

# COMPUTER NETWORKS

## PRACTICAL 2

*Submitted by*

**TAKOLIYA MANAV ANILBHAI (21BCE530)**

**B.TECH**

**in**

**COMPUTER SCIENCE AND ENGINEERING**

*Guided by*

**Dr. VIJAY UKANI**



**NIRMA INSTITUTE OF TECHNOLOGY AHMEDABAD**

**27 AUGUST 2022**

## **PRACTICAL 2**

### **Aim: Analyze ping command**

#### **Uses:**

1. Test network connectivity.
2. Test network interface card.
3. Test DNS name resolution issues.

#### **Steps:**

The first step in troubleshooting is to ensure you can ping locally. To do this:

1. Go to Start > Run, type CMD and press Enter.
2. Type ping 127.0.0.1 and press Enter.
3. If this fails, troubleshoot your firewall.

#### **If that step was successful:**

1. Type ping 25.x.x.x where 25.x.x.x is your own Hamachi IP.
2. If this fails, again revisit your firewall settings.

#### **If this was successful:**

1. Type ping 25.x.x.x where 25.x.x.x is the IP of the target computer.
2. If this fails, you'll need to troubleshoot the firewall on that machine

If you use IPv6 protocol mode, you need to type ping -6 <IPv6 address>. For example,

```
ping -6 2620:9b::586:5b0c
```

**Snapshot:**

```
C:\Users\MANAV TAKOLIYA>ping google.com

Pinging google.com [172.217.166.78] with 32 bytes of data:
Reply from 172.217.166.78: bytes=32 time=151ms TTL=116
Reply from 172.217.166.78: bytes=32 time=67ms TTL=116
Reply from 172.217.166.78: bytes=32 time=72ms TTL=116
Reply from 172.217.166.78: bytes=32 time=52ms TTL=116

Ping statistics for 172.217.166.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 52ms, Maximum = 151ms, Average = 85ms

C:\Users\MANAV TAKOLIYA>
```

**Observation:**

When we ping any server, our computer sends four data packets to the server. In reply, that server sends back those four data packets to us. This reply is called an "echo reply request."

If the server replies, then that means there is network connectivity between our computer and that server.

The server may be located on a local area network or on the internet.

If we did not get a reply from the server, then that means the server did not reply back, and it could mean that there is no connectivity between us and the server.

The cause of the server's failure to respond:

- 1.The server can be turned off.
2. The server is secured by a firewall.
3. "Destination host unreachable" means the route of destination could not be found.

The cause of getting the data packet 4:

- 1.NETWORK CONGESTION
2. Faulty Hardware (such as an incorrect Ethernet cable, wiring, modem, or network card)

We can also do a loopback test on our computer to check if our network card is working properly or not.

We have two options for that.

1. ping localhost ( loopback address)
2. 127.0.0.1 ( loopback address)

```
Reply from 142.250.67.174: bytes=32 time=562ms TTL=116
```

What is a byte: The size of the packet we send to the server is -32 bytes. 32 is the default size in Windows.

What is time : This indicate round trip time,time take be HOST A to HOST B and back to HOST A .

What is TTL : Time to live (TTL) refers to the amount of time or “hops” that a packet is set to exist inside a network before being discarded by a router.

**Aim: Analyze tracert command**

Tracert sends 3 data packets to every router and sends round trip time accordingly.

**Uses:**

1. used to show a data packet's path from source to destination.
2. Traceroute can help you find problems like bottlenecks (from where our network is lagging)

**Steps:**

1. Press Windows key + R to open the Run window.
2. Enter cmd and press Enter to open a Command Prompt.
3. Enter tracert, a space, then the IP address or web address for the destination site (for example: tracert www.lexis.com).
4. Press Enter.

**Snapshot:**

```
C:\Users\MANAV TAKOLIYA>tracert google.com

Tracing route to google.com [142.250.67.174]
over a maximum of 30 hops:

  1    2 ms    1 ms    1 ms  192.168.222.92
  2  125 ms   33 ms   50 ms  192.168.1.6
  3   89 ms   27 ms   35 ms  10.169.131.222
  4   58 ms   37 ms   32 ms  100.64.0.125
  5   74 ms   58 ms   59 ms  182.19.106.113
  6   71 ms   46 ms   58 ms  72.14.205.216
  7  202 ms   34 ms   40 ms  142.251.49.177
  8   88 ms   59 ms   58 ms  142.250.227.73
  9  204 ms   43 ms   73 ms  bom12s07-in-f14.1e100.net [142.250.67.174]

Trace complete.
```

**Observation:**

1. 1's column tells us about the hops taken by data packet. In our example, it is 9 hops.
2. The next 3 columns tell us about the round trip of our data packets from each router to our computer.
3. The last column tells us the IP address of each router and its final destination.
4. \* means There is a problem with the router, or it may be possible that the router is working fine but it was not configured to return traceroute replies.
5. Maximum of 30 hops means TTL sets a maximum of 30 hops which means if a data packet does not reach its destination after 30 hops, then it will be dropped.

-We can change maximum hops.

```
tracert -h 4 google.com
```

What is use of TTL:

TTL prevent data packets from travelling endless around the internet.

**Aim:- Analyze of nslookup****USE:**

Getting information from the DNS server

**Steps:**

1. Launch Windows Command Prompt by navigating to Start > Command Prompt or via Run > CMD.
2. Type NSLOOKUP and hit Enter. ...
3. Set the DNS Record type you wish to lookup by typing set type=## where ## is the record type, then hit Enter.

**Snapshot:**

```
C:\Users\MANAV TAKOLIYA>nslookup google.com
Server: UnKnown
Address: 192.168.222.92

Non-authoritative answer:
Name: google.com
Addresses: 2404:6800:4009:812::200e
          142.250.67.174

C:\Users\MANAV TAKOLIYA>nslookup 8.8.8.8
Server: UnKnown
Address: 192.168.222.92

Name: dns.google
Address: 8.8.8.8
```

**Observation :**

1. It resolves the name of the DNS server and it also resolves or configures the IP address.
2. nslookup is a simple but very practical command-line tool, which is principally used to find the IP address that corresponds to a host, or the domain name that corresponds to an IP address (a process called “Reverse DNS Lookup”).

## Aim: Analyze ipconfig command

### Use:

It displays the TCP/IP network configuration of the network adapters on a Windows computer.

used for troubleshooting issues.

### Steps:

Go to "Start > Run" and type "cmd" (no quotes), then select "OK"

Type "ipconfig/release" (no quotes) and press "Enter"

### Snapshot :

```
Wireless LAN adapter Wi-Fi:
    Connection-specific DNS Suffix  . : 
    Description . . . . . : Intel(R) Dual Band Wireless-AC 3165
    Physical Address. . . . . : 74-E5-F9-78-36-4C
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::a8af:cfe4:89a:a241%8(Preferred)
    IPv4 Address. . . . . : 192.168.222.76(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : 27 August 2022 18:57:17
    Lease Expires . . . . . : 27 August 2022 20:27:16
    Default Gateway . . . . . : 192.168.222.92
    DHCP Server . . . . . : 192.168.222.92
    DHCPv6 IAID . . . . . : 91547129
    DHCPv6 Client DUID. . . . . : 00-01-00-01-21-E7-9A-4F-8C-16-45-09-81-11
    DNS Servers . . . . . : 192.168.222.92
    NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
    Description . . . . . : Bluetooth Device (Personal Area Network)
    Physical Address. . . . . : 74-E5-F9-78-36-50
    DHCP Enabled. . . . . : Yes
```

### Observation:

IPCONFIG displays things like IP addresses, subnet masks, and the default gateway.

1. IPv4 is the private IP address that has been assigned to us by the DHCP server. That's built into our router and modem/router combo that's in our home and office .



2. Default Gateway: This is the IP address of your home's router or modem/router combo that connects to your network. which allows you to communicate with different networks.
3. We have assigned IPv4 and IPv6 addresses.
4. The `ipconfig/all` command displays your network adapters' complete TCP/IP configuration.
5. The `ipconfig/flushdns` command clears the computer's DNS resolver cache.
6. Because the computer only understands numbers and not the name of the site, we must convert the name into an IP address.
7. DNS resolver cache stores a history of domain names and their corresponding IP addresses for a period of time. The purpose of this is to make the browser fast.
8. When can we use `ipconfig /flushdns`: We can use this command when we can't access some site.
9. When can we use `ipconfig/flushdns`? We can use this command when we can't access some site.

**Aim: Analyze netstat -r command**

**Use:**

to display current network connectivity and port activity on your computer.

Available on various operating systems,

**Steps:**

1. Launch Windows Command Prompt by navigating to Start > Command Prompt or via Run > CMD.
2. Type netstat -options and hit Enter. ...

**Snapshot:**

```

=====
Active Routes:
Network Destination        Netmask          Gateway         Interface      Metric
0.0.0.0                    0.0.0.0          192.168.222.92  192.168.222.76    55
127.0.0.0                  255.0.0.0         On-link         127.0.0.1        331
127.0.0.1                  255.255.255.255   On-link         127.0.0.1        331
127.255.255.255            255.255.255.255   On-link         127.0.0.1        331
192.168.222.0              255.255.255.0     On-link         192.168.222.76   311
192.168.222.76             255.255.255.255   On-link         192.168.222.76   311
192.168.222.255            255.255.255.255   On-link         192.168.222.76   311
224.0.0.0                  240.0.0.0         On-link         127.0.0.1        331
224.0.0.0                  240.0.0.0         On-link         192.168.222.76   311
255.255.255.255            255.255.255.255   On-link         127.0.0.1        331
255.255.255.255            255.255.255.255   On-link         192.168.222.76   311
=====
Persistent Routes:
None

```

**Observation:**

1. netstat -n returns the IP address instead of the domain name.
2. netstat -a displays TCP and UDP ports
3. netstat -b displays the protocol along with the application name.
4. netstat -f displays the domain name rather than the IP address in foreign addresses.
5. netstat -r display the routing table

We can combine all these switches (attributes).

**Aim: Analyze arp -a command**

**Use:**

Displays and modifies address resolution, including ATM (Asynchronous Transfer Mode) interfaces.

It is used to convert IP addresses to Mac addresses.

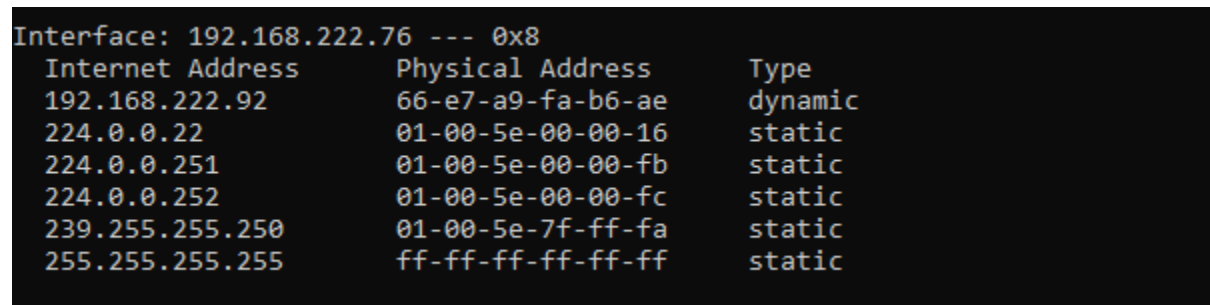
Devices need the mac address for communication on the local network.

Use arp to acquire a mac address for that device.

**-a :** To Display ARP Entries

**Steps :**

1. Open cmd
2. Type arp – a and hit enter
- 3.

**Snapshot:**

Interface: 192.168.222.76 --- 0x8		
Internet Address	Physical Address	Type
192.168.222.92	66-e7-a9-fa-b6-ae	dynamic
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

**Observation :**

How it works:-

Our computer sends a request for the mac address of a network device. A correspondent device on the network will respond to it by sending its mac address.

Now our computers store the IP address and Mac address of that computer in the arp cache.

An ARP cache is used to make a network more efficient.

Arp entries are classified into two types:

- 1.static : The static entry is where someone manually enters an IP to MAC address association using the ARP command line utility.
2. dynamic: it is generated automatically when a device broadcasts a message over the network.