Richard Stretanski

CIS-527-001

DLN Student

Active Measurements of Routes, Losses, and Delays

Abstract (summary)

In this paper I will analyze the connection between my local machine to the network locations of five different websites across the globe. I will be tracing the route from my machine to the remote locations as well as measuring packet loss and round-trip time ten times over the span of a week. I have decided to both trace the route and measure packet loss and round-trip time for the following five websites: www.microsoft.com, www.ford.com, www.dhs.gov, www.ox.as.uk, www.momat.go.jp.

Introduction (background and hypothesis)

Website Rationale

I decided to choose the websites in the following chart for reasons such as physical distance, regional diversity, perceived reliability.

Name	URL	IP	Assumed Hosting Location
Microsoft	www.microsoft.com	23.79.193.241	Seattle, WA
Ford	www.ford.com	23.0.53.101	Dearborn, MI
Department of Homeland Security	www.dhs.gov	104.95.235.101	Washington, D.C.
Oxford University	www.ox.ac.uk	129.67.242.154	Oxford, England
Tokyo Museum of Modern Art	www.momat.go.jp	202.236.109.30	Tokyo, Japan

I ended up choosing three websites from the United States, one website from Europe, and one website from Asia totaling 5 websites.

First, I chose Ford's website because I wanted a benchmark for a website that I perceived to be extremely close to my local machine (my local machine is located in Dearborn, MI). There were two quality options for websites that are hosted in Dearborn, MI, ford.com and umdearborn.edu. Both of these options I considered to be dependable, but I expected ford.com to have more traffic and I also expected most of the other students to be analyzing umdearborn.edu, so I ended up settling on ford.com.

From there I also wanted one east coast US website and one west coast US website. There are loads of good websites hosted on the west coast, but I settled on Microsoft.com because I thought they were

very similar to ford.com in terms of reliability and traffic. The last US website I chose was the home of the Department of Homeland Security, dhs.gov. The Department of Homeland Security headquarters is located in Washington, D.C.

I decided that I needed one website location to be in Europe and one website location to be in Asia after making the first three spread across the United States. I wanted a one university website URL, so I chose Oxford University's website ox.ac.uk which is located in Oxford, England. This website was chosen mostly due to its location and reliability. Lastly, I chose momat.go.jp, the website for the Tokyo Museum of Modern Art located in Tokyo, Japan. I decided on this website because I wanted a government run URL that was extremely far from my local PC and on a different continent than Oxford. For all tests I will use the IP addresses associated with these websites in the chart above. This will ensure consistency of routing paths since some websites can have multiple IP addresses associated with them.

Background

There are two major tests that will be run in this paper. A ping test and a traceroute. The ping test will be run by using the following command in Command Prompt: *ping -n 14 xxx.xxx.xxx.xxx*. This will send 14 packets containing 32 bytes of data to the IP address: *xxx.xxx.xxx.xxx*. The command will return each packet's round trip time (RTT) as well as the Max RTT, Min RTT, Average RTT, and the percent of packet lost. Because I will not include all 50 results from the ping tests in this paper, here is an example of a ping test run on IP address:

```
Microsoft Windows [Version 10.0.16299.125]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\rich>ping -n 14 23.79.193.241

Pinging 23.79.193.241 with 32 bytes of data:
Reply from 23.79.193.241: bytes=32 time=23ms TTL=54
Reply from 23.79.193.241: bytes=32 time=26ms TTL=54
Reply from 23.79.193.241: bytes=32 time=19ms TTL=54
Reply from 23.79.193.241: bytes=32 time=27ms TTL=54
Reply from 23.79.193.241: bytes=32 time=24ms TTL=54
Reply from 23.79.193.241: bytes=32 time=21ms TTL=54
Reply from 23.79.193.241: bytes=32 time=29ms TTL=54
Reply from 23.79.193.241: bytes=32 time=26ms TTL=54
Reply from 23.79.193.241: bytes=32 time=22ms TTL=54
Reply from 23.79.193.241: bytes=32 time=21ms TTL=54
Reply from 23.79.193.241: bytes=32 time=30ms TTL=54
Reply from 23.79.193.241: bytes=32 time=24ms TTL=54
Reply from 23.79.193.241: bytes=32 time=20ms TTL=54
Reply from 23.79.193.241: bytes=32 time=23ms TTL=54

Ping statistics for 23.79.193.241:
    Packets: Sent = 14, Received = 14, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 30ms, Average = 23ms

C:\Users\rich>_
```

I will also be running a traceroute on all of the chosen IP addresses. A trace route is run by entering the following command into command prompt: *tracert xxx.xxx.xxx.xxx*. The trace route command sends 3 packets of data to a destination and records the RTT and IP address of each router hop.

Hypothesis

It is my hypothesis that the ford.com tests will have the best and most stable and consistent results. Due to the close proximity of where I presume ford.com is located in relation to my local machine, I think we will see the lowest Min RTT, Max RTT, and Average RTT as well as the most consistent average RTT overall, and the smallest difference between the Min RTT and Max RTT in general. This is all just based on the location and dependability of their website. Packet loss will likely be the least of all the tested websites just because there is less of an opportunity to lose a packet than some of the websites that are further away. Aside from opportunity, packet loss is more or less random and is usually based on traffic. For the traceroute test, I expect ford.com to have the least amount of hops by a large margin.

I expect Microsoft.com and dhs.gov to be very similar in all respects. Microsoft.com is a lot further being on the west coast US, but Microsoft.com likely has a lot more traffic, and I think that would reduce the number of hops it takes to get to Microsoft.com. I think both of these websites will have higher Min RTT, Max RTT and average RTT than ford.com but still significantly smaller than the non-US websites. I think average RTT will be consistent in general but not as consistent as ford.com's averages. Microsoft and DHS should have more hops to reach their destination than Ford, and also have a slightly higher packet loss percentage than Ford.

Oxford University's website should have a significantly higher Min/Max RTT as well as have a higher average RTT. It would also be not surprising if there were outliers where one test could have an average RTT or Max RTT that is significantly higher than the rest of Oxford's results. I expect more inconsistency between Min/Max RTT and Average RTT, and a higher packet loss rate, and take more hops to reach their destination than the previously mentioned websites.

Lastly the Tokyo Museum of Modern Art's website should be the highest in terms of Min/Max RTT and average RTT. I expect even greater outliers and less consistency than Oxford, as well as a greater packet loss rate than oxford, and the most hops for each packet to reach their destination. I would not be surprised if the path to momat.go.jp changes the most frequently and has the most router timeouts considering the distance is even further than Oxford.

Methodology

I will perform 2 ping tests and 2 tracert tests per day for a total of 5 days, testing the following 5 IP addresses: 23.79.193.241 (Ford), 23.0.53.101 (Microsoft), 104.95.235.101 (DHS), 129.67.242.154 (Oxford), and 202.236.109.30 (MOMAT). Each website will be tested twice per day. I will end up having results for 50 ping tests and 50 tracert tests. I will not worry about the exact time of day or an exact time in between tests but I will make sure there is at least 5 hours in between tests. All tests will be imported into a spreadsheet immediately after taken and a number will be assigned to each test. For example, Ping1 will include one ping result for each of the 5 websites on the first round of testing on the first day, the numbering will go up to Ping10 and the same numbering will be applied to tracert tests. Please see the accompanying spreadsheet for detailed info on the exact results for every single test.

After already going through most of the days' worth of results, I realize that the assignment called for 120 echo requests. I had already captured most of the ping results at 14 echo requests like in the example and since I couldn't start all of the tests over, I made the decision that it would be better especially for Min RTT, Max RTT, and packet loss that I keep a consistent number of echo requests in each ping test (14). Average RTT should not really be affected.

Results

Ping results – Overall
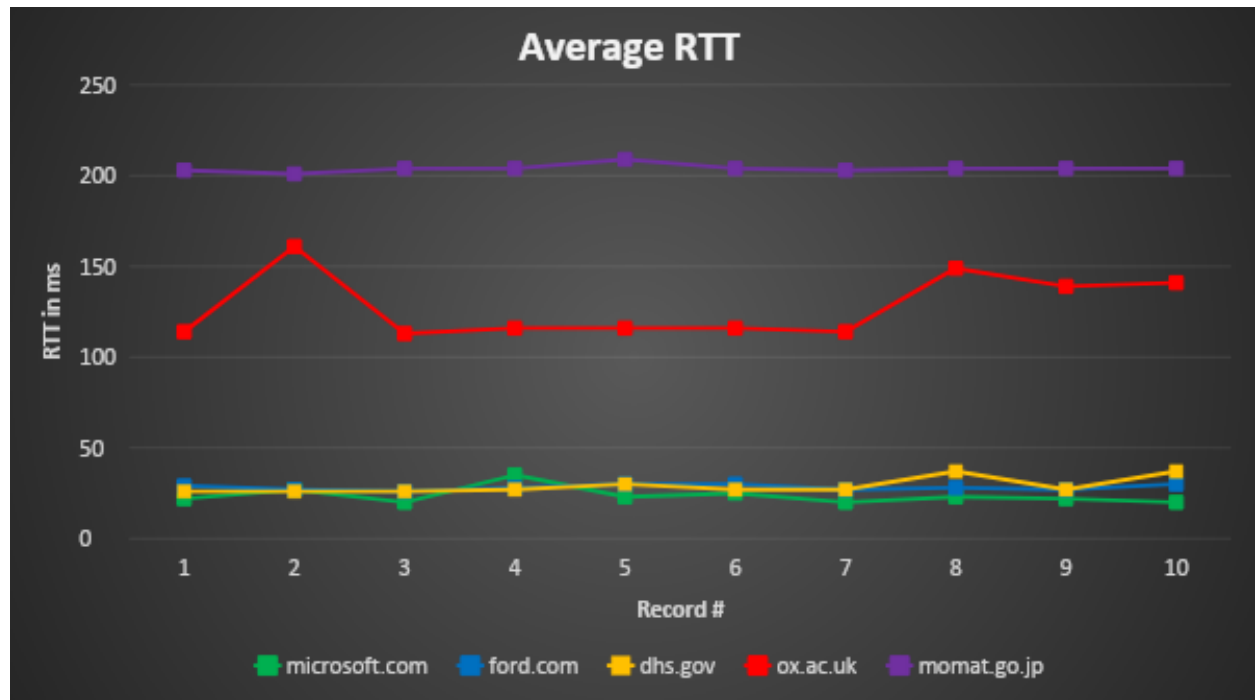
In this chart, Record 1 and 2 would be day one, record 3 and 4 would be day 2 and so on. This is the record scheme used throughout the results. As you can see in the above graph, Microsoft, Ford and DHS all had very similar average RTT throughout the week. What is surprising about this is that Ford is significantly closer to my local computer than Microsoft and DHS.   More info about the reason behind this might be available in the tracert section of results. The average RTT of Oxford and MOMAT are about as expected but what is really interesting about the MOMAT average RTT is how consistent it is. It is actually the most consistent average RTT of all 5 websites with a range of 201 – 209ms AVG RTT while Ford has a range of 26 – 30ms AVG RTT and by comparison DHS has a range of 26 – 37ms AVG RTT.

Ping results – Microsoft

Record #	% Loss	Min RTT	Max RTT	Avg RTT
		Microsoft.com		
1	0	19	27	22
2	0	24	33	27
3	0	18	23	20
4	0	25	46	35
5	0	19	28	23
6	0	18	53	25
7	0	18	25	20
8	0	19	36	23
9	0	18	32	22
10	0	18	25	20
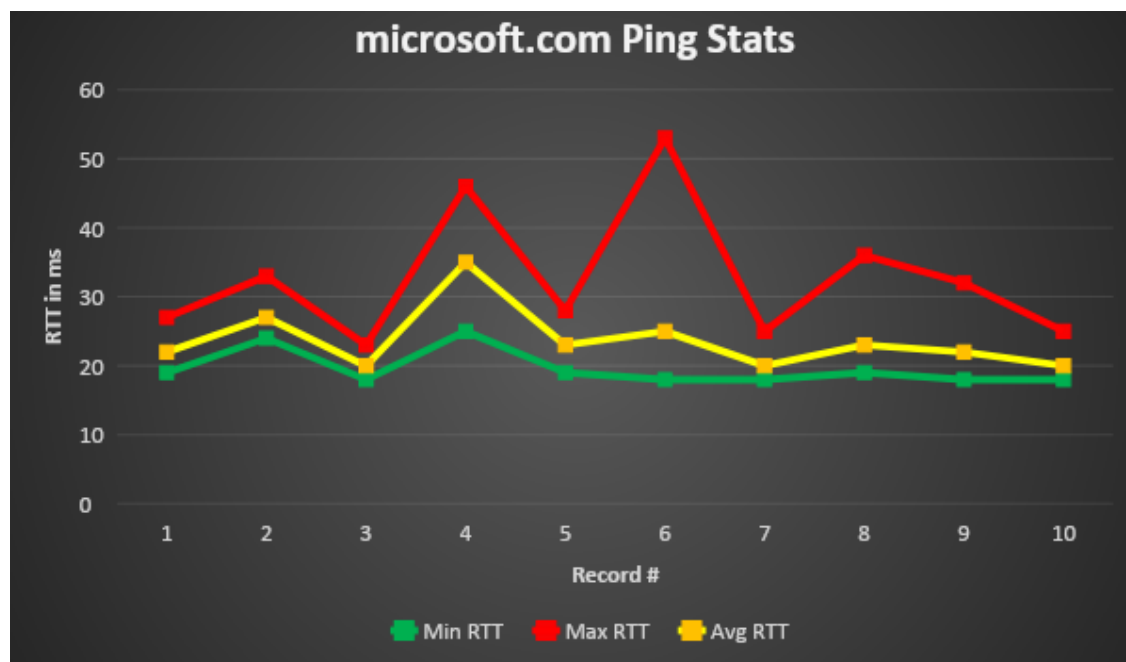
Microsoft's RTT was actually the lowest across the board despite them being on the other side of the US. They had an average Min RTT of 19.6ms, an average Max RTT of 32.8ms and an average AVG RTT of 23.7ms. These would be averages of every single echo, 140 in total.   Despite having the lowest RTTs across the board, it was also the least consistent of all of the US websites with a range of 20 – 35 ms. This could mean that having a low RTT may not be based entirely on distance like I initially hypothesized, but instead it may be RTT consistency that is more dependent on distance. Microsoft also had a 0% packet loss across all 140 echoes.

Ping results – Ford

Record #	% Loss	Ford.com		
		MinRTT	MaxRTT	Avg RTT
1	0	25	36	29
2	0	23	35	27
3	0	24	29	26
4	0	24	40	28
5	0	24	39	30
6	0	27	44	30
7	0	24	35	27
8	0	25	47	28
9	0	24	34	27
10	0	25	76	30

ford.com Ping Stats
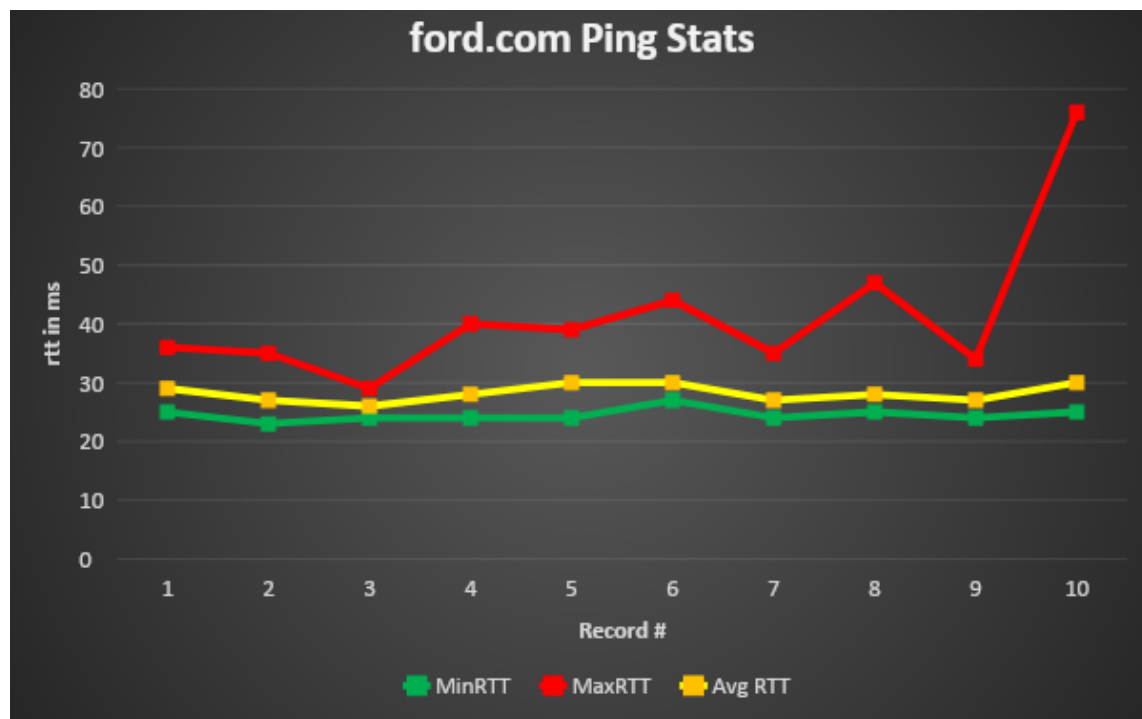
Despite not having the lowest average RTTs at an average Min RTT of 24.5, an average Max RTT of 41.5 and an average Avg RTT of 28.5, it was still lower than DHS in both average Max RTT and average Avg RTT, and tied with DHS for average Min RTT. Ford also had the most consistent Avg RTT with a range of 26 – 30 ms. This also supports the new hypothesis that distance has a greater affect on RTT consistency than having a low RTT. Ford also had a 0% packet loss across all 140 echoes.

Ping results – Department of Homeland Security

| Recor d #	% Loss	dhs.gov MinRT T	MaxRT T	Avg RTT
1	0	25	28	26
2	0	25	28	26
3	0	24	30	26
4	0	25	32	27
5	0	26	38	30
6	0	25	32	27
7	0	24	34	27
8	0	25	138	37
9	0	23	34	27
10	0	23	143	37
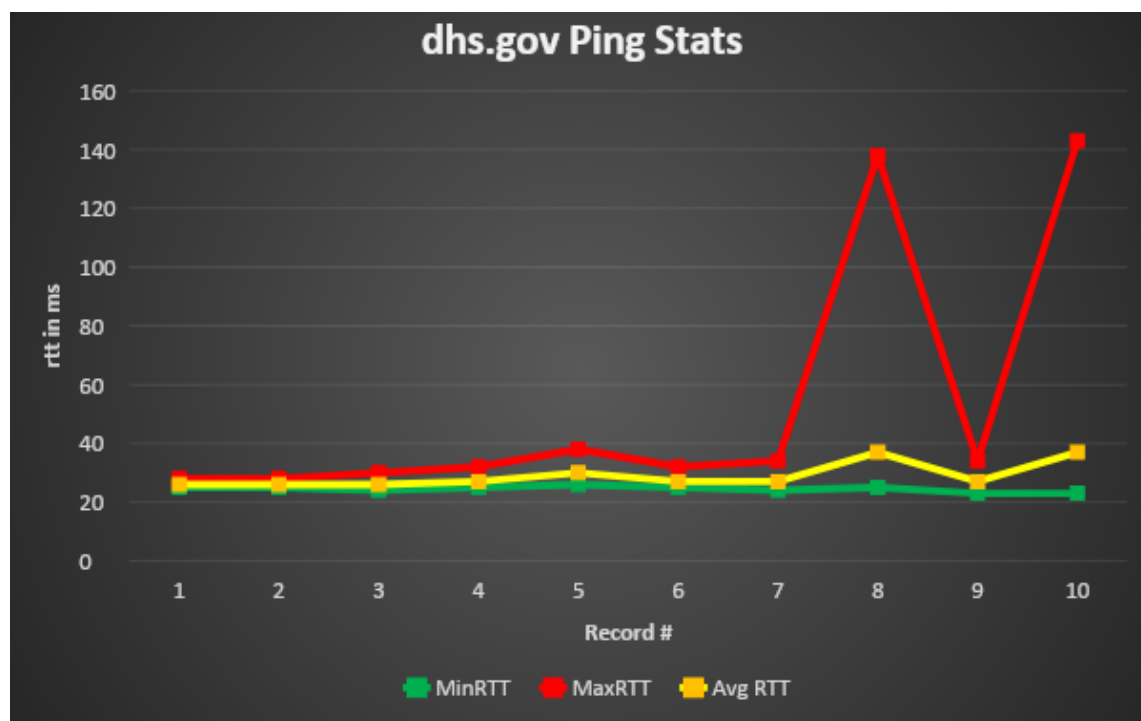
The Department of Homeland Security website followed a similar pattern as the rest of the US websites. Towards the end of the week it had a couple of spikes in Max RTT, but still had relatively low averages. It tied for the second lowest average Min RTT of 24.5ms and it also had an average Max RTT of 53.7ms and an average Avg RTT of 29ms. The Max RTT spikes are not exclusive to DHS, in fact Microsoft was the only website to not have Max RTT spikes on record attempts 8 and 10. Since my machine is the only common factor in this case I can only assume that a program was updating in the background during these tests or

something to that extent. DHS also had an Avg RTT range of 26 – 37 ms. DHS also had a 0% packet loss across all 140 echoes.

Ping results – Oxford

| Record #	% Loss	ox.ac.uk		
		MinRTT	MaxRTT	Avg RTT
1	0	112	116	114
2	0	115	273	161
3	0	113	114	113
4	0	111	131	116
5	0	112	123	116
6	0	110	127	116
7	0	112	124	114
8	0	111	289	149
9	0	111	247	139
10	0	112	305	141
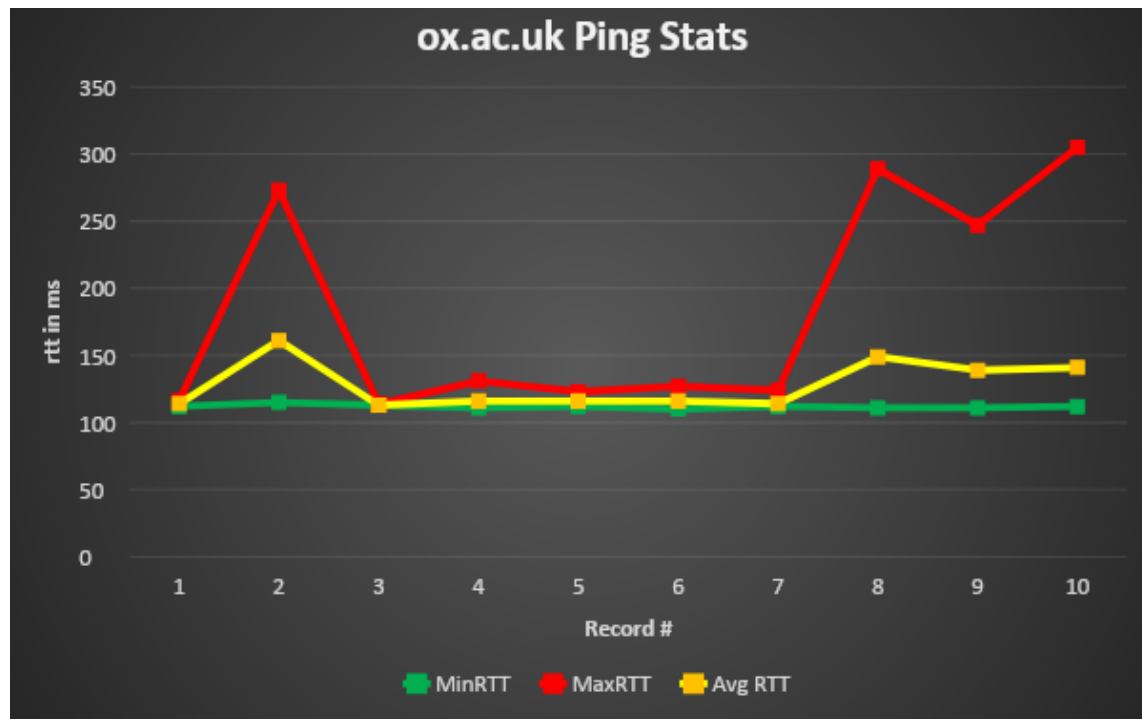
Oxford University unsurprisingly had the second highest average RTTs of all 5 websites with an average Min RTT of 111.9ms, an average Max RTT of 184.9ms and an average Avg RTT of 127.9ms. This is consistent with my hypothesis. Oxford also had an Avg RTT range of 114 – 161ms. That is the widest range across all 5 websites, and while I did hypothesize that Oxford would be inconsistent, I did not expect MOMAT to be more consistent than them. Oxford also had a 0% packet loss across all 140

echoes. This was extremely surprising even with only 140 echoes, that should be enough of a sample size to at least drop one packet.

Ping results – Museum of Modern Art, Tokyo

| Record #	% Loss	momat.go.jp		
		MinRTT	MaxRTT	Avg RTT
1	0	200	209	203
2	0	200	202	201
3	0	202	206	204
4	0	201	213	204
5	0	202	247	209
6	0	199	216	204
7	0	200	208	203
8	0	200	224	204
9	0	201	212	204
10	0	199	219	204
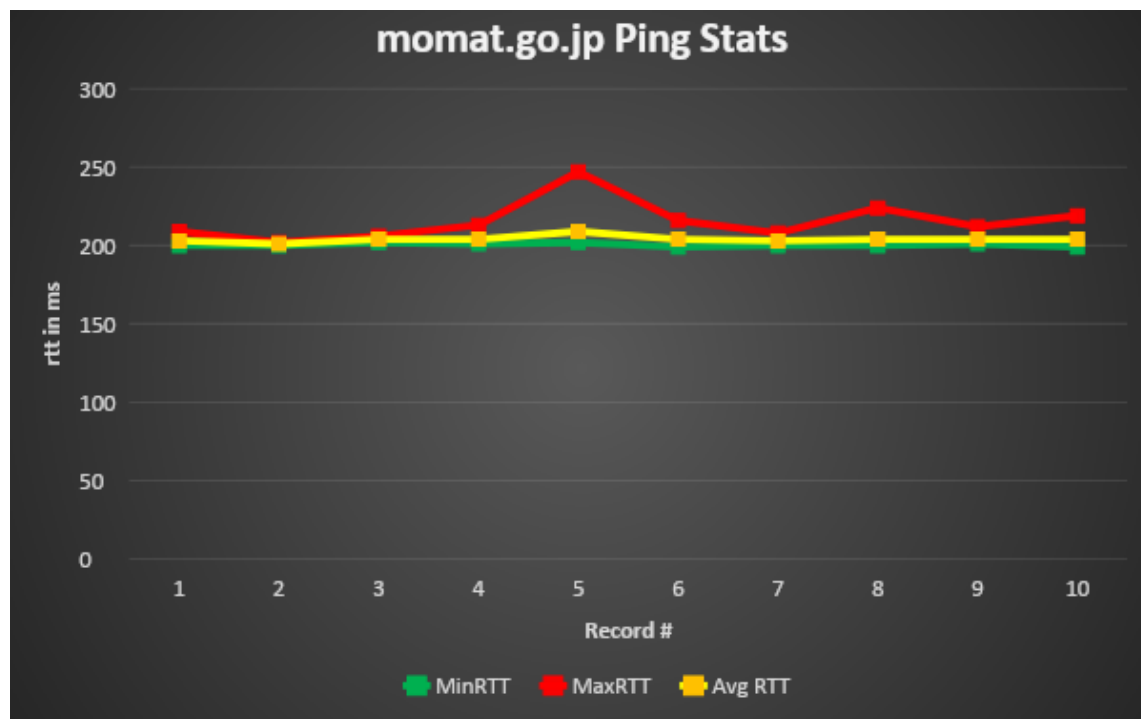
MOMAT had an incredibly surprising amount of consistency in all aspects of their data. They had an expectedly high average Min RTT of 200.4ms, average Max RTT of 215.6ms, and average Avg RTT of 204ms. They are the furthest distance of any website and have the highest RTTs, but have the second smallest Avg RTT range of 201 – 209ms and thus the second most consistent behind only Ford. This kills my newer hypothesis that distance has a greater impact on consistency than low RTT. MOMAT also had

a 0% packet loss across all 140 echoes. This was again extremely surprising even with only 140 echoes, that should be enough of a sample size to at least drop one packet. Even if that were extrapolated over the 1200 echoes requested, even if a few packets were dropped here and there, it should still hover around 0%.

Tracert - Hop Analysis

Trace Route Hops					
Record #	Microsoft.com	Ford.com	dhs.gov	ox.ac.uk	momat.go.jp
1	11	10	10	22	21
2	11	10	10	22	21
3	11	10	10	22	21
4	11	10	10	22	21
5	11	10	10	22	21
6	11	10	10	22	21
7	11	10	10	22	21
8	11	10	10	23	21
9	11	10	10	23	21
10	11	10	10	23	21
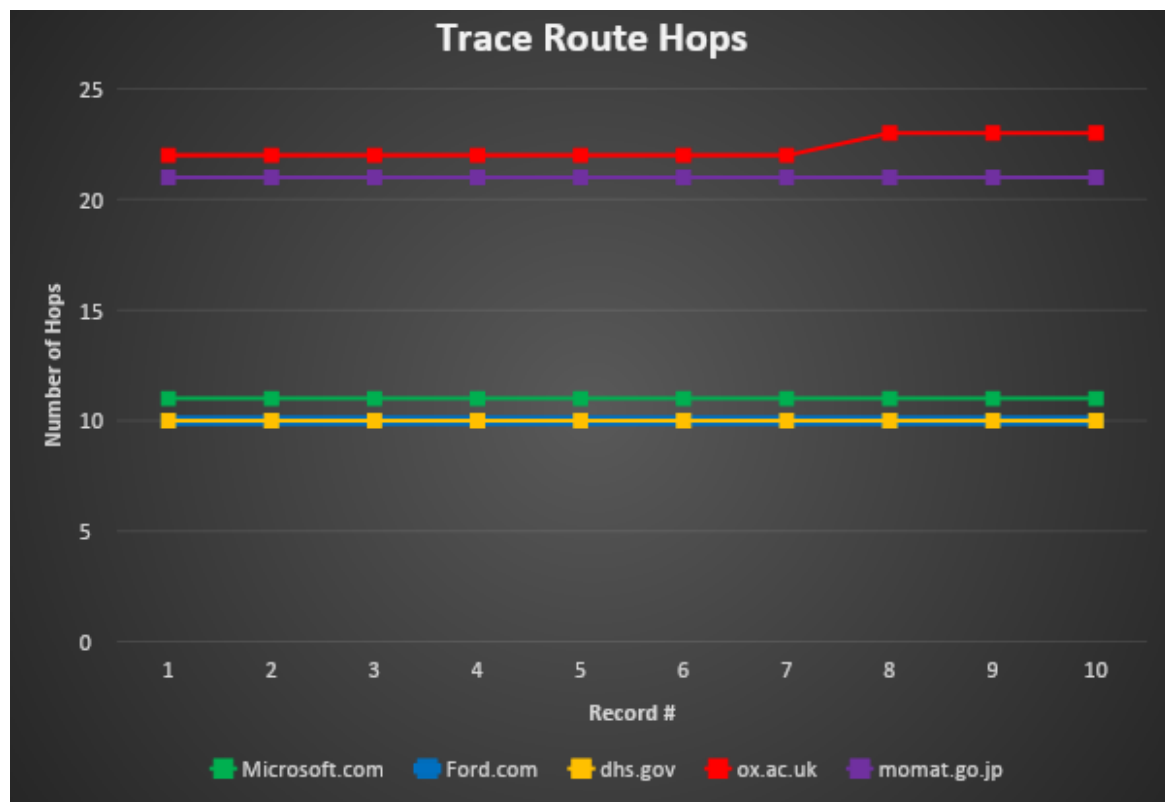
A couple interesting points overall about the number of hops each packets took to reach their destinations are first, it's surprising that it took less hops to reach MOMAT than Oxford. It also took more hops to get to Microsoft than Ford and DHS. When you combine this with our observations from the ping tests, Ford and DHS had more consistent Avg RTTs than Microsoft, and MOMAT had more consistent Avg RTTs than Oxford. There appears to be a correlation between hops and consistent Avg RTT ranges but it is not clear if there is any causation one way or another. The only other interesting point about this data is that Oxford adds a hop during record #8.

Path Analysis

For all 5 destinations, at least the first 6 destinations are always the same. The first two hops are my local network. The 3rd hop is always an address located in Michigan used by the WOW ISP. The 4th, 5th, and 6th hops goes through a WOW ISP child organization in GA, USA. This is where it branches out. For Microsoft, it keeps hopping on the same network in GA until the 9th hop where it hops to Amsterdam where it stays until it finally goes to Cambridge, MA on its 11th and last hop. This appears to be where the website Microsoft.com is actually hosted. The route for Microsoft.com does not change across all tests.

Both Ford and DHS have the exact same path oddly enough. They both have the same first 6 destinations as the rest, except they stay in GA for the 7th and 8th hops. They then hop to CA, USA under the EQUINIX organization. After that they both hop to Cambridge, MA, USA for their 10th hop where they appear to be hosted just like Microsoft.com. So even though I intended to have diversely located websites, all the US websites appear to be hosted in MA. These two paths also do not change across all records.

The path to Oxford is more complicated. It begins with its first 9 hops that it has in common with Microsoft. It then stays in Amsterdam under the RIPE organization for all of its remaining hops, where it appears to be hosted. This path does eventually change on record #7, and 8, however for the 3 hops that change in record #7 and the 4 hops that change in record #8, it just changes IP addresses even though it stays on the RIPE network in Amsterdam.

MOMAT goes through the same first 7 hops as MSFT and Oxford, it stays on the WOW network in GA for one more hop before heading to CO, USA under the Level 3 Communications organization, where it usually times out. The 9th and 10th hops in this path are either timed out, or change between many CO IPs on that same Level 3 Communications network. That is the only real change encountered on this path. For the 11th hop it heads to NY, USA under the IIJ-AMERICA-NET network. It then hops to an Asia pacific network in Brisbane (Asia Pacific Network Information Centre) where it remains hopping between IPs on that network in Brisbane.

<u>Conclusions</u>

My initial reasons for deciding which websites which was based on location was wrong. Despite the company locations, all 3 US websites ended up being hosted in Cambridge, MA rendering any differences in RTT marginal or circumstantial. Ford and MOMAT ended up having the most consistency but I don't necessarily have an answer to why, but I could speculate that it was due to the number of networks that they had to hop through for a packet to arrive.

Lessons Learned

I learned that companies don't tend to host their own websites anymore, at least among the intended diverse lot that I picked. I also learned that there are a very similar first 6-8 hops that my packets always go through whether my packets were headed to Cambridge, Amsterdam, or Brisbane.