

Computer Networks Lab (CS 212)

Lab Assignment – 1

2. Warm up Questions

1. By typing the command "**hostname**" and "**hostname -I**" we get my laptop "**hostname : chilaka**" and "**Ip address : 10.196.5.141**".

2. By typing the command "**arp -n**" we get the next hop router's ip address and mac address.

3. by typing the command "**cat /etc/resolv.conf**" we get the local DNS server's IP address under "nameserver".

local DNS server's IP address : 127.0.0.53

4. The **/etc/protocols** file contains information regarding the known protocols used in the DARPA Internet.

Items are separated by any number of blanks or tabs, or both. A # in a line indicates the beginning of a comment — any characters after a #, up to the end of the line, aren't interpreted by routines that search the file.

Protocol names may contain any printable character other than a field delimiter, newline, or comment character.

5. the port number associated with applications:

ssh : 22,

ftp : 21,

nfs : 2049,

smtp : 25.

All this info is found in '**cat /etc/services**' file.

6. Yes, we can get the hostname, ip address, DNS server's ip address for android phone.



```
Activities Terminal Jan 22 2:21 PM chilaka@chilaka: ~
chilaka@chilaka:~$ hostname
chilaka
chilaka@chilaka:~$ hostname -I
10.196.5.141
chilaka@chilaka:~$ arp -n
Address HWtype HWaddress Flags Mask Iface
35.224.99.156 (incomplete)
10.196.3.250 ether 02:94:96:9a:82:e8 C eno1
chilaka@chilaka:~$ cat /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0
chilaka@chilaka:~$
```

3. Questions:

1. Using 'ping' command to ping different ip addresses.

Cases: My phone(10.196.7.83) and the local DNS server(10.250.200.3).

Results:

For the DNS server:

13 packets transmitted, 13 received, 0% packet loss, time 31ms
rtt min/avg/max/mdev = 2.716/4.640/15.976/3.362 ms

For my phone:

13 packets transmitted, 13 received, 0% packet loss, time 29ms
rtt min/avg/max/mdev = 48.491/162.136/433.982/119.249 ms

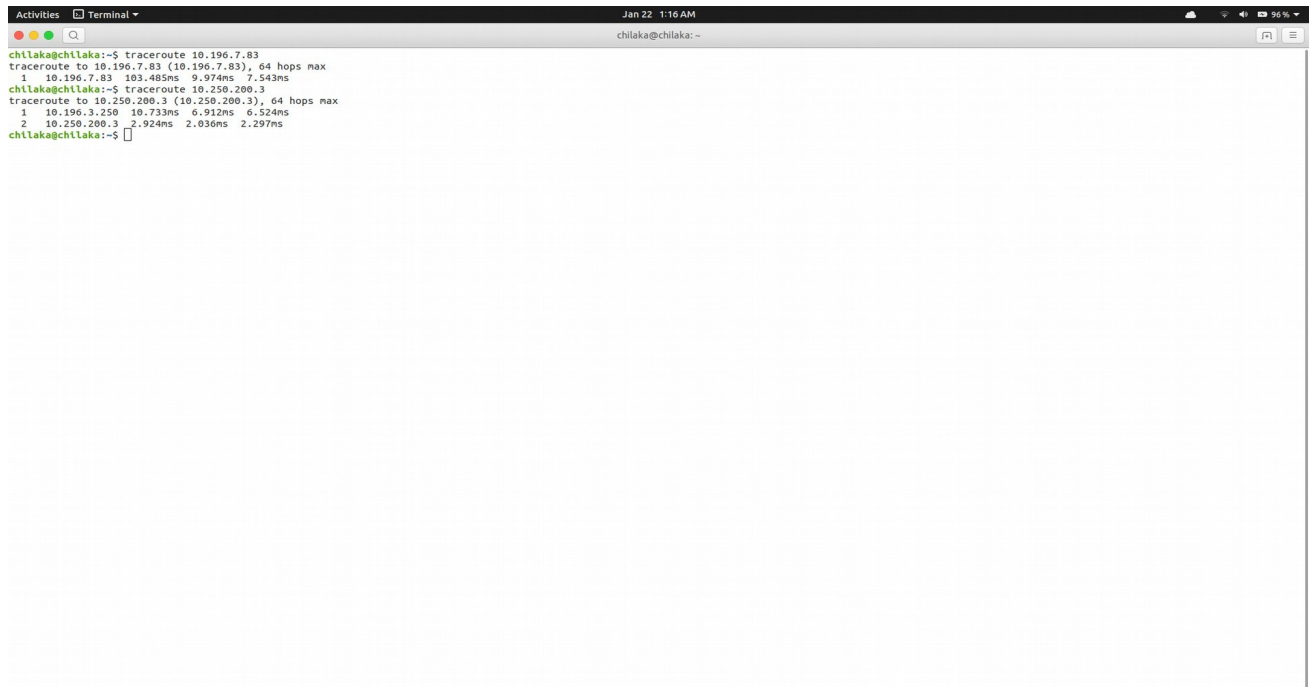
Report:

a) When a packet sent and reaches the destination then ping is success. When a packet fails to reach the destination then ping is failure. Reasons for a ping failure can be low bandwidth, network congestion or attacks on the network(Example: Denial of Service.)

b) RTT depends on the network infrastructure, the hardware of the destination device and also on the physical distance between the devices.

```
Activities Terminal Jan 22 1:11 AM
chilaka@chilaka:~$ ping 10.250.200.3
PING 10.250.200.3 (10.250.200.3) 56(84) bytes of data:
64 bytes from 10.250.200.3: icmp_seq=1 ttl=63 time=3.26 ms
64 bytes from 10.250.200.3: icmp_seq=2 ttl=63 time=3.13 ms
64 bytes from 10.250.200.3: icmp_seq=3 ttl=63 time=3.98 ms
64 bytes from 10.250.200.3: icmp_seq=4 ttl=63 time=15.10 ms
64 bytes from 10.250.200.3: icmp_seq=5 ttl=63 time=3.24 ms
64 bytes from 10.250.200.3: icmp_seq=6 ttl=63 time=3.07 ms
64 bytes from 10.250.200.3: icmp_seq=7 ttl=63 time=3.66 ms
64 bytes from 10.250.200.3: icmp_seq=8 ttl=63 time=2.72 ms
64 bytes from 10.250.200.3: icmp_seq=9 ttl=63 time=5.58 ms
64 bytes from 10.250.200.3: icmp_seq=10 ttl=63 time=3.10 ms
64 bytes from 10.250.200.3: icmp_seq=11 ttl=63 time=4.81 ms
64 bytes from 10.250.200.3: icmp_seq=12 ttl=63 time=3.51 ms
64 bytes from 10.250.200.3: icmp_seq=13 ttl=63 time=4.38 ms
^C
--- 10.250.200.3 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 31ms
rtt min/avg/max/mdev = 2.716/4.640/15.976/3.362 ms
chilaka@chilaka:~$ ping 10.196.7.83
PING 10.196.7.83 (10.196.7.83) 56(84) bytes of data:
64 bytes from 10.196.7.83: icmp_seq=1 ttl=64 time=162 ms
64 bytes from 10.196.7.83: icmp_seq=2 ttl=64 time=81.9 ms
64 bytes from 10.196.7.83: icmp_seq=3 ttl=64 time=113 ms
64 bytes from 10.196.7.83: icmp_seq=4 ttl=64 time=259 ms
64 bytes from 10.196.7.83: icmp_seq=5 ttl=64 time=48.5 ms
64 bytes from 10.196.7.83: icmp_seq=6 ttl=64 time=75.10 ms
64 bytes from 10.196.7.83: icmp_seq=7 ttl=64 time=95.7 ms
64 bytes from 10.196.7.83: icmp_seq=8 ttl=64 time=240 ms
64 bytes from 10.196.7.83: icmp_seq=9 ttl=64 time=50.8 ms
64 bytes from 10.196.7.83: icmp_seq=10 ttl=64 time=361 ms
64 bytes from 10.196.7.83: icmp_seq=11 ttl=64 time=80.2 ms
64 bytes from 10.196.7.83: icmp_seq=12 ttl=64 time=166 ms
64 bytes from 10.196.7.83: icmp_seq=13 ttl=64 time=434 ms
^C
--- 10.196.7.83 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 29ms
rtt min/avg/max/mdev = 48.491/162.136/433.982/119.249 ms
chilaka@chilaka:~$
```

2. Using the command - 'traceroute'



```
chilaka@chilaka:~$ traceroute 10.196.7.83
traceroute to 10.196.7.83 (10.196.7.83), 64 hops max
 1  10.196.7.83  103.485ms  9.974ms  7.543ms
chilaka@chilaka:~$ traceroute 10.250.200.3
traceroute to 10.250.200.3 (10.250.200.3), 64 hops max
 1  10.196.3.250  10.733ms  6.912ms  6.524ms
 2  10.250.200.3  2.924ms  2.036ms  2.297ms
chilaka@chilaka:~$
```

a) traceroute to my phone:

traceroute 10.196.7.83 gives the following output

traceroute to 10.196.7.83 (10.196.7.83), 64 hops max
1 10.196.7.83 (10.196.7.83) 103.485 ms 9.974 ms 7.543 ms

traceroute to the DNS server:

traceroute to 10.250.200.3 gives the following output

traceroute to 10.250.200.3 (10.250.200.3), 64 hops max
1 10.196.3.250 10.733ms 6.912ms 6.524ms
2 10.250.200.3 2.924ms 2.036ms 2.297ms

b) Maximum hop number can be changed using the flag '-m'

c) Traceroute sends three packages per TTL increment. Each column corresponds to the time it took to get one packet back(RTT).

d) When TTL becomes zero at a certain point in the network, the packet gets discarded and an ICMP message is sent back to the origin of the packet which can trigger a resend.

3: Goal:

Look at the following files and understand what they are for

/etc/hostname, /etc/hosts, /etc/network/interfaces, /etc/resolv.conf, /etc/protocols, /etc/services

- **/etc/hostname**-contains the hostname of my machine.
- **/etc/hosts**-contains the list of hostnames and ip addresses on our machine.
- **/etc/network/interfaces**-describes the network interfaces available on the system and how to activate them.
- **/etc/resolv.conf**-has information regarding the DNS server.
- **/etc/protocols**-describes the various protocols available.
- **/etc/services**-contains various services and the associated ports to them.

a) Hostname and ip address:

The hostname of the machine is found out with the help of the **'hostname'** command. It simply prints the hostname on the command line.

The ip address is found out by the **'ifconfig'** command.

It returns all the ip addresses of all network connections on the device.

b) First by using the command **'traceroute'** and after by using **'arp -a'**

c) The local DNS server's ip address is found in **'/etc/resolv.conf'** file under the name **'nameserver'**.

d) The numbers are the official numbers for the protocols as they would appear in the ip header.

e) **ssh:22, ftp:21, nfs:2049, smtp:25**. All this info is found in **'cat /etc/services'** file.

4.Goal :

a) OK

b) Packets in black color mean they have a problem.

c) **ip.src == 10.196.5.141 && http ; tcp.port==80**

d) UDP is much faster than TCP. DNS servers need to be optimized for higher performance hence the use of UDP. Whereas TCP makes sure that the requests are intact from both the client and the server.

