Experiment 4

Aim: Observing TCP and UDP using Netstat

Explain common netstat command parameters and outputs.

Theory:

Netstat (Network Statistics) is a command-line network utility tool that provides information about network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. It is widely used for diagnosing network problems and determining network statistics.

Common Netstat Command Parameters

-a: Displays all active connections and listening ports.

-t: Shows only TCP connections.

-u: Shows only UDP connections.

-n: Displays addresses and port numbers in numerical form.

-p: Shows the PID and name of the program to which each socket belongs.

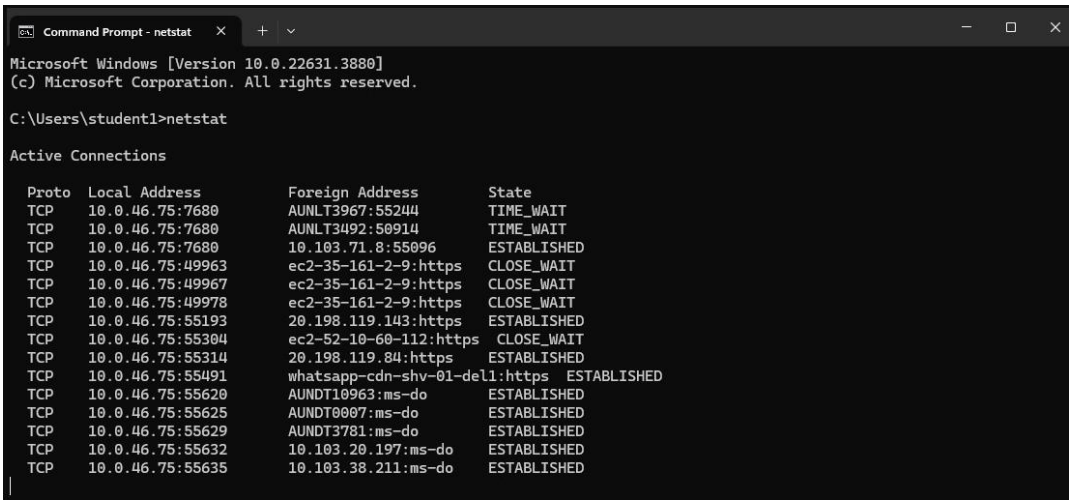
-r: Displays the routing table.

-s: Provides network statistics for each protocol.

-i: Displays a table of all network interfaces.

Observations:

Code was performed in command prompt and here are the screenshots:



```
Command Prompt - netstat
Microsoft Windows [Version 10.0.22631.3880]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student1>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.0.46.75:7680        AUNLT3967:55244        TIME_WAIT
  TCP    10.0.46.75:7680        AUNLT3492:50914        TIME_WAIT
  TCP    10.0.46.75:7680        10.103.71.8:55096      ESTABLISHED
  TCP    10.0.46.75:49963       ec2-35-161-2-9:https   CLOSE_WAIT
  TCP    10.0.46.75:49967       ec2-35-161-2-9:https   CLOSE_WAIT
  TCP    10.0.46.75:49978       ec2-35-161-2-9:https   CLOSE_WAIT
  TCP    10.0.46.75:55193       20.198.119.143:https   ESTABLISHED
  TCP    10.0.46.75:55304       ec2-52-10-60-112:https  CLOSE_WAIT
  TCP    10.0.46.75:55314       20.198.119.84:https    ESTABLISHED
  TCP    10.0.46.75:55491       whatsapp-cdn-shv-01-del1:https  ESTABLISHED
  TCP    10.0.46.75:55620       AUNDT10963:ms-do       ESTABLISHED
  TCP    10.0.46.75:55625       AUNDT0007:ms-do        ESTABLISHED
  TCP    10.0.46.75:55629       AUNDT3781:ms-do        ESTABLISHED
  TCP    10.0.46.75:55632       10.103.20.197:ms-do    ESTABLISHED
  TCP    10.0.46.75:55635       10.103.38.211:ms-do    ESTABLISHED
```

```
Command Prompt - netstat -

  TCP    10.0.46.75:56003       150.171.69.254:https   ESTABLISHED
  TCP    10.0.46.75:56004       13.107.3.254:https     ESTABLISHED
  TCP    10.0.46.75:56005       204.79.197.222:https   ESTABLISHED

C:\Users\student1>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            AUNDT10541:0           LISTENING
  TCP    0.0.0.0:445            AUNDT10541:0           LISTENING
  TCP    0.0.0.0:5040           AUNDT10541:0           LISTENING
  TCP    0.0.0.0:7680           AUNDT10541:0           LISTENING
  TCP    0.0.0.0:8081           AUNDT10541:0           LISTENING
  TCP    0.0.0.0:38000          AUNDT10541:0           LISTENING
  TCP    0.0.0.0:39000          AUNDT10541:0           LISTENING
  TCP    0.0.0.0:49664          AUNDT10541:0           LISTENING
  TCP    0.0.0.0:49665          AUNDT10541:0           LISTENING
  TCP    0.0.0.0:49666          AUNDT10541:0           LISTENING
  TCP    0.0.0.0:49667          AUNDT10541:0           LISTENING
  TCP    0.0.0.0:49670          AUNDT10541:0           LISTENING
  TCP    0.0.0.0:49672          AUNDT10541:0           LISTENING
  TCP    0.0.0.0:49724          AUNDT10541:0           LISTENING
  TCP    0.0.0.0:49736          AUNDT10541:0           LISTENING
  TCP    10.0.46.75:139         AUNDT10541:0           LISTENING
  TCP    10.0.46.75:7680        10.103.41.35:52199     TIME_WAIT
  TCP    10.0.46.75:49963       ec2-35-161-2-9:https   CLOSE_WAIT
  TCP    10.0.46.75:49967       ec2-35-161-2-9:https   CLOSE_WAIT
  TCP    10.0.46.75:49978       ec2-35-161-2-9:https   CLOSE_WAIT
```

```
Command Prompt

  TCP    10.0.46.75:56040       10.101.2.209:7680      TIME_WAIT

C:\Users\student1>netstat -e
Interface Statistics

                           Received            Sent

Bytes                    2011150536       358801104
Unicast packets             543288         1623268
Non-unicast packets          81560            4356
Discards                         0               0
Errors                           0               0
Unknown protocols                0

C:\Users\student1>netstat -u

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-i] [-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.
  -f            Displays Fully Qualified Domain Names (FQDN) for foreign
                addresses.
  -i            Displays the time spent by a TCP connection in its current state.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -q            Displays all connections, listening ports, and bound
                nonlistening TCP ports. Bound nonlistening ports may or may not
                be associated with an active connection.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  -t            Displays the current connection offload state.
  -x            Displays NetworkDirect connections, listeners, and shared
                endpoints.
```

```
Command Prompt

                Cannot be combined with the other options.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display.  Press CTRL+C to stop redisplaying
                statistics.  If omitted, netstat will print the current
                configuration information once.

C:\Users\student1>netstat -s

IPv4 Statistics

  Packets Received                   = 522346
  Received Header Errors             = 0
  Received Address Errors            = 0
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 2640
  Received Packets Delivered         = 520911
  Output Requests                    = 406684
  Routing Discards                   = 0
  Discarded Output Packets           = 1
  Output Packet No Route             = 5
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

IPv6 Statistics

  Packets Received                   = 16166
  Received Header Errors             = 0
  Received Address Errors            = 6
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 12
  Received Packets Delivered         = 17488
  Output Requests                    = 1456
  Routing Discards                   = 0
  Discarded Output Packets           = 0
  Output Packet No Route             = 0
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

ICMPv4 Statistics
```

```
Command Prompt

  UDP    [fe80::495f:231c:9fe0:1bed%6]:61817  *:*

C:\Users\student1>
C:\Users\student1>netstat -r
===========================================================================
Interface List
 13...30 03 c8 96 b9 fd ......Realtek RTL8822CE 802.11ac PCIe Adapter
  4...b2 03 c8 96 b9 fd ......Microsoft Wi-Fi Direct Virtual Adapter
  7...32 03 c8 96 b9 fd ......Microsoft Wi-Fi Direct Virtual Adapter #3
  6...84 69 93 71 73 37 ......Realtek PCIe GbE Family Controller
 16...30 03 c8 96 b9 fe ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      10.0.47.254       10.0.46.75     35
         10.0.46.0    255.255.254.0         On-link        10.0.46.75    291
         10.0.46.75  255.255.255.255         On-link        10.0.46.75    291
        10.0.47.255  255.255.255.255         On-link        10.0.46.75    291
          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
          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        10.0.46.75    291
    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        10.0.46.75    291
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  6    291 fe80::/64                On-link
  6    291 fe80::495f:231c:9fe0:1bed/128
                                    On-link
  1    331 ff00::/8                 On-link
  6    291 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Result: Successfully observed TCP and UDP using Netstat

Experiment 5

Aim:

Part 1: Build and Configure the Network

Part 2: Use Ping Command for Basic Network Testing

Part 3: Use Tracert and Traceroute Commands for Basic Network Testing

Part 4: Troubleshoot the Topology

Theory:

1) Build and Configure the Network:

- Design the topology by adding routers, switches, and PCs.
- Assign IP addresses to devices and configure routing protocols like RIP or OSPF.
- Test connectivity by pinging devices using the command-line interface (CLI).

2) Use Ping Command for Basic Network Testing:

- The ping command tests reachability and measures round-trip time using `ping <destination IP>`.
- Output shows packets sent, received, lost, and round-trip time.
- Verifies device connectivity, checks for packet loss and latency, and identifies unreachable devices.

3) Use Tracert and Traceroute Commands for Basic Network Testing:

- Tracert (Windows) and Traceroute (Linux) determine the path packets take and identify delays.
- Use `tracert <destination IP>` on Windows and `traceroute <destination IP>` on Linux.
- Output lists each hop and round-trip time.
- Maps packet routes, diagnoses network slowdowns, and detects routing issues.

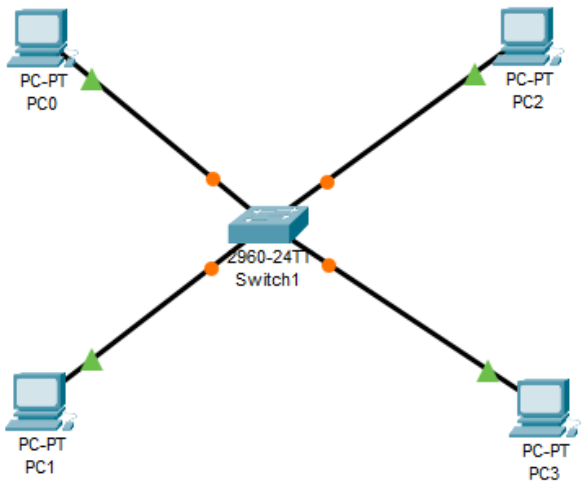
4) Troubleshoot the Topology:

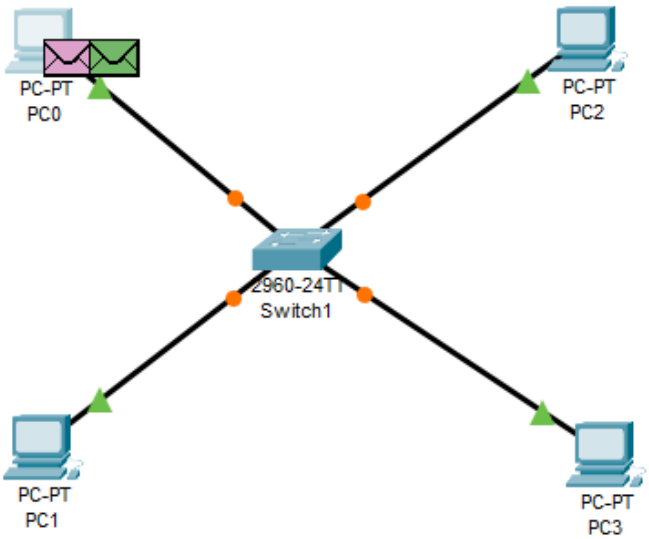
- Identify issues using ping and tracert/traceroute.
- Check configurations like IP addresses, subnet masks, and routing.
- Inspect connections to ensure cables are secure and correct.

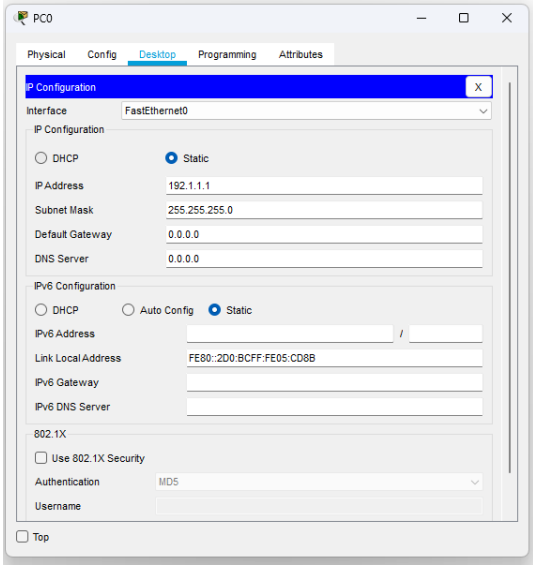
- Examine logs for error messages.
- Resolve problems by reconfiguring devices, replacing cables, or updating routing.

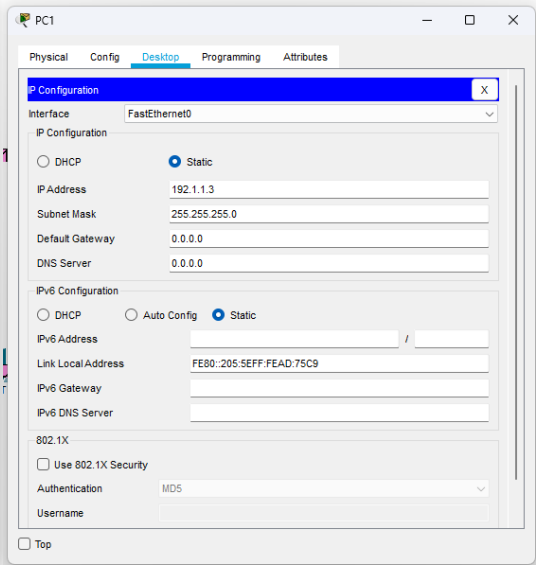
Observations:

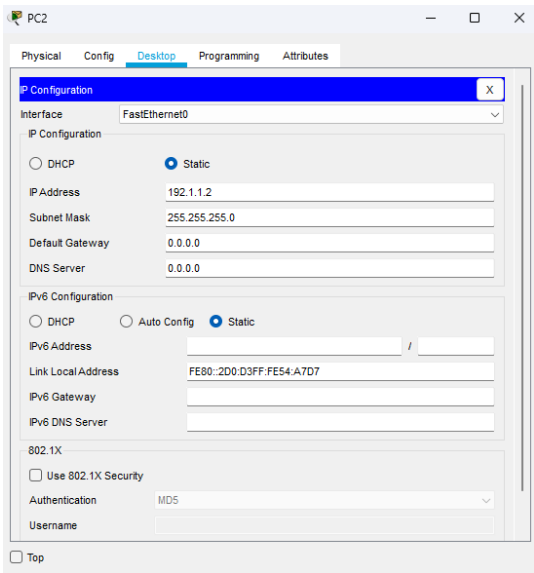
1) : Build and Configure the Network

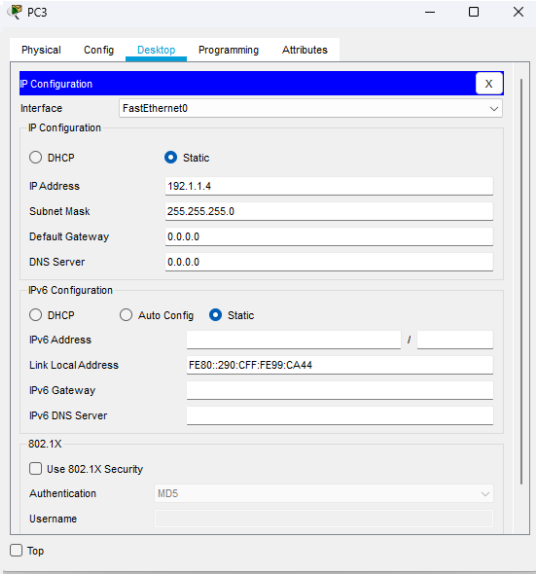




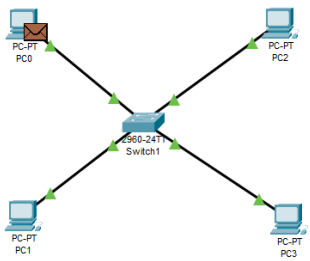


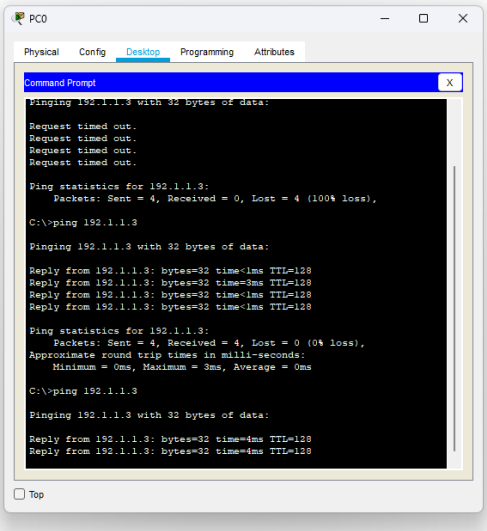


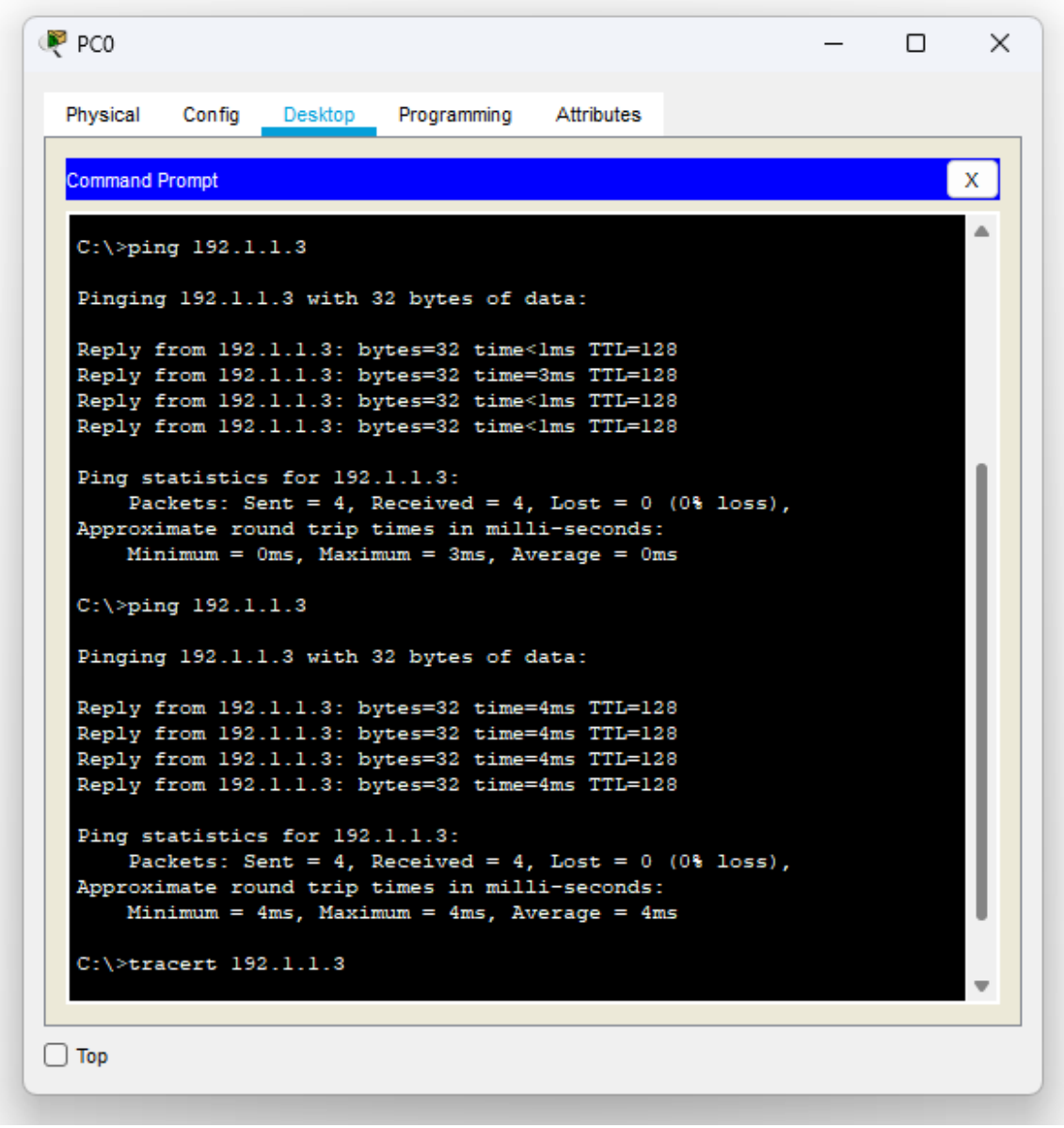




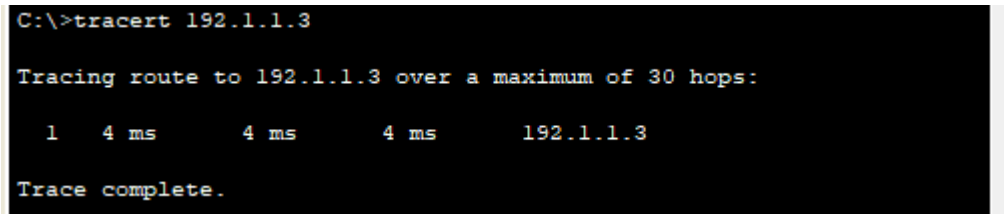
2) Use Ping Command for Basic Network Testing







3) Use Tracert and Traceroute Commands for Basic Network Testing



Result: Successfully performed the following task- Build and Configure the Network, Use Ping Command for Basic Network Testing, Use Tracert and Traceroute Commands for Basic Network Testing, Troubleshoot the Topology.