CS 342: Computer Networks Lab- Assignment -1

Sahil Kumar Gupta (200123081)

Q1

a) The option required to specify the number of echo requests to send with *ping* command is **-c**.
b) The interval between two successive ping ECHO_REQUESTs can be set using **-i** option. However, normal users can't set the value less than 2 seconds.
c) The respective command for the asked questions is **-I** option. The limit for sending such ECHO_REQUESTs by normal users is 3.=
d) It can be done using the **-s** option. The actual packet size will be slightly larger due to the addition of ICMP Header Data (8 bytes). Hence, total packet size for 32 bytes would be 40 (32 +8) bytes.

Q2

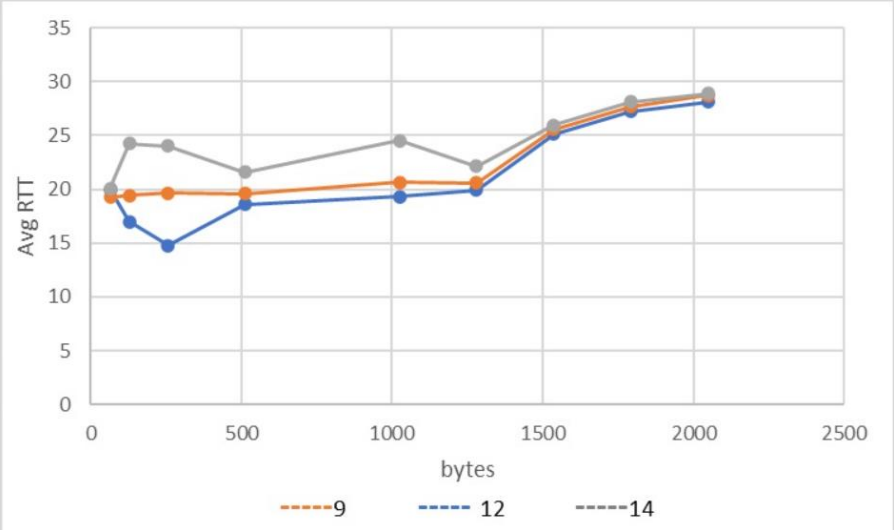
Destination Source Address	IP Address	Geographic Location	Avg RTT1 (ms)	Avg RTT2 (ms)	Avg RTT3 (ms)	Total Avg RTT (ms)	Distance in km
amazon.com	176.32.103.205	Viriginia - USA	19.963	19.285	20.124	19.791	12869
sprinklr.com	13.249.120.64	Georgia-USA	35.854	36.539	37.128	36.507	13501
codeforces.com	213.248.110.126	Sankt-Peterburg	116.696	116.535	117.236	116.822	5931
cricbuzz.com	35.200.167.142	Mumbai-India	251.995	255.564	264.199	257.252	2731
youtube.com	74.125.136.91	California-USA	34.195	34.170	35.001	34.456	12292
interviewbit.com	13.226.100.104	Georgia-USA	35.115	37.232	36.141	36.163	13501

The above table is created by taking data at 3 different times having packet size = 64 bytes.

For me there was no case in which packet loss was greater than 0%. But in general, due to network traffic and congestion, packet loss might be higher than 0%. The originating IP address that allows access content might be limited. Due to firewall blockage, certain packets may not be able to reach their destination in a timely manner, resulting in packet loss. There could occasionally be a complete packet loss.

In general, there exists **weak** positive correlation between distance and Round-Trip Time (RTT). But for my data, this answer is varying as it can be seen that cricbuzz.com is taking much more time even its distance is less than amazon.com but also amazon.com is taking lesser time than sprinklr.com which goes well with positive correlation. Hence, we can say that it depends on more factors.
Reasons of weak positive correlation can be given as:
Increased number of hops and increased propagation delay. There may be a delay at each router, thus if packets have to travel further and via more routers, the RTT will be greater. It is a weak relationship since it depends on so many other things, like network traffic and server capabilities.

Size (Bytes)	64	128	256	512	1024	1280	1536	1792	2048
Avg RTT 1 (ms)	19.963	17.095	14.789	18.595	19.306	19.924	25.162	27.224	28.147
Avg RTT 2 (ms)	19.285	19.454	19.64	19.61	20.63	20.606	25.554	27.668	28.756
Avg RTT 3 (ms)	20.124	24.232	24.005	21.607	24.525	22.122	25.98	28.11	28.887



Graph – Average RTT time vs Packet Size
(data taken at 9am, 12pm, 2pm)

It can be clearly seen that the average RTT time is **increasing** as the packet size is increases. But after 1280 bytes there is sudden jump. This is because Maximum Transmission Unit (MTU) by default is 1500 bytes. This means that only 1 frame is sent for packets less than 1500 bytes but for more than 1500 bytes there are 2 frames which is resulting in sudden increase of RTT time after 1500 bytes.
Variation of RTT time with respect to time can be understood as it depends on different working hours of different countries which implies that at different time the congestion in network is different.

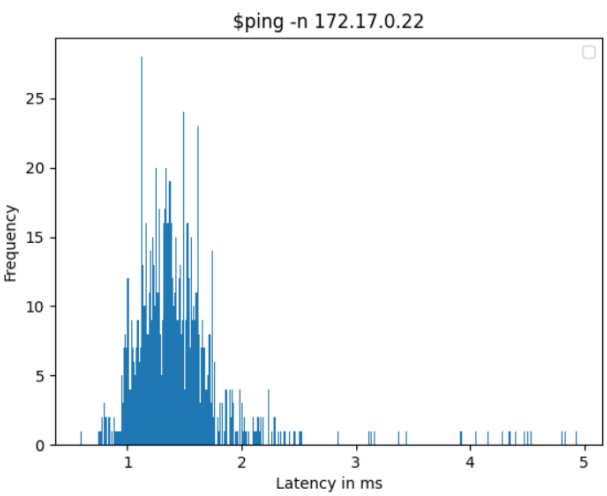
Q3

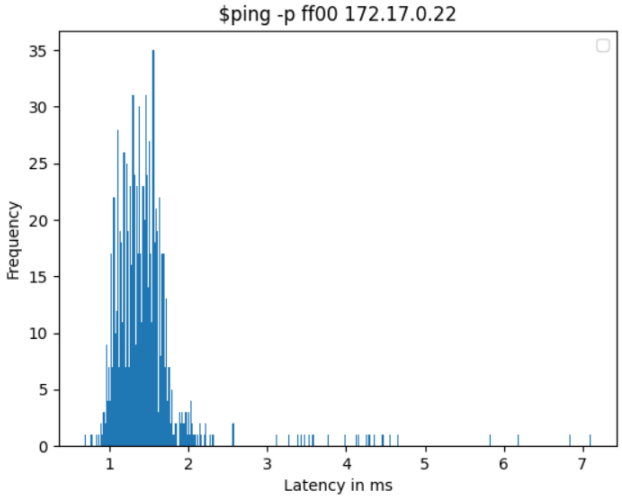
a) b) c) I chose IP Address as **172.17.0.22**

Command	Packets Sent	Packets Received	Packet Loss Rate	Min Latency	Max Latency	Mean Latency	Median Latency
$ ping -n 172.17.0.22	1000	912	8.8%	0.678	4.935	1.469	1.4
$ ping -p -ff00 172.17.0.22	1000	904	9.6%	0.586	7.107	1.449	1.38

d) When the -p flag is used, there is a greater package loss than when the -n flag is used. This is because no attempt is made to seek for symbolic names for host addresses when the -n option is used, so that no DNS resolution occurs. The -p option, however, results in decreased mean and median latency. It adds 16 bytes, or size ff00, to the packet.

Below are the histograms for the two cases -





Q4

a) **ifconfig** is used to display the status of currently active interfaces. My machine has **enp0s3 and lo** as

```
sahil@sahil-VirtualBox:~/xv6-public$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::ff59:202e:b752:f751  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:3e:e7:09  txqueuelen 1000  (Ethernet)
        RX packets 111136  bytes 127205626 (127.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 75177  bytes 12049622 (12.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 10588  bytes 1984969 (1.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10588  bytes 1984969 (1.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

as the active interfaces on the system.
enp0s3 is the first Ethernet interface.
lo is the loopback interface which the system uses to communicate with itself.
inet, inet6: IPv4 and IPv6 addresses assigned to the interface respectively.

broadcast: It is used to denote the broadcast address associated with the respective interface.
RUNNING: It tells that the interface is ready to accept data.
MULTICAST: Tells that the Ethernet interface supports multicasting.
UP: A flag to indicate the kernel modules which are related to Ethernet and have been loaded.
mtu 1500: Size of the maximum transmission unit received by the Ethernet card.
txqueuelen: Length of the transmit queue of the NIC.
RX, TX bytes: Indicates the total amount of data that has passed through the interface either way.
RX packets: The total number of packets received. Overruns: The number of received packets that have data overruns. Dropped: The number of packets lost due to reception failures. Frame: The number of received packets that encountered frame faults. Errors: The number of corrupted packets received.
TX packets: Total number of sent packets. Overruns: The number of sent packets that encountered data overruns. Dropped: The number of sent packets that were lost due to transmission problems. Carrier: The number of received packets that encountered carrier failure. Collisions: The number of packets that collide while travelling the network as a result of network congestion. Errors: The number of packets that had a transmission error.

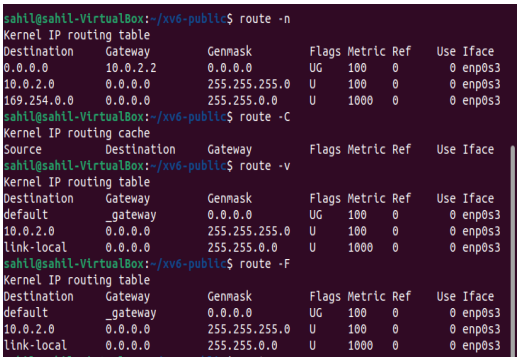
b) Four options for ifconfig:

- **-v:** for verbose mode. It is used to display additional information for each network interface.
- **-a:** It displays information in both active and inactive mode for all network interfaces
- **UP** and **DOWN** flag is responsible for activation and deactivation of interface
- **metric N:** The interface matrix set by it used by the interface to make routing decision.

c) The **destination** column tells us about the IP of the destination network. 0.0.0.0 means that our destination is locally connected on the interface and no more hops are needed to get it. The **Genmask** column shows the netmask on the network. 0.0.0.0 means that there is no netmask. Some of **the Flags are: U(route is up), G(use gateway), H(target is host). Metric** is the distance to the target counted in hops. **Ref** is the number of references to this route. **Irtt** stands for the initial round trip time. The **Iface** column shows the name of the network interface.

d) Four options of the route command:

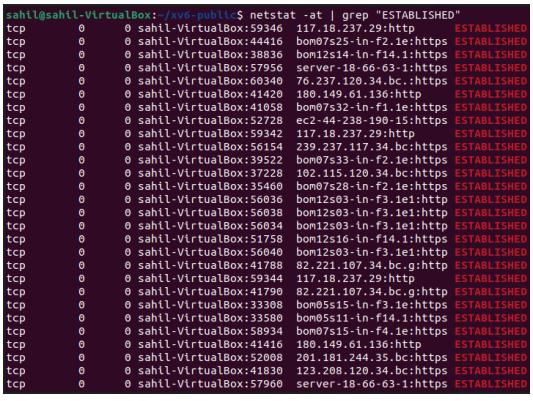
- **-n:** Displays host and network names numerically when reporting results of a flush or of any action in verbose mode.
- **-C:** is used to list the kernel's routing cache information.
- **-v:** Specifies verbose mode and prints additional details.
- **-f:** Purges all entries in the routing table that are not associated with network interfaces.

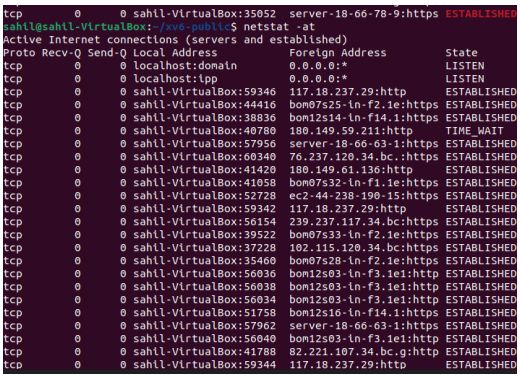


Q5

a) A networking utility for configuration and troubleshooting that may also be used to keep track of network connections is the **network statistics (netstat)** command. This command is frequently used with routing tables, port listening, incoming connections, and use statistics. It shows data for Ethernet, IPv4 and IPv6, IPv4 and IPv6 ports, IP routing table, active TCP connections, and active TCP connections. It is one of the simplest tools for troubleshooting network services.

b) To list out TCP connections which are established I used **$ netstat -at | grep "ESTABLISHED"**. -at is used to list out all the TCP connections while | grep "ESTABLISHED" is used to list only the established connections.





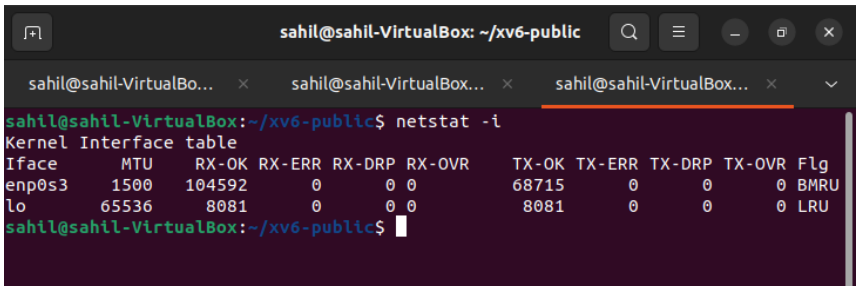
Explanation of different fields

- **Proto –** Gives the name of the protocol used (TCP in this case)
- **Recv-Q –** The counts of bytes not copied by the user program connected to this socket.
- **Send-Q –** The count of bytes yet to be acknowledged by the remote host.
- **Local Address –** Gives the address and port number of the local end of the socket.

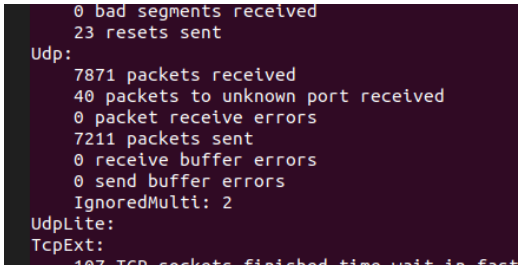
- **Foreign Address -** Gives the address and port number of the remote end of the socket.
- **State -** Indicates the state of a TCP connection. These states represent the thee way handshake communication system that TCP uses.

c) The r-option of netstat displays the **IP routing table**. Various fields: 1) **Destination –** Shows the destination network. 2) **Gateway -** The router through which packets are forwarded. 3) **Genmask -** The netmask for the destination net; 255.255.255.0 for a host destination and 0.0.0.0 for the default host. 4) **Flags -** The U flag indicates that the route is up. The G flag indicates that the route is to a gateway. The H flag indicates that the destination is a fully qualified host address, rather than a network. 5) **MSS –** Tells about the default maximum segment size for TCP connection over route. 6) **Windows -** Maximum amount of data the system will accept in a single burst from a remote host. 7) **irtt –** Tells about the initial round trip time. 8) **Iface –** Tells about the interface to which packets for this route will be sent.

d) **netstat -i** command shows the state of the network interfaces that are configured on the local system. From the output, I can conclude that there are 2 interfaces on my system namely: **enp0s3** and **lo**



e) The netstat -s option displays per protocol statistics for the UDP, TCP, ICMP, and IP protocols.



f) The computer communicates with itself via a unique virtual network interface called the loopback interface. It is mostly used to connect to servers that are operating on the local PC for diagnostic and troubleshooting purposes. No communication on a network interface is possible when it is unplugged, not even between the computer and the computer. Applications operating on the computer may always connect to servers running on the same machine thanks to the loopback interface, which does not reflect any physical hardware. For instance, if you manage a web server and have access to every online document, you may go over each file individually on your local computer.

Q6

Host Name	Hop Count #1 (10am)	Hop Count #2 (2pm)	Hop Count #3 (4pm)
amazon.com	27	27	27
sprinklr.com	64(max)	64(max)	64(max)
codeforces.com	17	18	18
cricbuzz.com	10	10	11
youtube.com	24	24	24
interviewbit.com	28	28	28

a) There are 2 obvious common hops i.e., my device (14.139.196.14) and the IP address of the destination in every case. Apart from them IP address (10.12.5.220) is also common in all as it is the IP address of my hostel.

b) Yes, for cricbuzz.com and codeforces.com the number of hops is different for different times. It is because of network congestion. The packets are redirected by the nodes to take a route having less traffic.

c) Yes, traceroute for sprinklr.com did not find complete route to the host as it exceeds the maximum hops (64) allowed. Some servers/hosts along the path may not have been configured to respond to the ICMP Traffic or may have set up firewalls which block the ICMP traffic or we might need to increase max hops.

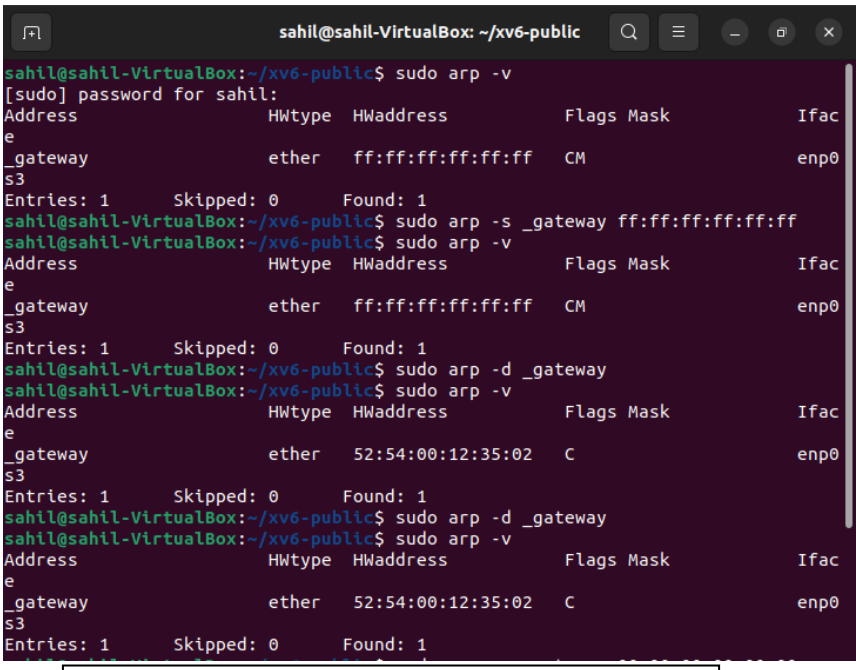
d) Yes. Ping and traceroute both use the ICMP Packets but their working is different. Ping is straight ICMP and failing ping might be because of blocked packet transmission. Traceroute sends packets with TTL values that increase from packet to packet. That's why it might be possible to find the route to certain hosts.

Q7

a) ARP stands for Address Resolution Protocol. We can view the full ARP table using **arp -a or arp -v** command. The table has 6 columns. Address: Represents IP address of network connections. HWtype: Represents hardware type of the machine. HWaddress: Shows the hardware address of the machine over the network. Flags: Complete entries are marked with C flag, permanent with M and published with P. Mask: Represents Genmask. Iface: Represents network interfaces

b) How to:

- Add: arp -s <IP_Address> <MAC Address>
- Delete: arp -d <IP_Address>
- Change: We can first delete and then add the edited entry



Screenshot to demonstrate all the necessary operations of part a and b.

c) Entries in the ARP table are cached for 60 seconds. To determine the timeout value by trial and error, put a temporary entry in the ARP table and monitor the ARP table at regular intervals. The time it takes to disappear is about equal to the cache timeout. Reduce the interval length for a better estimate. Alternatively, binary search may be used to determine the cache time. If suppose at time t entry is removed, then we can try checking at time t/2. This way binary search can be implemented.

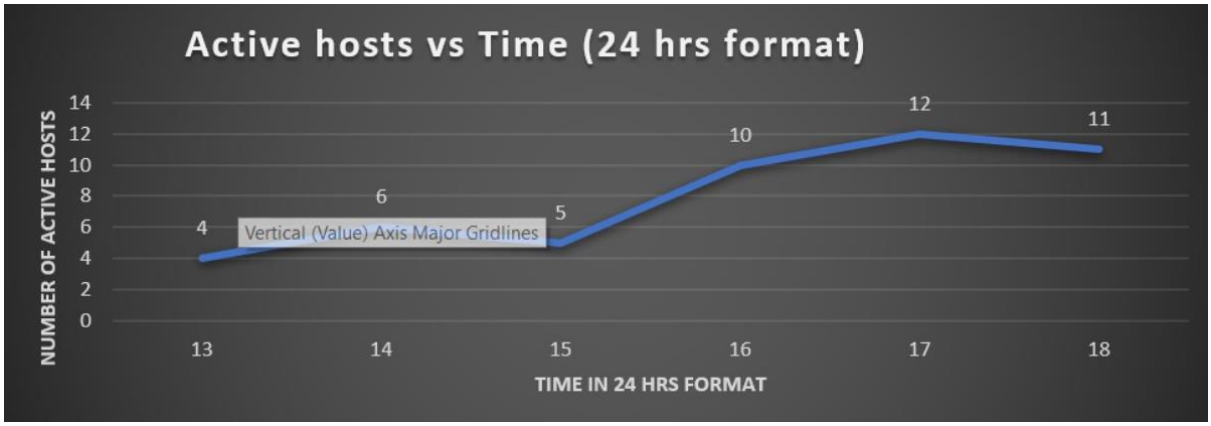
d) When a router or gateway joins two or more subnet ranges, two IP addresses might map to the same Ethernet address. The MAC address routes package when connecting with machines on the same subnet range. In the ARP database, the IP addresses of devices connected in the other subnet range have the same Ethernet address/MAC address as the Router or Gateway that links the two subnet ranges. The ARP table converts these IP addresses to MAC addresses before sending packets. The router then utilizes its routing database to route the packet to the relevant device.

Q8

The following command is used for this question. The IP's analysed are of **Brahmaputra Hostel**.

nmap -n -sP 10.12.5.220/22

I observed that the number of active hosts were more in the evening as compared to afternoon. Below is the graph of number of active hosts vs time of the day (1024 IP addresses are scanned).



Q9

Various commands are as follows –

a) To find IP address type – nslookup www.example.com
b) To find domain name of an IP address type – nslookup IP address
c) To find mail servers for a domain type - **nslookup -querytype=mx domain name**

```
sahil@sahil-VirtualBox:~/xv6-public$ nslookup www.facebook.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.facebook.com        canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 31.13.79.35
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f12f:183:face:b00c:0:25de

sahil@sahil-VirtualBox:~/xv6-public$ nslookup 31.13.79.35
35.79.13.31.in-addr.arpa        name = edge-star-mini-shv-02-bom1.facebook.com.

Authoritative answers can be found from:
79.13.31.in-addr.arpa   nameserver = b.ns.facebook.com.
79.13.31.in-addr.arpa   nameserver = a.ns.facebook.com.
b.ns.facebook.com       has AAAA address 2a03:2880:f0fd:c:face:b00c:0:35
b.ns.facebook.com       internet address = 129.134.31.12
a.ns.facebook.com       has AAAA address 2a03:2880:f0fc:c:face:b00c:0:35
a.ns.facebook.com       internet address = 129.134.30.12
```

```
sahil@sahil-VirtualBox:~/xv6-public$ nslookup -querytype=mx facebook.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
facebook.com    mail exchanger = 10 smtpin.vvv.facebook.com.

Authoritative answers can be found from:
facebook.com    nameserver = b.ns.facebook.com.
facebook.com    nameserver = d.ns.facebook.com.
facebook.com    nameserver = a.ns.facebook.com.
facebook.com    nameserver = c.ns.facebook.com.
a.ns.facebook.com       internet address = 129.134.30.12
a.ns.facebook.com       has AAAA address 2a03:2880:f0fc:c:face:b00c:0:35
b.ns.facebook.com       internet address = 129.134.31.12
b.ns.facebook.com       has AAAA address 2a03:2880:f0fd:c:face:b00c:0:35
c.ns.facebook.com       internet address = 185.89.218.12
c.ns.facebook.com       has AAAA address 2a03:2880:f1fc:c:face:b00c:0:35
d.ns.facebook.com       internet address = 185.89.219.12
d.ns.facebook.com       has AAAA address 2a03:2880:f1fd:c:face:b00c:0:35
```