WORKSHEET 1.2

Student Name: Vishal Kumar **UID: 21BCS2303**

Branch: CSE **Section/Group: 606 “A”**

Semester: 4th **Date of Performance: 20-02-2023**

Subject Name: Computer Networks **Subject Code: 21CSH-256**

Aim:

Study the basic network command and Network configuration commands like ping, variations of ipconfig, tracert, nslookup, netstat, arp, rarp, hostname, pathping etc.

Objective: Students will be able to troubleshoot networks

S/W Requirement: Command Prompt

H/W Requirement:

- Processor – Any suitable Processor e.g. Celeron
- Main Memory - 128 MB RAM
- Hard Disk – minimum 20 GB IDE Hard Disk
- Removable Drives–1.44 MB Floppy Disk Drive –52X IDE CD-ROM Drive
- PS/2 HCL Keyboard and Mouse

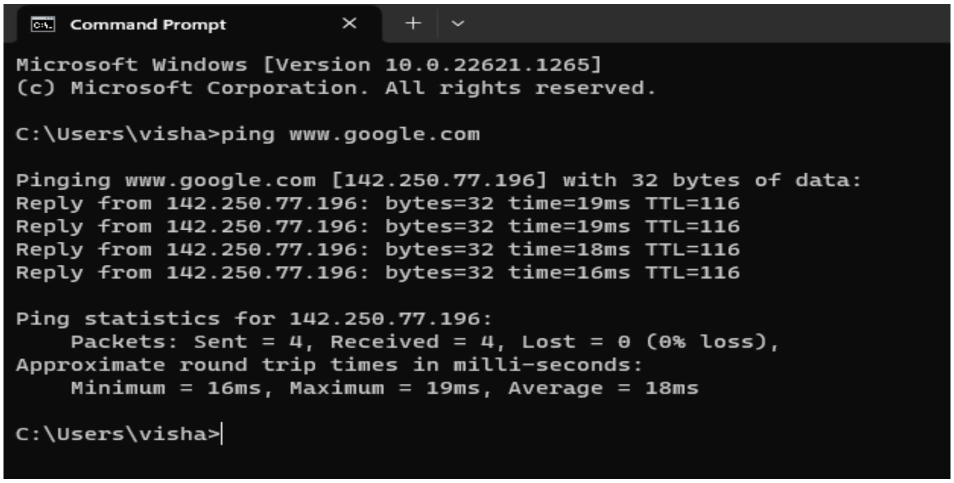
Method:

Go to command prompt and type the commands

I. Ping

In order to test and confirm that a specific destination IP address exists and can accept requests for computer network management, a user can use a basic Internet software called ping (also known as Packet Internet or Inter-Network Groper). The abbreviation was created to sound like the phrase used by submariners to describe the sound of a returning sonar pulse.

Result:

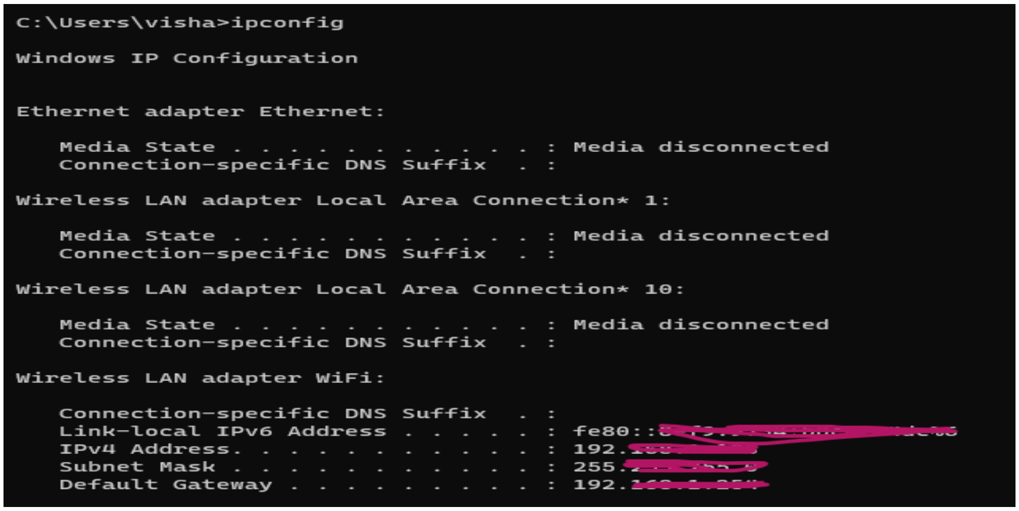


```
Microsoft Windows [Version 10.0.22621.1265]
(c) Microsoft Corporation. All rights reserved.

C:\Users\visha>ping www.google.com

Pinging www.google.com [142.250.77.196] with 32 bytes of data:
Reply from 142.250.77.196: bytes=32 time=19ms TTL=116
Reply from 142.250.77.196: bytes=32 time=19ms TTL=116
Reply from 142.250.77.196: bytes=32 time=18ms TTL=116
Reply from 142.250.77.196: bytes=32 time=16ms TTL=116

Ping statistics for 142.250.77.196:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 19ms, Average = 18ms

C:\Users\visha>
```

II. Ipconfig:

(Internet Protocol CONFIGuration) A command-line tool used to view and control the machine's allocated IP address. The current IP, subnet mask, and default gateway addresses of the computer are shown in Windows when you type ipconfig without any other options.

Result:

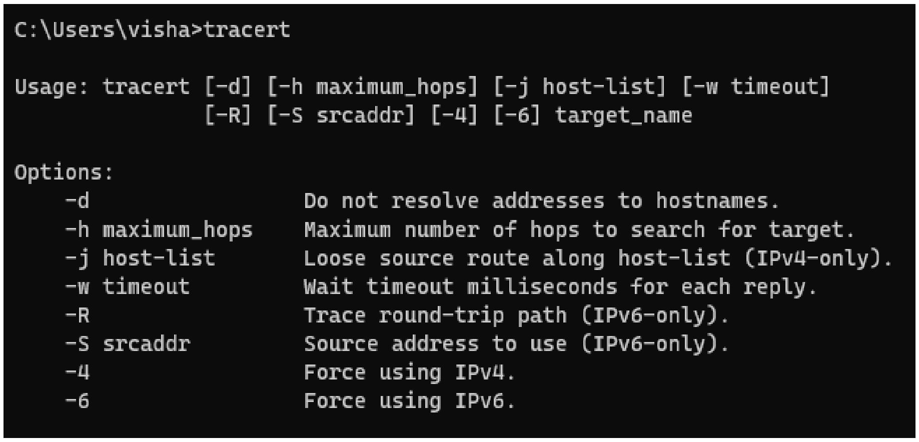


```
C:\Users\visha>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

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

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  . :

Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::[redacted]
   IPv4 Address. . . . . . . . . . . : 192.[redacted]
   Subnet Mask . . . . . . . . . . . : 255.[redacted]
   Default Gateway . . . . . . . . . : 192.[redacted]
```

III. Tracert:

A network analysis tool that may be used to determine the route a packet takes from its source to its destination is the tracert command (in Windows) or the traceroute command (in Linux or Mac).

Result:

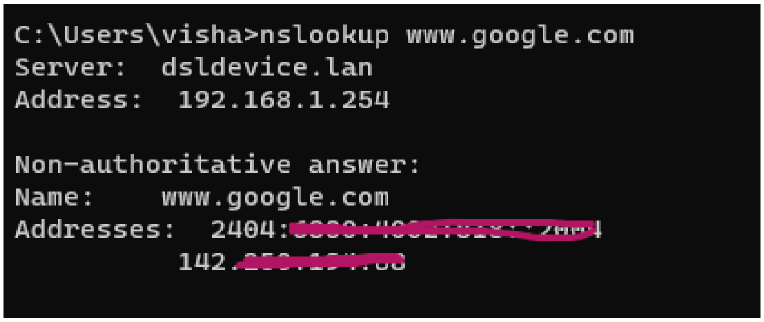


```
C:\Users\visha>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```

IV. Nslookup

The command Nslookup, which stands for "Name Server Lookup," is helpful for retrieving data from the DNS server. It is a tool for network administration that queries the Domain Name System (DNS) to retrieve any given DNS record, such as a domain name or IP address mapping. It is also employed to solve DNS-related issues.

Result:

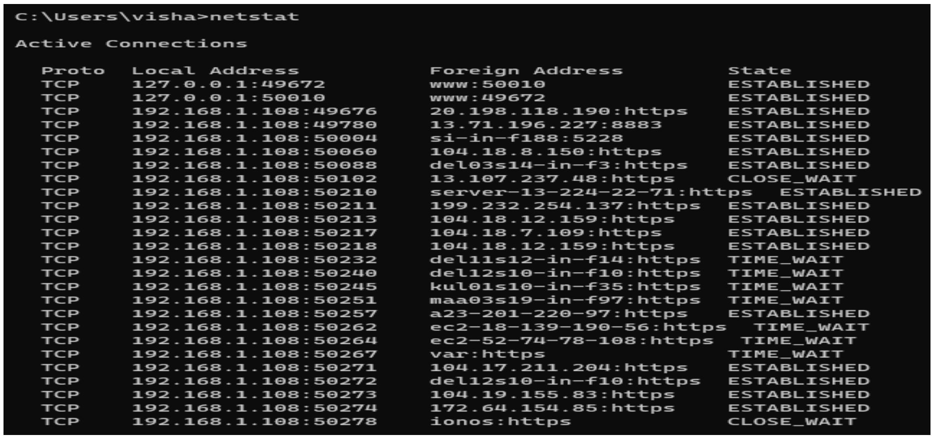


```
C:\Users\visha>nslookup www.google.com
Server:  dsldevice.lan
Address:  192.168.1.254

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:[redacted]
          142.[redacted]
```

V. Netstat

The application known as Netstat, which stands for "network statistics," is run by issuing commands from the command line. It provides users with basic statistics on all network activity, lets them know which TCP and UDP connections are active on which ports and addresses, and which ports are available for tasks.

Result:

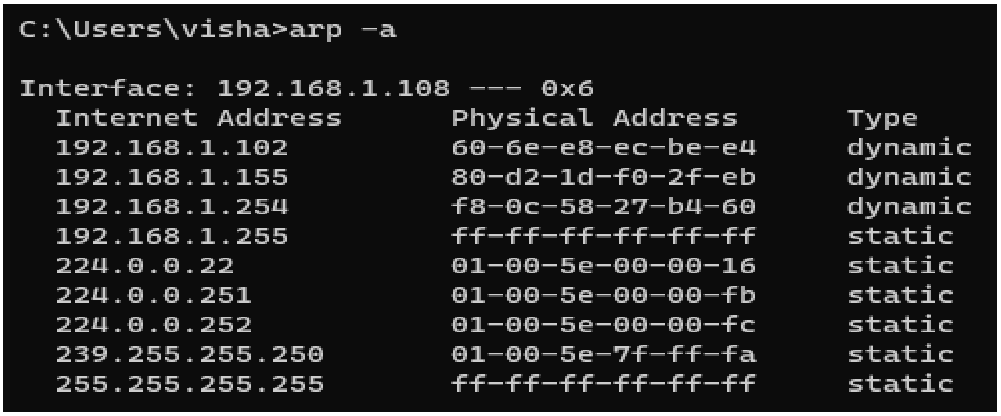


```
C:\Users\visha>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49672        www:50010              ESTABLISHED
  TCP    127.0.0.1:50010        www:49672              ESTABLISHED
  TCP    192.168.1.108:49676    20.198.118.190:https   ESTABLISHED
  TCP    192.168.1.108:49780    13.71.196.227:8883     ESTABLISHED
  TCP    192.168.1.108:50004    si-in-f188:5228        ESTABLISHED
  TCP    192.168.1.108:50060    104.18.8.150:https     ESTABLISHED
  TCP    192.168.1.108:50088    del03s14-in-f3:https   ESTABLISHED
  TCP    192.168.1.108:50102    13.107.237.48:https    CLOSE_WAIT
  TCP    192.168.1.108:50210    server-13-224-22-71:https  ESTABLISHED
  TCP    192.168.1.108:50211    199.232.254.137:https  ESTABLISHED
  TCP    192.168.1.108:50213    104.18.12.159:https    ESTABLISHED
  TCP    192.168.1.108:50217    104.18.7.109:https     ESTABLISHED
  TCP    192.168.1.108:50218    104.18.12.159:https    ESTABLISHED
  TCP    192.168.1.108:50232    del11s12-in-f14:https  TIME_WAIT
  TCP    192.168.1.108:50240    del12s10-in-f10:https  TIME_WAIT
  TCP    192.168.1.108:50245    kul01s10-in-f35:https  TIME_WAIT
  TCP    192.168.1.108:50251    maa03s19-in-f97:https  TIME_WAIT
  TCP    192.168.1.108:50257    a23-201-220-97:https   ESTABLISHED
  TCP    192.168.1.108:50262    ec2-18-139-190-56:https  TIME_WAIT
  TCP    192.168.1.108:50264    ec2-52-74-78-108:https  TIME_WAIT
  TCP    192.168.1.108:50267    var:https              TIME_WAIT
  TCP    192.168.1.108:50271    104.17.211.204:https   ESTABLISHED
  TCP    192.168.1.108:50272    del12s10-in-f10:https  ESTABLISHED
  TCP    192.168.1.108:50273    104.19.155.83:https    ESTABLISHED
  TCP    192.168.1.108:50274    172.64.154.85:https    ESTABLISHED
  TCP    192.168.1.108:50278    ionos:https            CLOSE_WAIT
```

VI. Arp

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).

Result:

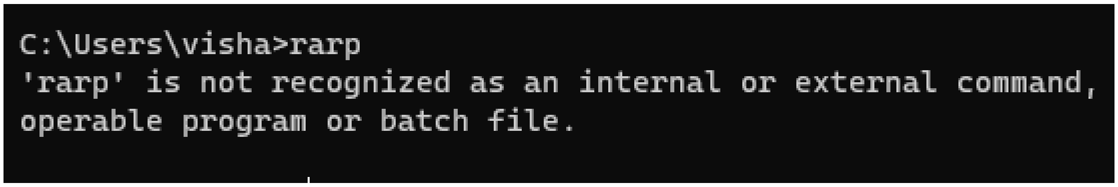


```
C:\Users\visha>arp -a

Interface: 192.168.1.108 --- 0x6
  Internet Address      Physical Address      Type
  192.168.1.102         60-6e-e8-ec-be-e4     dynamic
  192.168.1.155         80-d2-1d-f0-2f-eb     dynamic
  192.168.1.254         f8-0c-58-27-b4-60     dynamic
  192.168.1.255         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
```

VII. Rarp

Reverse Address Resolution Protocol (RARP) is a network-specific standard protocol. It is described in RFC 903. Some network hosts, such as a diskless workstation, do not know their own IP address when they are booted. To determine their own IP address, they use a mechanism similar to ARP, but now the hardware address of the host is the known parameter, and the IP address is the queried parameter.

Result:

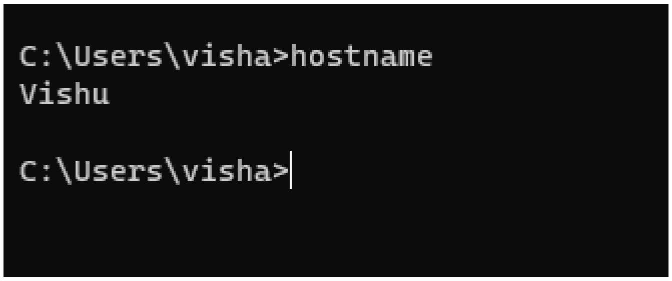


```
C:\Users\visha>rarp
'rarp' is not recognized as an internal or external command,
operable program or batch file.
```

VIII. Hostname

A hostname is a label assigned to a device (a host) on a network. It distinguishes one device from another on a specific network or over the internet. The hostname for a computer on a home network may be something like new laptop, Guest-Desktop, or FamilyPC.

Result:

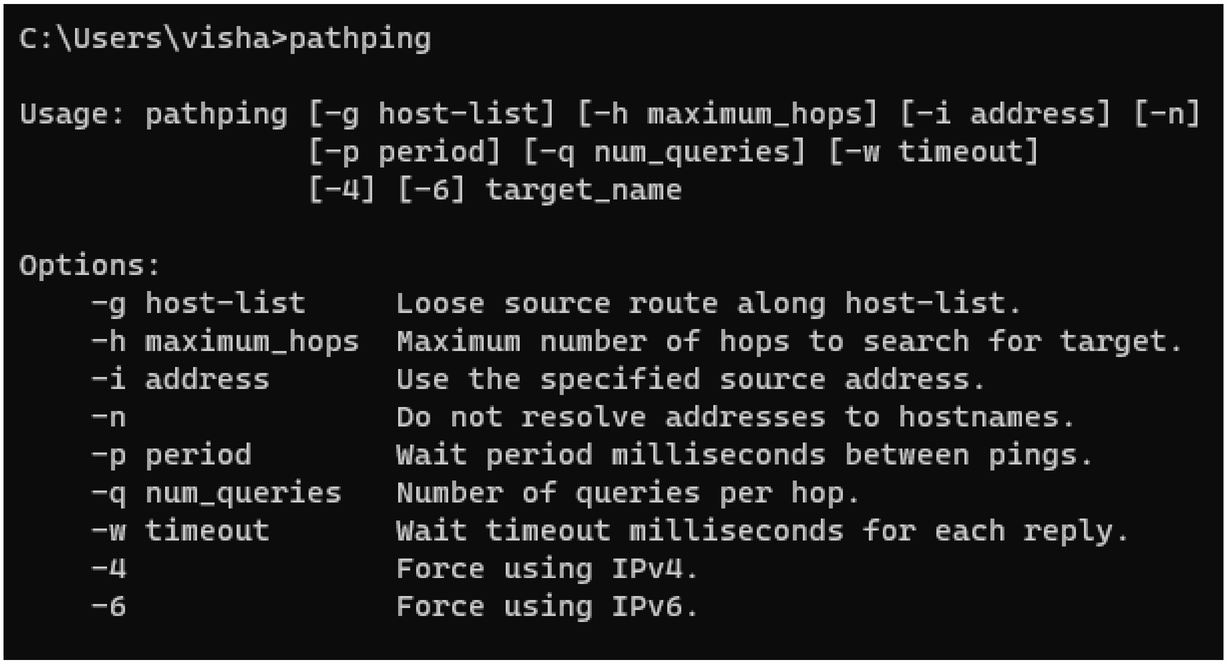


```
C:\Users\visha>hostname
Vishu

C:\Users\visha>
```

IX. Pathping

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.

Result:



```
C:\Users\visha>pathping

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
                [-p period] [-q num_queries] [-w timeout]
                [-4] [-6] target_name

Options:
    -g host-list     Loose source route along host-list.
    -h maximum_hops  Maximum number of hops to search for target.
    -i address       Use the specified source address.
    -n               Do not resolve addresses to hostnames.
    -p period        Wait period milliseconds between pings.
    -q num_queries   Number of queries per hop.
    -w timeout       Wait timeout milliseconds for each reply.
    -4               Force using IPv4.
    -6               Force using IPv6.
```