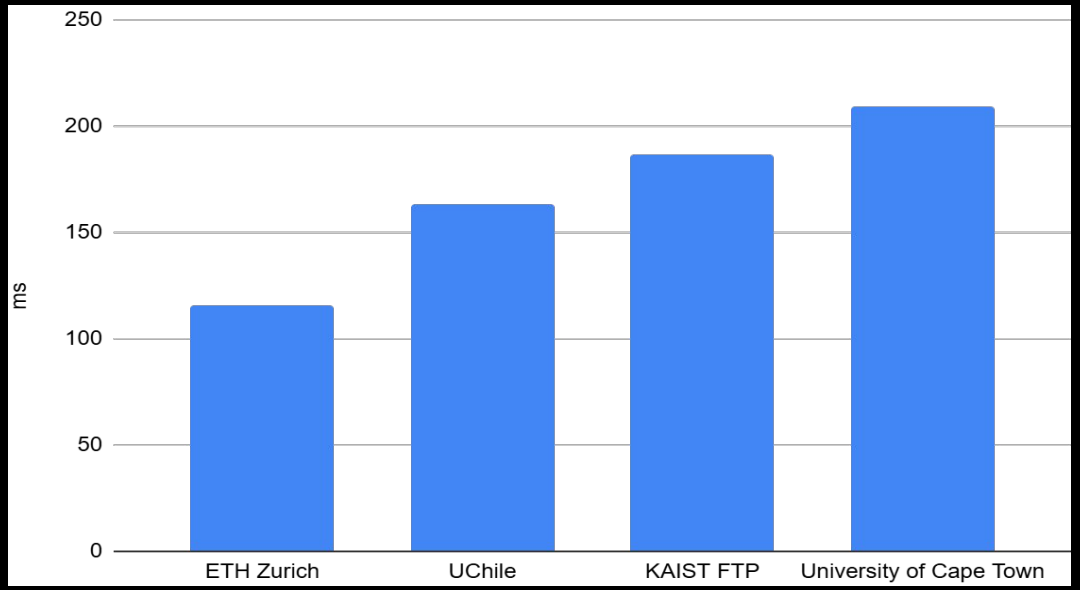
The Road to South Africa

- Similar to the trace to UChile, the trace to University of Cape Town took Internet2 down to Jacksonville
- This router serves as a gateway to the submarine cable that our data took over to Cape Town
- Once in Cape Town, the data was now traveling on Tenet, South Africa's national research and education network

```
13    85 ms    51 ms    42 ms  fourhundredge-0-0-0-6.4079.core1.jack.net.internet2.edu [163.253.1.5]
14   222 ms   206 ms   231 ms  et-0-1-4-1973-cpt3-pe1.net.tenet.ac.za [155.232.71.4]
```

Fast and Slow Paths Around the World

- Based on the final RTT Europe appears to have the lowest latency connection, followed by South America, Asia, and finally Africa
  - However, this is a very small sample size and may not be representative of entire continents



Barrier #2: The Security Wall

- In both Chile and South Africa, the traces successfully reached local university networks but the final hops timed out and I never got a response from the destinations.
- The most likely explanation is that these servers were configured not to respond to public traceroute probes
    - This common security measure prevents network scanning

```
16   220 ms   209 ms   204 ms  et-0-0-1-0-cpt7-pe1.net.tenet.ac.za [155.232.64.70]
17   218 ms   206 ms   204 ms  154.114.124.1
18     *        *        *     Request timed out.
19     *        *        *     Request timed out.
20     *        *        *     Request timed out.
21     *        *        *     Request timed out.
22     *        *        *     Request timed out.
23     *        *        *     Request timed out.
24     *        *        *     Request timed out.
25     *        *        *     Request timed out.
26     *        *        *     Request timed out.
27     *        *        *     Request timed out.
28     *        *        *     Request timed out.
29     *        *        *     Request timed out.
30     *        *        *     Request timed out.
```

```
18   171 ms   170 ms   160 ms  ra-uchile-rai.reuna.cl [146.83.242.26]
19   161 ms   160 ms   160 ms  172.16.40.177
20   160 ms   164 ms   167 ms  172.16.40.177
21     *        *        *     Request timed out.
22     *        *        *     Request timed out.
23     *        *        *     Request timed out.
24     *        *        *     Request timed out.
25     *        *        *     Request timed out.
26     *        *        *     Request timed out.
27     *        *        *     Request timed out.
28     *        *        *     Request timed out.
29     *        *        *     Request timed out.
30     *        *        *     Request timed out.
```

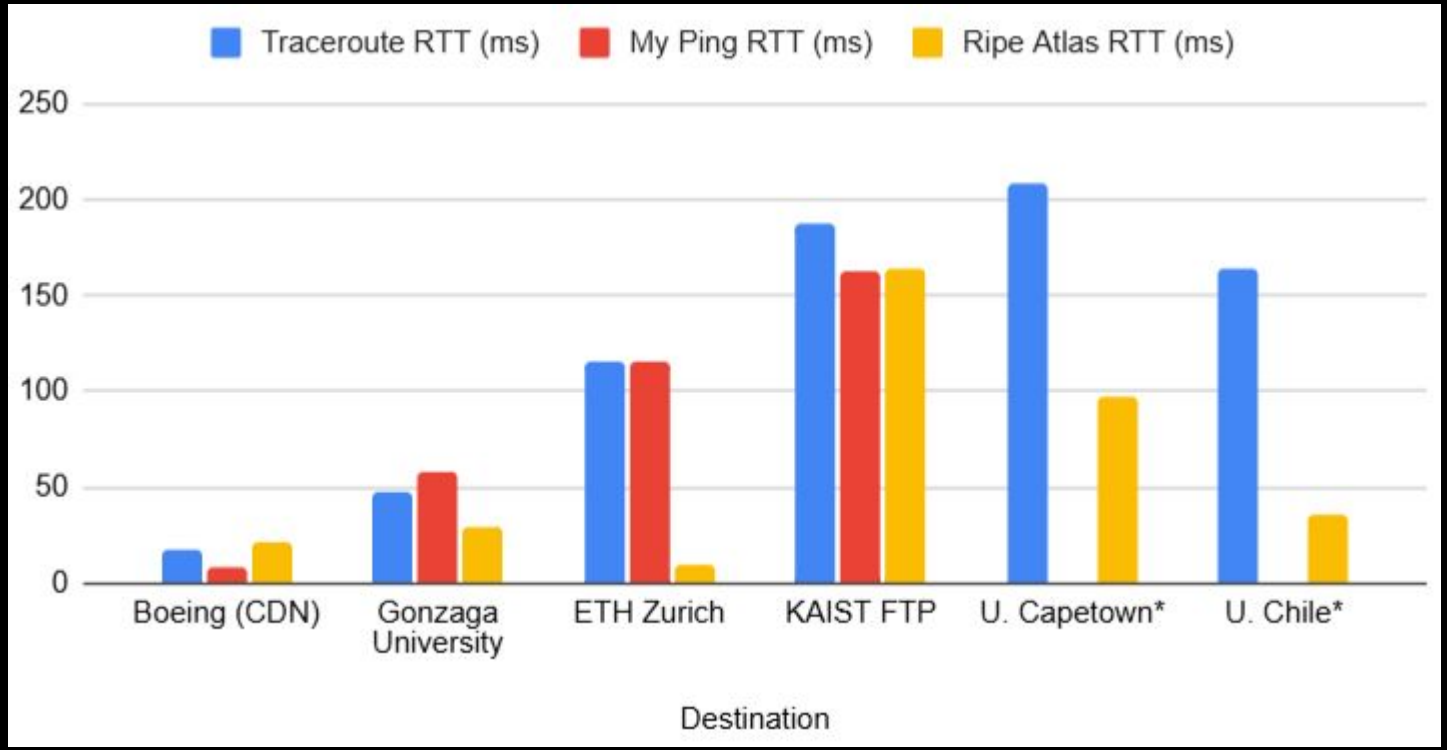
Where does our Data Spend the Most Time?

- The Internet2 network is incredibly fast, often taking ~50 ms to traverse
- The vast majority of time was spent traversing submarine cables, which makes sense given their distances.
- The single longest hop was between Jacksonville and Cape Town, totalling ~160 ms

```
13    85 ms    51 ms    42 ms  fourhundredge-0-0-0-6.4079.core1.jack.net.internet2.edu [163.253.1.5]
14   222 ms   206 ms   231 ms  et-0-1-4-1973-cpt3-pe1.net.tenet.ac.za [155.232.71.4]
```

Ping vs. Traceroute vs. RIPE Atlas

All averages



Pings to U. Cape Town and U. Chile failed, supporting my security wall theory

The Ripe Atlas was considerably faster. RIPE probes are measuring latency to local data centers hosting major services

Key Takeaways

- I found 2 paths that Carleton uses to access the internet. Internet2 for reaching other universities and MICE exchange for corporate sites.
- CDNs bring data closer to us, the Boeing trace went to an Amazon server in MSP and not to their headquarters. CDNs make mapping the internet difficult.
- Data is handed off between major networks at specific peering points.
- The vast majority of time data spends traveling is across huge submarine fiber optic cables.
- Many servers are configured not to respond to pings or traceroutes for security purposes.

Sources

- https://bgp.he.net/ip/146.83.242.26
- https://www.arin.net/resources/registry/whois/rdap/
- https://aws.amazon.com/what-is/cdn/
- https://www.cloudflare.com/learning/cdn/what-is-a-cdn/
- https://www.cloudns.net/blog/ftp-vs-http-file-transfer-protocol-hypertext-transfer-protocol/
- https://www.digitalrealty.com/resources/articles/what-is-internet-peering-and-why-is-it-beneficial
- https://www.kentik.com/blog/diving-deep-into-submarine-cables-undersea-lifelines-of-internet-connectivity/
- https://azure.microsoft.com/en-us/explore/global-infrastructure/geographies
- https://micemn.net/
- https://www.namehero.com/blog/tracert-request-timed-out-what-it-means-and-how-to-fix-it/
- https://prophaze.com/learn/cdn/how-do-attackers-bypass-a-cdn/
- https://www.ripe.net/analyse/internet-measurements/ripe-atlas/how-ripe-atlas-works/
- https://serverfault.com/questions/725092/does-blocking-icmp-also-block-traceroute
- https://superuser.com/questions/318870/why-do-companies-block-ping