# ELT-53107 Computer Networking II: Internet investigation homework

## 1. Introduction

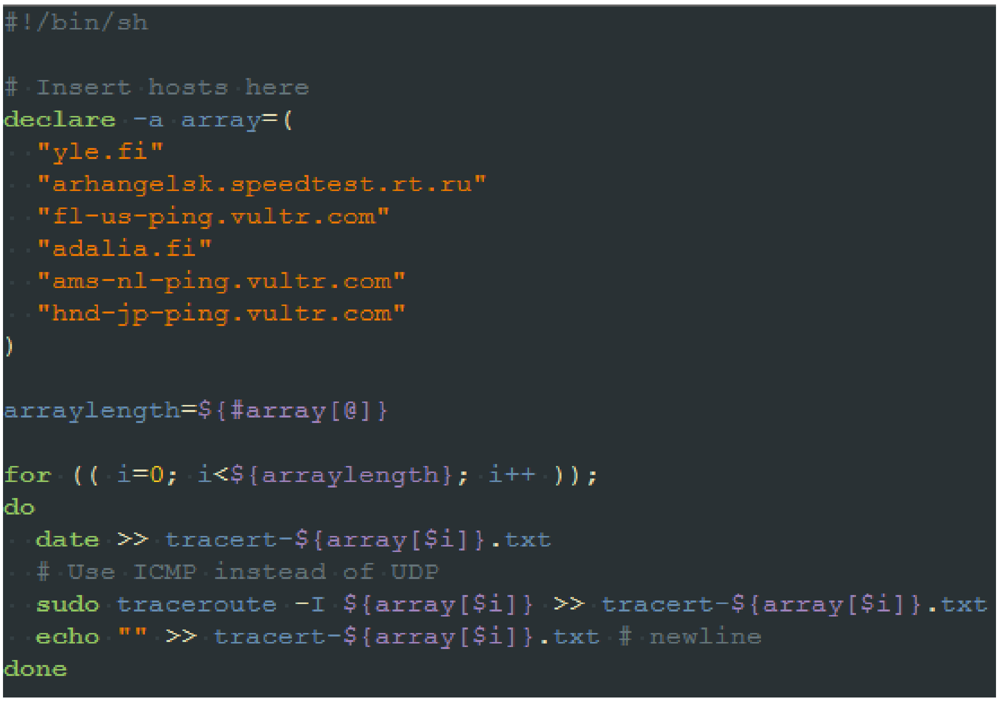
A total of six hosts were chosen for the investigation, based on student number. The hosts are

1. yle.fi
2. adalia.fi
3. arhangelsk.speedtest.rt.ru
4. ams-nl-ping.vultr.com
5. fl-us-ping.vultr.com
6. hnd-jp-ping.vultr.com

1 & 2 are from Finland, 3 & 4 from Europe and 5 & 6 from further away. Number 3 was originally speedtest.arhangelsk.u-disk.ru in hosts.txt, but the host was down. Instead arhangelsk.speedtest.rt.ru was chosen, as it was the closest in relation to the original one. Some of the hosts also had their IP changed from the one written down in the hosts.txt file.

## 2. Measurements and investigation

Measurements were performed on a home Linux machine, using a shell script (Figure 1) which was set to run hourly as a cronjob. Measuring was performed May 4th, 2018.



```
#!/bin/sh

# Insert hosts here
declare -a array=(
  "yle.fi"
  "arhangelsk.speedtest.rt.ru"
  "fl-us-ping.vultr.com"
  "adalia.fi"
  "ams-nl-ping.vultr.com"
  "hnd-jp-ping.vultr.com"
)

arraylength=${#array[@]}

for (( i=0; i<${arraylength}; i++ ));
do
  date >> tracert-${array[$i]}.txt
  # Use ICMP instead of UDP
  sudo traceroute -I ${array[$i]} >> tracert-${array[$i]}.txt
  echo "" >> tracert-${array[$i]}.txt # newline
done
```

***Figure 1.*** *Source for the shell script*

As it can be seen, ICMP was used instead of UDP for pinging the hosts.

## 2.1 yle.fi

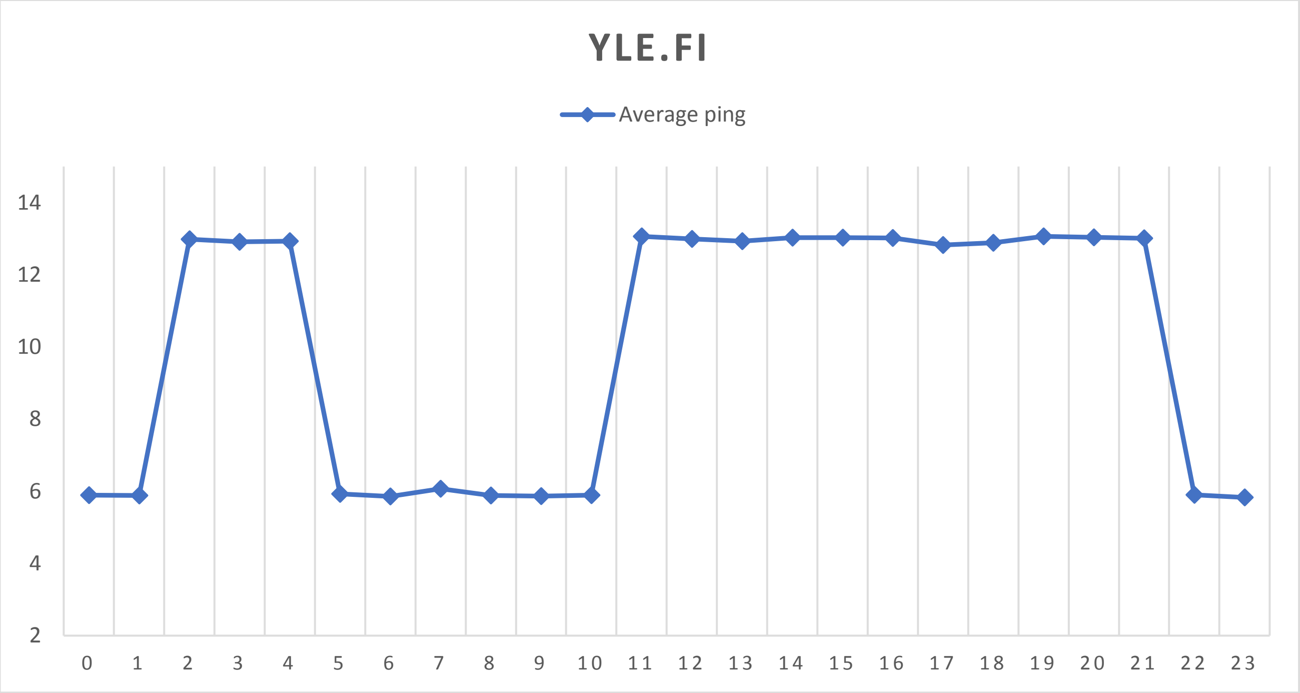


***Figure 2.*** *Average ping vs time of day for yle.fi*

Total variance of the ping is 12,72 ms². It's worth noting that the host has two very different pings, which are 6 and 13 ms. While there is a lot of variance in ping, it is still hard to determine the peak hour from the graph, as the different pings are very flat. A look in the traceroute log explains the two very different pings. Yle.fi is using Cloudfront, and the host is constantly resolving to different IP addresses. Looks like the addresses 13.33.244.x have low ping and 13.33.76.x high ping. The route is also changing constantly, and hop count varies between 8 and 13. Also, the route to 13.33.76.x seems to spend more time in ISP's network: there are twice the amount of *.telia.net hosts, in which the delay is introduced.

Looks like the packets won't leave Tampere at all – all the Cloudfront-servers are located here in Tampere. The map would look rather silly, so I won't include it here.

## 2.2 adalia.fi

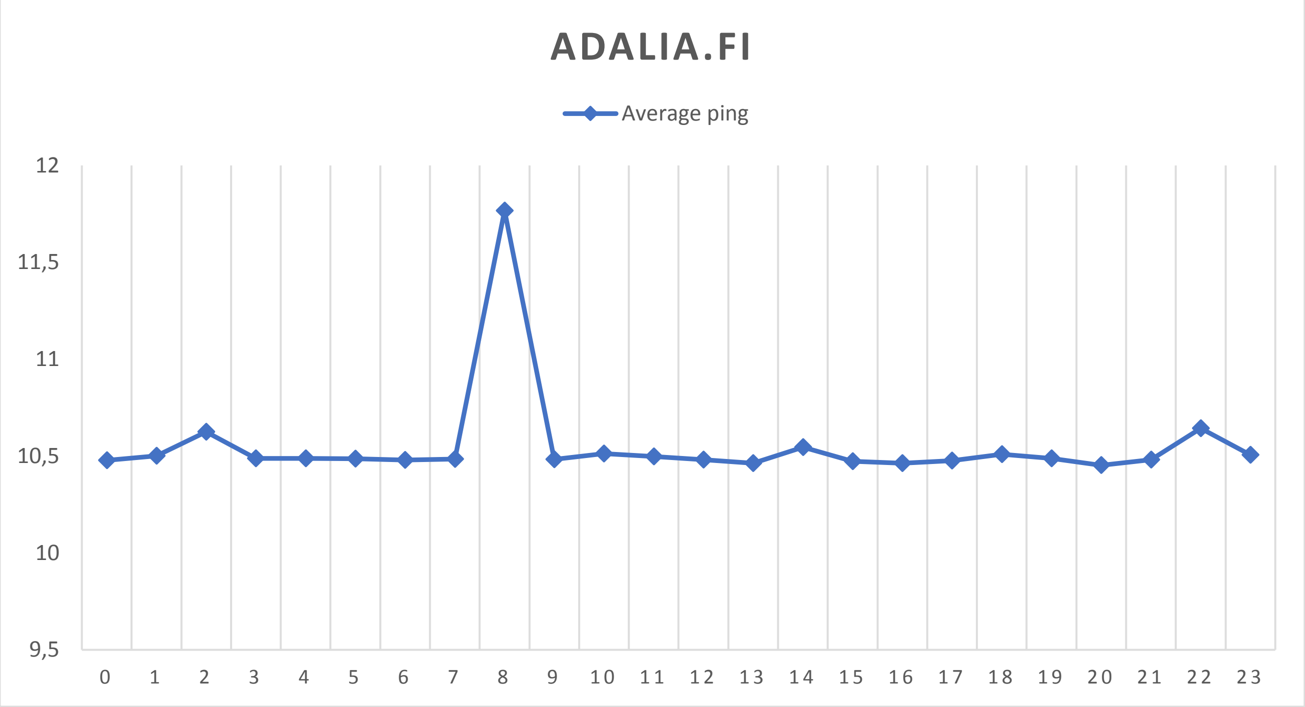


***Figure 3.*** *Average ping vs time of day for adalia.fi*

Total variance of the ping is 0,069 $ms^2$. The peak hour seems to be at 8:00 by looking at the spike, and there are small spikes at 2:00 and 22:00 as well. Variance is still rather low here, and it looks like the host is always resolving to IP 109.204.224.41. Hop count (11) and the route is the same in all performed traceroutes. There is not much going on in here, based on the logs.

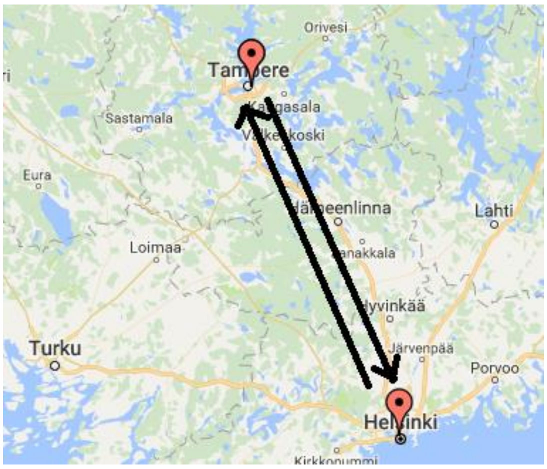


***Figure 4.*** *Route to adalia.fi*

The route to adalia.fi is from Tampere to Helsinki and then back to Tampere, as shown in Figure 4.

## 2.3 arhangelsk.speedtest.rt.ru

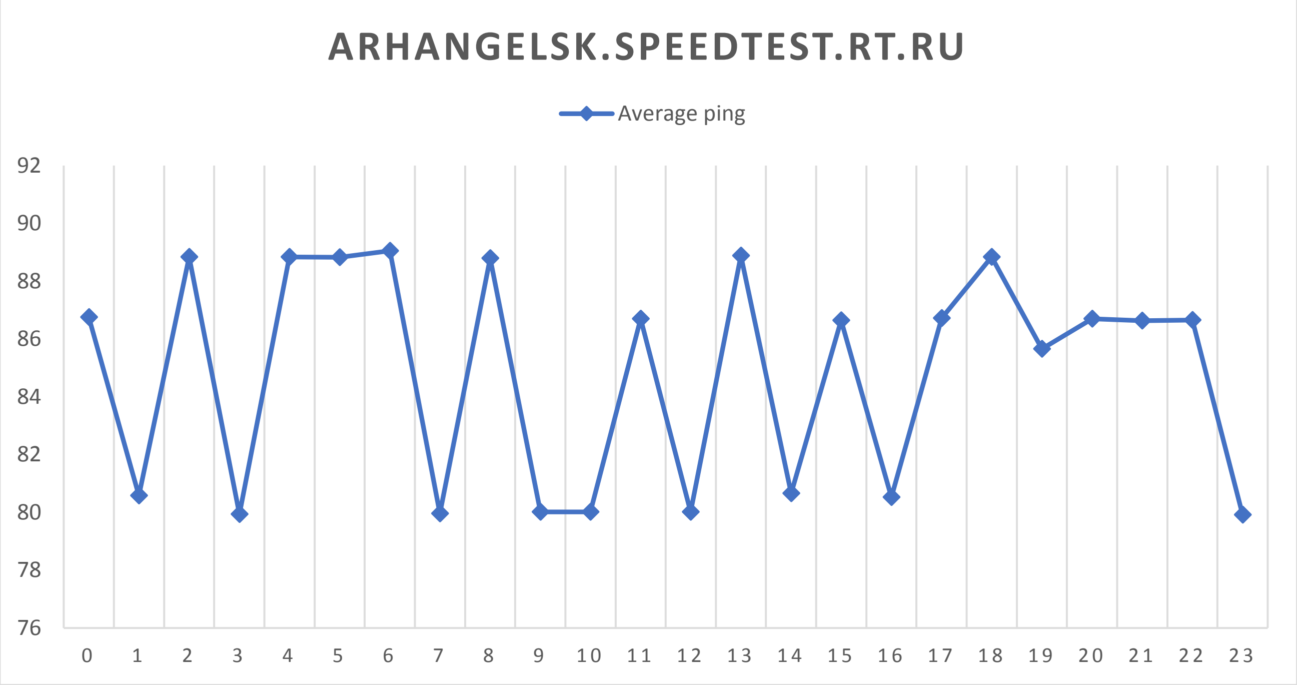


***Figure 5.*** *Average ping vs time of day for arhangelsk.speedtest.rt.ru*

Total variance of the ping is 14,53 ms², which is high. Ping is bouncing between 80 and 90, and the peak hours seem to be between 17 and 22 (hard to name a specific hour), because the ping doesn't go down during the time at all. Traceroute logs show that the next hop to the last one is alternating between two addresses during the investigation. When the traffic is routed through 213.59.211.109, the ping is higher, and during 87.226.183.75, the ping is lower. Hop delay to 87.226.183.75 is stable 66 ms but ping to 213.59.211.109 is alternating in 90 - 100 ms.

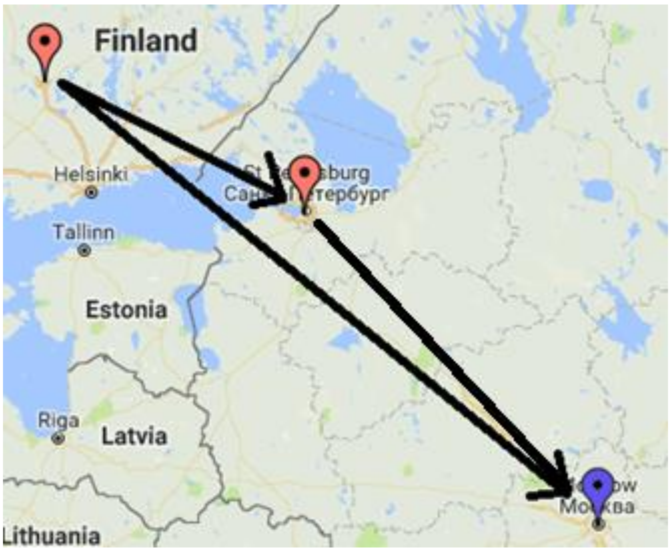


***Figure 6.*** *Routes to arhangelsk.speedtest.rt.ru*

Route is from Tampere to Moscow (in some cases through St. Petersburg, which was slower, like showed earlier), as shown in Figure 6.

# 2.4 ams-nl-ping.vultr.com

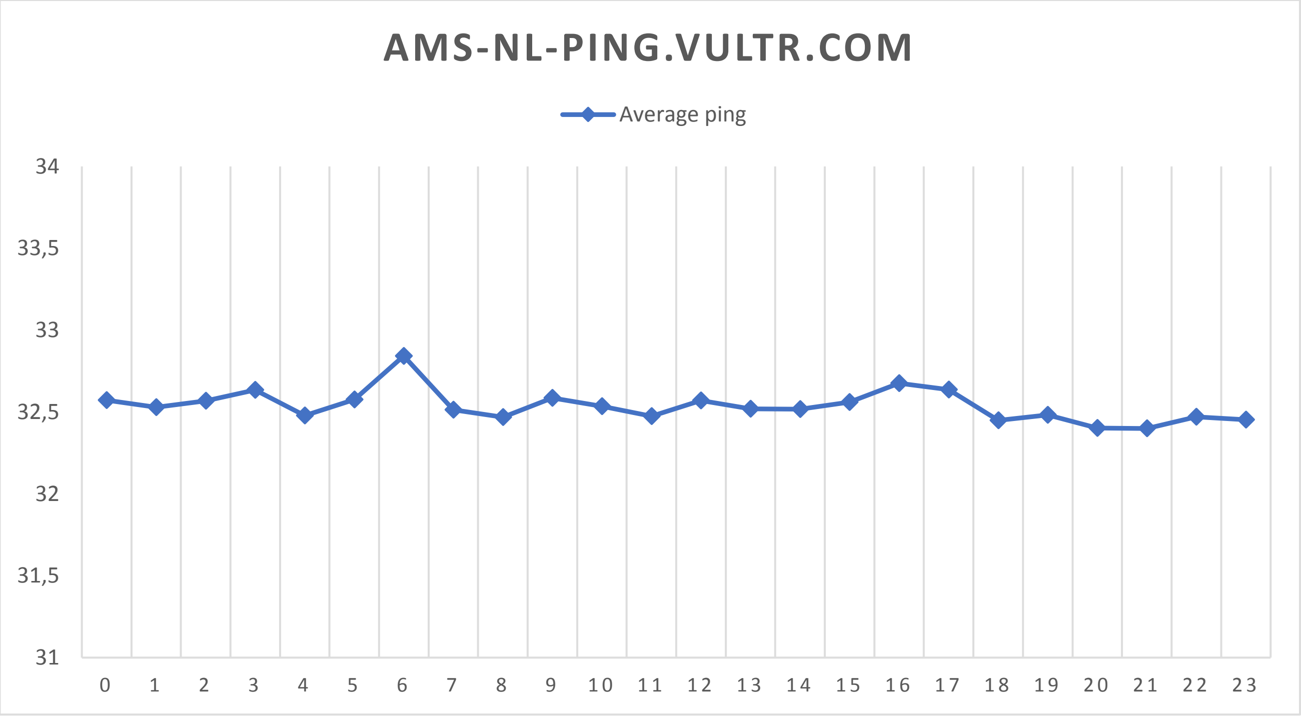


***Figure 7.*** *Average ping vs time of day for ams-nl-ping.vultr.com*

Total variance of the ping is 0,0092 ms². Busiest hour based on the picture is at 6:00. There is not much going on in here, as the route is always the same with 10 hops, and the host resolves to the same IP (108.61.198.102) in all traceroutes. Most of the delay is introduced in ISP side, which is stable 30 ms, and the variance is just normal small variance, and nothing special can be seen from the logs.

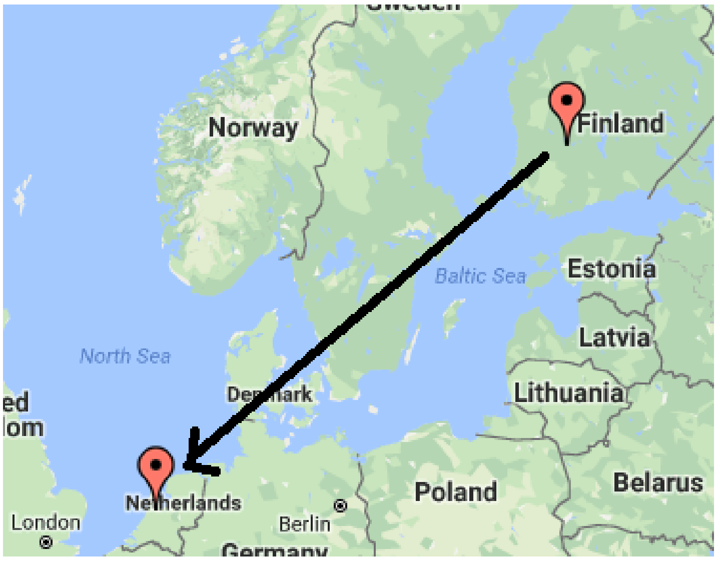


***Figure 8.*** *Route to ams-nl-ping.vultr.com*

Route is from Tampere to Amsterdam, as shown in Figure 8. There may also be an unspecified hop somewhere else in Europe (IP 62.115.58.194), but its location cannot be pinpointed.

## 2.5 fl-us-ping.vultr.com

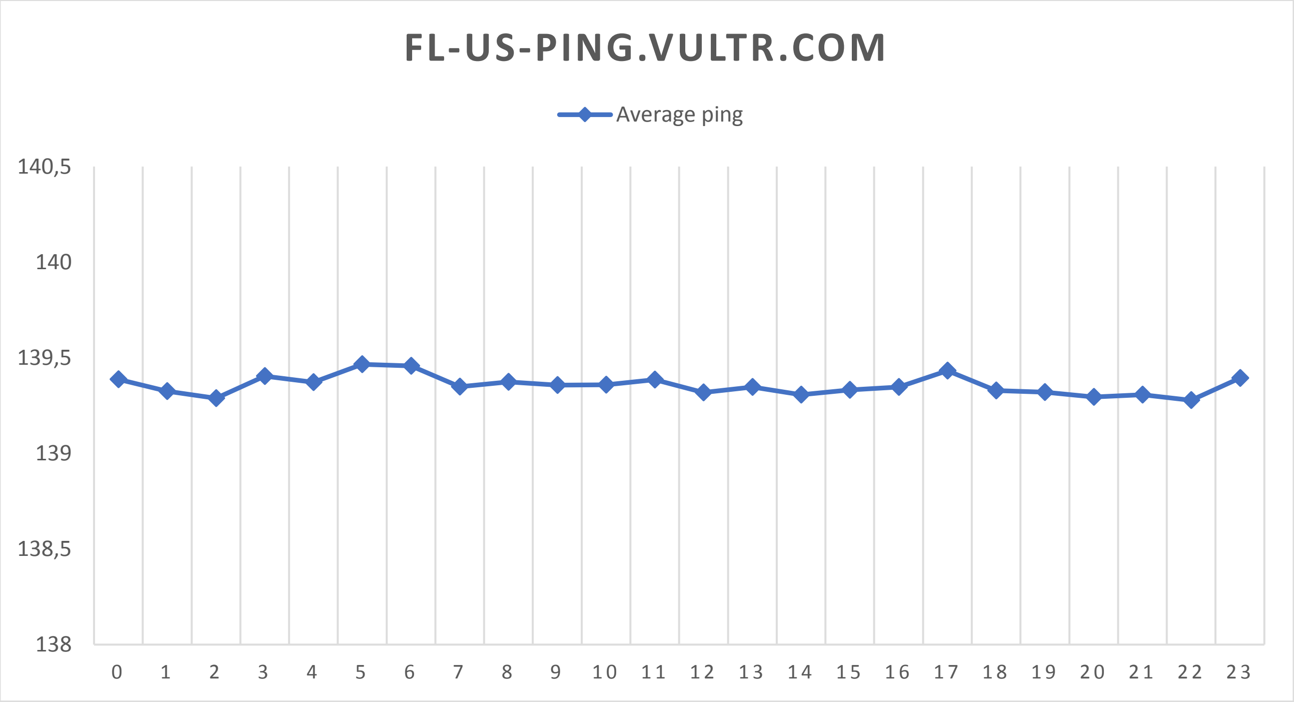


***Figure 9.*** *Average ping vs time of day for fl-us-ping.vultr.com*

Total variance of the ping is 0,0026 ms². This measurement has the lowest variance, even though the ping is somewhat high. It is impossible to name a busy hour, because the pings are so stable. Most of the delay is in ISP side, like in the previous host. Hop count is constantly 12 and the host resolves to 104.156.244.232 all time. There is not much going on in here either.

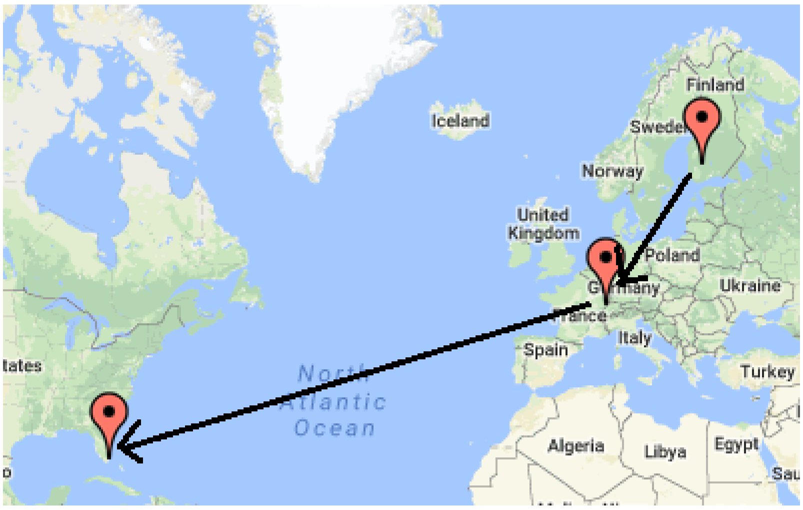


***Figure 10.*** *Route to ams-nl-ping.vultr.com*

Route is from Tampere to Miami, US, routed through Europe (unspecified), as shown in Figure 10.

# 2.6 hnd-jp-ping.vultr.com

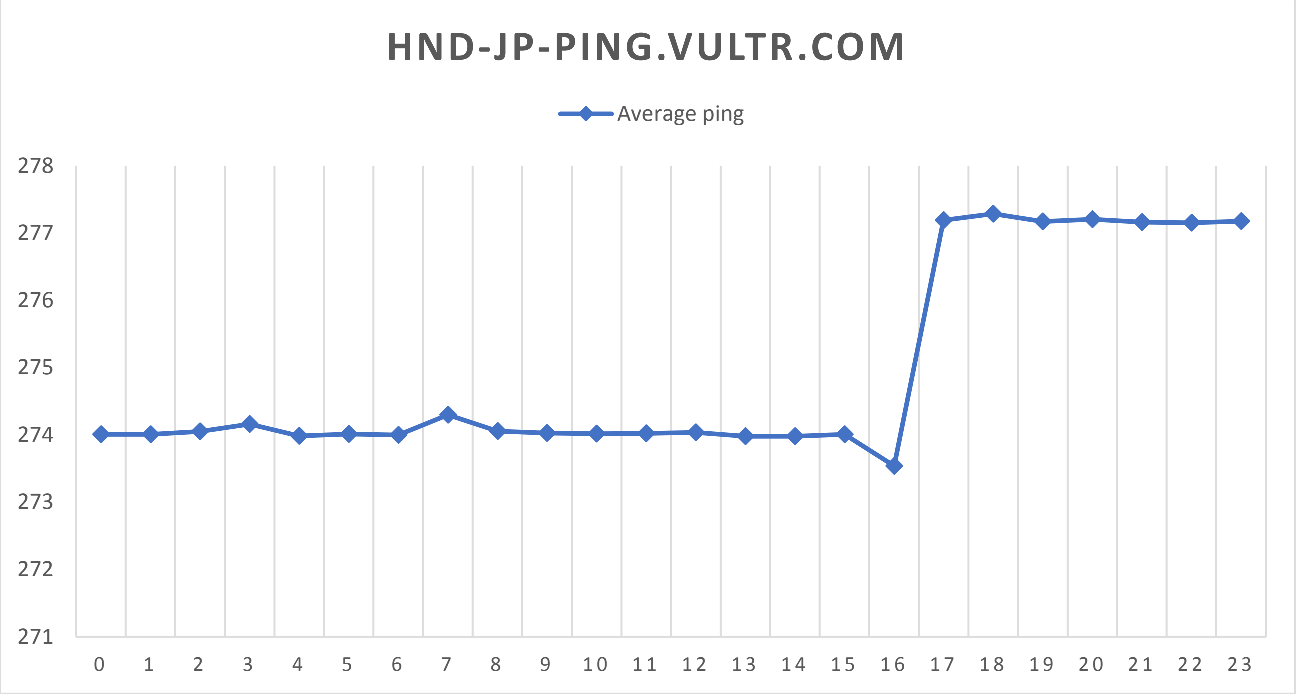


***Figure 11.*** *Average ping vs time of day for hnd-jp-ping.vultr.com*

Total variance of the ping is 2,20 ms². This measurement has the highest ping overall and peak hours are during 17:00 – 23:00.  On the contrary to the two previous hosts, there is not much delay introduced in the home ISP side. There are two distinct pings, which are 274 and 277, even while based on the logs the route (18 hops) and host is always the same. It looks like the delay is in the server backbone based in Japan.

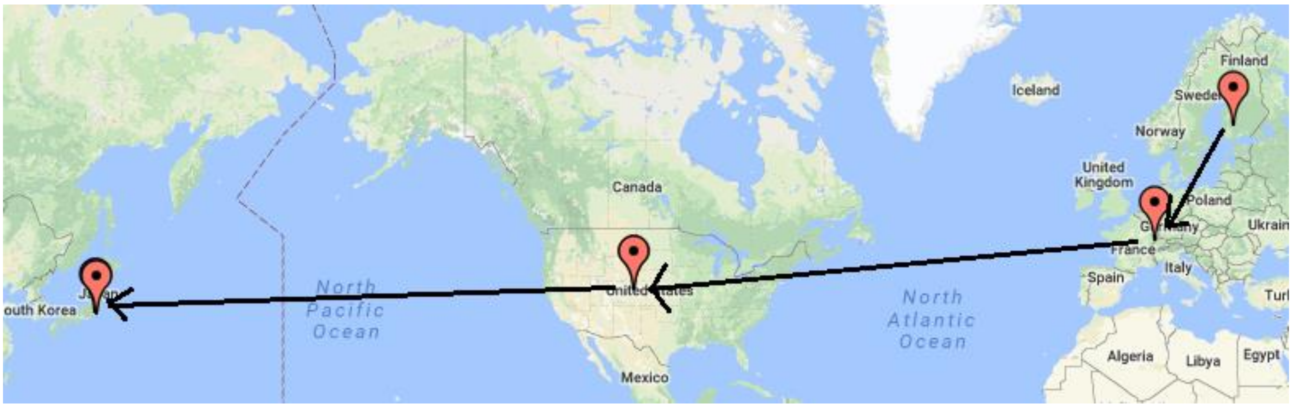


***Figure 12.*** *Route to hnd-jp-ping.vultr.com*

Route is from Tampere to Europe to United States, and then to Japan, as shown in Figure 10. By looking at the map, it seems that the variance in latency is introduced in US rather than in the server backbone in Japan – a correction to the earlier comment.

# 3. Follow-up questions

For all the measurements, major delay sources were inside individual AS’s. Most often the AS was local ISP of the home network. Packets spend most of their time inside AS’s and the interconnections between them are usually quite fast. Routing is slow and long transmit distances take time as well, and those are usually performed inside individual AS’s.

The daily delay changes are mostly influenced by network load. For the close-by hosts, the traffic is only routed locally, so the busy hours when the load is high are usually during one time of day. For further hosts, time zones influence daily delays a lot, and the load can be high during multiple parts of the day.

The home internet connection was not under high load during the day of measurement, so it should have only little impact on the results. The latency from home to ISP’s network was also low in all traceroutes, so it indicates that the network wasn’t overloaded during the tests. But, of course, the internet connection still has an impact on the measurements – it is also a consumer network after all.