T.E SEM-VI E&TC Jan-May, 24

Subject Code: ECL602

Computer Communication Network Laboratory

Sr. no	Title
1	Basic Networking commands
2	Basic LAN network using Cisco Packet Tracer (CPT)
3	Configuration and comparison of network topologies using CPT
4	Configuration of static routes in a network using CPT
5	Configuration of a network with RIP using CPT
6	Classification of IP addresses using Octave
7	DNS server configuration using CPT
8	Subnetting using CPT
9	HDLC bit stuffing and de-stuffing using C++
10	Assignments

Exp-no 1

Aim: Study of basic networking commands and Network configuration Commands

Theory:

Networking means a transfer of information between two or more computers connected by a physical or non-physical link.

Networking commands are tools used in command line interfaces to execute various network tasks. They allow users to diagnose network problems, modify network settings, transfer files, and establish distant connections. These commands provide essential functionality for network administrators and trouble shooters, allowing for efficient network control and troubleshooting. Networking commands are essential tools for managing and troubleshooting computer networks. From assessing connectivity with "ping" to configuring interfaces using "if config" or "ipconfig," these commands provide crucial insights.

Commands such as "nslookup," is used for resolving Domain Name system or securing connections with "ssh," mastering these tools is fundamental for effective network administration.

Basic networking commands:

Ping

It is one of the basic networking commands to test the connection between the local machine and the host server.

This command sends a small amount of data to the host server, and in return, the host server sends a reply to the computer.

Information like the IP address of the host server, the amount of data sent, time to live, and time needed for sending and receiving the data are recorded and displayed to the user.

```
C:\Users\USER>ping www.codingninjas.com

Pinging www.codingninjas.com [54.230.65.11] with 32 bytes of data:
Reply from 54.230.65.11: bytes=32 time=9ms TTL=248
Reply from 54.230.65.11: bytes=32 time=8ms TTL=248
Reply from 54.230.65.11: bytes=32 time=8ms TTL=248
Reply from 54.230.65.11: bytes=32 time=8ms TTL=248

Ping statistics for 54.230.65.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 9ms, Average = 8ms
```

-a

The "-a" option resolves the hostname to the respective IP address.

```
C:\Users\USER>ping -a www.codingninjas.com

Pinging www.codingninjas.com [54.230.65.72] with 32 bytes of data:
Reply from 54.230.65.72: bytes=32 time=17ms TTL=246
Reply from 54.230.65.72: bytes=32 time=17ms TTL=246
Reply from 54.230.65.72: bytes=32 time=17ms TTL=246
Reply from 54.230.65.72: bytes=32 time=17ms TTL=246

Ping statistics for 54.230.65.72:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 17ms, Average = 17ms
```

-w timeout

The option "-w timeout" sets the timeout, the time after which the data packet will be rejected for each ping. The timeout is in milliseconds.

```
C:\Users\USER>ping -w 20 www.codingninjas.com

Pinging www.codingninjas.com [54.230.65.10] with 32 bytes of data:
Reply from 54.230.65.10: bytes=32 time=9ms TTL=248
Reply from 54.230.65.10: bytes=32 time=8ms TTL=248
Reply from 54.230.65.10: bytes=32 time=9ms TTL=248
Reply from 54.230.65.10: bytes=32 time=11ms TTL=248

Ping statistics for 54.230.65.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 11ms, Average = 9ms
```

ipconfig

This gives information about the IP address. It not only gives the IP address of the computer it is executed on but also much more information as DNS addresses are stored in the

cache. It has options to show even the computer's MAC address, renew the IP address, release the current IP address, flush the DNS cache, and help.

```
C:\Users\USER>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1f6e:8b00:a1ed:a25a%17
   IPv4 Address. . . . . . . . . . . : 192.168.124.51
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Default Gateway . . . . . . . . . : 192.168.124.1

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Address Resolution Protocol (ARP)

This command is used to display and modify the IP to the physical address translation table used by the address resolution protocol.

It has many options, of which a few are to display current ARP entries, specify an internet address, delete a host in the ARP table, specify a physical address, and many more.

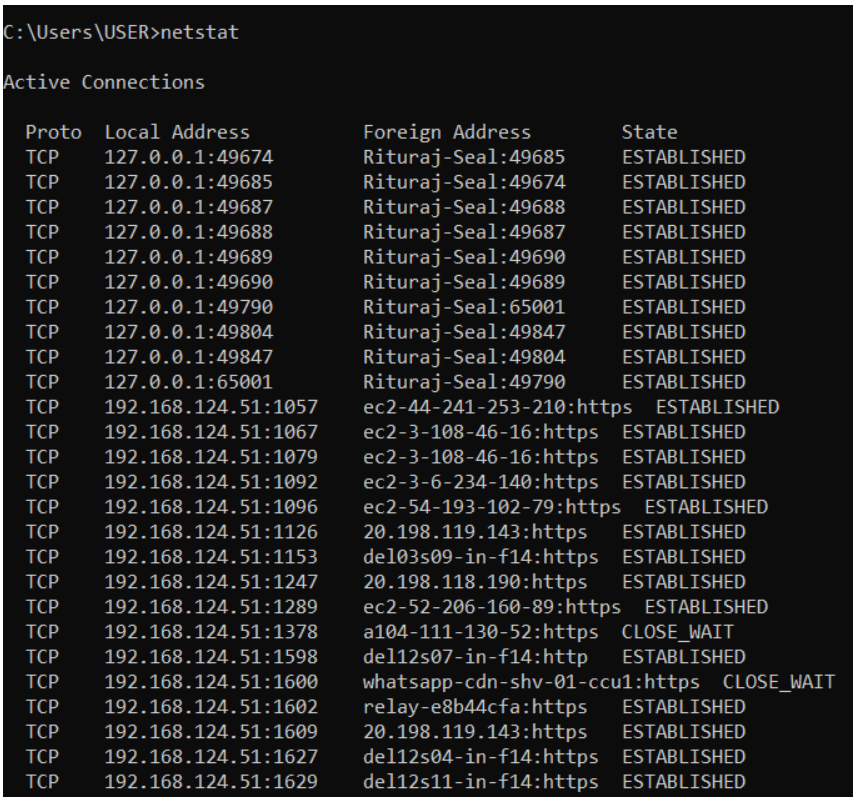
-a

The "-a" command in arp displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and physical addresses for only the specified computer are displayed.

```
C:\Users\USER>arp -a

Interface: 192.168.124.51 --- 0x11
  Internet Address      Physical Address      Type
  192.168.124.1         24-e9-b3-70-3b-bf     dynamic
  192.168.124.13        c0-3e-ba-29-2b-e6     dynamic
  192.168.124.94        d4-81-d7-b3-4c-85     dynamic
  192.168.124.171       50-eb-f6-2f-95-d1     dynamic
  192.168.124.196       cc-32-e5-8f-21-d7     dynamic
  192.168.124.207       e0-1c-fc-f3-76-ad     dynamic
  192.168.125.107       f4-69-d5-c4-bc-45     dynamic
  192.168.125.168       4c-eb-bd-64-60-c7     dynamic
  192.168.125.180       80-3f-5d-d2-19-77     dynamic
  192.168.125.187       30-24-a9-a3-c3-c5     dynamic
  192.168.126.45        c8-4d-44-25-b5-a4     dynamic
  192.168.126.157       00-e0-6c-38-ff-56     dynamic
  192.168.126.209       24-4b-fe-88-5f-bc     dynamic
  192.168.126.213       00-e0-4f-68-ff-cb     dynamic
  192.168.126.228       5c-a6-e6-b6-27-90     dynamic
  192.168.127.253       c0-c9-e3-7a-3d-45     dynamic
  192.168.127.255       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
  224.0.0.113           01-00-5e-00-00-71     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  230.0.0.1             01-00-5e-00-00-01     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Netstat

This command displays the connections active on the computer and the ports the computer is listening to. The command displays the four parameters: proto, local address, foreign address, and state. The proto column shows the type of connection, and the local address shows the IP address and the port number of the connection local machine. The proto column also indicates the foreign address, specifies the IP address and port number of the connection in the host server, and the state shows whether the connection is established or not.



```
C:\Users\USER>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49674        Rituraj-Seal:49685     ESTABLISHED
  TCP    127.0.0.1:49685        Rituraj-Seal:49674     ESTABLISHED
  TCP    127.0.0.1:49687        Rituraj-Seal:49688     ESTABLISHED
  TCP    127.0.0.1:49688        Rituraj-Seal:49687     ESTABLISHED
  TCP    127.0.0.1:49689        Rituraj-Seal:49690     ESTABLISHED
  TCP    127.0.0.1:49690        Rituraj-Seal:49689     ESTABLISHED
  TCP    127.0.0.1:49790        Rituraj-Seal:65001     ESTABLISHED
  TCP    127.0.0.1:49804        Rituraj-Seal:49847     ESTABLISHED
  TCP    127.0.0.1:49847        Rituraj-Seal:49804     ESTABLISHED
  TCP    127.0.0.1:65001        Rituraj-Seal:49790     ESTABLISHED
  TCP    192.168.124.51:1057    ec2-44-241-253-210:https  ESTABLISHED
  TCP    192.168.124.51:1067    ec2-3-108-46-16:https  ESTABLISHED
  TCP    192.168.124.51:1079    ec2-3-108-46-16:https  ESTABLISHED
  TCP    192.168.124.51:1092    ec2-3-6-234-140:https  ESTABLISHED
  TCP    192.168.124.51:1096    ec2-54-193-102-79:https  ESTABLISHED
  TCP    192.168.124.51:1126    20.198.119.143:https   ESTABLISHED
  TCP    192.168.124.51:1153    del03s09-in-f14:https  ESTABLISHED
  TCP    192.168.124.51:1247    20.198.118.190:https   ESTABLISHED
  TCP    192.168.124.51:1289    ec2-52-206-160-89:https  ESTABLISHED
  TCP    192.168.124.51:1378    a104-111-130-52:https  CLOSE_WAIT
  TCP    192.168.124.51:1598    del12s07-in-f14:http   ESTABLISHED
  TCP    192.168.124.51:1600    whatsapp-cdn-shv-01-ccu1:https  CLOSE_WAIT
  TCP    192.168.124.51:1602    relay-e8b44cfa:https   ESTABLISHED
  TCP    192.168.124.51:1609    20.198.119.143:https   ESTABLISHED
  TCP    192.168.124.51:1627    del12s04-in-f14:https  ESTABLISHED
  TCP    192.168.124.51:1629    del12s11-in-f14:https  ESTABLISHED
```

Tracert

The tracert command traces the route from a computer to a host server. It traces the connection for a fixed maximum number of hops. It is one of the basic networking commands. It is used to diagnose path-related problems. The information it displays about the connection route includes the IP addresses for each intermediate server and 3 round trips for each server.

Also used to resolve names of intermediate server IP addresses, the maximum number of hops in the path, and the maximum amount of time to wait for a reply.

```
C:\Users\USER>tracert www.codingninjas.com

Tracing route to www.codingninjas.com [54.230.65.72]
over a maximum of 30 hops:

  1    27 ms    <1 ms    18 ms  192.168.124.1
  2     2 ms     2 ms     2 ms  192.168.5.20
  3     4 ms     3 ms     4 ms  118.185.152.161
  4    18 ms    17 ms    16 ms  42.104.78.22
  5    20 ms    18 ms    18 ms  182.19.111.41
  6    17 ms     *       17 ms  99.83.89.252
  7    17 ms     *       22 ms  150.222.220.84
  8    34 ms    19 ms    18 ms  150.222.220.231
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14    17 ms    16 ms    16 ms  server-54-230-65-72.ccu50.r.cloudfront.net [54.230.65.72]

Trace complete.
```

-d

The "-d" option tells the tracert not no resolve the IP addresses to hostnames.

```
C:\Users\USER>tracert -d www.codingninjas.com

Tracing route to www.codingninjas.com [54.230.65.10]
over a maximum of 30 hops:

  1     3 ms    <1 ms    <1 ms  192.168.124.1
  2     2 ms     2 ms     2 ms  192.168.5.20
  3     4 ms     3 ms     3 ms  118.185.152.161
  4    20 ms     *       18 ms  42.104.78.22
  5    20 ms    20 ms    20 ms  182.19.111.41
  6    18 ms    21 ms    24 ms  99.83.89.252
  7    23 ms    18 ms    19 ms  150.222.220.84
  8    21 ms    20 ms    21 ms  150.222.220.231
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14    20 ms    20 ms    20 ms  54.230.65.10

Trace complete.
```

-h maximum_hops

The "-h maximum_hops" option sets the maximum number of hops for which the tracert command will trace the connection.

```
C:\Users\USER>tracert -h 20  www.codingninjas.com

Tracing route to www.codingninjas.com [54.230.65.72]
over a maximum of 20 hops:

  1     1 ms    <1 ms     4 ms  192.168.124.1
  2     2 ms     2 ms     1 ms  192.168.5.20
  3     4 ms     3 ms     3 ms  118.185.152.161
  4    16 ms    18 ms    18 ms  42.104.78.22
  5    23 ms    18 ms    18 ms  182.19.111.41
  6    16 ms    16 ms    16 ms  99.83.89.252
  7    17 ms    16 ms    16 ms  150.222.220.84
  8    20 ms    18 ms    20 ms  150.222.220.231
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14    16 ms    17 ms    16 ms  server-54-230-65-72.ccu50.r.cloudfront.net [54.230.65.72]

Trace complete.
```

-w timeout

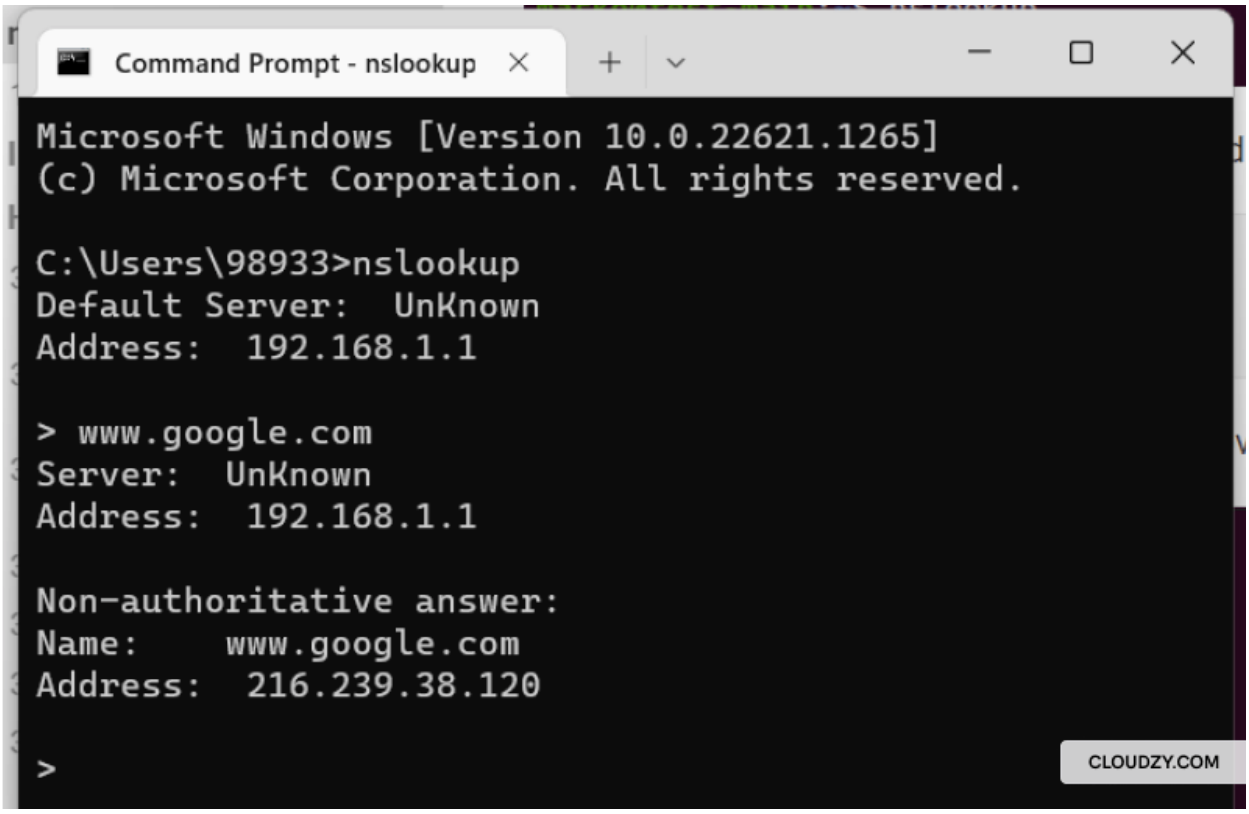
The "-w timeout" option sets the timeout time for each reply.

```
C:\Users\USER>tracert -w 50 www.codingninjas.com

Tracing route to www.codingninjas.com [54.230.65.102]
over a maximum of 30 hops:

  1    19 ms    14 ms     5 ms  192.168.124.1
  2     2 ms     2 ms     2 ms  192.168.5.20
  3     2 ms     2 ms     2 ms  14.139.216.97
  4     3 ms     5 ms     3 ms  10.134.7.113
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7    32 ms    31 ms    32 ms  10.119.234.162
  8    32 ms    32 ms    33 ms  136.232.148.177.static.jio.com [136.232.148.177]
  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     *        *        *     Request timed out.
 19    55 ms    56 ms    56 ms  server-54-230-65-102.ccu50.r.cloudfront.net [54.230.65.102]

Trace complete.
```

NsLookup

The NsLookup command is a command-line utility. It is used in networking to query the Domain Name System (DNS). Then it obtains information about domain names, IP addresses, and other DNS-related data. When you run the NsLookup command followed by a domain name or IP

address, it will display the corresponding DNS records associated with that domain or IP. This command is commonly used to troubleshoot DNS-related issues, check DNS resolution, and gather information about domain configurations.



HostName

The Host Name command is used to display the host name of the computer or device in a network. When you run the Host Name command in a command prompt or terminal, it will return the name assigned to the device on the local network. The host name is a unique identifier used to distinguish devices in a network and is used in various networking protocols and configurations.

SystemInfo

The SystemInfo command is used to retrieve detailed information about the hardware and software configuration of a Windows-based computer. When you run the SystemInfo command in a command prompt, it will display a comprehensive report containing information. It will display the operating system version, system manufacturer, processor details, memory size, network adapter details, and more. This command is helpful for system administrators and users to gather system-related information and diagnose issues.

-d
The "-d" option tells the tracert not no resolve the IP addresses to hostnames.

-h maximum_hops
The "-h maximum_hops" option sets the maximum number of hops for which the tracert command will trace the connection.

-w timeout
The "-w timeout" option sets the timeout time for each reply.

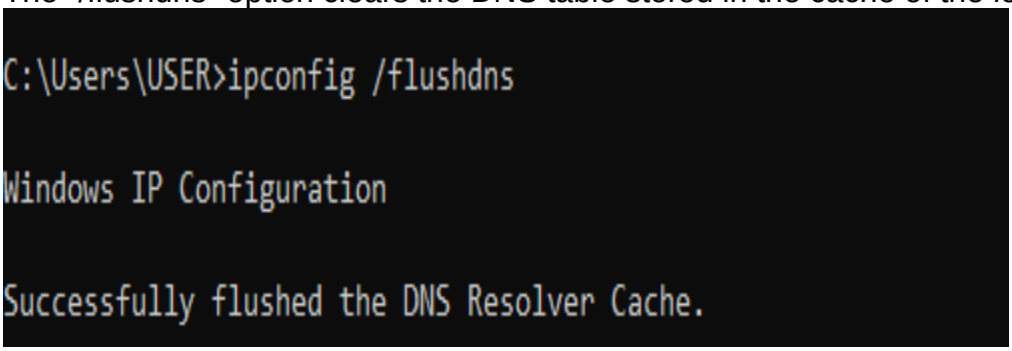
Ipconfig

As the command name suggests, it gives information about the IP address. It not only gives the IP address of the computer it is executed on but also much more information as DNS addresses are stored in the cache.

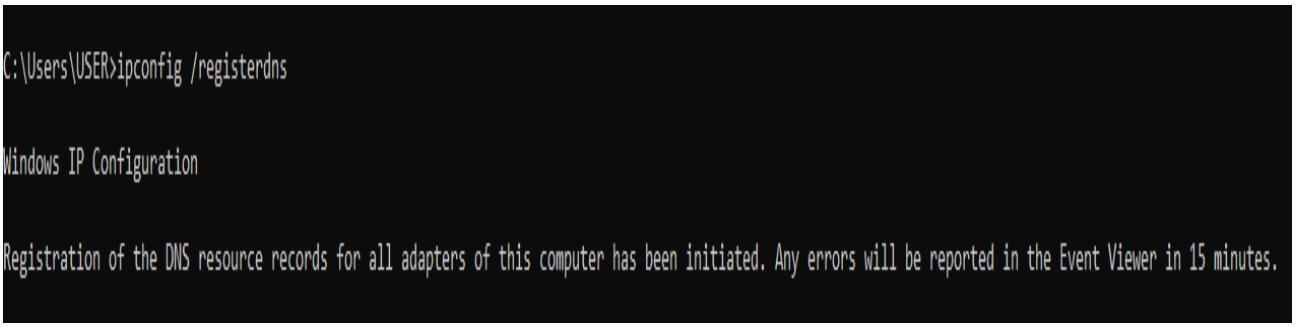
/all
The "/all" option of the ipconfig command displays the full configuration information.

```
C:\Users\USER>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Rituraj-Seal
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : C8-B2-9B-17-3B-81
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : CA-B2-9B-17-3B-80
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek Gaming GbE Family Controller
   Physical Address. . . . . . . . . : 84-2A-FD-70-3C-D9
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::1f6e:8b00:a1ed:a25a%17(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.124.51(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Default Gateway . . . . . . . . . : 192.168.124.1
   DHCPv6 IAID . . . . . . . . . . . : 260319997
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-99-9A-85-84-2A-FD-70-3C-D9
   DNS Servers . . . . . . . . . . . : 192.168.5.20
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
   Physical Address. . . . . . . . . : A6-DA-77-B2-1E-6B
   DHCP Enabled. . . . . . . . . . . : Yes
```

/flushdns
The "/flushdns" option clears the DNS table stored in the cache of the local machine



/registerdns
The "/registerdns" option refreshes all DHCP leases and re-registers the DNS names in the local machine's cache.



Conclusion: Basic networking commands were studied.

Experiment No. 2

To find the class of a given IP address.

Software tools : Matlab/ Octave

Theory: In classified addressing, number of bits allotted for host and network are as per the following table.

Class	Number of Network bits	Number of Host bits
A	8	24
B	16	16
C	24	8

Class D is used for multicasting
Class E is reserved for research purpose

The bit pattern of the first byte determines the IP address:
X denotes 0 or 1. It has no impact on classification

Class	BIT PATTERN
A	0xxx xxxx
B	10xx xxxx
C	110x xxxx
D	1110 xxxx
E	1111 0xxx

In decimal notation the range for first byte is

Class A : 0 – 127
Class B : 128 -191
Class C : 192 – 223
Class D : 224 -239
Class E : 240 -255