Student Name	**Swanand Garge**
SRN No	202201589
Roll No	39
Program	Computer Engg.
Year	Third Year
Division	D
Subject	Computer Network Laboratory (BTECCE22506)
Assignment No	Two

Assignment Number - 02

Title : Study of Linux and Windows Network commands

Problem Statement Studying Linux and Windows network commands. [ping, pathping, ipconfig/ifconfig, arp, netstat, nbtstat, nslookup, route, traceroute/tracert, nmap, etc]

Try to execute following commands on linux terminal or Windows command prompt.

- **Ipconfig / ifconfig**
- **ping**
- **Tracert/Traceroute/Tracepath**
- **Finger**
- **NSlookup**
- **Netstat**
- **Hostname**
- **Port Scan / nmap**
- **Arp Route**
- **Whois**

Theory :

1) **Ipconfig / ifconfig :**

```
C:\Users\lunna>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

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

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::fcc5:3cd4:c52d:8ccb%13
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

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  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:1b89:5700:6041:88df:585b:1dad
   Temporary IPv6 Address. . . . . . : 2401:4900:1b89:5700:95da:b91f:f62b:179
   Link-local IPv6 Address . . . . . : fe80::e308:8f5b:a258:f245%4
   IPv4 Address. . . . . . . . . . . : 172.20.10.8
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Default Gateway . . . . . . . . . : fe80::b8e6:cff:fed5:64%4
                                       172.20.10.1
```

Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

2) Ping :

```
C:\Users\lunna>ping 10.25.2.206

Pinging 10.25.2.206 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.25.2.206:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\lunna>ping 172.20.10.1

Pinging 172.20.10.1 with 32 bytes of data:
Reply from 172.20.10.1: bytes=32 time=6ms TTL=64
Reply from 172.20.10.1: bytes=32 time=58ms TTL=64
Reply from 172.20.10.1: bytes=32 time=8ms TTL=64
Reply from 172.20.10.1: bytes=32 time=7ms TTL=64

Ping statistics for 172.20.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 58ms, Average = 19ms
```

The PING (Packet Internet Groper) command is used to check the network connectivity between the host and server/host. This command takes as input the IP address or the URL and sends a data packet to the specified address with the message “PING” and gets a response from the server/host this time is recorded which is called latency. Fast ping with low latency means a faster connection. Ping uses ICMP(Internet Control Message Protocol) to send an ICMP echo message to the specified host if that host is available then it sends an ICMP reply message. Ping is generally measured in milliseconds every modern operating system has this ping pre-installed.

3) Tracert /Traceroute/Tracepath :

```
C:\Users\lunna>tracert google.co.in

Tracing route to google.co.in [2404:6800:4009:809::2003]
over a maximum of 30 hops:

  1    11 ms     3 ms     3 ms  2401:4900:1b89:5700:b151:dcae:bf65:1356
  2     *        *        *     Request timed out.
  3    67 ms   294 ms    74 ms  2401:4900:84:4409::3:85
  4    59 ms    37 ms    79 ms  2404:a800:2a00:101::79
  5    59 ms    46 ms    88 ms  2404:a800::167
  6    85 ms    68 ms    78 ms  2001:4860:1:1::2d62
  7    81 ms    64 ms    30 ms  2404:6800:8013::1
  8     *       97 ms   204 ms  2001:4860:0:1::2038
  9    73 ms    77 ms    39 ms  2001:4860:0:1::1315
 10    71 ms    76 ms    79 ms  bom05s11-in-x03.1e100.net [2404:6800:4009:809::2003]

Trace complete.
```

This command determines the path by sending the first echo Request message with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum number of hops is reached. The maximum number of hops is 30 by default and can be specified using the **/h** parameter.

The path is determined by examining the ICMP time Exceeded messages returned by intermediate routers and the echo Reply message returned by the destination. However, some routers don't return time Exceeded messages for packets with expired TTL values and are invisible to the **tracert** command. In this case, a row of asterisks (*) is displayed for that hop. The path displayed is the list of near/side router interfaces of the routers in the path between a source host and a destination. The near/side interface is the interface of the router that is closest to the sending host in the path.

4) **Finger :**
5) **nslookup :**

```
C:\Users\lunna>nslookup vupune.ac.in
Server:  UnKnown
Address:  fe80::b8e6:cff:fed5:64

Non-authoritative answer:
Name:    vupune.ac.in
Address:  3.7.106.3
```

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.

6) **Netstat :**

```
C:\Users\lunna>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:54462        admin:65001            ESTABLISHED
  TCP    127.0.0.1:54473        admin:54491            ESTABLISHED
  TCP    127.0.0.1:54491        admin:54473            ESTABLISHED
  TCP    127.0.0.1:65001        admin:54462            ESTABLISHED
  TCP    172.20.10.8:54540      20.249.115.161:https   ESTABLISHED
  TCP    172.20.10.8:54542      relay-8a6d3372:https   ESTABLISHED
  TCP    172.20.10.8:54625      104.18.13.52:https     ESTABLISHED
  TCP    172.20.10.8:54640      20.249.168.239:https   ESTABLISHED
  TCP    172.20.10.8:54653      20.212.88.117:https    ESTABLISHED
  TCP    172.20.10.8:54660      72.25.64.2:https       ESTABLISHED
  TCP    172.20.10.8:54973      whatsapp-chatd-edge-shv-01-pnq1:5222  ESTABLISHED
  TCP    172.20.10.8:55024      sl-in-f188:5228        ESTABLISHED
  TCP    172.20.10.8:55084      104.18.156.37:https    ESTABLISHED
  TCP    [2401:4900:1b89:5700:95da:b91f:f62b:179]:54559  [2603:1040:a06:6::1]:https  ESTABLISHED
  TCP    [2401:4900:1b89:5700:95da:b91f:f62b:179]:54661  [2603:1040:a06:6::1]:https  ESTABLISHED
  TCP    [2401:4900:1b89:5700:95da:b91f:f62b:179]:54798  g2600-140f-ec00-0000-0000-0000-17df-f45a:https  CLOSE_WAIT
  TCP    [2401:4900:1b89:5700:95da:b91f:f62b:179]:55095  [2406:da1a:e20:7901:d575:c8e3:2be:f51c]:https  TIME_WAIT
  TCP    [2401:4900:1b89:5700:95da:b91f:f62b:179]:55098  [2406:da1a:e20:7901:d575:c8e3:2be:f51c]:https  TIME_WAIT
```

Netstat — derived from the words network and statistics — is a program that's controlled via commands issued in the command line. It delivers basic statistics on all network activities and informs users on which ports and addresses the corresponding connections – TCP and UDP – are running and which ports are open for tasks.

7) **Hostname :**

```
C:\Users\lunna>hostname
admin
```

Displays the host name portion of the full computer name of the computer.

8) PortScan / nmap :

```
manav@ubuntulinux: ~
manav@ubuntulinux:~$ nmap 172.217.27.174
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-19 14:55 UTC
Nmap scan report for del11s03-in-f14.1e100.net (172.217.27.174)
Host is up (0.019s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.02 seconds
manav@ubuntulinux:~$
```

9) Arp Route :

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

Interface: 172.20.10.8 --- 0x4
  Internet Address      Physical Address      Type
  172.20.10.1           ba-e6-0c-d5-00-64     dynamic
  172.20.10.15          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
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0xd
  Internet Address      Physical Address      Type
  192.168.56.255        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
```

Address Resolution Protocol (ARP) is a protocol or procedure that connects an ever-changing Internet Protocol (IP) address to a fixed physical machine address, also known as a media access control (MAC) address, in a local-area network (LAN).

This mapping procedure is important because the lengths of the IP and MAC addresses differ, and a translation is needed so that the systems can recognize one another. The most used IP today is IP version 4 (IPv4). An IP address is 32 bits long. However, MAC addresses are 48 bits long. ARP translates the 32-bit address to 48 and vice versa.

10) Whois :

```
Command Prompt

D:\whois>whois google.com

Whois v1.21 - Domain information lookup
Copyright (C) 2005-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to COM.whois-servers.net...

WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2083895740
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2021-01-19T17:30:34Z <<<
```

The WHOIS command is a widely-used protocol for retrieving registration information about domain names and IP addresses. Originally intended for system administrators and network engineers to diagnose network issues, it has now become a popular tool for anyone looking to gather information on a domain or IP address. When you initiate a WHOIS query, your computer sends a request to a WHOIS server - a database of registered domain names and IP addresses. In response, the server provides registration information for the requested domain or IP address.
The data obtained by the WHOIS command can include the name and contact details of the domain or IP address owner and also details of the registration date, and the expiration date. It can also give technical information about the domain, such as its name servers and associated DNS records.

Conclusion : The network commands available on Linux and Windows are fundamental for system administrators and network engineers. They provide essential insights into network configurations, troubleshooting, and security. While most of these commands have similar counterparts across both operating systems, Linux generally offers more flexibility and additional features, often making it the preferred choice for network diagnostics and analysis. Windows provides a user-friendly environment but may require additional tools for advanced network management tasks.