Genba Sopanrao Moze College of Engineering, Balewadi, Pune-45

Department of Electronics And Telecommunication

Academic year 2022_23

Roll No: **Subject: Control System Lab**

Date : **Staff Sign:**

Experiment no:-2

AIM: Simulating various Networks (LAN, WAN) using relevant network devices on Simulator using Ping, ipconfig / ifconfig, Host name, Whois, Netstat, Route, Tracert /Traceroute /Tracepath, NSlookup ARP, Finger Port Scan, nmap.

REQUIREMENT:

WINDOWS 10 with LAN Connectivity.

Software : Cisco Packet Tracer/ CMD

ALGORITHM:

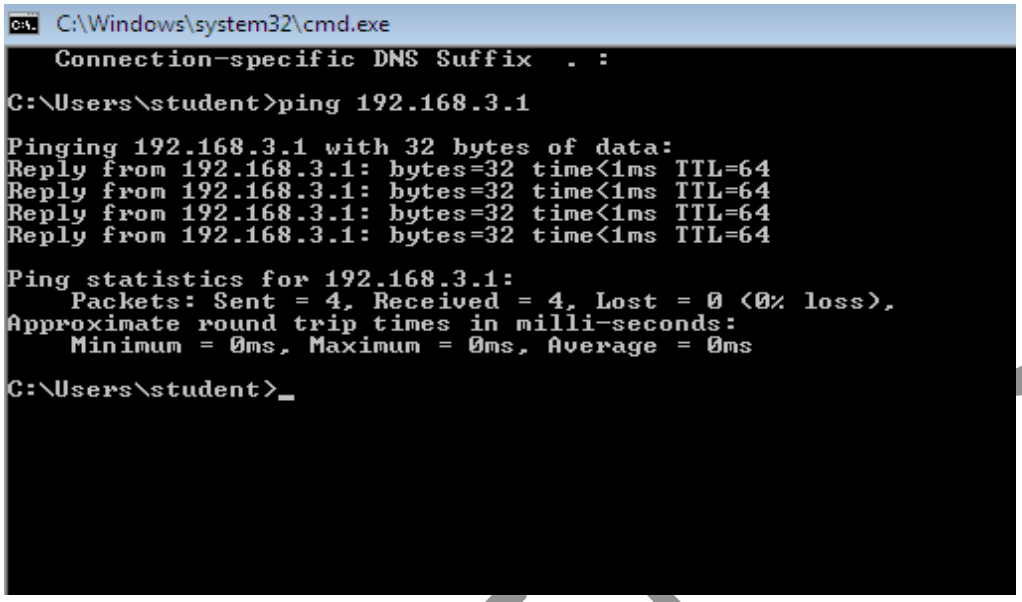
1. Open Command Prompt on your PC and type following Commands.

CONGIURATION USING PACKET TRACER:

1. **Ping**

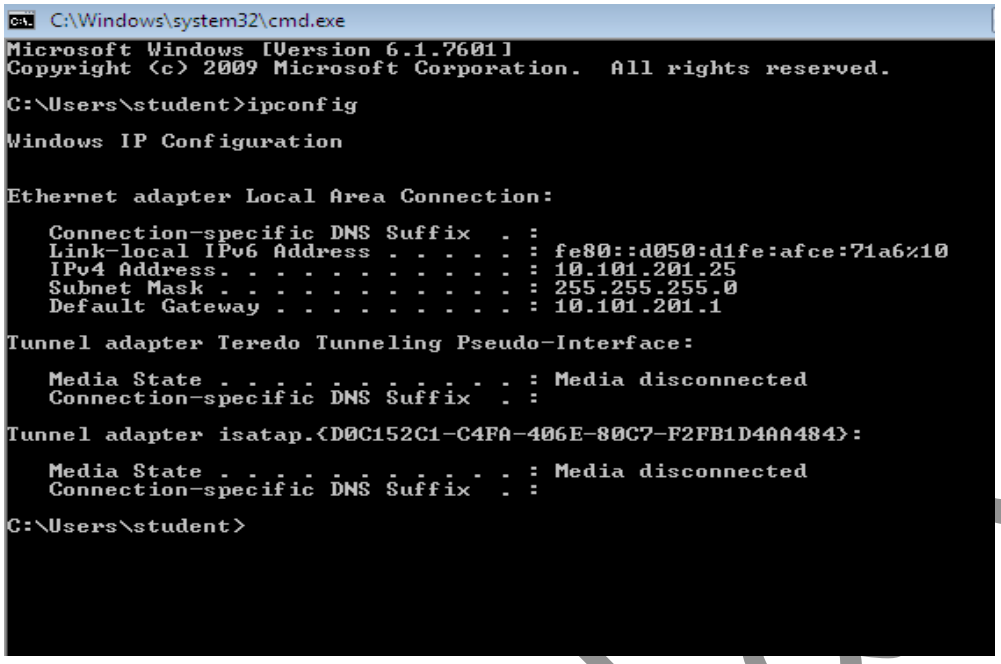
Ping is used to testing a network host capacity to interact with another host. Just enter the command Ping, followed by the target host's name or IP address. The ping utilities seem to be the most common network tool. This is performed by using the Internet Control Message Protocol, which allows the echo packet to be sent to the destination host and a listening mechanism. If

the destination host reply to the requesting host, that means the host is reachable.



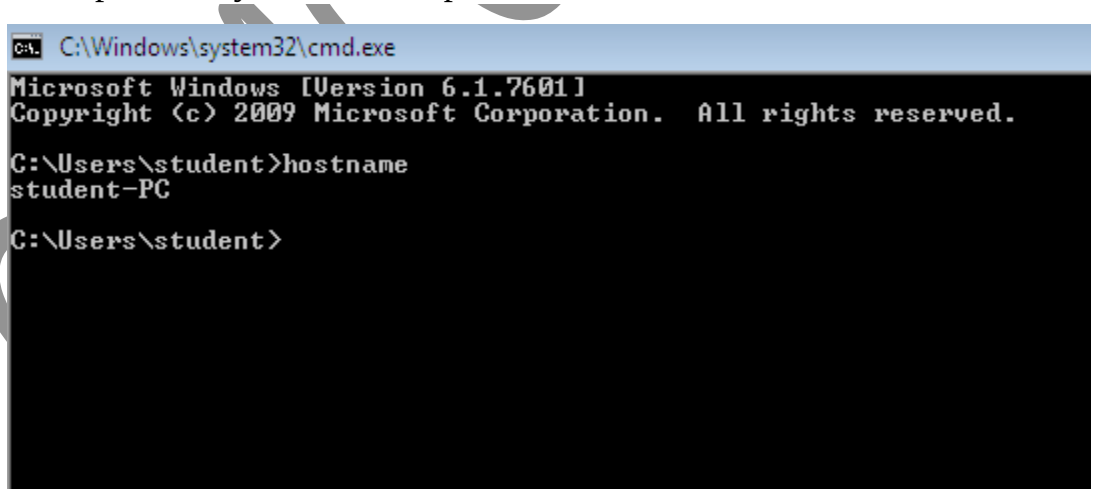
2. Ipconfig/ Ifconfig

The command IP config will display basic details about the device's IP address configuration. Just type IP config in the Windows prompt and the IP, subnet mask and default gateway that the current device will be presented.



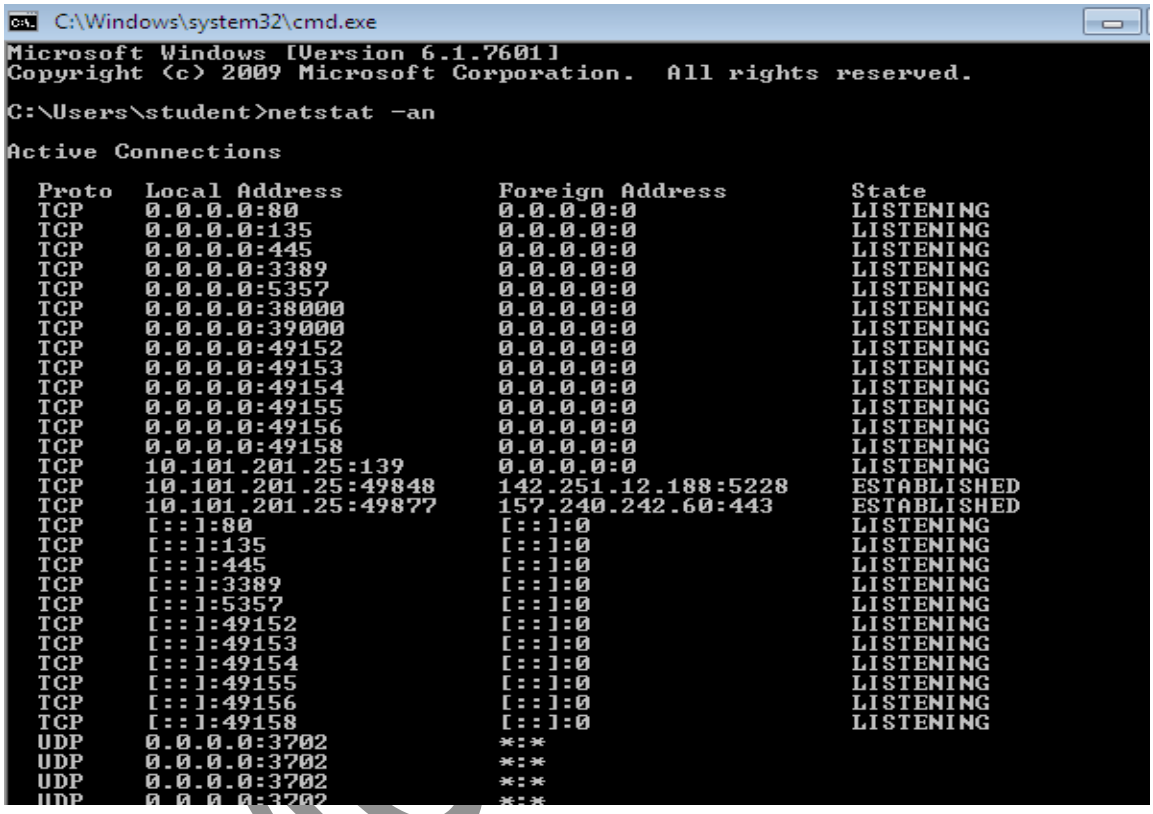
3. Host name

To communicate with each and other, the computer needs a unique address. A hostname can be alphabetic or alphanumeric and contain specific symbols used specifically to define a specific node or device in the network.



4. Netsat

Netstat is a Common TCP – IP networking command-line method present in most Windows, Linux, UNIX, and other operating systems. The netstat provides the statistics and information in the use of the current TCP-IP Connection network about the protocol.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\student>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:38000          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:39000          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49158          0.0.0.0:0              LISTENING
  TCP    10.101.201.25:139      0.0.0.0:0              LISTENING
  TCP    10.101.201.25:49848    142.251.12.188:5228    ESTABLISHED
  TCP    10.101.201.25:49877    157.240.242.60:443     ESTABLISHED
  TCP    [::]:80                [::]:0                 LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:3389              [::]:0                 LISTENING
  TCP    [::]:5357              [::]:0                 LISTENING
  TCP    [::]:49152             [::]:0                 LISTENING
  TCP    [::]:49153             [::]:0                 LISTENING
  TCP    [::]:49154             [::]:0                 LISTENING
  TCP    [::]:49155             [::]:0                 LISTENING
  TCP    [::]:49156             [::]:0                 LISTENING
  TCP    [::]:49158             [::]:0                 LISTENING
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
```

5. Route

In IP networks, routing tables are used to direct packets from one subnet to another. The Route command provides the device's routing tables. To get this result, just type route print. The Route command returns the routing table, and the user can make changes by Commands such as Route Add, Route Delete, and Route Change, which allows modifying the routing table as a requiremen

C:\Windows\system32\cmd.exe

```
C:\Users\student>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. This
               option is not supported in Windows 95.

  -4           Force using IPv4.

  -6           Force using IPv6.

  command      One of these:
                 PRINT     Prints  a route
                 ADD       Adds    a route
                 DELETE    Deletes a route
                 CHANGE    Modifies an existing route
  destination  Specifies the host.
  MASK         Specifies that the next parameter is the 'netmask' value.
  netmask      Specifies a subnet mask value for this route entry.
               If not specified, it defaults to 255.255.255.255.
  gateway      Specifies gateway.
  interface    the interface number for the specified route.
  METRIC       specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Pattern match is only allowed in PRINT command.
Diagnostic Notes:
    Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
    Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
             The route addition failed: The specified mask parameter is invalid.
 (Destination & Mask) != Destination.

Examples:

    > route PRINT
```

C:\Windows\system32\cmd.exe

```
    > route DELETE 3ffe::/32

C:\Users\student>route print
===========================================================================
Interface List
 10...8c 89 a5 7b 92 3f ......Realtek PCIe GBE Family Controller
  1...........................Software Loopback Interface 1
 15...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
 13...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     10.101.201.1    10.101.201.25     20
     10.101.201.0    255.255.255.0         On-link     10.101.201.25    276
    10.101.201.25  255.255.255.255         On-link     10.101.201.25    276
   10.101.201.255  255.255.255.255         On-link     10.101.201.25    276
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link     10.101.201.25    276
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link     10.101.201.25    276
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    306 ::1/128                  On-link
 10    276 fe80::/64                On-link
 10    276 fe80::d050:d1fe:afce:71a6/128
                                    On-link
  1    306 ff00::/8                 On-link
 10    276 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None

C:\Users\student>
```

6. Tracert

The tracert command is a Command Prompt command which is used to get the network packet being sent and received and the number of hops required for that packet to reach to target. This command can also be referred to as a traceroute. It provides several details about the path that a packet takes from the source to the specified destination.

```
C:\Users\student>rout table
'rout' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\student>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2     *        *        1 ms  103.243.115.173
  3   105 ms    97 ms    98 ms  nsg-static-105.23.76.182-airtel.com [182.76.23.1
05]
  4     *      101 ms   105 ms  116.119.57.24
  5     *        6 ms     5 ms  72.14.212.48
  6     *        *       54 ms  216.239.57.17
  7     *        *        *     Request timed out.
  8   114 ms     *      134 ms  dns.google [8.8.8.8]

Trace complete.

C:\Users\student>
```

C:\Windows\system32\cmd.exe

```
C:\Users\student>tracert google.com

Tracing route to google.com [142.250.76.206]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2     *        *        *     Request timed out.
  3    98 ms   111 ms   131 ms  nsg-static-105.23.76.182-airtel.com [182.76.23.1
05]
  4   101 ms   101 ms     *     116.119.57.24
  5     5 ms     *        *     72.14.212.48
  6     *        6 ms     *     172.253.69.227
  7     *      102 ms   102 ms  74.125.253.167
  8   101 ms   101 ms   102 ms  bom12s10-in-f14.1e100.net [142.250.76.206]

Trace complete.

C:\Users\student>
```

7. NSlookup

The Nslookup, which stands for name server lookup command, is a network utility command used to obtain information about internet servers. It provides name server information for the DNS (Domain Name System), i.e. the default DNS server's name and IP Address.

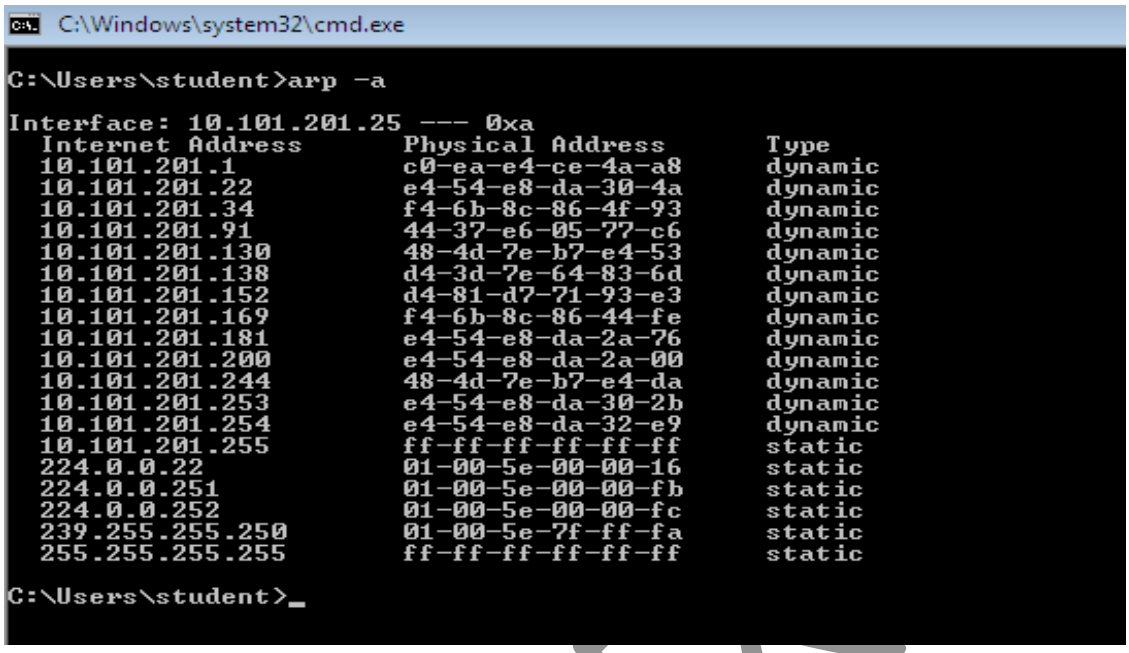
```
Trace complete.

C:\Users\student>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server:  UnKnown
Address:  fe80::be22:28ff:fe3b:7e3d

>
```

8. ARP

ARP stands for Address Resolution Protocol. Although network communications can readily be thought of as an IP address, the packet delivery depends ultimately on the media access control (MAC). This is where the protocol for address resolution comes into effect. You can add the remote host IP address, which is an arp -a command, in case you have issues to communicate with a given host. The ARP command provides information like Address, Flags, Mask, IFace, Hardware Type, Hardware Address, etc.



```
C:\Windows\system32\cmd.exe

C:\Users\student>arp -a

Interface: 10.101.201.25 --- 0xa
  Internet Address      Physical Address      Type
  10.101.201.1          c0-ea-e4-ce-4a-a8     dynamic
  10.101.201.22         e4-54-e8-da-30-4a     dynamic
  10.101.201.34         f4-6b-8c-86-4f-93     dynamic
  10.101.201.91         44-37-e6-05-77-c6     dynamic
  10.101.201.130        48-4d-7e-b7-e4-53     dynamic
  10.101.201.138        d4-3d-7e-64-83-6d     dynamic
  10.101.201.152        d4-81-d7-71-93-e3     dynamic
  10.101.201.169        f4-6b-8c-86-44-fe     dynamic
  10.101.201.181        e4-54-e8-da-2a-76     dynamic
  10.101.201.200        e4-54-e8-da-2a-00     dynamic
  10.101.201.244        48-4d-7e-b7-e4-da     dynamic
  10.101.201.253        e4-54-e8-da-30-2b     dynamic
  10.101.201.254        e4-54-e8-da-32-e9     dynamic
  10.101.201.255        ff-ff-ff-ff-ff-ff     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

C:\Users\student>_
```

Result Printouts:

CONCLUSION: