Practical – 1

Aim: Execution of basic TCP/IP utilities and commands.

- ## Transmission Control Protocol/Internet Protocol (TCP/IP):

The Transmission Control Protocol / Internet Protocol (TCP/IP) is a nonproprietary, routable network protocol suite that enables computers to communicate over all types of networks. TCP/IP is the native protocol of the Internet and is required for Internet Connectivity. The TCP/IP protocol suite includes a network/node address structure, tools for static and dynamic address assignment, name resolution services, and utilities for testing and configuration.

- ## Windows-Network Commands for TCP/IP:

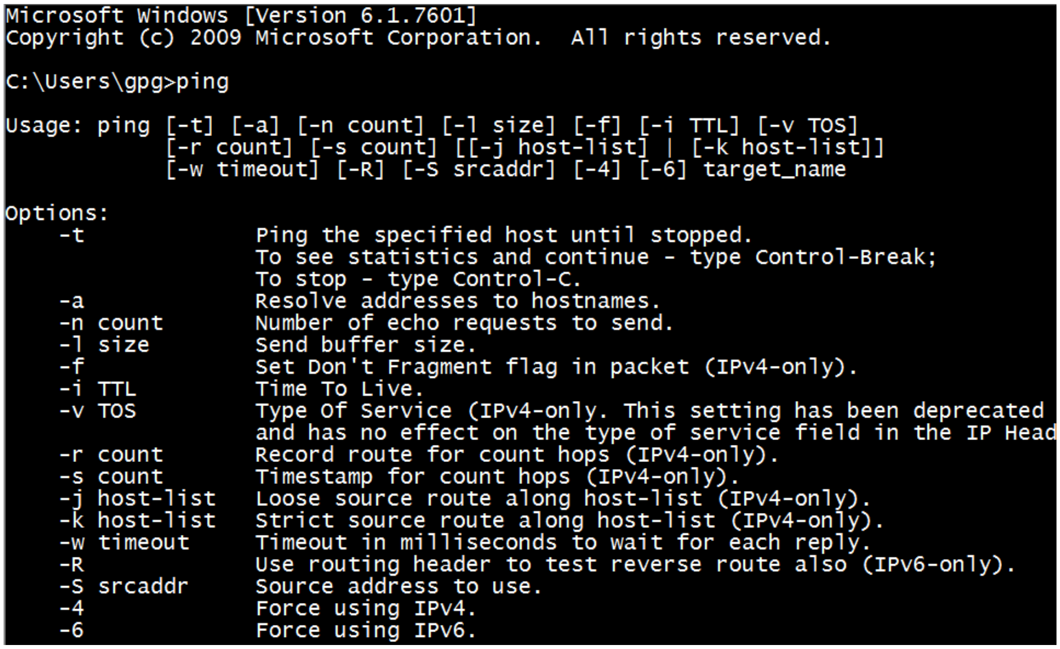
1. Ping:

→ Ping is used to test the network connection with a remote IP address.

```
ping-t [IP or host]
ping-l 1024 [IP or host]
```

→ The **-t** option is used to ping continuously until **Ctrl-C** is pressed. If you specify the -t option you can always get statistics without interrupting pings by pressing **Ctrl + Break.**

→ This command is also useful to generate network load by specifying the size of the packet with the -l option and the packet size in bytes.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\gpg>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP Head
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
    -S srcaddr     Source address to use.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

2. IpConfig:

→ Displays or refreshes the TCP/IP configuration.

```
ipconfig /all [/release [adapter]] [/renew [adapter]]
/flushdns /displaydns/registerdns [-a] [-a] [-a]
```

→ This command, when executed with no options, displays the current IP address, the subnet mask and default gateway (network interfaces of the local machine).

1. **/all:**
   Displays all network configuration, including DNS, WINS, DHCP servers, etc...
2. **/renew [adapter]:**
   Renews DHCP configuration for all adapters (if adapter is not specified) or a specific adapter indicated by the [adapter] parameter.
3. **/release [adapter]:**
   Sends a DHCPRELEASE message to the DHCP server to release the current DHCP configuration and cancel the IP address configuration for all adapters (if adapter is not specified) or a specific adapter indicated by

the [adapter] parameter. This parameter disables TCP/IP for network cards configured to automatically obtain an IP address.

4. **/flushdns:**

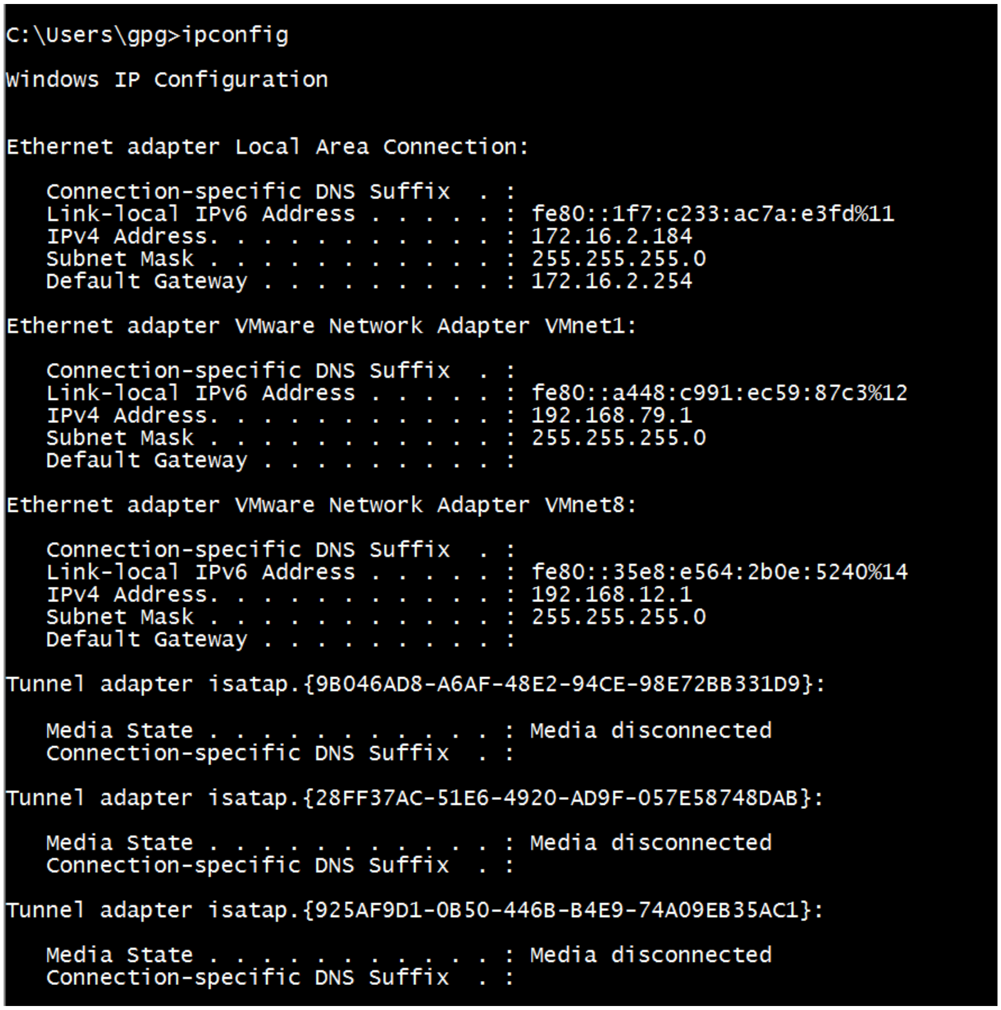
   Empty and reset the DNS client resolver cache. This option is useful to exclude negative entries and all other entries added dynamically to the cache.

5. **/displaydns:**

   Displays the DNS client resolver cache, which includes entries preloaded from the local host file and any recently obtained records for name queries resolved by the host computer. The DNS Client service uses this information to quickly resolve frequently queried names, before querying the configured DNS servers.

6. **/registerdns:**

   Refreshes all DHCP leases and re-registers DNS names.



```
C:\Users\gpg>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1f7:c233:ac7a:e3fd%11
   IPv4 Address. . . . . . . . . . . : 172.16.2.184
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.2.254

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a448:c991:ec59:87c3%12
   IPv4 Address. . . . . . . . . . . : 192.168.79.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::35e8:e564:2b0e:5240%14
   IPv4 Address. . . . . . . . . . . : 192.168.12.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{9B046AD8-A6AF-48E2-94CE-98E72BB331D9}:

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

Tunnel adapter isatap.{28FF37AC-51E6-4920-AD9F-057E58748DAB}:

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

Tunnel adapter isatap.{925AF9D1-0B50-446B-B4E9-74A09EB35AC1}:

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

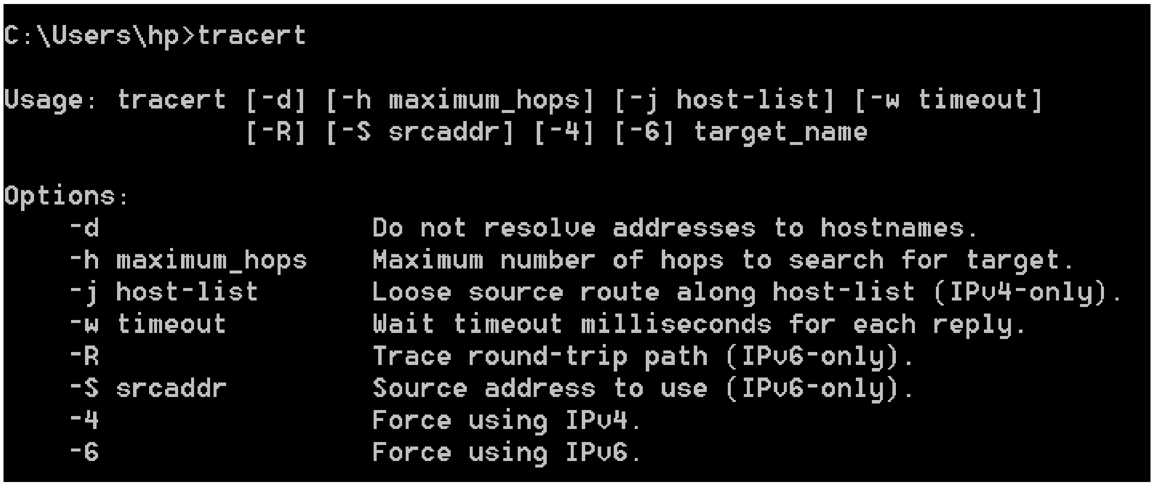
3. Tracert:

→ Tracert command-line tool is used to trace the path that an Internet Protocol(IP) packet takes to its destination from a source.

→ Tracert will determine the path taken to a destination.

```
tracert [@IP or host]
tracert -d [@IP or host]
```

→ This command is useful if the ping command does return any data, to determine at what level the connection failed.



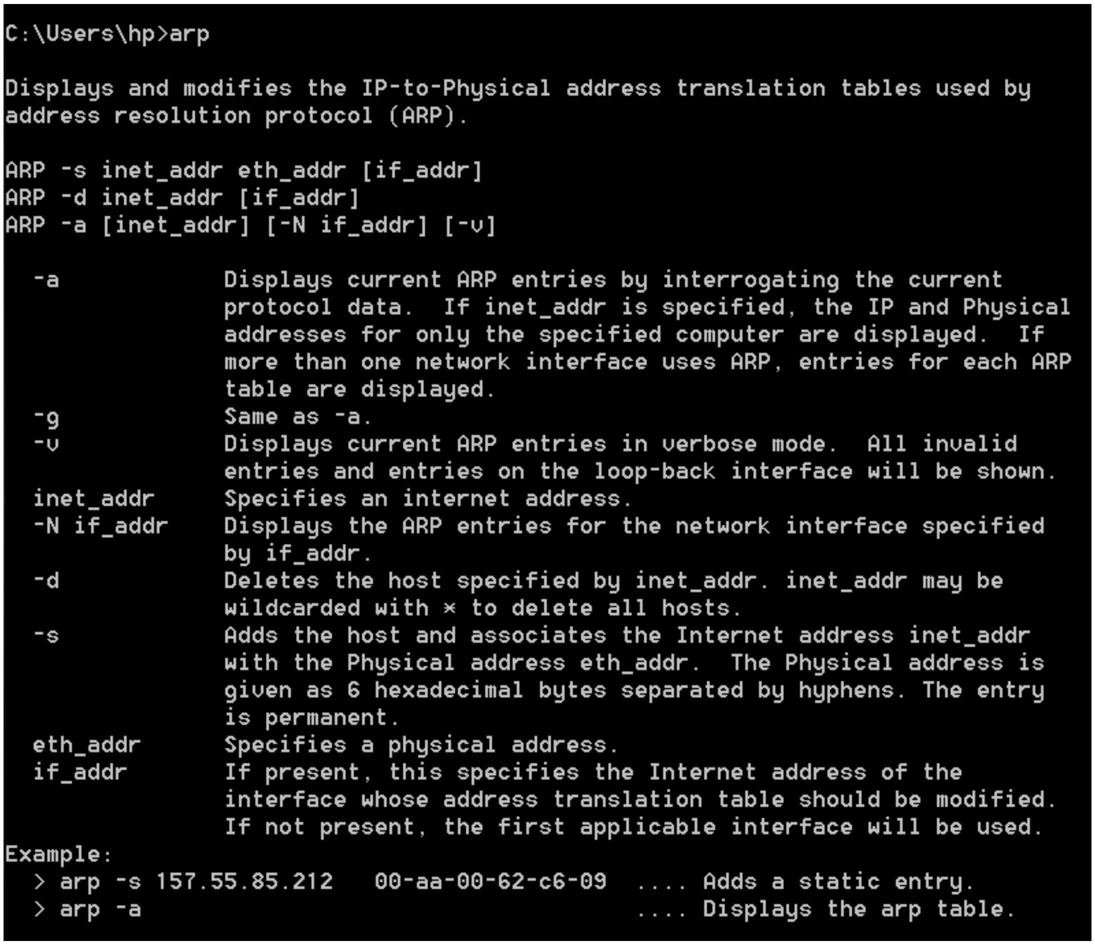
```
C:\Users\hp>tracert

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.
```

4. Address Resolution Protocol (ARP):

→ It display and modifies the translation tables of IP Addresses to physical addresses used by the ARP.

```
ARP -s adr_inet adr_eth [adr_if]
ARP -d adr_inet [adr_if]
ARP -a [adr_inet] [-N adr_if]
```

1. **–a**:
   Displays active ARP entries by interrogating the current data protocol. If adr_inet is specified, only the physical and IP addresses of the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.
2. **–g**:
   is the same as -a
3. **adr_inet**:
   Specifies an internet address.
4. **-N adr_if**:
   Displays ARP entries for the network interface specified by adr_if.
5. **–d**:
   Deletes the host specified by adr_inet.
6. **–s**:
   Adds the host and associates the adr_inet internet address with the adr_eth physical address. The physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.
7. **adr_eth**:
   Specifies a physical address.
8. **adr_if**:
   Specifies the internet interface whose address translation table should be modified. When not specified, the first applicable interface will be used.



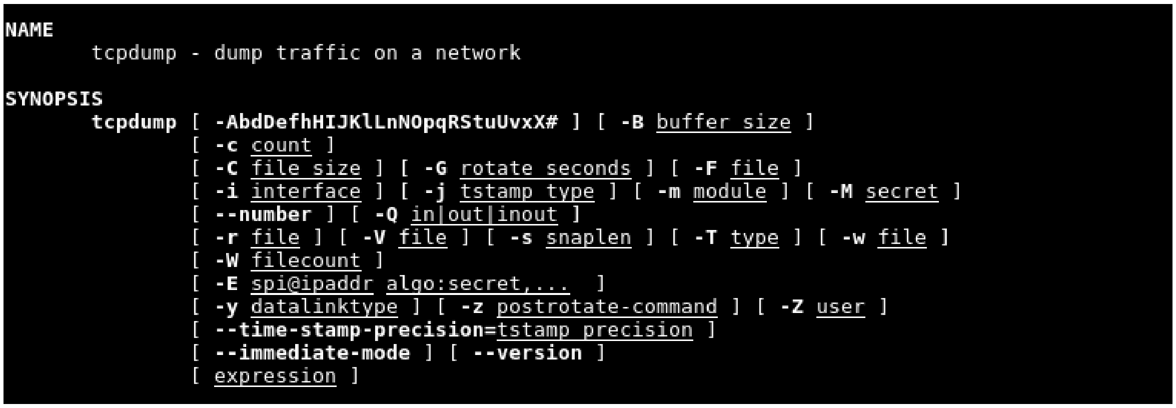
```
C:\Users\hp>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            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.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

5. TCP Dump:

→ It dumps the traffic on a network.

→ TCPDump is a common packet analyzer that runs under the command line. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.

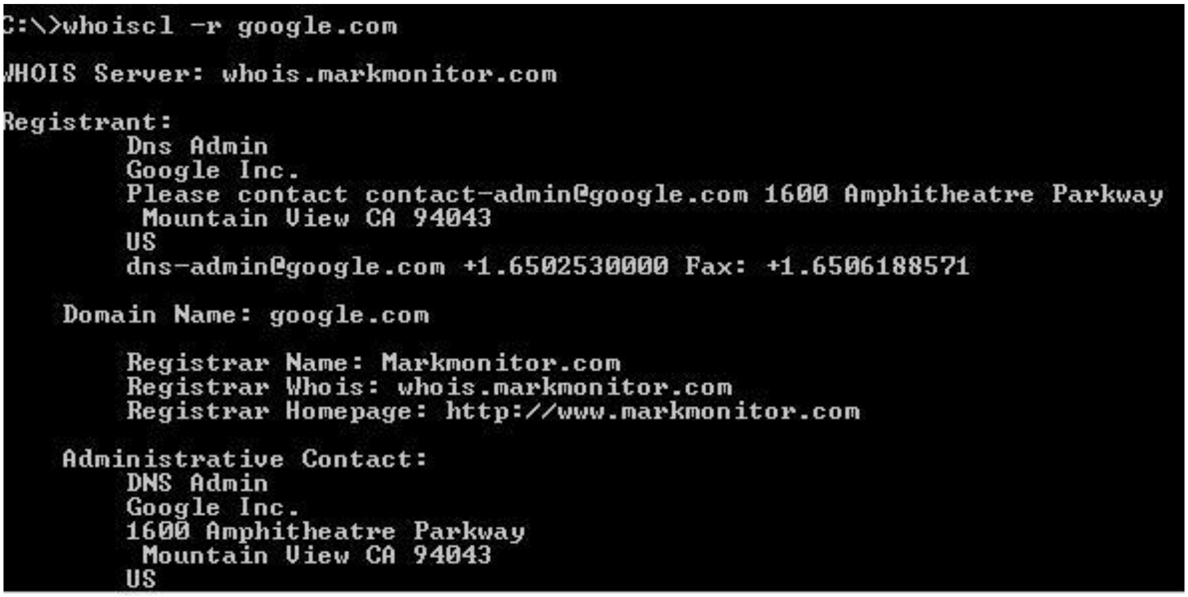
→ TCPDump prints the contents of network packets. It can read packets from a network interface card or from a previously created saved packet file. TCPDump can write packets to standard output or a file.



```
NAME
       tcpdump - dump traffic on a network

SYNOPSIS
       tcpdump [ -AbdDefhHIJKlLnNOpqRStuUvxX# ] [ -B buffer_size ]
               [ -c count ]
               [ -C file_size ] [ -G rotate_seconds ] [ -F file ]
               [ -i interface ] [ -j tstamp_type ] [ -m module ] [ -M secret ]
               [ --number ] [ -Q in|out|inout ]
               [ -r file ] [ -V file ] [ -s snaplen ] [ -T type ] [ -w file ]
               [ -W filecount ]
               [ -E spi@ipaddr algo:secret,...  ]
               [ -y datalinktype ] [ -z postrotate-command ] [ -Z user ]
               [ --time-stamp-precision=tstamp_precision ]
               [ --immediate-mode ] [ --version ]
               [ expression ]
```

6. WhoIs:

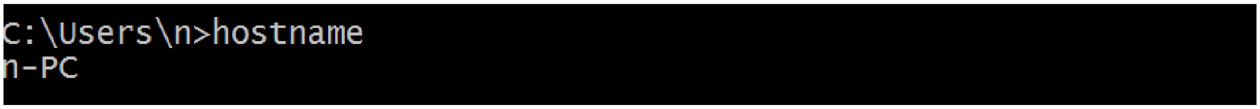
→ WhoIs command helps to allow a user to identify a domain name. This command provides information about a domain name much like the WHOIS on network solutions.



```
C:\>whoiscl -r google.com

WHOIS Server: whois.markmonitor.com

Registrant:
        Dns Admin
        Google Inc.
        Please contact contact-admin@google.com 1600 Amphitheatre Parkway
         Mountain View CA 94043
        US
        dns-admin@google.com +1.6502530000 Fax: +1.6506188571

    Domain Name: google.com

        Registrar Name: Markmonitor.com
        Registrar Whois: whois.markmonitor.com
        Registrar Homepage: http://www.markmonitor.com

    Administrative Contact:
        DNS Admin
        Google Inc.
        1600 Amphitheatre Parkway
         Mountain View CA 94043
        US
```

7. Hostname:

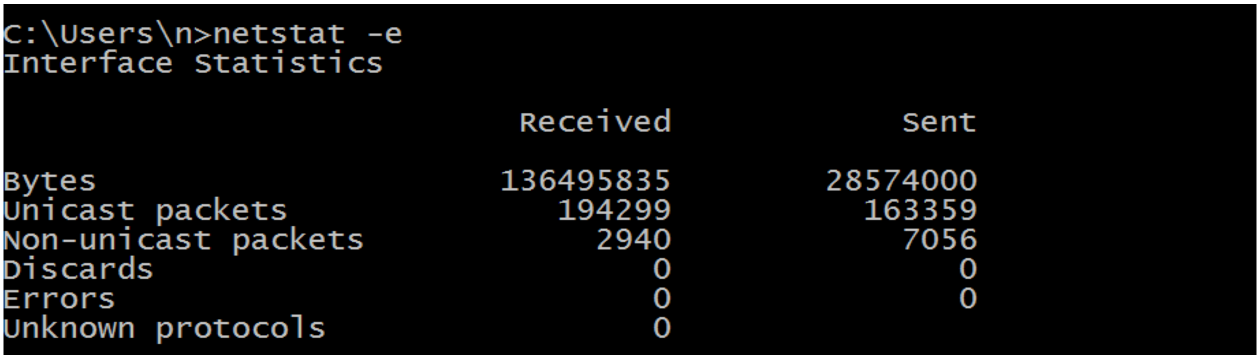
→ The hostname command is used to show or set a computer’s hostname and domain name.



```
C:\Users\n>hostname
n-PC
```

8. NetStat:

→ The NetStat command is used to display the network summary information for the device.



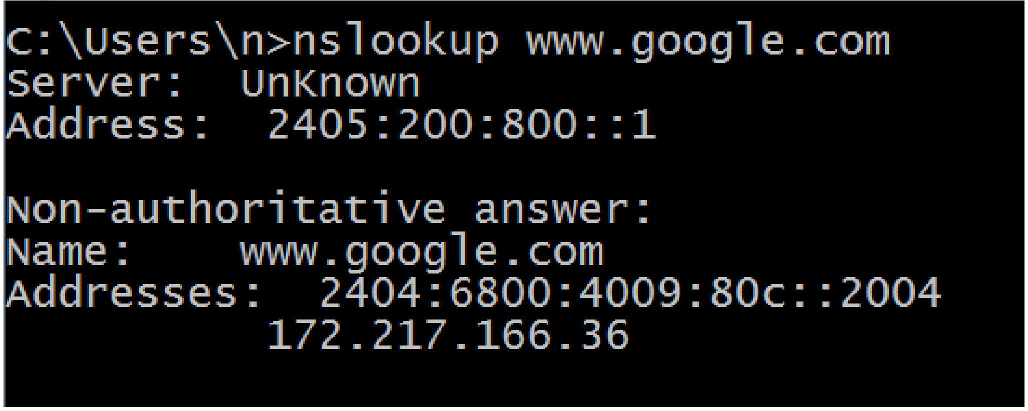
```
C:\Users\n>netstat -e
Interface Statistics

                           Received            Sent

Bytes                     136495835        28574000
Unicast packets              194299          163359
Non-unicast packets            2940            7056
Discards                          0               0
Errors                            0               0
Unknown protocols                 0
```

9. NSLookup:

→ This command sends DNS requests to a DNS server.

```
nslookup [domain] [dns server]
```

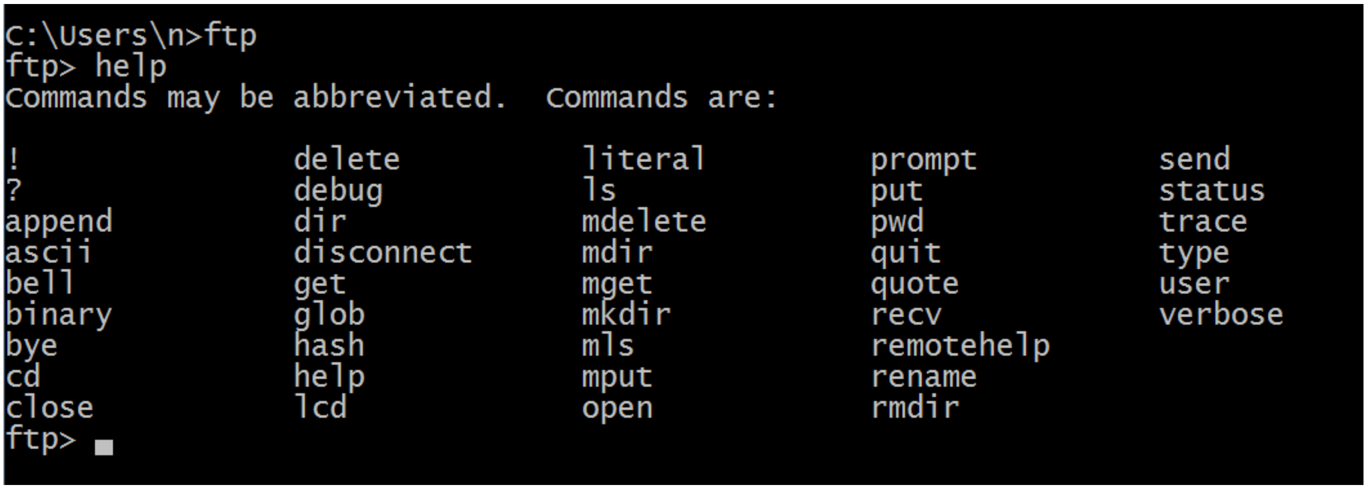
→ The nslookup command to send DNS requests to a server. By default, if you do not specify the DNS server, the command will use the one that is configured for your network interface (the one you use to surf the internet, for example).



```
C:\Users\n>nslookup www.google.com
Server:  UnKnown
Address:  2405:200:800::1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4009:80c::2004
          172.217.166.36
```

10. FTP:

→ FTP (File Transfer Protocol) is a standard network protocol used to exchange files between computers on a private or through the internet.

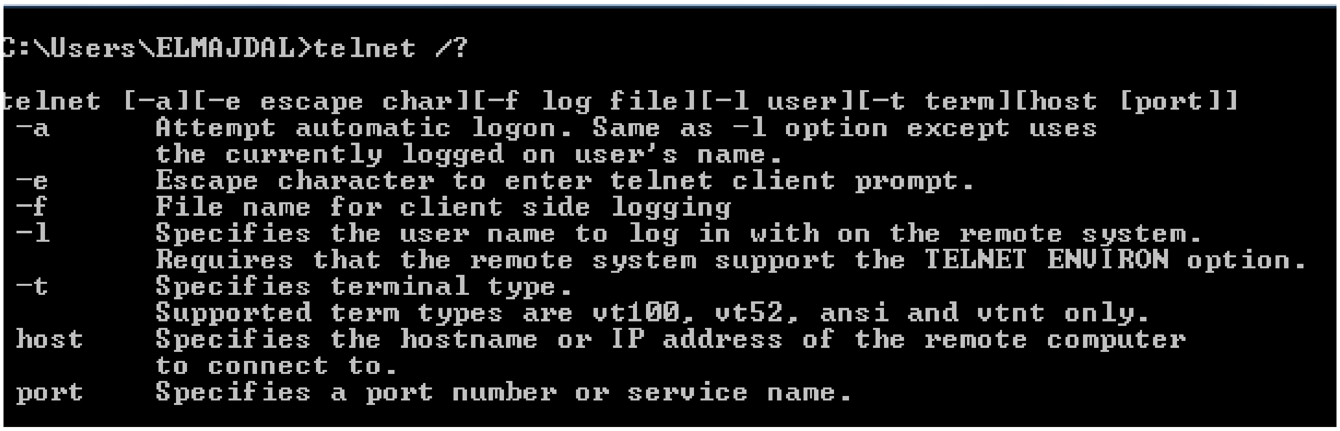


```
C:\Users\n>ftp
ftp> help
Commands may be abbreviated.  Commands are:

!               delete          literal         prompt          send
?               debug           ls              put             status
append          dir             mdelete         pwd             trace
ascii           disconnect      mdir            quit            type
bell            get             mget            quote           user
binary          glob            mkdir           recv            verbose
bye             hash            mls             remotehelp
cd              help            mput            rename
close           lcd             open            rmdir
ftp>
```

11. Telnet:

→ This command is used to access a remote host in Terminal mode (passive screen).

→ It also allows you to check if any TCP service is running on a remote server by specifying the IP address after the TCP port number.

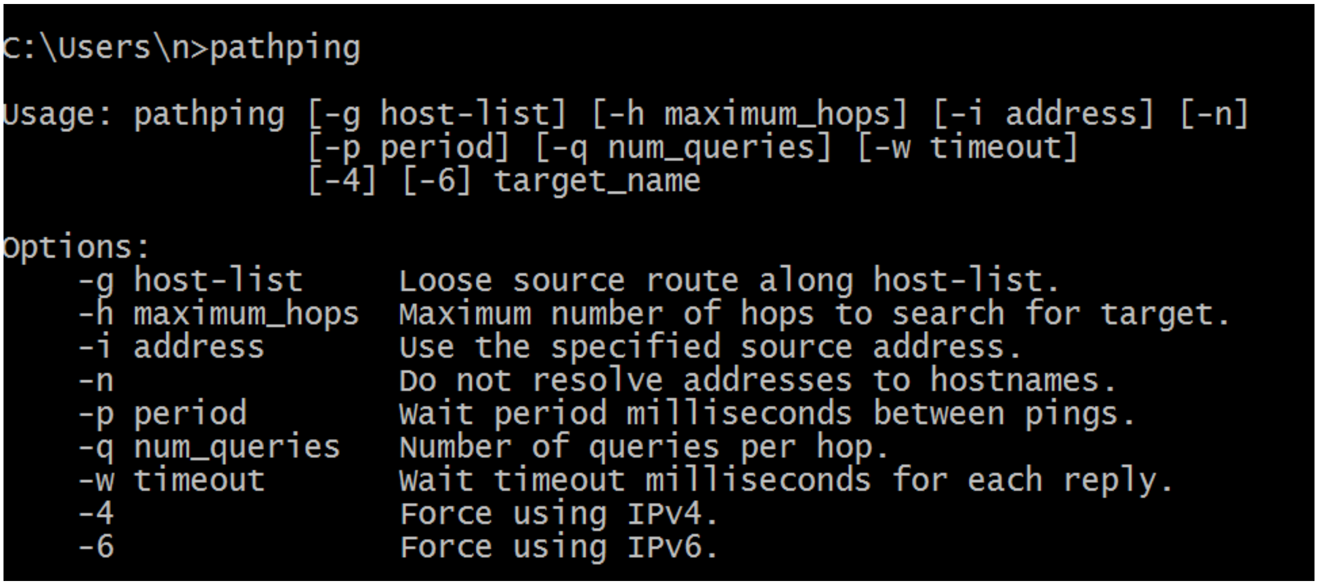


```
C:\Users\ELMAJDAL>telnet /?

telnet [-a][-e escape char][-f log file][-l user][-t term][host [port]]
 -a       Attempt automatic logon. Same as -l option except uses
          the currently logged on user’s name.
 -e       Escape character to enter telnet client prompt.
 -f       File name for client side logging
 -l       Specifies the user name to log in with on the remote system.
          Requires that the remote system support the TELNET ENVIRON option.
 -t       Specifies terminal type.
          Supported term types are vt100, vt52, ansi and vtnt only.
 host     Specifies the hostname or IP address of the remote computer
          to connect to.
 port     Specifies a port number or service name.
```

12. PathPing:

→ The PathPing tool is a utility that combines the best aspects of Tracert and Ping.

→ Entering the PathPing command followed by a hostname initiates what looks like a somewhat standard Tracert process.

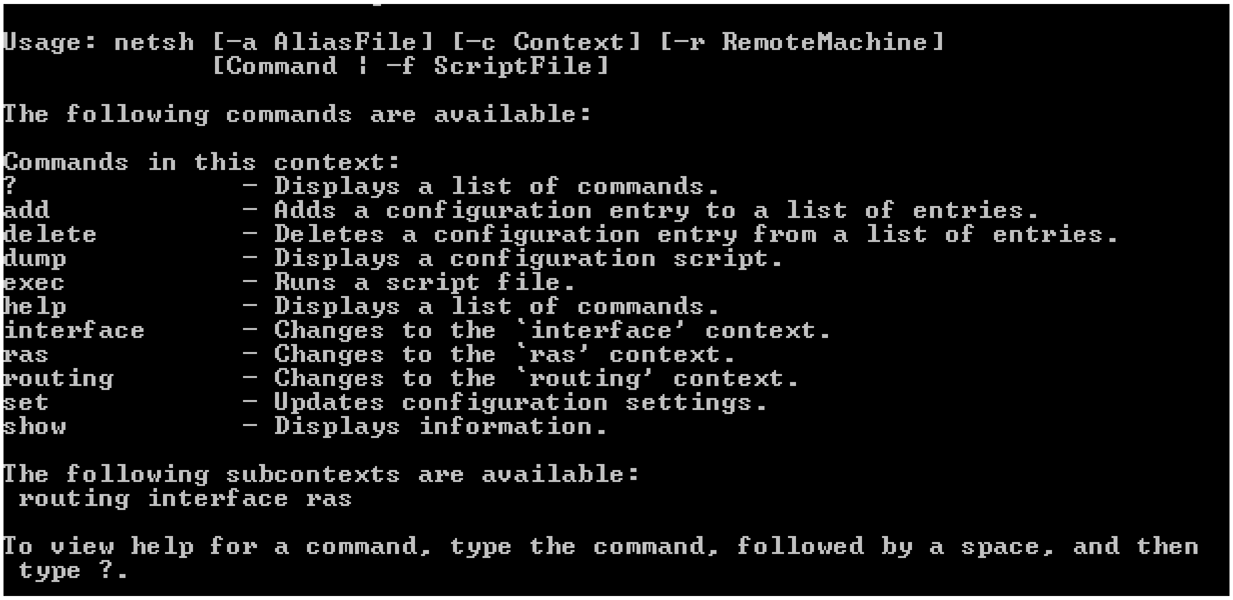


```
C:\Users\n>pathping

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.
```

13. NETSH:

→ NETSH, is a suite of command line networking tools. It comes with its own shell or interface and is contained in a number of Windows operating systems.

→ The Network Services Shell is opened by entering netsh into a regular command promt.



```
Usage: netsh [-a AliasFile] [-c Context] [-r RemoteMachine]
             [Command | -f ScriptFile]

The following commands are available:

Commands in this context:
?              - Displays a list of commands.
add            - Adds a configuration entry to a list of entries.
delete         - Deletes a configuration entry from a list of entries.
dump           - Displays a configuration script.
exec           - Runs a script file.
help           - Displays a list of commands.
interface      - Changes to the `interface' context.
ras            - Changes to the `ras' context.
routing        - Changes to the `routing' context.
set            - Updates configuration settings.
show           - Displays information.

The following subcontexts are available:
 routing interface ras

To view help for a command, type the command, followed by a space, and then
 type ?.
```

14. Route:

→ Displays or modifies the routing table

```
ROUTE [-f] [command [destination] [MASK network
mask] [gateway]
```

1. **-f:**

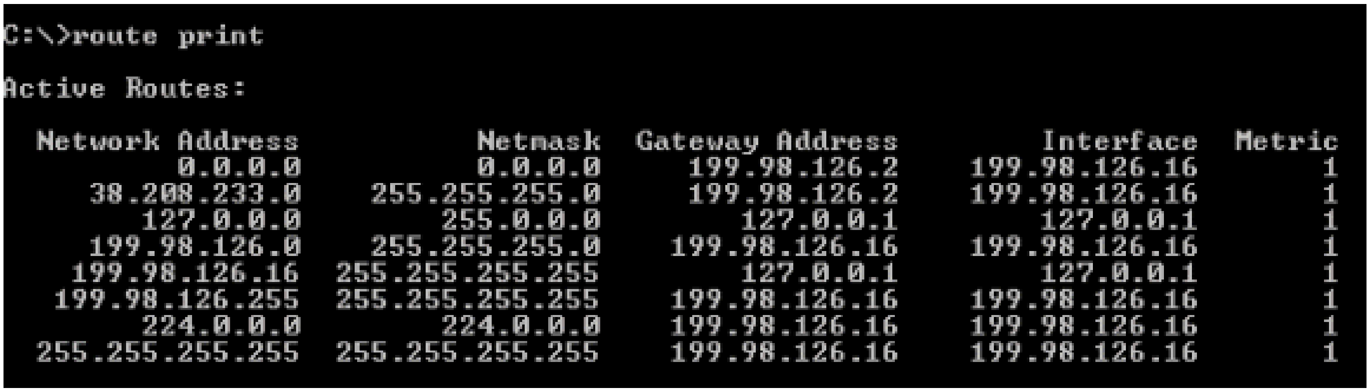
   Clears the routing tables of all gateway entries. Used in conjunction with one of the below "commands", the tables are cleared before executing the command.

2. **–p:**

   Makes the entry into the table, residual (after reboot).

→ Specify one of four commands:

1. **DELETE:** Deletes a route.
2. **PRINT:** Displays a route.
3. **ADD:** Adds a route.
4. **CHANGE:** Modifies an existing route.
5. **destination:** Specifies the host.
6. **MASK:** If the MASK keyword is present, the next parameter is interpreted as the network mask parameter.
7. **netmask:** Provided, it specifies the value of the subnet mask to be associated with this route entry. Unspecified, it takes the default value of 255.255.255.255.
8. **Gateway:** Specifies the gateway.
9. **METRIC:** Specifies the cost metric for the destination.



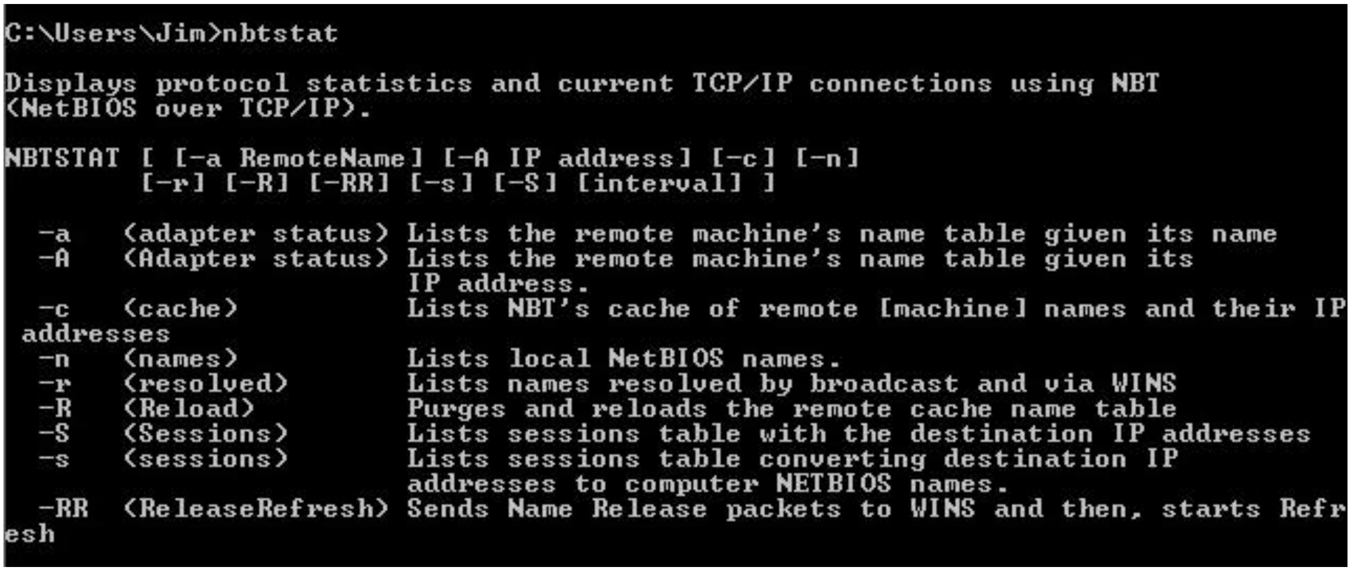
```
C:\>route print

Active Routes:

  Network Address          Netmask  Gateway Address       Interface  Metric
          0.0.0.0          0.0.0.0     199.98.126.2   199.98.126.16       1
     38.208.233.0    255.255.255.0     199.98.126.2   199.98.126.16       1
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
     199.98.126.0    255.255.255.0    199.98.126.16   199.98.126.16       1
    199.98.126.16  255.255.255.255        127.0.0.1       127.0.0.1       1
   199.98.126.255  255.255.255.255    199.98.126.16   199.98.126.16       1
        224.0.0.0        224.0.0.0    199.98.126.16   199.98.126.16       1
  255.255.255.255  255.255.255.255    199.98.126.16   199.98.126.16       1
```

15. Nbtstat:

→ Update cache of the LMHOSTS file. Displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP).

```
NBTSTAT [-a Remote Name] [-A IP address] [-c] [-n]
[-  r] [-R] [-s] [S] [interval]
```

1. **-a (adapter status):**
   Display the table (names) of the remote machine (known name).
2. **-A (adapter status):**
   Display the table (names) of the remote machine (IP address).
3. **-c (cache):**
   Display the remote name cache including the IP addresses.
4. **-n (names):**
   Lists local NetBIOS names.
5. **-r (resolved):**
   Lists names resolved by broadcast and via WINS.
6. **-R (Reload):**
   Clear and reload the table cache with the remote names.
7. **-S (Sessions):**
   Lists the sessions table with the destination IP addresses.
8. **-s (sessions):**
   Lists the sessions table with the destination IP addresses converted to host names via the hosts file.



```
C:\Users\Jim>nbtstat

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (adapter status) Lists the remote machine's name table given its name
  -A   (Adapter status) Lists the remote machine's name table given its
                        IP address.
  -c   (cache)          Lists NBT's cache of remote [machine] names and their IP
 addresses
  -n   (names)          Lists local NetBIOS names.
  -r   (resolved)       Lists names resolved by broadcast and via WINS
  -R   (Reload)         Purges and reloads the remote cache name table
  -S   (Sessions)       Lists sessions table with the destination IP addresses
  -s   (sessions)       Lists sessions table converting destination IP
                        addresses to computer NETBIOS names.
  -RR  (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refr
esh
```