ASSIGNMENT – 01

(Study of some Networking Commands and Protocols)

Q. Commands — (Ping, ipconfig/ifconfig, traceroute/tracert, nslookup, netstat) Protocols — (telnet, ssh, ftp)

Try executing the above commands and provide a writeup containing purpose of the command or protocol, syntax/usage, important options (if any)

PING : PING (Packet Internet Groper) command is used to check the network connectivity between host and server/host. This command takes as input the IP address or the URL and sends a data packet to the specified address with the message "PING" and get a response from the server/host this time is recorded which is called latency. Fast ping low latency means faster connection.

Syntax: ping [options] hostname or IP address / ping www.destination_host_name.com.

Use : 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

Ping command syntax for windows :

-t Pings the specified host until stopped. To stop - type Control-C

-a Resolve adresses to hostnames

-n Number of echo requests to send

-l Send buffer size

-f Set Don't Fragmet flag in packet (IPv4-only)

-i Set Time To Live

-v Set Type of Service (Setting has been deprecated)

-r Record route for count hops (IPv4-only)

-s Timestamp for count hops (IPv4-only)

-j Loose source route along host-list (IPv4-only)

-k Strict source route along host-list (IPv4-only)

-w Timeout in milliseconds to wait for each reply

-R Use routing header to test reverse route also (IPv6-only, deprecated per RFC 5095)

-S Source address to use

-c Routing compartment identifier

-p Ping a Hyper-V Network Virtualization provider address

-4 Force using IPv4

-6 Force using Ipv6

Default Size :- OptionUse-n counts Count determines the number of echo request to send. The default is 4 request. Also, -l give the size enable opportunity to change the size of packet. The default is 32 bytes. We can set between 32 to 65,527 bytes.

PORT :- ping test used ICMP, so there is no real port. Port number belong to transport layer protocols, such as TCP and UDP.

ICMP basically sits on the top of the IP Address. So, it is not a layer 4 protocols. We can ping a specific port, On linux by using -> Telnet, Netcat, Network Mapper.

On windows by using -> Telnet, PowerShell.

This make a test simple, fast and effective. Also less Random

Failed Case :- If we pinging specific IP address on our local netwok and we enter the wrong IP for the host computer the attempt would fail because there is nothing to connect.

Also, may be network not properly configured or an incorrect IP Address may be provide. There could be a firewall software blocking the ping request. For that, disabled the firewall.

There may be a failure come from hardware failure such as bad cable, router, Ethernet adapter, etc...

Is ICMP a connection-oriented or connectionless protocol : ICMP is connectionless because it does not require hosts to handshake before establishing a connection.

```
C:\Users\sagar>ping www.google.com

Pinging www.google.com [2404:6800:4009:82f::2004] with 32 bytes of data:
Reply from 2404:6800:4009:82f::2004: time=59ms
Reply from 2404:6800:4009:82f::2004: time=70ms
Reply from 2404:6800:4009:82f::2004: time=91ms
Reply from 2404:6800:4009:82f::2004: time=73ms

Ping statistics for 2404:6800:4009:82f::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 59ms, Maximum = 91ms, Average = 73ms
```

Ipconfig/Ifconfig :- IPCONFIG stands for **Internet Protocol Configuration.**

The IPCONFIG network command provides a comprehensive view of information regarding the IP address configuration of the device we are currently working on.

The IPConfig command also provides us with some variation in the primary command that targets specific system settings or data, which are:

- IPConfig/all - Provides primary output with additional information about network adapters.
- IPConfig/renew - Used to renew the system's IP address.

- IPConfig/release - Removes the system's current IP address.

Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, **ipconfig** displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

Synatx : ipconfig [/allcompartments] [/all] [/renew [<adapter>]] [/release [<adapter>]] [/renew6[<adapter>]] [/release6 [<adapter>]] [/flushdns] [/displaydns] [/registerdns] [/showclassid <adapter>] [/setclassid <adapter> [<classID>]]

```
C:\Users\sagar>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5a67:c127:e39a:c7f8%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:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:4041:d01:24e2:c798:bd52:5d60:3f3a
   Temporary IPv6 Address. . . . . . : 2409:4041:d01:24e2:6d04:b252:bf09:9a89
   Link-local IPv6 Address . . . . . : fe80::6c2:8c57:5f14:ddc2%18
   IPv4 Address. . . . . . . . . . . : 192.168.43.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::f88d:bcff:fe00:9a36%18
                                       192.168.43.1

Ethernet adapter Bluetooth Network Connection:

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

traceroute/tracert : The TRACERT command is used to trace the route during the transmission of the data packet over to the destination host and also provides us with the “hop” count during transmission.

Using the number of hops and the hop IP address, we can troubleshoot network issues and identify the point of the problem during the transmission of the data packet.

Syntax : tracert IP-address OR tracert www.destination_host_name.com.

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\sagar>tracert www.google.com

Tracing route to www.google.com [142.251.42.36]
over a maximum of 30 hops:

  1     2 ms     1 ms     2 ms  172.26.0.53
  2     3 ms     1 ms     2 ms  14.139.121.97
  3     5 ms     3 ms     2 ms  10.119.237.81
  4    82 ms    13 ms    90 ms  10.154.7.145
  5    13 ms    14 ms    14 ms  10.255.239.170
  6    13 ms    15 ms    16 ms  10.152.7.214
  7    16 ms    19 ms    38 ms  142.250.172.80
  8    14 ms    16 ms    19 ms  74.125.37.7
  9    24 ms    25 ms    17 ms  142.251.69.43
 10    13 ms    14 ms    14 ms  bom12s20-in-f4.1e100.net [142.251.42.36]

Trace complete.
```

nslookup :- **Nslookup** (stands for “Name Server Lookup”) is a useful command for getting information from the DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS-related problems.

Syntax: **nslookup** [- option] [name | -] [server]

```
C:\Users\sagar>nslookup google.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4009:815::200e
          172.217.174.78


C:\Users\sagar>nslookup
Default Server:  dns.google
Address:  8.8.8.8
```

Netstat :- The Netstat command as the name suggests displays an overview of all the network connections in the device. The table shows detail about the connection protocol, address, and the current state of the network.

Command to enter in Prompt – netstat

Syntax :- `netstat [-m] [-n] [-s] [-i | -r] [-f` *address_family*]

NETSTAT [-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

-a Displays all connections and listening ports.

-b Displays the executable involved in creating each connection or listening port. In some cases well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed. In this case the executable name is in [] at the bottom, on top is the component it called, and so forth until TCP/IP was reached. Note that this option can be time-consuming and will fail unless you have sufficient permissions.

-e Displays Ethernet statistics. This may be combined with the -s option.

-f Displays Fully Qualified Domain Names (FQDN) for foreign addresses.

-i Displays the time spent by a TCP connection in its current state.

-n Displays addresses and port numbers in numerical form.

-o Displays the owning process ID associated with each connection.

-p proto Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s option to display per-protocol statistics, proto may be any of:

IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.

-q Displays all connections, listening ports, and bound nonlistening TCP ports. Bound nonlistening ports may or may not be associated with an active connection.

-r Displays the routing table.

-s Displays per-protocol statistics. By default, statistics are shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6; the -p option may be used to specify a subset of the default.

-t Displays the current connection offload state.

-x Displays NetworkDirect connections, listeners, and shared endpoints.

-y Displays the TCP connection template for all connections. Cannot be combined with the other options.

interval Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

```
C:\Users\sagar>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            SAGARSPC:0             LISTENING
  TCP    0.0.0.0:445            SAGARSPC:0             LISTENING
  TCP    0.0.0.0:5040           SAGARSPC:0             LISTENING
  TCP    0.0.0.0:6646           SAGARSPC:0             LISTENING
  TCP    0.0.0.0:7680           SAGARSPC:0             LISTENING
  TCP    0.0.0.0:49664          SAGARSPC:0             LISTENING
  TCP    0.0.0.0:49665          SAGARSPC:0             LISTENING
  TCP    0.0.0.0:49666          SAGARSPC:0             LISTENING
  TCP    0.0.0.0:49667          SAGARSPC:0             LISTENING
  TCP    0.0.0.0:49668          SAGARSPC:0             LISTENING
  TCP    0.0.0.0:49670          SAGARSPC:0             LISTENING
  TCP    127.0.0.1:27017        SAGARSPC:0             LISTENING
  TCP    127.0.0.1:49674        SAGARSPC:49675         ESTABLISHED
  TCP    127.0.0.1:49675        SAGARSPC:49674         ESTABLISHED
  TCP    127.0.0.1:49678        SAGARSPC:49679         ESTABLISHED
  TCP    127.0.0.1:49679        SAGARSPC:49678         ESTABLISHED
  TCP    172.26.12.162:139      SAGARSPC:0             LISTENING
  TCP    172.26.12.162:49453    20.198.119.143:https   ESTABLISHED
  TCP    172.26.12.162:59934    52.108.44.14:https     ESTABLISHED
  TCP    172.26.12.162:59959    13.76.153.29:https     ESTABLISHED
  TCP    172.26.12.162:59963    bom12s18-in-f10:https  ESTABLISHED
^C
```

Protocols — (telnet, ssh, ftp)

Telnet :- Telnet stands for **Tel**etype **Net**work. It is a type of protocol that enables one computer to connect to local computer. It used as a standard TCP/IP protocol for virtual terminal service which is provided by ISO. The computer which starts the connection is known as the **local computer**. The computer which is being connected to i.e. which accepts the connection known as the **remote computer**. During telnet operation, whatever is being performed on the remote computer will be displayed by the local computer. Telnet operates on client/server principle. The local computer uses telnet client program and the remote computers uses telnet server program.

Syntax :- telnet <IP ADDRESS OF SERVER PC> <PORT>

Usage : Telnet can be used to check whether or not a port on the Voyager server is open to you.

To use it, you need to know the IP address or hostname (typically using IP address is preferred in this situation) of your Voyager server.

You also need to know which port you want to check (see this Article: Network ports used by Voyager)

You can use telnet with any port.

SSH :- SSH stands for **Secure Shell or Secure Socket Shell**

SSH(Secure Shell) is access credential that is used in the SSH Protocol. In other words, it is a cryptographic network protocol that is used for transferring encrypted data over network. It allows you to connect to a server, or multiple servers, without having you to remember or enter your password for each system that is to login remotely from one system into another.

Syntax :- ssh user_name@host(IP Address/Domain_name)

The popular usages of SSH protocol are given below:

- It provides secure access to users and automated processes.
- It is an easy and secure way to transfer files from one system to another over an insecure network.
- It also issues remote commands to the users.
- It helps the users to manage the network infrastructure and other critical system components.
- It is used to log in to shell on a remote system (Host), which replaces **Telnet and rlogin** and is used to execute a single command on the host, which replaces **rsh**.
- It combines with **rsync** utility to backup, copy, and mirror files with complete security and efficiency.
- It can be used for forwarding a port.
- By using SSH, we can set up the automatic login to a remote server such as OpenSSH.
- We can securely browse the web through the encrypted proxy connection with the SSH client, supporting the SOCKS protocol.

FPT :- FTP stands for File Transfer Protocol.

- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.

Syntax :- FTP [-options] [-s:filename] [-w:buffer] [host]

FTP ?

Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

Objective of FTP

- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

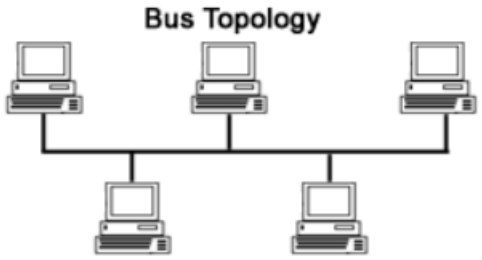
ASSIGNMENT -02

(Study of LAN Topologies — (BUS, Ring, Star, Mesh, Tree, Hybrid))

Q. Provide a writeup containing — a brief description of the topologies, block Diagram, their advantages and drawbacks.

BUS :- Bus topology, also known as line topology.

Bus topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.



Advantages of bus topology

- It works well when you have a small network.
- It's the easiest network topology for connecting computers or peripherals in a linear fashion.
- It requires less cable length than a star topology.

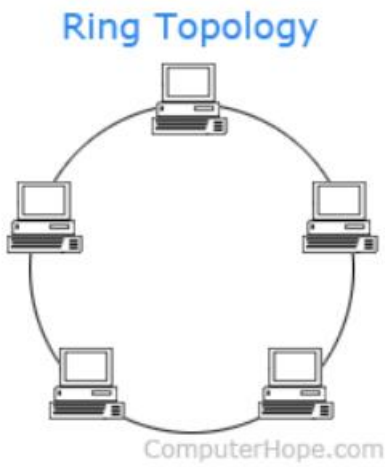
Disadvantages of bus topology

- It can be difficult to identify the problems if the whole network goes down.
- It can be hard to troubleshoot individual device issues.
- Bus topology is not great for large networks.
- Terminators are required for both ends of the main cable.
- Additional devices slow the network down.
- If a main cable is damaged, the network fails or splits into two.

Ring Topology :-

A **ring topology** is a network configuration where device connections create a circular data path. Each networked device is connected to two others, like points on a circle. Together, devices in a ring topology are called a **ring network**.

In a ring network, packets of data travel from one device to the next until they reach their destination. Most ring topologies allow packets to travel only in one direction, called a **unidirectional** ring network. Others permit data to move in either direction, called **bidirectional**.



Ring topologies may be used in either LANs (local area networks) or WANs (wide area networks). Depending on the network card used in each computer of the ring topology, a coaxial cable or an RJ-45 network cable is used to connect computers together.

Advantages of a ring topology

- All data flows in one direction, reducing the chance of packet collisions.
- A network server is not needed to control network connectivity between each workstation.
- Data can transfer between workstations at high speeds.
- Additional workstations can be added without impacting performance of the network.

Disadvantages of a ring topology

- All data being transferred over the network must pass through each workstation on the network, which can make it slower than a star topology.
- The entire network will be impacted if one workstation shuts down.
- The hardware needed to connect each workstation to the network is more expensive than Ethernet cards and hubs/switches.
- The major disadvantage of a ring topology is that if any individual connection in the ring is broken, the entire network is affected.

Star Topology :- Also known as star network. **star topology** is one of the most common network setups. Every node connects to a central network device in this configuration, like a hub, switch, or computer. The central network device acts as a server, and the peripheral devices act as clients. In a star topology setup, either a coaxial or RJ-45 network cable is used, depending on each computer's type of network card. The image shows how this network setup gets its name, as it is shaped like a star.

There technically is no limit to how many computers can connect in a star topology. However, network performance can decrease as more computers are connected, resulting in slower network speeds.

Advantages of star topology

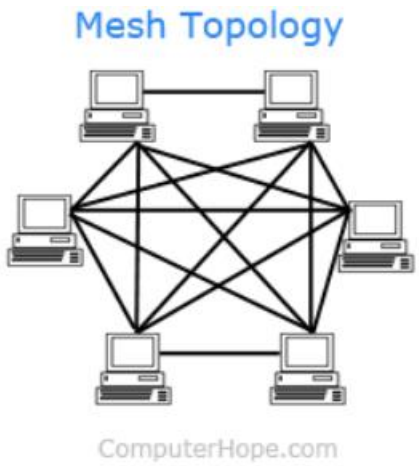
- Centralized management of the network through the use of the central computer, hub, or switch.
- Easy to add another computer to the network.
- If one computer on the network fails, the rest of the network continues to function normally.

Disadvantages of star topology

- It may have a higher cost to implement, especially when using a switch or router as the central network device.
- The central network device determines the performance and number of nodes the network can handle.
- If the central computer, hub, or switch fails, the entire network goes down, and all computers are disconnected from the network.

Mesh Topology :-

A mesh topology is a network setup where each computer and network device is interconnected with one another. This topology setup allows for most transmissions to be distributed even if one of the connections goes down. It is a topology commonly used for wireless networks. Below is a visual example of a simple computer setup on a network using a **mesh topology**.



Advantages of a mesh topology

- Manages high amounts of traffic, because multiple devices can transmit data simultaneously.
- A failure of one device does not cause a break in the network or transmission of data.
- Adding additional devices does not disrupt data transmission between other devices.

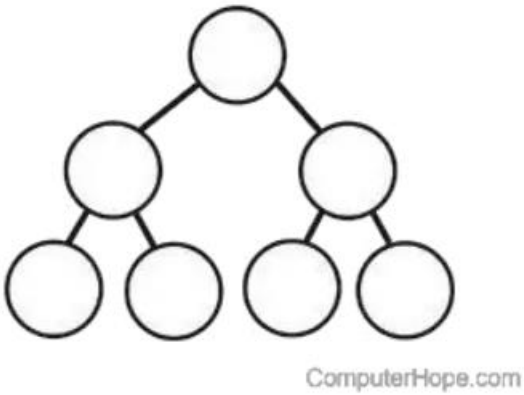
Disadvantages of a mesh topology

- The cost to implement is higher than other network topologies, making it a less desirable option.
- Building and maintaining the topology is difficult and time consuming.
- The chance of redundant connections is high, which adds to the high costs and potential for reduced efficiency.

Tree Topology :-

A **tree topology** is a special type of structure where many connected elements are arranged like the branches of a tree. For example, tree topologies are frequently used to organize the computers in a corporate network, or the information in a database.

In a tree topology, there can be only one connection between any two connected nodes. Because any two nodes can have only one mutual connection, tree topologies create a natural parent and child hierarchy.



Advantages of Tree Topology :

- This topology is the combination of bus and star topology.
- This topology provides a hierarchical as well as central data arrangement of the nodes.
- As the leaf nodes can add one or more nodes in the hierarchical chain, this topology provides high scalability.
- The other nodes in a network are not affected if one of their nodes gets damaged or does not work.
- Tree topology provides easy maintenance and easy fault identification can be done.
- A callable topology. Leaf nodes can hold more nodes.
- Supported by several hardware and software vendors.
- Point-to-point wiring for individual segments.
- Tree Topology is highly secure.
- It is used in WAN.
- Tree Topology is reliable.
-

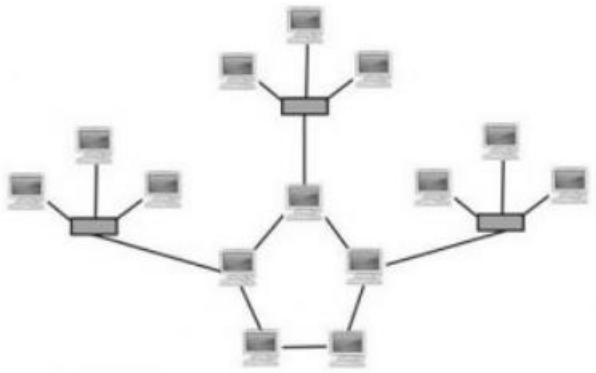
Disadvantages of Tree Topology :

- This network is very difficult to configure as compared to the other network topologies.
- The length of a segment is limited & the limit of the segment depends on the type of cabling used.
- Due to the presence of a large number of nodes, the network performance of tree topology becomes a bit slow.
- If the computer on the first level is erroneous, the next-level computer will also go under problems.
- Requires a large number of cables compared to star and ring topology.
- As the data needs to travel from the central cable this creates dense network traffic.
- The Backbone appears as the failure point of the entire segment of the network.
- Treatment of the topology is pretty complex.
- The establishment cost increases as well.
- If the bulk of nodes is added to this network, then the maintenance will become complicated.

Hybrid Topology :-

A **hybrid topology** is a type of network topology that uses two or more differing network topologies. These topologies can include a mix of bus topology, mesh topology, ring topology, star topology, and tree topology.

The choice to use a hybrid topology over a standard topology depends on the needs of a business, school, or the users. The number of computers, their location, and desired network performance are all factors in the decision.



Hybrid Topology

Advantages of Hybrid Topology:

- This type of topology combines the benefits of different types of topologies in one topology.
- Can be modified as per requirement.
- It is extremely flexible.
- It is very reliable.
- It is easily scalable as Hybrid networks are built in a fashion which enables easy integration of new hardware components.
- Error detecting and troubleshooting are easy.
- Handles a large volume of traffic.
- It is used to create large networks.
- The speed of the topology becomes fast when two topologies are put together.

Disadvantages of Hybrid Topology :

- It is a type of network expensive.
- The design of a hybrid network is very complex.
- There is a change in the hardware to connect one topology with another topology.
- Usually, hybrid architectures are larger in scale so they require a lot of cables in the installation process.

- Hubs which are used to connect two distinct networks are very costly. And hubs are different from usual hubs as they need to be intelligent enough to work with different architectures.
- Installation is a difficult process.