Computer Networks Lab

Assignment No. 1

Submitted By:

Ashish Kumar Poddar

Roll No.: 150123049

Mathematics and Computing

IIT Guwahati

Date - 20^{th} January, 2018

Question 1

Unix has a variety of commands that enable us to specify the behaviour of our `ECHO_REQUEST`s in every way possible. Some of the ones required are listed as below.

- `ping <IP Address> -c N` - This UNIX command is used to specify the number of echo requests to send with ping. Here, N is the number of requests to send.
- `ping <IP Address> -i T` - This command enables us to change the time interval between subsequent echo requests to T seconds.
- `ping -f <IP Address>` - This command floods the receiver as it sends echo requests continually without waiting for a reply. Normal users are not allowed to use this command. Only superusers can use this.
- `ping -s S <IP Address>` - This command changes the packet size from the standard 64 bits to (S+8) bits. If PacketSize is set to 64 bits, the total packet size becomes 72 bits.

Question 2

For the experiment, I have used the hosts of 5 institutes worldwide. They are listed along with their RTTs -

	`iitg.ac.in`	`berkeley.edu`	`stanford.edu`	`web.mit.edu`	`yale.edu`
01:00 AM	379.078	69.878	66.360	13.741	13.307
06:00 PM	280.512	69.427	66.718	5.660	12.940
12:00 PM	268.480	69.649	66.367	20.058	12.983

As is evident, there is a strong relationsip between the geographical distance and the RTTs.

The graph implies that the RTT varies almost linearly with the size of the packets transmitted.

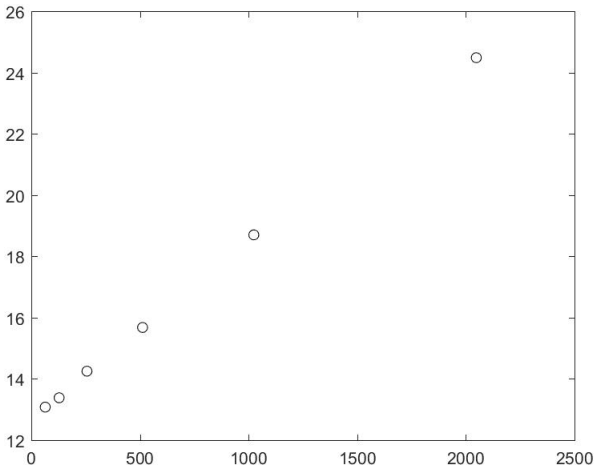

Figure 1: RTT v/s PacketSize Graph
This graph resulted from pinging the `yale.edu` site.

It was observed that the RTTs for some servers were higher during certain times of the day while for some others were higher for some other times of the day. This may be attributed to the fact that the server may be handling an increased number of requests at those times of the day.

Question 3

We selected the address `202.141.80.14` for our task in this question. Here are the answers as required.

The packet loss rate for command one was 0% while that for the second command was 3%.

The following table provides the values for the two commands as required.

Maximum	Minimum	Mean	Median
2.57	0.161	0.303	0.282
0.648	0.179	0.299	0.288

The -n command directs the system to use numeric output only and it does not try to look up symbolic names for host addresses. `-p ff00` fills the packet with byte stuffing ff00. The -p command can specify up to 16 pad bytes per packet we send. It is useful for diagnosting data dependent problems.

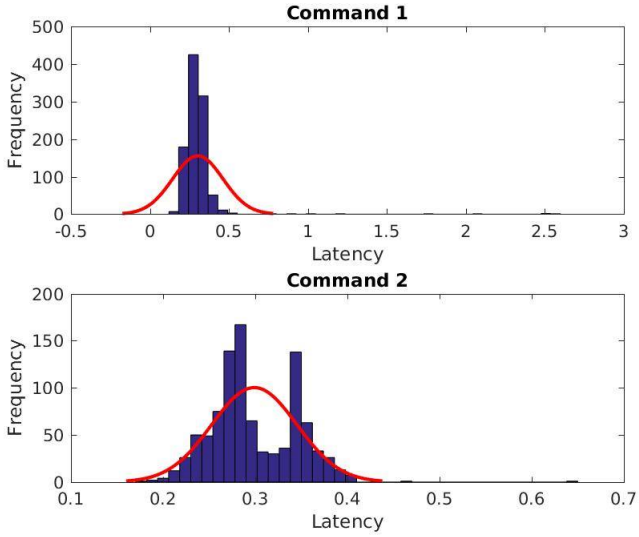

Figure 2: Question 3

Question 4

The `ifconfig` command shows the details of the network interfaces that are up and running in a computer. The `Link encap` show the type of interface of a network. The `HWaddr` shows the MAC address of the computer. The `inet addr` is the IP and the `Bcast` denotes the broadcast address. The `Mask` is the network Mask. `UP` indicates the required kernel modules have been loaded while `BROADCAST` denotes that the device supports broadcasting. `RUNNING` means the interface is ready to accept and `MULTICAST` means that multicasting is allowed. The `MTU` shows the Maximum Transmission Unit i.e the size of the received packets. `Metric` shows the priority of the device.

`RX Packets` and `TX Packets` show the total number of packets received and transmitted respectively. `collisions` show a positive value only if there is the packets are colliding while traversing the network. This is a sign of network congestion. `txqueuelen` denotes the length of the transmit queue of the device. `RX bytes` and `TX bytes` show the amount of data that has been received and transmitted respectively. `Interrupt` specifies the interrupt number the interface is using.

`route` command is used to show or manipulate the IP routing table. It can set up static routes to specific hosts or networks. It has a lot of useful commands. `route -F` operate on Kernel's FIB routing table. `route-C` operates on the Kernel routing cache. `route -v` selects the verbose operation. `route add` and `route del` are used to add and delete a route respectively.

Question 5

Netstat is a command-line network utility tool that can display nework connections for the TCP, routing tables and a number of network interface and network protocol statistics. The `netstat -at` command is used to display the list of established tcp connections.

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:mysql         *:*                     LISTEN
tcp        0      0 Maths56:domain          *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 172.16.68.56:51666      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51756      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51702      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51752      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51736      202.141.80.24:3128      ESTABLISHED
tcp       32      0 172.16.68.56:51758      202.141.80.24:3128      CLOSE_WAIT
tcp        0      0 172.16.68.56:51734      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51644      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51650      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51552      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51686      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51652      202.141.80.24:3128      ESTABLISHED
tcp      390      0 172.16.68.56:51748      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51718      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51502      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51754      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51704      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51660      202.141.80.24:3128      ESTABLISHED
tcp       32      0 172.16.68.56:51750      202.141.80.24:3128      CLOSE_WAIT
tcp        0      0 172.16.68.56:51646      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51624      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51740      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51706      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51746      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51712      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51432      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51664      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51546      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51760      202.141.80.24:3128      TIME_WAIT
tcp        0      0 172.16.68.56:51630      202.141.80.24:3128      ESTABLISHED
tcp        0      0 172.16.68.56:51744      202.141.80.24:3128      ESTABLISHED
tcp6       0      0 [::]:61415              [::]:*                  LISTEN
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
tcp6       0      0 [::]:31415              [::]:*                  LISTEN
```

The `Proto` displays the protocol of the connection while the `Recv-Q` and `Send-Q` list the number of bytes that are currently in a receive and a send buffer respectively. The `local address` lists the IP of the local computer(i.e. my device) and the ports which are connected to the foreign address, i.e. the remote computers to which the connection is present. The `State` column lists the current state of the connection.

The `netstat -r` is similar to the `route` command and lists the Kernel IP routing table. The `Destination` column identifies the destination network. The `Gateway` column identifies the defined gateway for the specified network, to which the packet is to be forwarded. The `Genmask` lists the netmask for the network. The `Iface` column shows the network interface.

Flas lists different symbols having different meaning for the routing of the packets. Metric is the distance to the user counted in hops. `Ref` is the number of references to the route.

`netstat -i` can be used to display the network interface status. My computer has two interfaces - the `Ethernet` interface and the `local loopback`.

The `loopback interface` is used to identify the device. A client requesting data from a network service running on the same machine can use `127.0.0.1` to reach instead of any real IP address that is configured to it and this is guranteed to work regardless of the state of the physical interfaces. This is the main function of the `loopback interface`.

Question 6

The following table lists the hopcounts for the websites at different hours of the day.

	`iitg.ac.in`	`berkeley.edu`	`stanford.edu`	`web.mit.edu`	`yale.edu`
01:00 AM	16	12	11	6	4
08:00 PM	16	12	11	6	4
12:00 PM	16	12	11	4	4

In the above table, we see that while all other websites stick to their routes in all three instances, the `web.mit.edu` site has only 4 hopcounts in one of the instances instead of 6. The two routes have no hop in common here.

The route to the same host changes at different times of the day in some cases. This is because of the fact that the Packets that are being sent don't always follow the same route. There are numerous paths to the same host and the packet can take any path at any given instant of time.

We have not faced any cases where the complete path was not found. But, this situation can occur in various situations. The basic condition when it occurs it is when any intermediate router does not respond to the ping at all. This may occur due to a lot of reasons. The router may be busy or the ping may have hit a firewall.

It is not possible to find the path to hosts which fail to respond to the ping experiment because the traceroute works using ping.

Question 7

The `arp` command shows the full arp table for our machine. Tha arp table maps the `IP address` with the physical or MAC address of the machine. The `Address` and the `HWaddress` thus represent the respective values. The `Iface` and the `HWtype` show the interface and the network protocol types respectively. The `Flag` indicates whether the `HWaddress` has been learned, manually set, published or incomplete.

A normal user is not permitted to add, delete or change entries in the arp table. When we try to do this, we get the `SIOCSARP: Operation not permitted` error. It is possible only with sudo or netadmin privileges.

With sudo privileges, we can run the `sudo arp -d <IP address>` to delete the specific entry by the IP Address. For adding an entry, we need to run the `sudo arp -s <IP Address> HWAddress` to add an entry to the table. Adding two entries has the following effect.

Address	HWtype	HWaddress	Flags	Mask	Iface
10.4.23.4	ether	ff:ff:ff:ff:ff:00	CM		eth0
10.4.2.7	ether	ff:ff:ff:ff:ff:ff	CM		eth0
10.4.0.254	ether	4c:4e:35:97:1e:ef	C		eth0

After Adding 2 two entries into the ARP table

Address	HWtype	HWaddress	Flags	Mask	Iface
10.4.23.4	ether	ff:ff:ff:ff:ff:00	CM		eth0
10.4.2.10	ether	ff:ff:ff:00:11:a7	C		eth0
10.4.2.7	ether	ff:ff:ff:ff:ff:ff	CM		eth0
10.4.0.254	ether	4c:4e:35:97:1e:ef	C		eth0
10.4.2.1	ether	4c:4e:35:21:18:fe	CM		eth0

The `arp` cache entry timeout is 60 seconds. It can be viewed by running the command `cat /proc/sys/net/ipv4/neigh/default/gc_stale_time` in the terminal.

Having two IP addresses with same MAC address is possible in cases when we use a virtual machine like vmware. This does not cause any conflict. Since the Hub or Switch maintains an `IP Address` to `MAC Address` table, each IP has only once `MAC Address` and it is routed accordingly thus avoiding any conflict.

Question 8

Here, we have to query our LAN to discover which hosts are online. We take a range of hosts `10.4.22.1-23` in our local network and use the `nmap -n -sP 10.4.22.1-23` to do so. As is clear, the number of computers which are online are fewer during the day than the night. This may be attributed to the fact that students attend classes during the day apart from not having access to the internet services during the day.

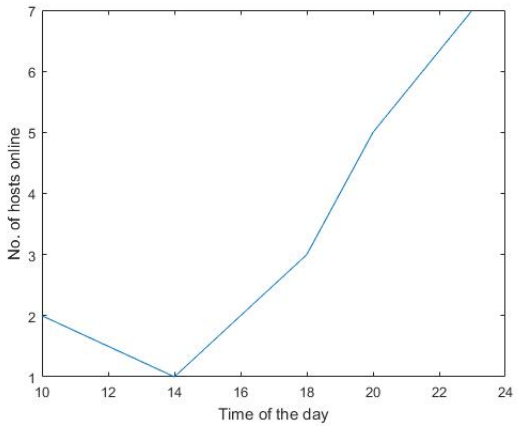

Figure 3: Question 8
No. of Hosts online v/s Time of the day