Batch: SY_IT (B2) **Experiment Number: 1**

Roll Number: 16010423076 **Name: Ritesh Jha**

Aim of the Experiment: Study of various networking commands.

Program/ Steps:

1)Ping

2)ipconfig

3) tracert

4) Arp

5) Netstat

6) Nslookup

Nslookup is a network administration command-line tool for querying the Domain Name System to obtain the mapping between domain name and IP address.

7) Systeminfo

Displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties (such as RAM, disk space, and network cards).

Output/Result:

1)Ping kjsce.somaiya.edu

```
C:\Users\SVVAdmin>ping kjsce.somaiya.edu

Pinging application-load-balancer-1808612506.ap-south-1.elb.amazonaws.com [13.126.208.18] with 32 bytes of data:
Reply from 13.126.208.18: bytes=32 time=5ms TTL=242
Reply from 13.126.208.18: bytes=32 time=5ms TTL=242
Reply from 13.126.208.18: bytes=32 time=5ms TTL=242
Reply from 13.126.208.18: bytes=32 time=5ms TTL=242

Ping statistics for 13.126.208.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 5ms, Average = 5ms
```

2)ipconfig

```
C:\Users\SVVAdmin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3830:fdb1:8325:ef9%7
   IPv4 Address. . . . . . . . . . . : 172.17.16.166
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 172.17.17.254
```

3) tracert kjsce.somaiya.edu

```
C:\Users\SVVAdmin>tracert kjsce.somaiya.edu

Tracing route to application-load-balancer-1808612506.ap-south-1.elb.amazonaws.com [52.66.96.181]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  172.17.17.254
  2     1 ms     1 ms     1 ms  172.17.52.240
  3    <1 ms    <1 ms    <1 ms  172.30.250.250
  4    24 ms    39 ms    27 ms  14.142.143.97.static-mumbai.vsnl.net.in [14.142.143.97]
  5     *       21 ms    22 ms  172.23.78.237
  6     *        *        *     Request timed out.
  7    22 ms    23 ms    23 ms  121.244.71.190.static-lvsb.vsnl.net.in [121.244.71.190]
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
```

4) Arp -a -N 172.17.16.166

```
C:\Users\SVVAdmin>Arp -a -N 172.17.16.166

Interface: 172.17.16.166 --- 0x7
  Internet Address      Physical Address      Type
  172.17.16.14          d8-cb-8a-0c-88-11     dynamic
  172.17.16.61          64-4e-d7-6d-69-dc     dynamic
  172.17.16.110         c4-71-54-33-03-4f     dynamic
  172.17.16.133         3c-52-82-70-5e-1e     dynamic
  172.17.16.169         64-4e-d7-6d-69-ce     dynamic
  172.17.16.207         64-4e-d7-6d-6d-6d     dynamic
  172.17.16.225         64-4e-d7-6d-6b-e1     dynamic
  172.17.16.245         40-b0-34-3a-79-ae     dynamic
  172.17.17.228         f8-bc-12-5f-cc-6f     dynamic
  172.17.17.254         b0-aa-77-66-d1-41     dynamic
  172.17.17.255         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
```

5) Netstat -a

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

                           Received            Sent

Bytes                    1523825737       215591712
Unicast packets             1226757          459844
Non-unicast packets          713419            3073
Discards                          0               0
Errors                            0               0
Unknown protocols                 0
```

```
C:\Users\SVVAdmin>Netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             16DITB212-06:0         LISTENING
  TCP    0.0.0.0:135            16DITB212-06:0         LISTENING
  TCP    0.0.0.0:443            16DITB212-06:0         LISTENING
  TCP    0.0.0.0:445            16DITB212-06:0         LISTENING
  TCP    0.0.0.0:3306           16DITB212-06:0         LISTENING
  TCP    0.0.0.0:5040           16DITB212-06:0         LISTENING
  TCP    0.0.0.0:5357           16DITB212-06:0         LISTENING
  TCP    0.0.0.0:5432           16DITB212-06:0         LISTENING
  TCP    0.0.0.0:6880           16DITB212-06:0         LISTENING
  TCP    0.0.0.0:7680           16DITB212-06:0         LISTENING
  TCP    0.0.0.0:33060          16DITB212-06:0         LISTENING
  TCP    0.0.0.0:49664          16DITB212-06:0         LISTENING
  TCP    0.0.0.0:49665          16DITB212-06:0         LISTENING
  TCP    0.0.0.0:49666          16DITB212-06:0         LISTENING
  TCP    0.0.0.0:49667          16DITB212-06:0         LISTENING
  TCP    0.0.0.0:49669          16DITB212-06:0         LISTENING
  TCP    0.0.0.0:49694          16DITB212-06:0         LISTENING
  TCP    127.0.0.1:30523        16DITB212-06:0         LISTENING
  TCP    127.0.0.1:49695        16DITB212-06:49696     ESTABLISHED
  TCP    127.0.0.1:49696        16DITB212-06:49695     ESTABLISHED
  TCP    127.0.0.1:49697        16DITB212-06:49698     ESTABLISHED
  TCP    127.0.0.1:49698        16DITB212-06:49697     ESTABLISHED
  TCP    127.0.0.1:49718        16DITB212-06:0         LISTENING
  TCP    127.0.0.1:49886        16DITB212-06:0         LISTENING
  TCP    127.0.0.1:57925        16DITB212-06:0         LISTENING
  TCP    127.0.0.1:62540        16DITB212-06:0         LISTENING
```

6) Nslookup

```
C:\Users\SVVAdmin>NSLOOKUP
Default Server:  svvpdc.svv.local
Address:  172.31.0.25
```

7)Systeminfo

```
C:\Users\SVVAdmin>SystemInfo

Host Name:                 16DITB212-06
OS Name:                   Microsoft Windows 10 Pro for Workstations
OS Version:                10.0.19045 N/A Build 19045
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          admin
Registered Organization:
Product ID:                00391-90090-60463-AA621
Original Install Date:     10/4/2022, 12:25:31 AM
System Boot Time:          7/29/2024, 4:06:14 PM
System Manufacturer:       LENOVO
System Model:              10HJA02AHF
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 60 Stepping 3 GenuineIntel ~1000 Mhz
BIOS Version:              LENOVO FCKT69AUS, 4/10/2015
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     8,105 MB
Available Physical Memory: 3,084 MB
Virtual Memory: Max Size:  11,686 MB
Virtual Memory: Available: 4,360 MB
Virtual Memory: In Use:    7,326 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    AAA
Logon Server:              \\16DITB212-06
Hotfix(s):                 26 Hotfix(s) Installed.
                           [01]: KB5041168
                           [02]: KB5028853
                           [03]: KB4562830
                           [04]: KB4570334
```

Post Lab Question-Answers:

1. ICMP is used in both Ping & Traceroute.
2. Route command is used to manipulate TCP/IP routing table.
3. Select the false statement from the following.

   c) Pathping combines the functionality of ping with that of route

---

Outcomes:

CO1 **:** Understand the data communication systems, network topologies and network devices.

Conclusion (based on the Results and outcomes achieved):

By performing this experiment, I learnt about the basic networking commands and their usage on the command line. Every system is connected to numerous different networks and systems through internal or external network channels. These network settings often run into issues and affect the system's working. Such network problems can be resolved using 'networking commands.'

References:

Books/ Journals/ Websites:

- Behrouz A Forouzan, Data Communication and Networking, Tata Mc Graw hill, India, 4th Edition
- A. S. Tanenbaum, "Computer Networks", 4th edition, Prentice Hall

- Behrouz A Forouzan, Data Communication and Networking, Tata Mc Graw hill, India, 4th Edition
- A. S. Tanenbaum, "Computer Networks", 4th edition, Prentice Hall

Experiment No:1
Title: Networking Commands

Batch: **Roll No.:** **Experiment No. 1**

Aim: Study of various networking commands.

Resources needed: PC, Windows OS

Theory:

1. Ping

The **ping** command is used to test connectivity between two hosts. It sends ICMP echo request messages to the destination. The destination host replies with ICMP reply messages. If the ping command gets a reply from the destination host, it displays the reply along with round-trip times.

The **ping** command uses the following syntax.

ping *destination host IP or name*

The following command tests connectivity between the host computer and Google's server.

ping **google.com**

2. Ipconfig

This command displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. This command is mainly used to view the IP addresses on the computers that are configured to obtain their IP address automatically.

The following table lists some important options of the **ipconfig** command.

Used without parameters	Displays the IP address, subnet mask, and default gateway for all adapters.
/all	Displays the full TCP/IP configuration for all adapters.
/renew [Adapter]	Renews DHCP configuration for all adapters (if an adapter is not specified) or for a specific adapter if the Adapter parameter is included.
/release [Adapter]	Sends a DHCPRELEASE message to the DHCP server to release the current DHCP configuration and discard the IP address configuration for either all adapters (if an adapter is not specified) or for a specific adapter if the Adapter parameter is included.
/flushdns	Flushes and resets the contents of the DNS client resolver cache.

3. Tracert

This command is used to diagnose path-related problems. On an IP network, routers exchange IP packets between the source and the destination. They take IP packets from the source host and forward them in a sequence until they reach the destination host. The sequence of routers between the source and destination is known as the path. A path consists of all routers in a sequence that IP packets sent from the source host traverse to reach the destination host.The tracert command prints the path. If all routers on the path are functional, this command prints the full path. If a router is down on the path, this command prints the path up to the last operational router.

The **tracert** command uses the following syntax.

```
tracert  Destination Name or IP address
```

The following command traces the path to the host named www.google.co.in.

```
tracert www.google.co.in
```

The following table lists some important options of the **tracert** command.

Option	Description
-d	Do not resolve the IP addresses of intermediate routers to their names.
-h	Specifies the maximum number of hops (routers) to search on the path. The default is 30 hops.
-w	Specifies the amount of time in milliseconds to wait for a reply message from the router. If not received within the time-out, an asterisk (*) is displayed. The default time-out is 4000 (4 seconds).

4. Arp

To send IP packets, a computer needs two addresses. These addresses are the MAC address and the IP address. A MAC address is the physical or hardware address of the NIC. An IP address is the logical or software address of NIC. If a computer knows the IP address of the destination computer but it does not know the MAC address of the destination computer, it uses the ARP protocol to know the MAC address of the destination computer.

The ARP protocol broadcasts a given IP address over a local network. The corresponding host responds to the broadcast with its MAC address. To avoid repetition, ARP stores the answer in a table known as **ARP table**. ARP maintains a separate ARP table for each NIC.

To view the ARP table, you can use the following command.

```
arp
```

By default, this command displays the ARP table of the active NIC. If multiple NICs are installed on the computer, you can use the **-a** option with this command. If the -a option is used, the ARP command displays all ARP tables.

To display the ARP cache entry for a specific IP address, specify the IP address with the **-N** option. For example, the following command displays the ARP cache table for the interface that is assigned the IP address 192.168.42.171.

```
Arp -a -N 192.168.42.171
```

5. Netstat

This command displays active connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, and IP statistics.

The output of this command is organized in rows and columns. Each row represents a new connection or an entry in the output. It contains four columns. These columns provide the following information about the row.

Proto: - This column displays the name of the protocol (TCP or UDP).

Local Address: - This column displays the IP address of the local computer and the port number being used. If the port is not yet established, the port number is shown as an asterisk (*****).

Foreign Address: - This column displays the IP address and port number of the remote computer to which the port is connected.

State: - This column displays the status of the connection.

1. **Options and parameters**

The following table lists some common options of the **netstat** command.

Option	Description
-a	Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
-e	Displays Ethernet statistics, such as the number of bytes and packets sent and received.
-n	Displays active TCP connections, however, addresses and port numbers are expressed numerically, and no attempt is made to determine names.
-o	Displays active TCP connections and includes the process ID (PID) for each connection.
-p	Shows connections for the protocol specified by Protocol. In this case, the Protocol can be TCP, UDP, tcpv6, or udpv6.
-s	Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols.
-r	Displays the contents of the IP routing table.

Activity:

1. **Run all the commands mentioned in the theory and put the output in the results section.**

2. **Identify 2 new networking commands, run these commands, and paste the output in results section.**

Results:

Questions

1. ICMP is used in _____
   a) Ping
   b) Traceroute
   c) Ifconfig
   d) Both Ping & Traceroute
2. _____ command is used to manipulate TCP/IP routing table.
   a) route
   b) Ipconfig
   c) Ifconfig
   d) Traceroute

3. Select the false statement from the following.
   a) Nslookup is used to query a DNS server for DNS data
   b) Ping is used to check connectivity
   c) Pathping combines the functionality of ping with that of route
   d) Ifconfig can configure TCP/IP network interface parameters

---

Outcomes:

Conclusion:

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

References:

Books/ Journals/ Websites:

- Behrouz A Forouzan, Data Communication and Networking, Tata Mc Graw hill, India, 4th Edition
- A. S. Tanenbaum, "Computer Networks", 4th edition, Prentice Hall

- Behrouz A Forouzan, Data Communication and Networking, Tata Mc Graw hill, India, 4th Edition
- A. S. Tanenbaum, "Computer Networks", 4th edition, Prentice Hall