CS 349: Networks Lab Spring 2018

Assignment 1 — 25 Jan, 2018

Prof. T. Venkatesh *Roll: 150123051*

Q1 PING command

a) -c *count* (Eg. ping -c 5 google.com)

b) -i *interval* Wait 5 seconds (Eg. ping -i 5 IP)

c) -f (minimal interval allowed for user is 200ms, Super users can send hundred or more packets per second using -f option)

d) -s *packetsize* When we set the packet size to 64 bytes, the total packet size will be 92 bytes (Ping bytes Sent = Ping Packet Size + Ping Header Packet Size (28 bytes))

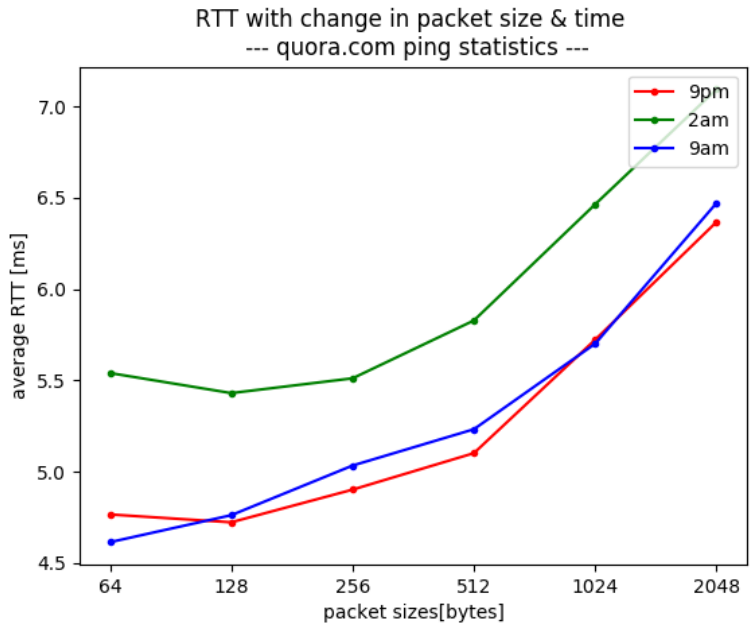
Q2 PING Statistics

Average RTT [ms] for each host at three different hours of the day.

Host	9pm	2am	9am
quora.com	4.765	5.540	4.613
www.nus.edu.sg	240.050	238.990	235.885
iitg.ac.in	283.994	289.329	288.040
facebook.com	13.142	12.647	12.587
flipkart.com	230.397	242.818	243.963
google.com	6.237	4.503	4.205
khanacademy.org	13.874	11.569	15.739

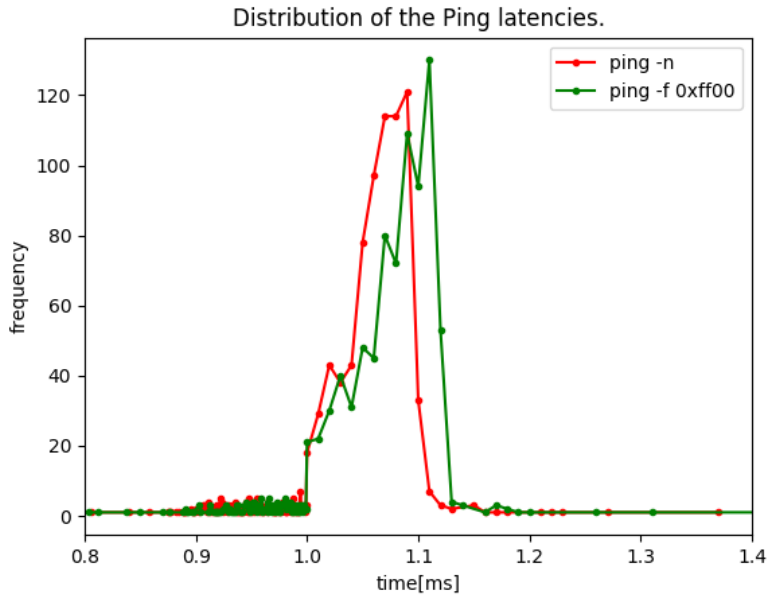
Here for all the above hosts there was `0%` packet loss. Packet loss is typically caused by network congestion.

Observations. Consider IIT G (India) or NUS (Singapore) or Flipkart (India), because of large geographic distance from ping utility (New Jersey) the RTT is more, for Quora (hosted at CA) and Google we observe less RTT. Hence from the above table readings, we observe a **strong correlation** between geographical distance and RTT. The farther the distance the larger the RTT. One of the reason for this may be an increased hop count.



Q3 ping -n & ping -p

		`ping -n 202.141.80.14`	`ping -p ff00 202.141.80.14`
a)	packet loss	`0.001%`	`0.001%`
b)	rtt min/avg/max/mdev	`0.330/1.022/1.374/0.123 ms`	`0.338/1.046/3.132/0.133 ms`
c)			



d) `-n` Numeric output only. No attempt will be made to lookup symbolic names for host addresses. `-p` *pattern* useful for diagnosing data-dependent problems in a network. The average ping latencies for pattern is greater when compared.

Q4 ifconfig & route

$ ifconfig

```
eth0      Link encap:Ethernet  HWaddr 1c:39:47:40:8b:f8
          inet addr:10.11.3.5  Bcast:10.11.63.255  Mask:255.255.192.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Global
          UP LOOPBACK RUNNING  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Here **eth0** - Ethernet & **lo** - loopback are names of active network interfaces running on the system.

- `Link encap:Ethernet` denotes that the interface is an Ethernet related device.
- `HWaddr 1c:39:47:40:8b:f8` is the hardware address or MAC address.
- `inet addr` tells machine IP address. `Bcast` the broadcast address. `Mask` is network mask.
- `UP` this flag indicates that the kernel modules related to Ethernet interface has been loaded.
- `BROADCAST` denotes that Ethernet device supports broadcasting.
- `MULTICAST` indicates that it supports multicasting (Multicast allows a source to send a packet(s) to multiple machines as long as the machines are watching out for that packet).
- `MTU` Maximum Transmission Unit, is the size of each packet received by the Ethenet card.
- `Metric` this decides the priority of the device (lower the value the more leverage it has).
- `RX packets`,`TX packets` total number of packets received and transmitted respectively.
- `collisions` Ideally $0, > 0 \implies$ packets are colliding while traversing the network(congestion).
- `RX Bytes`,`TX Bytes` total amt of data that has passed through Ethernet either way.

$ route

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.11.0.254     255.255.255.255 U     256    0        0 eth0
10.11.0.0       *               255.255.192.0   U     256    0        0 eth0
10.11.3.5       *               255.255.255.255 U     256    0        0 eth0
10.11.63.255    *               255.255.255.255 U     256    0        0 eth0
224.0.0.0       *               240.0.0.0       U     256    0        0 eth0
255.255.255.255 *               255.255.255.255 U     256    0        0 eth0
127.0.0.0       *               255.0.0.0       U     256    0        0 lo
127.0.0.1       *               255.255.255.255 U     256    0        0 lo
127.255.255.255 *               255.255.255.255 U     256    0        0 lo
224.0.0.0       *               240.0.0.0       U     256    0        0 lo
255.255.255.255 *               255.255.255.255 U     256    0        0 lo
```

- `Destination` the destination network/host.
- `Gateway` the gateway address or '$*$' if none set.
- `Genmask` netmask for destination net; `255.255.255.255` for a host destination.
- `Flags` **U** route is up **H** target is a host **G** use gateway ...
- `Metric` 'distance' to the target (usually counted in hops). `Ref` Number of ref to this route.
- `Iface` Interface to which packets for this route will be sent.

We can modify the routing tables by using **add** or **del** options.

Q5 netstat

netstat (Network Statistics) is tool for monitoring network connections both incoming and outgoing as well as viewing routing tables, interface statistics, masquerade connections, and multicast memberships.

netstat -at is used to show all the TCP(Transmission Control Protocol) connections established.

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.11.3.5:48396         202.141.80.24:3128      TIME_WAIT
tcp        0      0 10.11.3.5:48398         202.141.80.24:3128      TIME_WAIT
tcp        0      0 10.11.3.5:48416         202.141.80.24:3128      ESTABLISHED
tcp        0      0 10.11.3.5:48390         202.141.80.24:3128      ESTABLISHED
tcp        0      0 10.11.3.5:48388         202.141.80.24:3128      ESTABLISHED
tcp        0      0 10.11.3.5:48394         202.141.80.24:3128      TIME_WAIT
tcp        0      0 10.11.3.5:48350         202.141.80.24:3128      ESTABLISHED
```

```
tcp        0      0 10.11.3.5:48412         202.141.80.24:3128      ESTABLISHED
tcp        0      0 10.11.3.5:48404         202.141.80.24:3128      ESTABLISHED
tcp        0      0 10.11.3.5:48392         202.141.80.24:3128      TIME_WAIT
tcp        0      0 10.11.3.5:48410         202.141.80.24:3128      ESTABLISHED
tcp        0      0 10.11.3.5:48358         202.141.80.24:3128      TIME_WAIT
tcp        0      0 10.11.3.5:48382         202.141.80.24:3128      ESTABLISHED
tcp        0      0 10.11.3.5:48402         202.141.80.24:3128      ESTABLISHED
tcp        0      0 10.11.3.5:48408         202.141.80.24:3128      TIME_WAIT
tcp        0      0 10.11.3.5:48366         202.141.80.24:3128      ESTABLISHED
tcp        0      0 10.11.3.5:48384         202.141.80.24:3128      TIME_WAIT
tcp        0      0 10.11.3.5:48400         202.141.80.24:3128      ESTABLISHED
tcp        0      0 10.11.3.5:48386         202.141.80.24:3128      ESTABLISHED
tcp        0      0 10.11.3.5:48406         202.141.80.24:3128      ESTABLISHED
tcp6       0      0 [::]:3128               [::]:*                  LISTEN
tcp6       0      0 [::]:http               [::]:*                  LISTEN
```

netstat -r netstat and route command displays Kernel IP routing table.

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
```

Most of the colums are same as route command in Q4, others are

- `MSS` Maximum Segment Size, the size of the largest datagram the kernel will construct for transmission via this route.
- `Window` max amount of data the system will accept in a single burst from a remote host.
- `irtt` stands for 'initial round trip time.'

netstat -i can be used to display network interface status or Kernel Interface table.

```
Kernel Interface table
Iface   MTU Met   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0       1500 0          0      0      0 0             0      0      0      0 BMRU
lo         1500 0          0      0      0 0             0      0      0      0 LRU
```

The **loopback** is a 'virtual' network driver that exists on all systems that support TCP/IP and uses to communicate with itself. The loopback interface exists mainly for the purpose of testing, diagnostics and troubleshooting, and to connect to servers running on the local machine.

Like other network adapters, the loopback device shows up in the output of ifconfig with name **lo**.

For IPv4, the loopback interface is assigned all the IPs in the 127.0.0.0/8 address block. That is, 127.0.0.1 through 127.255.255.254 all represent your computer. For most purposes, though, it is only necessary to use one IP address, and that is 127.0.0.1. This IP has the hostname of localhost mapped to it.

If pinging 127.0.0.1 (`ping localhost`) does not work, then you should simply not bother with a physical interface because it will surely not work.

Q6 traceroute

1. Hop Count (TraceRoute from Network-Tools.com to *host*)

Host	4pm	10pm	2am	11am
quora.com	4	4	4	4
www.nus.edu.sg	19	19	19	19
iitg.ac.in	17	17	17	17
facebook.com	6	6	6	6
flipkart.com	15	15	15	15
google.com	5	5	5	5
khanacademy.org	17	19	19	17

2. Traceroute for Khanacademy.org changed at different times of the day. It is influenced by **load balancing** and you may have every time a different path. For remaning, the paths didn't change during any of the hours.

3. Traceroute maps out the pathways by sending ICMP ping packets. It includes a time limit value with the packet, called a Time to Live (TTL) or hop limit. It appears when routers do not respond to probes or when routers have a limit for ICMP responses.TTL value of an ICMP packet to force a timeout .

4. Yes, It may be because at destination ping is getting blocked or discarded, while traceroute uses an error message form a node/hop along the path to determine the route.

Q7 ARP - Address Resolution Protocol

ARP table of our system can be displayed by **arp** command, which outputs

- `Address` tells IP address.
- `HWtype` tells Hardware Types (ether for Ethernet).
- `HWaddress` is the hardware address or MAC address.
- `Flags` indicate if the mac address has been learned, manually set, published or is incomplete.
- `Iface` Iface stands for Interface (eth0 for Ethernet Interface).

`arp -d address` will **delete** a ARP table entry. Root or netadmin privilege is required to do this. The entry is found by IP address. To delete entries use `arp [-v] -d hostname [hostname...]`. If a hostname is given, it will be resolved before looking up the entry in the ARP table. Invoking arp using the -d switch deletes all ARP entries relating to the given host.For example

```
$ sudo arp -d 10.11.3.5
```

`arp -s address hw_addr` is used to **add** /set up a new table entry. For example

```
$ sudo arp -s 192.168.42.180 02:03:56:04:33:65
```

```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.42.182           ether   02:03:56:04:33:65   CM                    usb0
192.168.42.129           ether   1e:58:79:0a:c4:2c   C                     usb0
192.168.42.180           ether   02:03:56:04:33:65   CM                    usb0
```

The default ARP cache timeout is 60 seconds (until the entry is removed) however we can set it.

Trail-and-error method: Let F denote the time entries stay cached in the ARP table. We have $F : (0, \infty) \to \{true, false\}$ (whether entry is present in table or not) which has the property that if $F(i) = false$ (time-out value, false $\implies$ entry not present in ARP table), then $F(j) = false \, \forall \, j > i$. Thus we can use binary search / bisection method to discover the timeout value.

If two IP addresses map to the same Ethernet address in ARP table and if we try to ping one of them then all packets are lost. The packets are redirected to same IP.

ARP only works between devices in the same IP subnet. If **hosts belongs to a subnet** (machines plugged into the same set of hubs and switches) it can directly reach through its network interface(s); if it does, then devices uses ARP to map IP address to physical Ethernet address, then sends an Ethernet frame to that address.

Q8 Local network analysis using nmap on Subnet Range (`10.11.3.0/26`)