Department of Computer Engineering

Class: S.Y. B.Tech. **Semester: IV**

Course Code: DJ19CEL405 **Course Name: Computer Networks Lab**

Name: Varun Viswanath **SAP ID: 60004210105**

Date of Performance: 20/2/23 **Date of Submission: 27/2/23**

Experiment No: 2

Aim: To study different networking commands.

Theory:

1. **Ifconfig/ipconfig:**

Introduction:

In Windows, ipconfig is a console application designed to run from the Windows command prompt. **IPCONFIG** stands for **Internet Protocol Configuration**. This is a command-line application which displays all the current TCP/IP (Transmission Control Protocol/Internet Protocol) network configuration, refreshes the DHCP (Dynamic Host Configuration Protocol) and DNS (Domain Name Server). It also displays IP address, subnet mask, and default gateway for all adapters. This utility allows you to get the IP address information of a Windows computer. It also allows some control over your network adapters, IP addresses (DHCP-assigned specifically), even your DNS cache.

Ipconfig /all

This option displays the same IP addressing information for each adapter as the default option. Additionally, it displays DNS and WINS settings for each adapter as well as a whole host of additional information.

Department of Computer Engineering

Class: S.Y. B.Tech. **Semester: IV**

Course Code: DJ19CEL405 **Course Name: Computer Networks Lab**

Output:

```
C:\Users\djsce.student>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6c69:a5c8:9d73:8517%7
   IPv4 Address. . . . . . . . . . . : 10.120.63.75
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.120.63.1

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c7e1:ceb5:f86d:af5f%16
   IPv4 Address. . . . . . . . . . . : 192.168.58.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1c22:3167:4b09:7572%19
   IPv4 Address. . . . . . . . . . . : 192.168.175.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::eecb:9c02:2871:151b%14
   IPv4 Address. . . . . . . . . . . : 10.120.113.22
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 10.120.112.1
```

2. Netstat:

Introduction:

The netstat command, meaning *network statistics*, is a Command Prompt command used to display *very* detailed information about how your computer is communicating with other computers or network devices.

Specifically, it can show details about individual network connections, overall and protocol-specific networking statistics, and much more, all of which could help troubleshoot certain kinds of networking issues.

It executes the netstat command alone to show a relatively simple list of all active TCP connections which, for each one, will show the local IP address (your computer), the foreign IP address (the other computer or network device), along with their respective port numbers, as well as the TCP state.

-a:

This switch displays active TCP connections, TCP connections with the listening state, as well as UDP ports that are being listened to.

Output:

```
C:\Users\djsce.student>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.120.113.22:56538    a184-84-201-22:https   CLOSE_WAIT
  TCP    10.120.113.22:56539    a-0001:https           CLOSE_WAIT
  TCP    10.120.113.22:56623    a-0001:https           CLOSE_WAIT
  TCP    10.120.113.22:56624    a184-28-173-136:https  CLOSE_WAIT
  TCP    10.120.113.22:56626    131.253.33.254:https   CLOSE_WAIT
  TCP    10.120.113.22:56627    52.123.129.254:https   CLOSE_WAIT
  TCP    10.120.113.22:56628    13.107.6.254:https     CLOSE_WAIT
  TCP    10.120.113.22:56629    204.79.197.222:https   CLOSE_WAIT
  TCP    10.120.113.22:56713    199.232.254.137:https  ESTABLISHED
  TCP    10.120.113.22:56716    216.239.32.178:https   TIME_WAIT
  TCP    10.120.113.22:56749    20.198.118.190:https   ESTABLISHED
  TCP    10.120.113.22:56752    a184-28-173-123:https  CLOSE_WAIT
  TCP    10.120.113.22:56762    a23-35-6-201:https     CLOSE_WAIT
  TCP    10.120.113.22:56773    a184-28-173-97:https   CLOSE_WAIT
  TCP    10.120.113.22:56774    a184-28-173-97:https   CLOSE_WAIT
  TCP    10.120.113.22:56775    a184-28-173-97:https   CLOSE_WAIT
  TCP    10.120.113.22:56843    146:https              TIME_WAIT
  TCP    10.120.113.22:56894    sc-in-f154:https       TIME_WAIT
  TCP    10.120.113.22:56933    bom12s16-in-f4:https   TIME_WAIT
  TCP    10.120.113.22:56954    104.18.14.10:https     ESTABLISHED
  TCP    127.0.0.1:49682        MUM0922CPU0385:49683   ESTABLISHED
  TCP    127.0.0.1:49683        MUM0922CPU0385:49682   ESTABLISHED
  TCP    127.0.0.1:49744        MUM0922CPU0385:49745   ESTABLISHED
  TCP    127.0.0.1:49745        MUM0922CPU0385:49744   ESTABLISHED
  TCP    127.0.0.1:49746        MUM0922CPU0385:49747   ESTABLISHED
  TCP    127.0.0.1:49747        MUM0922CPU0385:49746   ESTABLISHED
```

3. Ping:

Introduction:

A ping (Packet Internet or Inter-Network Groper) is a basic Internet program that allows a user to test and verify if a particular destination IP address exists and can accept requests in computer network administration. The acronym was contrived to match the submariners' term for the sound of a returned sonar pulse.

Ping is also used diagnostically to ensure that a host computer the user is trying to reach is operating. Any operating system (OS) with networking capability, including most embedded network administration software, can use ping.

Output:

```
C:\Users\djsce.student>ping -t 10.120.63.75

Pinging 10.120.63.75 with 32 bytes of data:
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128
Reply from 10.120.63.75: bytes=32 time<1ms TTL=128

Ping statistics for 10.120.63.75:
    Packets: Sent = 21, Received = 21, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
```

4. **Pathping:**

Introduction:

PathPing is a Windows utility allowing the user to reveal the path between two hosts. Unlike other similar commands, with PathPing, each node is pinged by the command. Pathping resembles some other commands such as one called tracert that displays the trajectory of data packets and measures delivery delays through an IP network.

Output:

```
C:\Users\djsce.student>pathping 10.120.63.75

Tracing route to MUM0922CPU0385.SVKMGRP.COM [10.120.63.75]
over a maximum of 30 hops:
  0  MUM0922CPU0385.SVKMGRP.COM [10.120.63.75]
  1  MUM0922CPU0385.SVKMGRP.COM [10.120.63.75]

Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           MUM0922CPU0385.SVKMGRP.COM [10.120.63.75]
                                 0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  MUM0922CPU0385.SVKMGRP.COM [10.120.63.75]

Trace complete.
```

5. NSlookup:

Introduction:

The nslookup command queries internet domain name servers in two modes. Interactive mode allows you to query name servers for information about various hosts and domains, or to print a list of the hosts in a domain. In noninteractive mode, the names and requested information are printed for a specified host or domain.

The nslookup command enters interactive mode when no arguments are given, or when the first argument is a - (minus sign) and the second argument is the host name or internet address of a name server. When no arguments are given, the command queries the default name server. The nslookup command enters non-interactive mode when you give the name or internet address of the host to be looked up as the first argument. The optional second argument specifies the host name or address of a name server.

Output:

```
C:\Users\djsce.student>nslookup google.com
Server:  MUMDC-PRIM.SVKMGRP.COM
Address:  192.168.2.51

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4009:826::200e
          142.250.183.206
```

6. Hostname:

Introduction:

hostname command in Linux is used to obtain the DNS(Domain Name System) name and set the system's hostname or NIS(Network Information System) domain name. A hostname is a name which is given to a computer and it attached to the network. Its main purpose is to uniquely identify over a network. It displays the host name portion of the full computer name of the computer.

Output:

```
C:\Users\djsce.student>hostname
MUM0922CPU0385
```

7. Tracert:

Introduction:

The tracert command is a Command Prompt command that's used to show several details about the path that a packet takes from the computer or device you're on to whatever destination you specify.

/d: Stops attempts to resolve the IP addresses of intermediate routers to their names. This can speed up the return of results.

Output:

```
C:\Users\djsce.student>tracert 10.120.63.75

Tracing route to MUM0922CPU0385.SVKMGRP.COM [10.120.63.75]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  MUM0922CPU0385.SVKMGRP.COM [10.120.63.75]

Trace complete.
```

8. Arp:

Introduction:

ARP stands for "Address Resolution Protocol" is a protocol for mapping an IP address to a physical MAC address on a local area network.
Basically, ARP is a program used by a computer system to find another computer's MAC address based on its IP address.

Output:

```
C:\Users\djsce.student>arp -a 10.120.63.75
No ARP Entries Found.
```

9. Getmac:

Introduction:

Returns the media access control (MAC) address and list of network protocols associated with each address for all network cards in each computer, either locally or across a network. This command is particularly useful either when you want to enter the MAC address into a network analyzer, or when you need to know what protocols are currently in use on each network adapter on a computer.

Output:

```
C:\Users\djsce.student>getmac

Physical Address    Transport Name
=================== ============================================================
84-69-93-95-19-77   \Device\Tcpip_{46CD3CCE-06BD-4A0E-A3F6-1C0C583811CF}
8C-09-1B-8A-94-7C   \Device\Tcpip_{B9722671-3CFB-4FAE-AD82-1A0D502CFC27}
00-50-56-C0-00-01   \Device\Tcpip_{C02079D4-6BA5-4C3B-A605-91F7CFEB8DD6}
00-50-56-C0-00-08   \Device\Tcpip_{D8A604F1-6256-4DF7-A654-1F40636BD892}
```

10. Netsh:

Introduction:

Netsh is a command-line scripting utility that allows you to display or modify the network configuration of a computer that is currently running. Netsh commands can be run by typing commands at the netsh prompt and they can be used in batch files or scripts. Remote computers and the local computer can be configured by using netsh commands.

Netsh also provides a scripting feature that allows you to run a group of commands in batch mode against a specified computer. With netsh, you can save a configuration script in a text file for archival purposes or to help you configure other computers.

Output:

```
netsh>show helper
Helper GUID                             DLL Filename  Command
--------------------------------------  ------------  -------
{02BC1F81-D927-4EC5-8CBC-8DD65E3E38E8}  AUTHFWCFG.DLL  advfirewall
{FB10CBCA-5430-46CE-B732-079B4E23BE24}  AUTHFWCFG.DLL    consec
{35342B49-83B4-4FCC-A90D-278533D5BEA2}  AUTHFWCFG.DLL    firewall
{4BD827F7-1E83-462D-B893-F33A80C5DE1D}  AUTHFWCFG.DLL    mainmode
{4D0FEFCB-8C3E-4CDE-B39B-325933727297}  AUTHFWCFG.DLL    monitor
{00770721-44EA-11D5-93BA-00B0D022DD1F}  HNETMON.DLL   bridge
{6DC31EC5-3583-4901-9E28-37C28113656A}  DHCPCMONITOR.DLL  dhcpclient
{8A6D23B3-0AF2-4101-BC6E-8114B325FE17}  NETIOHLP.DLL  dnsclient
{8B3A0D7F-1F30-4402-B753-C4B2C7607C97}  FWCFG.DLL     firewall
{44F3288B-DBFF-4B31-A86E-633F50D706B3}  NSHHTTP.DLL   http
{0705ECA1-7AAC-11D2-89DC-006008B0E5B9}  IFMON.DLL     interface
{1C151866-F35B-4780-8CD2-E1924E9F03E1}  NETIOHLP.DLL    6to4
{97C192DB-A774-43E6-BE78-1FABD795EEAB}  NETIOHLP.DLL    httpstunnel
{725588AC-7A11-4220-A121-C92C915E8B73}  NETIOHLP.DLL    ipv4
C:\Windows\System32>8FD6-2171EA46428F}  NETIOHLP.DLL    ipv6
{90E1CBE1-01D9-4174-BB4D-EB97F3F6150D}  NETIOHLP.DLL      6to4
{90E1CBE1-01D9-4174-BB4D-EB97F3F6150D}  NETIOHLP.DLL      isatap
{1C151866-F35B-4780-8CD2-E1924E9F03E1}  NETIOHLP.DLL    isatap
{1C151866-F35B-4780-8CD2-E1924E9F03E1}  NETIOHLP.DLL    portproxy
{78197B47-2BEF-49CA-ACEB-D8816371BAA8}  NETIOHLP.DLL    tcp
{1C151866-F35B-4780-8CD2-E1924E9F03E1}  NETIOHLP.DLL    teredo
{D89E6430-9053-5211-187A-1C58D966C781}  NETIOHLP.DLL    udp
{F7E0BC27-BA6E-4145-A123-012F1922F3F1}  NSHIPSEC.DLL  ipsec
{F7E0BC29-BA6E-4145-A123-012F1922F3F1}  NSHIPSEC.DLL    dynamic
{F7E0BC28-BA6E-4145-A123-012F1922F3F1}  NSHIPSEC.DLL    static
{1D8240C7-48B9-47CC-9E40-4F7A0A390E71}  DOT3CFG.DLL   lan
{B572D5F3-E15B-4501-84F2-6626F762AFB1}  WWANCFG.DLL   mbn
{B341E8BA-13AA-4E08-8CF1-A6F2D8B0C229}  NETIOHLP.DLL  namespace
{931852E2-597D-40B9-B927-55FFC81A6104}  NETIOHLP.DLL  netio
{C9D9F27D-3B14-47C0-B4D3-1F52CDB2E0C0}  NETPROFM.DLL  nlm
{B7BE4347-E851-4EEC-BC65-B0C0E87B86E3}  P2PNETSH.DLL  p2p
{E35A9D1F-61E8-4CF5-A46C-0F715A9303B8}  P2PNETSH.DLL    group
{9AA625FC-7E31-4679-B5B5-DFC67A3510AB}  P2PNETSH.DLL      database
{FBFC037E-D455-4B8D-80A5-B379002DBCAD}  P2PNETSH.DLL    idmgr
{9E0D63D6-4644-476B-9DAC-D64F96E01376}  P2PNETSH.DLL    pnrp
{1DD4935A-E587-4D16-AE27-14E40385AB12}  P2PNETSH.DLL      cloud
{AD1D76C9-434B-48E0-9D2C-31FA93D9635A}  P2PNETSH.DLL      diagnostics
{6EC05238-F6A3-4801-967A-5C9D6F6CAC50}  P2PNETSH.DLL      peer
{0705ECA2-7AAC-11D2-89DC-006008B0E5B9}  RASMONTR.DLL  ras
{42E3CC21-098C-11D3-8C4D-00104BCA495B}  RASMONTR.DLL    aaaa
{90FE6CFC-B6A2-463B-AA12-25E615EC3C66}  RASMONTR.DLL    diagnostics
{13D12A78-D0FB-11D2-9B76-00104BCA495B}  RASMONTR.DLL    ip
{36B3EF76-94C1-460F-BD6F-DF0178D90EAC}  RASMONTR.DLL    ipv6
{592852F7-5F6F-470B-9097-C5D33B612975}  RPCNSH.DLL    rpc
{C07E293F-9531-4426-8E5C-D7EBBA50F693}  RPCNSH.DLL      filter
```