Ex.No:	
Date :	**Networking Basic Commands**

Objectives:

To analyze the network basic commands.

Introduction:

In networking there are various commands that can be used to check the connectivity of the networking devices and it is also required at time of troubleshooting of devices. We will be discussing few of the networking commands such as color help, ipconfig ,ipconfig/all ,nslookup ,tracert commands.

Requirements:

1. End Device (Command Prompt)
2. Ethernet & Internet Services
3. Commands

Commands Execution:

1. ipconfig:

This networking commands is used to the IP configuration details. This command provides you the details like IPv4 address ,Subnet Mask or Default Gateway.

C:\Users\KARE>ipconfig Output:

2. ipconfig /all:

This command can be understood as the updated version of the ipconfig command. This command tells us the physical address of our device. It tells us various details of our computer such as IPv4,IPv6 default Gateway ,subnet mask ,also it tells to which devices our device is connected ,configuration details of the devices to which are devices are connected.

C:\Users\KARE>ipconfig /all Output:

```
C:\Users\Chaitanya>ipconfig /all
Windows IP Configuration
    Host Name . . . . . . . . . . . . : Hanumaan
    Primary Dns Suffix  . . . . . . . :
    Node Type . . . . . . . . . . . . : Mixed
    IP Routing Enabled. . . . . . . . : No
    WINS Proxy Enabled. . . . . . . . : No
Ethernet adapter Ethernet 3:
    Connection-specific DNS Suffix  . :
    Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
    Physical Address. . . . . . . . . : 0A-00-27-00-00-02
    DHCP Enabled. . . . . . . . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::954:8724:c986:29e4%2(Preferred)
    IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . . :
    DHCPv6 IAID . . . . . . . . . . . : 688521255
    DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-2E-61-7B-F8-B5-4D-44-90-4E
    NetBIOS over Tcpip. . . . . . . . : Enabled
Wireless LAN adapter Local Area Connection* 3:
    Media State . . . . . . . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
    Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
    Physical Address. . . . . . . . . : F8-B5-4D-44-90-4F
    DHCP Enabled. . . . . . . . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
Wireless LAN adapter Local Area Connection* 4:
    Media State . . . . . . . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
    Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
    Physical Address. . . . . . . . . : FA-B5-4D-44-90-4E
    DHCP Enabled. . . . . . . . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
Wireless LAN adapter Wi-Fi:
    Connection-specific DNS Suffix  . :
    Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
    Physical Address. . . . . . . . . : F8-B5-4D-44-90-4E
    DHCP Enabled. . . . . . . . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IPv4 Address. . . . . . . . . . . : 192.168.206.28(Preferred)
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Lease Obtained. . . . . . . . . . : 19 December 2024 11:34:22
    Lease Expires . . . . . . . . . . : 19 December 2024 12:34:22
    Default Gateway . . . . . . . . . : 192.168.206.187
    DHCP Server . . . . . . . . . . . : 192.168.206.187
    DNS Servers . . . . . . . . . . . : 192.168.206.187
    NetBIOS over Tcpip. . . . . . . . : Enabled
```

3. hostname:

The hostname command displays the hostname of the system. The hostname command is much easier to use than going into the system settings to search for it.

C:\Users\KARE>hostname Output:

```
C:\Users\Chaitanya>hostname
Hanumaan
```

4. systeminfo:

This Command is used to display all the necessary information about our System such as configuration, version, hostname, processor details network card details etc.

C:\Users\KARE>systeminfo Output:

5. nslookup:

This command is use to transform the given searched words into their corresponding IP addresses.

C:\Users\KARE>nslookup

C:\Users\KARE>nslookup Destination Hostname / Destination IP Address Output:

6. ping:

Ping command is used to get to know if the particular site can be reached by the ping command. The ping command checks this by sending the packets of data to the destination address and if the data returns to us in the given time frame then it means that the particular website can be reached .We can do this by writing the ping and we write the IP address of the site we want to search.

C:\Users\KARE>ping IPAddress   (or)   C:\Users\KARE>ping   hostname

C:\Users\KARE>ping -t IPAddress / Hostname

Output:

```
C:\Users\Chaitanya>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.
```

7. tracert:

This command can be understood as trace root. Which tells that our computer reaches or hits whichwhich server for reaching the particular root.

C:\Users\KARE>tracert IPAddress   (or)   C:\Users\KARE>tracert hostname

Output:

```
C:\Users\Chaitanya>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.
```

8. pathping:

pathping is similar to tracert, except it is more informative and takes a lot longer to execute. After sending out packets from you to a given destination, it analyzes the route taken and computes packet loss on a per-hop basis.

C:\Users\KARE>pathping IPAddress   (or)   C:\Users\KARE>pathping hostname Output:

```
C:\Users\Chaitanya>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.
```

9. netstat:

It is a command line tool that is identify and display the connections and ports connected to our computer when we write netstat command on CLI(Command Line Interface). It tells us active connections with our computer and it tells us local address ,foreign address and the state of the device. In local address first 8 digits specify the local address of our computer and and last 5 digits tells the port number to which our computer is connected . In netstat command there are various subcommands such as netstat -n, netstat -a,netstat -b, netstat -f.

C:\Users\KARE>netstat

Output:

```
C:\Users\Chaitanya>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49671        Hanumaan:49672         ESTABLISHED
  TCP    127.0.0.1:49672        Hanumaan:49671         ESTABLISHED
  TCP    127.0.0.1:49673        Hanumaan:49674         ESTABLISHED
  TCP    127.0.0.1:49674        Hanumaan:49673         ESTABLISHED
  TCP    127.0.0.1:49749        Hanumaan:49750         ESTABLISHED
  TCP    127.0.0.1:49750        Hanumaan:49749         ESTABLISHED
  TCP    127.0.0.1:49754        Hanumaan:49755         ESTABLISHED
  TCP    127.0.0.1:49755        Hanumaan:49754         ESTABLISHED
  TCP    192.168.206.28:3947    52.188.247.144:https   ESTABLISHED
```

10.getmac:

Getmac is a Windows command used to display the Media Access Control (MAC) addresses for each network adapter in the computer.

C:\Users\KARE>getmac Output:

```
C:\Users\Chaitanya>getmac

Physical Address     Transport Name
==================   =========================================================
F8-B5-4D-44-90-4E    \Device\Tcpip_{7CFEC0D4-EA3A-494E-A325-3C6D99161DE4}
0A-00-27-00-00-02    \Device\Tcpip_{04965853-9EB7-4A5E-BF0C-5F19290C9FEA}
```

11.ARP:

The arp command displays and modifies the Internet-to-adapter address translation tables used by the Address in Networks and communication management. The arp command displays the current ARP entry for the host specified by the HostName variable. The host can be specified by name or number, using Internet dotted decimal notation.

C:\Users\KARE>arp -a

Output:

```
C:\Users\Chaitanya>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.
```

12. 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.

C:\Users\KARE>route   (or)   C:\Users\KARE>route print

Output:

```
C:\Users\Chaitanya>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
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.
```