

## **Experiment No : 02**

**Aim :** To execute and analyze basic networking commands.

### **1. Route**

The route command allows you to make manual entries into the network routing tables. The route command distinguishes between routes to hosts and routes to networks by interpreting the network address of the Destination variable, which can be specified either by symbolic name or numeric address. The route command resolves all

symbolic names into addresses, using either the /etc/hosts file or the network name server.

Routes to a particular host are distinguished from those to a network by interpreting the Internet address associated with the destination. The optional phs -net and -host force the destination to be interpreted as a network or a host, respectively. If the destination has a local address part of INADDR\_ANY or if the destination is the symbolic name of a network, then the route is assumed to be to a network; otherwise, it is presumed to be a route to a host.

For example, 128.32 is interpreted as -host 128.0.0.32; 128.32.130 is interpreted as -host 128.32.0.130; -net 128.32 is interpreted as 128.32.0.0; and -net 128.32.130 is interpreted as 128.32.130.0.

Command Prompt

Microsoft Windows [Version 10.0.19043.1466]  
(c) Microsoft Corporation. All rights reserved.

C:\Users\LENOVO>Route

Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]  
                  [MASK netmask]  [gateway] [METRIC metric]  [IF interface]

-f              Clears the routing tables of all gateway entries. If this is used in conjunction with one of the commands, the tables are cleared prior to running the command.

-p              When used with the ADD command, makes a route persistent across boots of the system. By default, routes are not preserved when the system is restarted. Ignored for all other commands, which always affect the appropriate persistent routes.

-4             Force using IPv4.

-6             Force using IPv6.

command        One of these:  
                 PRINT    Prints a route  
                 ADD      Adds a route  
                 DELETE   Deletes a route  
                 CHANGE   Modifies an existing route

destination    Specifies the host.

MASK           Specifies that the next parameter is the 'netmask' value.

netmask        Specifies a subnet mask value for this route entry.  
                 If not specified, it defaults to 255.255.255.255.

gateway        Specifies gateway.

interface      the interface number for the specified route.

METRIC        specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database file NETWORKS. The symbolic names for gateway are looked up in the host name database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard, (wildcard is specified as a star '\*'), or the gateway argument may be omitted.

If Dest contains a \* or ?, it is treated as a shell pattern, and only

```

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Pattern match is only allowed in PRINT command.

Diagnostic Notes:
    Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
    Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
              The route addition failed: The specified mask parameter is invalid. (Destination & Mask) != Destination.

Examples:
    > route PRINT
    > route PRINT -4
    > route PRINT -6
    > route PRINT 157*           .... Only prints those matching 157*
    > route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
        destination^      ^mask          ^gateway      metric^   ^
                                         Interface^
    If IF is not given, it tries to find the best interface for a given
    gateway.
    > route ADD 3ffe::/32 3ffe::1

    > route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2
        CHANGE is used to modify gateway and/or metric only.

    > route DELETE 157.0.0.0
    > route DELETE 3ffe::/32

C:\Users\LENOVO>

```

## 2. Ping

Ping is used to testing a network host capacity to interact with another host. Just enter the command Ping, followed by the target host's name or IP address.

The ping utilities seem to be the most common network tool. This is performed by using the Internet Control Message Protocol, which allows the echo packet to be sent to the destination host and a listening mechanism.

If the destination host reply to the requesting host, that means the host is reachable. This utility usually gives a basic image of where there may be a specific networking issue,

Command Prompt

Microsoft Windows [Version 10.0.19043.1466]  
(c) Microsoft Corporation. All rights reserved.

C:\Users\LENOVO>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] [-c compartment] [-p]  
[-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 Header).
-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). Per RFC 5095 the use of this routing header has been deprecated. Some systems may drop echo requests if this header is used.
-S srcaddr	Source address to use.
-c compartment	Routing compartment identifier.
-p	Ping a Hyper-V Network Virtualization provider address.
-4	Force using IPv4.
-6	Force using IPv6.

### 3. IP config

The command IP config will display basic details about the device's IP address configuration.

Just type IP config in the Windows prompt and the IP, subnet mask and default gateway that the current device will be presented.

If you have to see full information, then type on command prompt config-all and then you will see full information.

There are also choices to assist you in resolving DNS and DHCP issues.

```
Windows Command Prompt
Microsoft Windows [Version 10.0.19043.1466]
(c) Microsoft Corporation. All rights reserved.

C:\Users\LENOVO>ipconfig

Windows IP Configuration

Ethernet adapter VirtualBox Host-Only Network:

  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . : fe80::31ee:b202:269b:161b%7
  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:

  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . : fe80::4d83:6173:932c:4eea%4
  IPv4 Address. . . . . : 192.168.137.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:

  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . : fe80::d88e:4aeb:c157:705e%10
  IPv4 Address. . . . . : 192.168.0.104
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.0.1
```

## 4. Tracert

The *tracert* command (spelled *traceroute* in Unix/Linux implementations) is one of the key diagnostic tools for TCP/IP. It displays a list of all the routers that a packet must go through to get from the computer where *tracert* is run to any other computer on the Internet. Each one of these routers is called a *hop*, presumably because the original designers of the IP protocol played a lot of hopscotch when they were young. If you can't connect to another computer, you can use *tracert* to find out exactly where the problem is occurring.

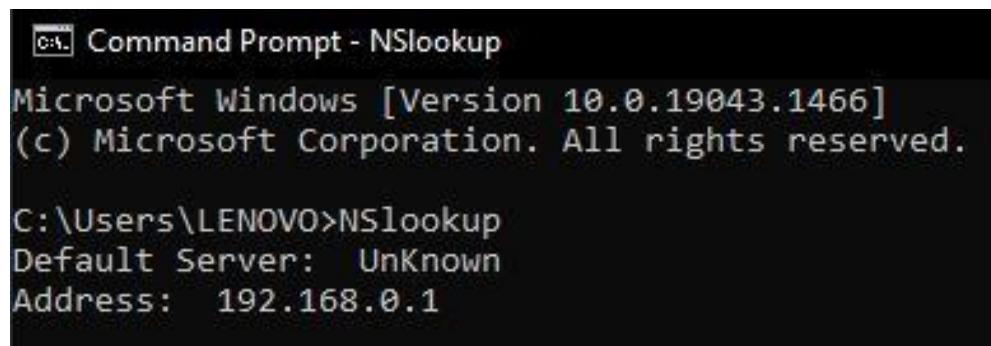
*tracert* makes three attempts to contact the router at each hop and displays the response time for each of these attempts. Then, it displays the DNS name of the router (if available) and the router's IP address.

```
[cmd] Command Prompt  
Microsoft Windows [Version 10.0.19043.1466]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\LENOVO>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.  
  
C:\Users\LENOVO>
```

## **5. NSLOOKUP**

The Nslookup, which stands for name server lookup command, is a network utility command used to obtain information about internet servers.

It provides name server information for the DNS (Domain Name System), i.e. the default DNS server's name and IP Address.



```
Command Prompt - NSlookup
Microsoft Windows [Version 10.0.19043.1466]
(c) Microsoft Corporation. All rights reserved.

C:\Users\LENOVO>NSlookup
Default Server: UnKnown
Address: 192.168.0.1
```

## **6. ARP**

ARP stands for Address Resolution Protocol. Although network communications can readily be thought of as an IP address, the packet delivery depends ultimately on the media access control (MAC).

This is where the protocol for address resolution comes into effect. You can add the remote host IP address, which is an arp -a command, in case you have issues to communicate with a given host.

```
Command Prompt
Microsoft Windows [Version 10.0.19043.1466]
(c) Microsoft Corporation. All rights reserved.

C:\Users\LENOVO>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.

C:\Users\LENOVO>
```

## 7. Host Name

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.

```
Command Prompt
Microsoft Windows [Version 10.0.19043.1466]
(c) Microsoft Corporation. All rights reserved.

C:\Users\LENOVO>Hostname
LAPTOP-VND8ON30

C:\Users\LENOVO>
```

## 8. Netstat

Netstat is a Common TCP – IP networking command-line method present in most Windows, Linux, UNIX, and other operating systems. The netstat provides the statistics and information in the use of the current TCP-IP Connection network about the protocol.

```
Command Prompt - netstat
Microsoft Windows [Version 10.0.19043.1466]
(c) Microsoft Corporation. All rights reserved.

C:\Users\LENOVO>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.0.104:53419  203.23.178.53:http    ESTABLISHED
  TCP    192.168.0.104:53428  20.198.162.76:https  ESTABLISHED
  TCP    192.168.0.104:53660  si-in-f188:5228      ESTABLISHED
  TCP    192.168.0.104:54194  whatsapp-cdn-shv-01-bom1:https ESTABLISHED
  TCP    192.168.0.104:54230  40.100.141.2:https   ESTABLISHED
  TCP    192.168.0.104:54344  13.107.4.254:https   FIN_WAIT_1
  TCP    192.168.0.104:54377  85:https                 ESTABLISHED
  TCP    192.168.0.104:54539  104.18.2.88:https    ESTABLISHED
  TCP    192.168.0.104:54546  8.247.52.123:https   ESTABLISHED
  TCP    192.168.0.104:54547  8.247.52.123:https   ESTABLISHED
  TCP    192.168.0.104:54552  8.247.52.123:https   ESTABLISHED
  TCP    192.168.0.104:54584  a-0001:https            ESTABLISHED
  TCP    192.168.0.104:54590  20.69.137.228:https  TIME_WAIT
  TCP    192.168.0.104:54591  40.100.138.130:https TIME_WAIT
  TCP    192.168.0.104:54594  13.107.42.254:https  TIME_WAIT
  TCP    192.168.0.104:54595  204.79.197.222:https TIME_WAIT
  TCP    192.168.0.104:54598  20.69.137.228:https  TIME_WAIT
  TCP    192.168.0.104:54599  bom07s30-in-f19:https  ESTABLISHED
  TCP    192.168.0.104:54600  40.100.138.130:https ESTABLISHED
```

**Conclusion :** Therefor we have successfully implemented and analysed the networking commands