INVESTIGATING NETWORKS

LAB # 02

Fall 2024

Submitted by: **Mohsin Sajjad**
Registration No: **22pwsce2149**

Class Section: **A**

"On my honor, as student of University of Engineering and Technology, I have neither given nor received unauthorized assistance on this academic work."

Student Signature: _____

Submitted to:
Dr. Yasir Saleem Afridi
Month Day, Year (26 02, 2025)

Department of Computer Systems Engineering
University of Engineering and Technology, Peshawar

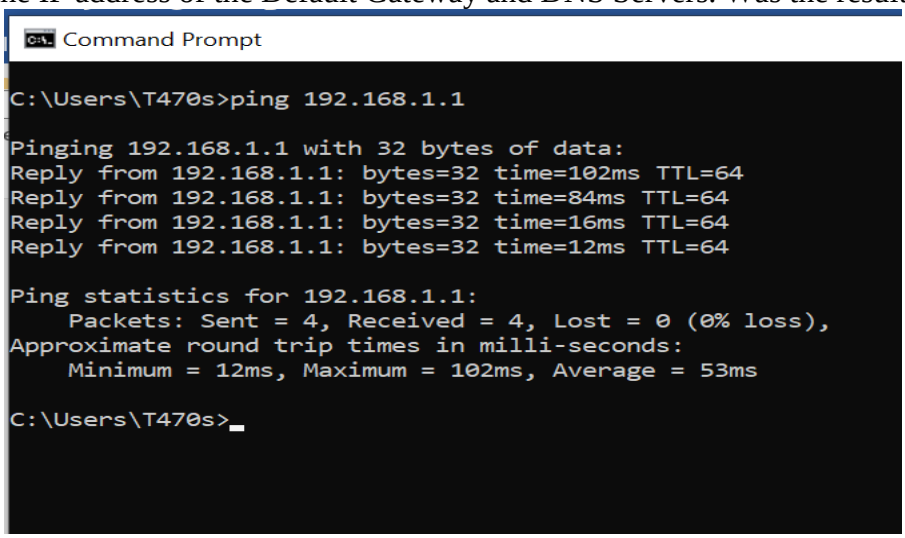
ABOUT PING

The original PING command stood for "Packet Internet Groper", and was a package of diagnostic utilities used by DARPA personnel to test the performance of the ARPANET. However, the modern Internet Ping command refers to a program written by Mike Muss in December, 1983, which has since become one of the most versatile and widely used diagnostic tools on the Internet.
Typical Diagnostic Tests Performed By Ping Command
Some of the internet diagnostic tests performed by ping command are:

- **Access –** Ping is used to determine whether the remote host is active or inactive. If a certain site is not pinged, but the other sites can, then it's a pretty good sign that your Internet network is fine and that site is down. On the other hand, if you can't ping any site, then likely your entire network connection is down that needs rebooting.
- **Time & distance –** Another use of Ping command is to determine how long it takes to bounce a packet off of another site. Thereby giving Internet distance in network terms. For example, a web site hosted on your neighbor's computer with a different Internet service provider (ISP) might go through more routers and be farther away in network distance than a site on the other side of the ocean with a direct connection to the Internet backbone. If a site seems slow, then ping distance of that site can be compared with that of other Internet sites to find out whether it is the site, the network, or your system that is slow. You can also compare ping times to get an idea of which sites have the fastest network access and would be most efficient for downloading, chatting, and other applications.
- **Domain IP address –** Typically, Ping command is used to probe either a domain name or an IP address; if a domain name is pinged, and then it displays the corresponding IP address in its response.

----------TASK 01----------

a) Ping the IP address of the Default Gateway and DNS Servers. Was the result successful?



b) Ping the computer's loop-back address. Type the following command: >> **ping 127.0.0.1**

```
Command Prompt
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

C:\Users\T470s>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\T470s>
```

c) What is the IP Address of www.yahoo.com: **212.82.117.205**
How much time did our ping took to reach www.yahoo.com: **252ms**

d) Ping the hostname of another computer**.** Try to ping the hostname of the computer that was recorded in the previous lab.

```
C:\Users\T470s>ping DESKTOP-BOJT8NU

Pinging DESKTOP-BOJT8NU [fe80::2ead:f6eb:44b0:510a%11] with 32 bytes of data:
Reply from fe80::2ead:f6eb:44b0:510a%11: time=76ms
Reply from fe80::2ead:f6eb:44b0:510a%11: time=325ms
Reply from fe80::2ead:f6eb:44b0:510a%11: time=14ms
Reply from fe80::2ead:f6eb:44b0:510a%11: time=20ms

Ping statistics for fe80::2ead:f6eb:44b0:510a%11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 325ms, Average = 108ms
```

e) Ping the hostname of another computer using –t. Try to ping repetitively, the hostname of the computer.

```
C:\Users\T470s>ping -t DESKTOP-F1QMP69

Pinging DESKTOP-F1QMP69 [fe80::a594:976e:1028:34a6%15] with 32 bytes of data:
Reply from fe80::a594:976e:1028:34a6%15: time<1ms
Reply from fe80::a594:976e:1028:34a6%15: time<1ms
Reply from fe80::a594:976e:1028:34a6%15: time<1ms
Reply from fe80::a594:976e:1028:34a6%15: time<1ms

Ping statistics for fe80::a594:976e:1028:34a6%15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\T470s>
```

f) How can we stop the ping**? Ctrl + C**

g) ping the IP address of the default gateway

Command Prompt

```
C:\Users\T470s>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=102ms TTL=64
Reply from 192.168.1.1: bytes=32 time=84ms TTL=64
Reply from 192.168.1.1: bytes=32 time=16ms TTL=64
Reply from 192.168.1.1: bytes=32 time=12ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 102ms, Average = 53ms

C:\Users\T470s>
```

h) ping the IP address of a DHCP or DNS server.

```
Command Prompt

C:\Users\T470s>ping 192.168.100.247

Pinging 192.168.100.247 with 32 bytes of data:
Reply from 192.168.100.247: bytes=32 time=49ms TTL=126
Reply from 192.168.100.247: bytes=32 time=161ms TTL=126
Reply from 192.168.100.247: bytes=32 time=5ms TTL=126
Reply from 192.168.100.247: bytes=32 time=4ms TTL=126

Ping statistics for 192.168.100.247:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 161ms, Average = 54ms

C:\Users\T470s>
```

----------TASK 03----------

a) Trace the route to the GOOGLE PAKISTAN website by typing:

>> tracert www.google.com.pk

The result shows the complete route to the site, along with the number of hops in the path.

```
Command Prompt

C:\Users\T470s>tracert www.google.com.pk

Tracing route to www.google.com.pk [172.217.19.195]
over a maximum of 30 hops:

  1    21 ms     1 ms    39 ms  192.168.1.1
  2     6 ms     2 ms    12 ms  10.110.110.1
  3     7 ms   103 ms     2 ms  192.168.100.200
  4  ^C
C:\Users\T470s>
```

b) Trace the route to the UET website using options listed in option description table.

Option Description

==========

-d (Do Not Resolve Addresses) Displays the route using numeric addresses only rather than showing both IP address and host

names, for faster display.
-h maximum_hops (Max. Hops) Specifies the maximum number of hops to use for tracing; Default is 30
-w timeout Specifies how long to wait for a reply to each Request in milliseconds; Default is 4000 [for 4 sec]

Command Prompt

```
C:\Users\T470s>tracert -d www.uetpeshawar.edu.pk

Tracing route to uetpeshawar.edu.pk [121.52.147.74]
over a maximum of 30 hops:

  1     1 ms     1 ms     2 ms  192.168.1.1
  2    21 ms    17 ms    51 ms  10.110.110.1
  3     4 ms     5 ms    14 ms  192.168.100.200
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18  ^C
C:\Users\T470s>
```

```
Tracing route to uetpeshawar.edu.pk [121.52.147.74]
over a maximum of 5 hops:

  1     5 ms     3 ms     4 ms  192.168.1.1
  2    10 ms     2 ms     3 ms  10.110.110.1
  3     4 ms    25 ms     4 ms  192.168.100.200
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.

Trace complete.

C:\Users\T470s>
```

```
Tracing route to uetpeshawar.edu.pk [121.52.147.74]
over a maximum of 30 hops:

  1     *      315 ms   160 ms  192.168.1.1
  2    43 ms    86 ms    16 ms  10.110.110.1
  3     *        8 ms    37 ms  ^C
C:\Users\T470s>
```

c) What is the difference between the following commands?
Tracert www.yahoo.com
Tracert –h 20 www.yahoo.com
Ans: Tracert www.yahoo.com: The trace will attempt to reach the destination with up to **30 hops** by default.
Tracert –h 20 www.yahoo.com: This command adds the `-h` option to limit the maximum number of hops in the traceroute to **20 hops**.

Task 04 (Long Life Learning)

Practice the following network commands and understand/report their usage

i) **netstat**

Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, netstat displays active TCP connections.

Try the following

a. _ **netstat -a**: Shows the state of all sockets, routing table entries, and interfaces.
b. _ **netstat -r**: Displays the routing table.
c. _ **netstat -i**: Displays the interface information.
d. _ **netstat -n**: Displays numbers instead of names.
e. _ **netstat -s**: Displays per-protocol statistics.

Command Prompt - netstat -a

```
C:\Users\T470s>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-F1QMP69:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-F1QMP69:0      LISTENING
  TCP    0.0.0.0:808            DESKTOP-F1QMP69:0      LISTENING
  TCP    0.0.0.0:902            DESKTOP-F1QMP69:0      LISTENING
  TCP    0.0.0.0:912            DESKTOP-F1QMP69:0      LISTENING
  TCP    0.0.0.0:3389           DESKTOP-F1QMP69:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-F1QMP69:0      LISTENING
  TCP    0.0.0.0:5357           DESKTOP-F1QMP69:0      LISTENING
  TCP    0.0.0.0:9001           DESKTOP-F1QMP69:0      LISTENING
```

Command Prompt

```
C:\Users\T470s>netstat -r
===========================================================================
Interface List
  4...8c 16 45 e2 71 14 ......Intel(R) Ethernet Connection I219-LM
  9...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 15...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
 11...20 16 b9 76 0b 8d ......Intel(R) Dual Band Wireless-AC 8260
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.120     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
      192.168.1.0    255.255.255.0         On-link     192.168.1.120    311
```

Command Prompt

```
C:\Users\T470s>netstat -i

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

  -a            Displays all connections and listening ports.
  -b            Displays the executable involved in creating each connection or
                listening port. In some cases well-known executables host
                multiple independent components, and in these cases the
                sequence of components involved in creating the connection
                or listening port is displayed. In this case the executable
                name is in [] at the bottom, on top is the component it called,
                and so forth until TCP/IP was reached. Note that this option
                can be time-consuming and will fail unless you have sufficient
                permissions.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
```

```
Command Prompt
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

C:\Users\T470s>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.120:53450    20.198.119.84:443      ESTABLISHED
  TCP    192.168.1.120:53453    20.198.119.84:443      ESTABLISHED
  TCP    192.168.1.120:53466    142.250.27.188:5228    ESTABLISHED
  TCP    192.168.1.120:53467    20.212.88.117:443      ESTABLISHED
  TCP    192.168.1.120:53488    13.107.226.62:443      CLOSE_WAIT
  TCP    192.168.1.120:53491    34.207.136.156:80      ESTABLISHED
  TCP    192.168.1.120:53523    144.2.15.25:443        CLOSE_WAIT
  TCP    192.168.1.120:53524    23.10.239.251:80       LAST_ACK
  TCP    192.168.1.120:53533    23.217.111.96:443      LAST_ACK
  TCP    192.168.1.120:53534    40.99.27.2:443         FIN_WAIT_1
  TCP    192.168.1.120:53537    52.123.129.254:443     LAST_ACK
```

```
Command Prompt

C:\Users\T470s>netstat -s

IPv4 Statistics

  Packets Received                   = 3738874
  Received Header Errors             = 0
  Received Address Errors            = 104
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 27594
  Received Packets Delivered         = 3783413
  Output Requests                    = 1842952
  Routing Discards                   = 0
  Discarded Output Packets           = 39896
  Output Packet No Route             = 2792
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0
```

ii) **pathping**

Provides information about network latency and network loss at intermediate hops between a source and destination. Pathping sends multiple Echo Request messages to

each router between a source and destination over a period of time and then computes results based on the packets returned from each router.

Command Prompt

```
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

C:\Users\T470s>pathping

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
                [-p period] [-q num_queries] [-w timeout]
                [-4] [-6] target_name

Options:
    -g host-list     Loose source route along host-list.
    -h maximum_hops  Maximum number of hops to search for target.
    -i address       Use the specified source address.
    -n               Do not resolve addresses to hostnames.
    -p period        Wait period milliseconds between pings.
    -q num_queries   Number of queries per hop.
    -w timeout       Wait timeout milliseconds for each reply.
    -4               Force using IPv4.
    -6               Force using IPv6.

C:\Users\T470s>
```

iii) **telnet**

Telnet is software that allows users to remotely access another computer such as a server, network device, or other computer. With telnet users can connect to a device or computer, manage a network device, setup a device, transfer files, etc.

iv) **nslookup**

Displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Before using this tool, you should be familiar with how DNS works. The Nslookup command-line tool is available only if you have installed the TCP/IP protocol.

Command Prompt - nslookup

```
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

C:\Users\T470s>nslookup
Default Server:  UnKnown
Address:  192.168.100.247
```

v) **getmac**

Command used to show both local and remote MAC addresses. When run with no parameters (ie. getmac) it displays MAC addresses for the local system. When run with the /s parameter (eg. getmac /s \\foo) it displays MAC addresses for the remote computer.

When the /v parameter is used, it also displays the associated connection name and network adapter name.

- **getmac /s 192.168.1.1** – Get MAC Address by IP Address
- **getmac /s localhost** – Get local MAC Address

```
C:\Users\T470s>getmac

Physical Address    Transport Name
=================== ==========================================================
8C-16-45-E2-71-14   Media disconnected
20-16-B9-76-0B-8D   \Device\Tcpip_{8D66587B-9679-4A69-B12F-E6850D70345E}
00-50-56-C0-00-01   \Device\Tcpip_{6BE6A27F-1222-4AE2-9B0D-B4BD226F3B8A}
00-50-56-C0-00-08   \Device\Tcpip_{9A5EFBCB-B942-4BF0-A67A-2EB6C4972E4F}

C:\Users\T470s>_
```

vi) **ARP Command**.

Using the arp command allows you to display and modify the Address Resolution Protocol (ARP) cache. An ARP cache is a simple mapping of IP addresses to MAC addresses

Use **arp -a** to see the entire ARP table.

Command Prompt

```
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

C:\Users\T470s>arp -a

Interface: 192.168.238.1 --- 0x9
  Internet Address      Physical Address      Type
  192.168.238.254       00-50-56-e5-4d-da     dynamic
  192.168.238.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  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
```

vii) **Tracert Command:**

Traces the route packets take to reach a destination, showing each "hop" along the way (e.g., tracert google.com).

```
Command Prompt

C:\Users\T470s>tracert www.google.com.pk

Tracing route to www.google.com.pk [172.217.19.195]
over a maximum of 30 hops:

  1   169 ms     3 ms   134 ms  192.168.1.1
  2   172 ms   256 ms   150 ms  ^C
C:\Users\T470s>_
```

viii) nbtstat Command:

Displays NetBIOS over TCP/IP statistics and connections.

Other Useful Commands

```
Command Prompt

C:\Users\T470s>nbtstat

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (adapter status) Lists the remote machine's name table given its name
  -A   (Adapter status) Lists the remote machine's name table given its
                        IP address.
  -c   (cache)          Lists NBT's cache of remote [machine] names and their IP addresses
  -n   (names)          Lists local NetBIOS names.
  -r   (resolved)       Lists names resolved by broadcast and via WINS
  -R   (Reload)         Purges and reloads the remote cache name table
  -S   (Sessions)       Lists sessions table with the destination IP addresses
  -s   (sessions)       Lists sessions table converting destination IP
                        addresses to computer NETBIOS names.
```

ix) net command:

A powerful command for managing various network aspects, including shares, users, and services.

```
C:\Users\T470s>net user

User accounts for \\DESKTOP-F1QMP69

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
T470s                    WDAGUtilityAccount
The command completed successfully.


C:\Users\T470s>
```

x) **route command:**

Displays and modifies the IP routing table.

Command Prompt

```
C:\Users\T470s>route

Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]
                  [MASK netmask]  [gateway] [METRIC metric]  [IF interface]

  -f           Clears the routing tables of all gateway entries.  If this is
               used in conjunction with one of the commands, the tables are
               cleared prior to running the command.

  -p           When used with the ADD command, makes a route persistent across
               boots of the system. By default, routes are not preserved
               when the system is restarted. Ignored for all other commands,
               which always affect the appropriate persistent routes.

  -4           Force using IPv4.

  -6           Force using IPv6.
```

xi) **Systeminfo command**:

Provides detailed information about your system configuration, including network adapters.

```
Command Prompt

C:\Users\T470s>systeminfo

Host Name:                 DESKTOP-F1QMP69
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19045 N/A Build 19045
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          T470s
Registered Organization:
Product ID:                00330-50943-75248-AAOEM
Original Install Date:     21/04/2024, 3:50:09 am
System Boot Time:          28/02/2025, 11:55:06 pm
System Manufacturer:       LENOVO
System Model:              20JTS1GQ15
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 78 Stepping 3 GenuineIntel ~2396 Mhz
BIOS Version:              LENOVO N1WET74W (1.53 ), 26/02/2024
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
```

xii) Hostname command:

Shows your computer's name.

```
Command Prompt

C:\Users\T470s>hostname
DESKTOP-F1QMP69

C:\Users\T470s>
```