CN

▼ Practical

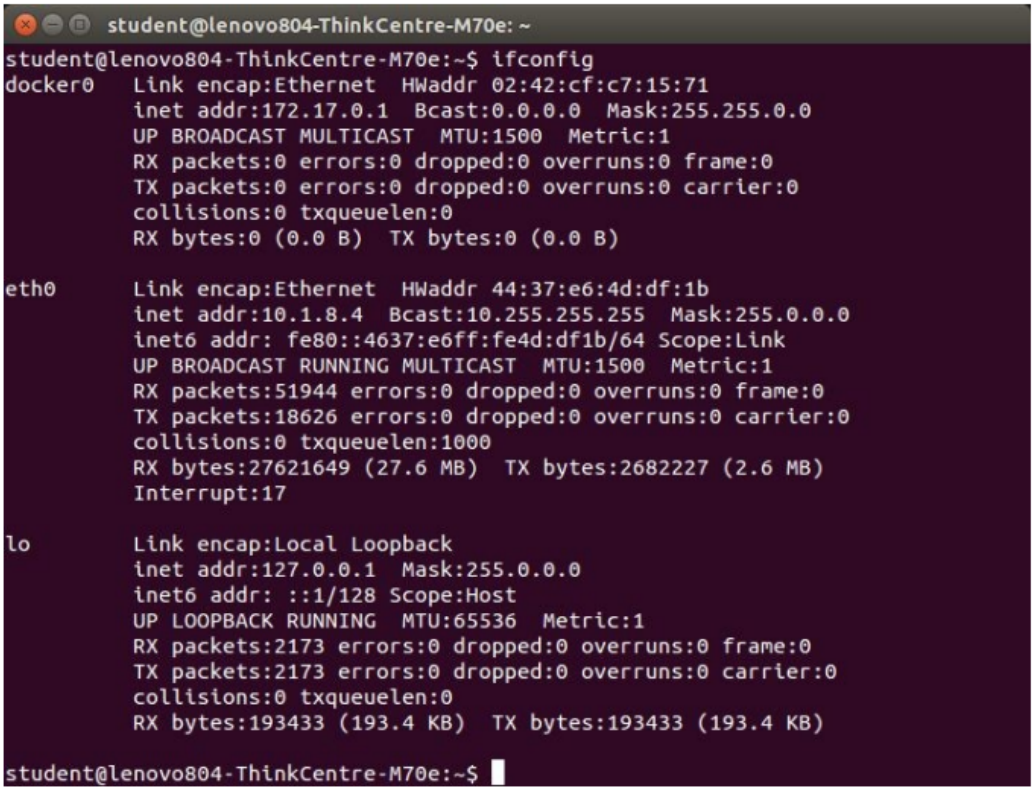
▼ EXP 1: Use of Crimping Tool for RJ45

- Registered Jack is connector for catalogue cables
- Bandwidth and range differ with versions
- 8 wires in RJ45

▼ Exp 2: Basic networking commands in Linux

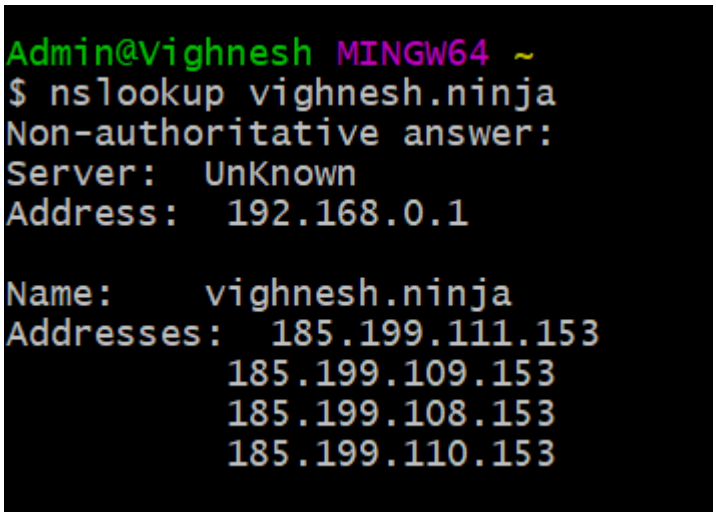
▼ `ifoconfig`

- interface configuration
- to view and change configuration of network interfaces on system
- `ifconfig -a` → all configs
- `ifconfig eth0` → specific config
- `sudo ifconfig eth1 up|down` → enabling/disabling interface
- `ifconfig -v` → verbose mode display addition information for certain error conditions



▼ `nslookup`

- Name server lookup
- network admin tool to obtain domain name or IP address mapping or any other specific DNS record
- Useful to troubleshoot DNS related probles
- `nslookup https://vighnesh.ninja`



▼ `ping`

- Packet Inter-network Groper pre-installed in modern OS
- to check network connectivity between server and host
- take IP or URL as input sends data packet with message “PING” and get response from host records this time in milliseconds called latency
- Lower the latency faster the connection
- uses ICMP (Internet Control Message Protocol)

```
Admin@Vighnesh MINGW64 ~
$ ping vighnesh.ninja

Pinging vighnesh.ninja [185.199.111.153] with 32 bytes of data:
Reply from 185.199.111.153: bytes=32 time=389ms TTL=59
Reply from 185.199.111.153: bytes=32 time=3ms TTL=59
Reply from 185.199.111.153: bytes=32 time=3ms TTL=59
Reply from 185.199.111.153: bytes=32 time=7ms TTL=59

Ping statistics for 185.199.111.153:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 389ms, Average = 100ms
```

▼ `tracert`

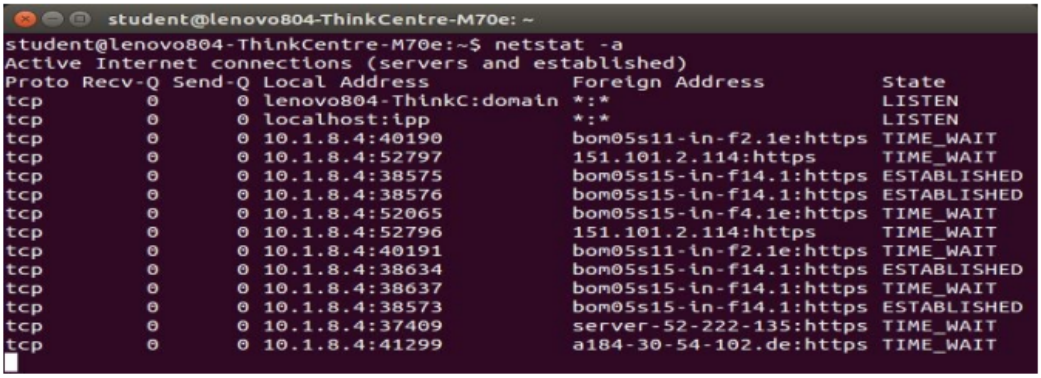
- Prints route that a packets takes to reach the host
- useful for getting information about route and hops that packet takes
- `tracert vighnesh.ninja`

```
Admin@Vighnesh MINGW64 ~
$ tracert vighnesh.ninja

Tracing route to vighnesh.ninja [185.199.108.153]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2    <1 ms    <1 ms    <1 ms  TL-MR3420 [192.168.1.1]
  3     2 ms     1 ms    <1 ms  43.225.162.106.airnetnetworks.com [43.225.162.106]
  4     *        6 ms     4 ms  43.225.162.105.airnetnetworks.com [43.225.162.105]
  5     6 ms     3 ms     *     as54113.bom.extreme-ix.net [103.77.108.145]
  6     4 ms     4 ms     7 ms  cdn-185-199-108-153.github.com [185.199.108.153]

Trace complete.
```

▼ `netstat`

- network related infromation such as
  - network connections
  - routing tables

- interface
- interface statistics
- masquerade connections
- multicast membership



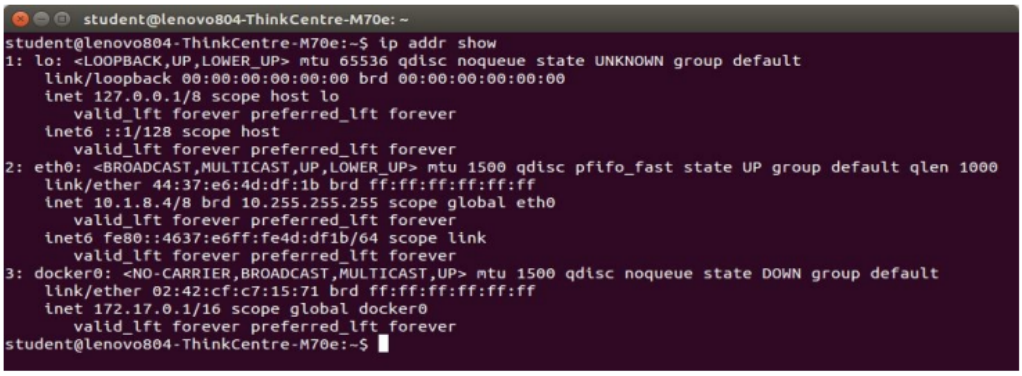
▼ `arp`

- display and modify IP-to-Physical (MAC) address translation tables used by ARP, and works between level 2 (data link layer) and level 3 (network layer)
- Address Resolution Protocol
- manipulate system's ARP cache
- allows ARP cache dump

▼ `ip`

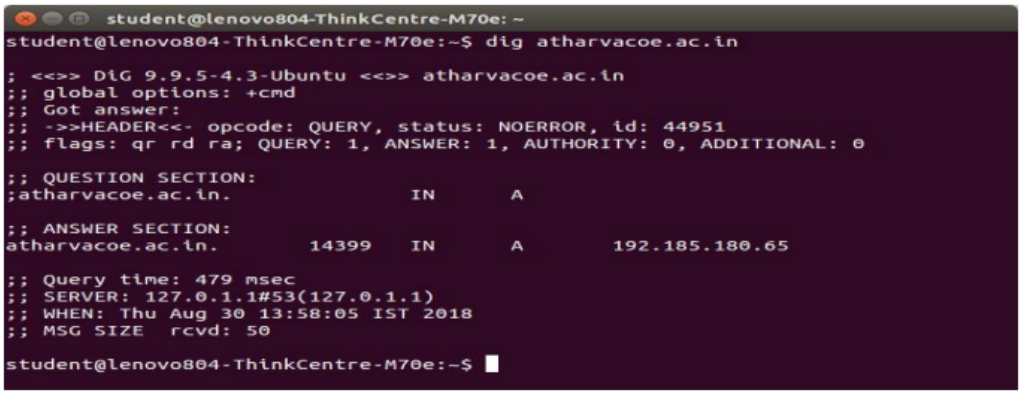
- similar to `ifconfig` but more powerful
- perform several tasks such as
  - manipulate routing devices and tunnels
  - assigning address to network interface or configuring network interface parameters

- configuring or modifying default and static routing
- setting tunnel over IP
- listing IP addresses and property information
- modifying status of interfave
- assigning, deleting and setting up IP addresses and routes



▼ `dig`

- Domain Information Groper
- retrieving information about DNS servers
- verifying and troubleshooting DNS problems and perform DNS lookups
- replaces older tools such as `nslookup` and `host`



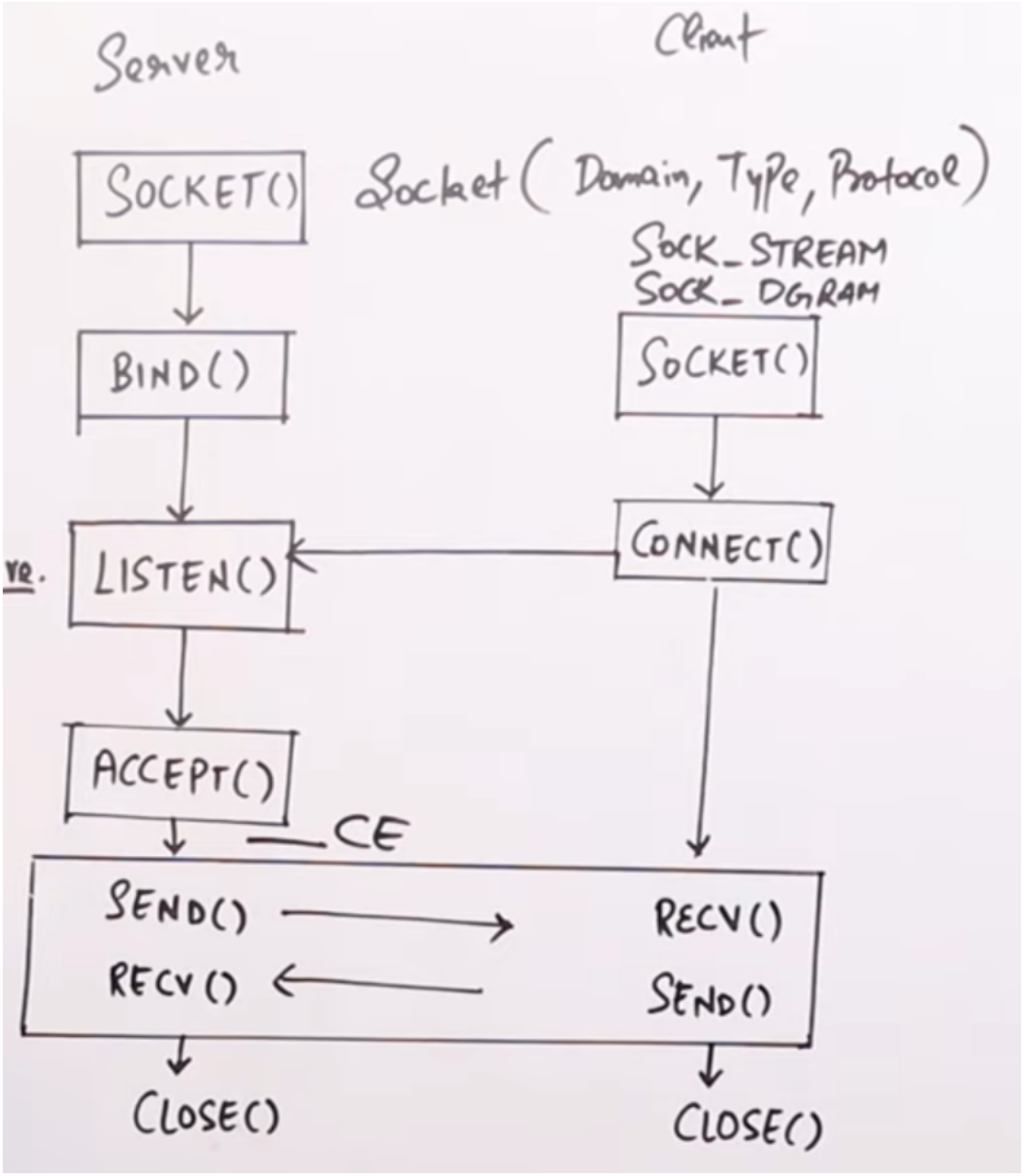
▼ Exp 3: Network discovery tools

Nmap

- Network mapper
- Free and open source tool used for vulnerability checking, port scanning and network mapping
- sends specially crafted packets to the target host and then analyzes the responses
- accounts for network conditions such as latency fluctuations, network congestion, target interference with the scan during the run
- It can determine Operating system of target, name and versions of listening services, estimated uptime, type of device, and presence of firewall
- Features
    - Host discovery
        - Identify host on network
        - For examples, listing the hosts which responds to ping or have a particular port open
    - Port Scanning
        - Enumerating the open ports on one or more target hosts
    - Version detection
        - Interrogating listening network services
        - listening one remote devices to determine the application name and version number
    - OS detection
        - Remotely determining OS and some h/w characteristics of network devices
- Basic commands
    - Targe specifications → namp <target URL or IP with spaces between them>
    - OS detection → nmap -O <target URL or IP>
    - version detection → namp -sV <target URL or IP>
        - -sV → service and version

▼ Exp 4: Socket Programming

- Socket is one endpoint of two way communication link between two programs
- Establish named contact points for inter process communication (IPC)
- It is created using “socket” system call.
- Bidirectional FIFO communication facility
- Each socket has specific address composed of IP and port
- Server creates socket and attaches it to network port addresses then waits for client to contact
- Client creates a socket and attempts to connect the server socket
- Data transfer takes place after connection is established
- Types
    - Datagram (UDP)
        - Connection less point for sending and receiving packets
        - Not reliable but fast
        - similar to mailbox
    - Stream (TCP)
        - Connection-oriented,
        - Requires connection establishment before data transmission and connection termination after data transmission
        - Reliable but slow → order of data is maintained
        - similar to Bluetooth connection



Function call	Description
Create()	To create a socket
Bind()	It’s a socket identification like a telephone number to contact
Listen()	Ready to receive a connection
Connect()	Ready to act as a sender
Accept()	Confirmation, it is like accepting to receive a call from a sender
Write()	To send data

Function call	Description
Read()	To receive data
Close()	To close a connection

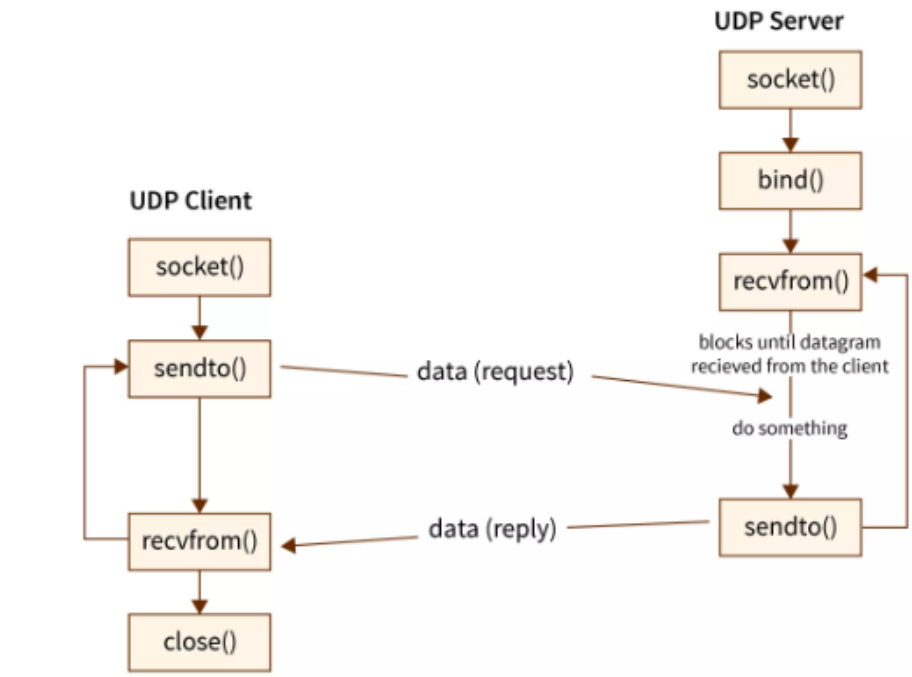
▼ Not necessary

The steps involved in establishing a socket on the ***client*** side are as follows:

- Create a socket with the socket() system call
- Connect the socket to the address of the server using the connect() system call
- Send and receive data. There are a number of ways to do this, but the simplest is to use the read() and write() system calls.

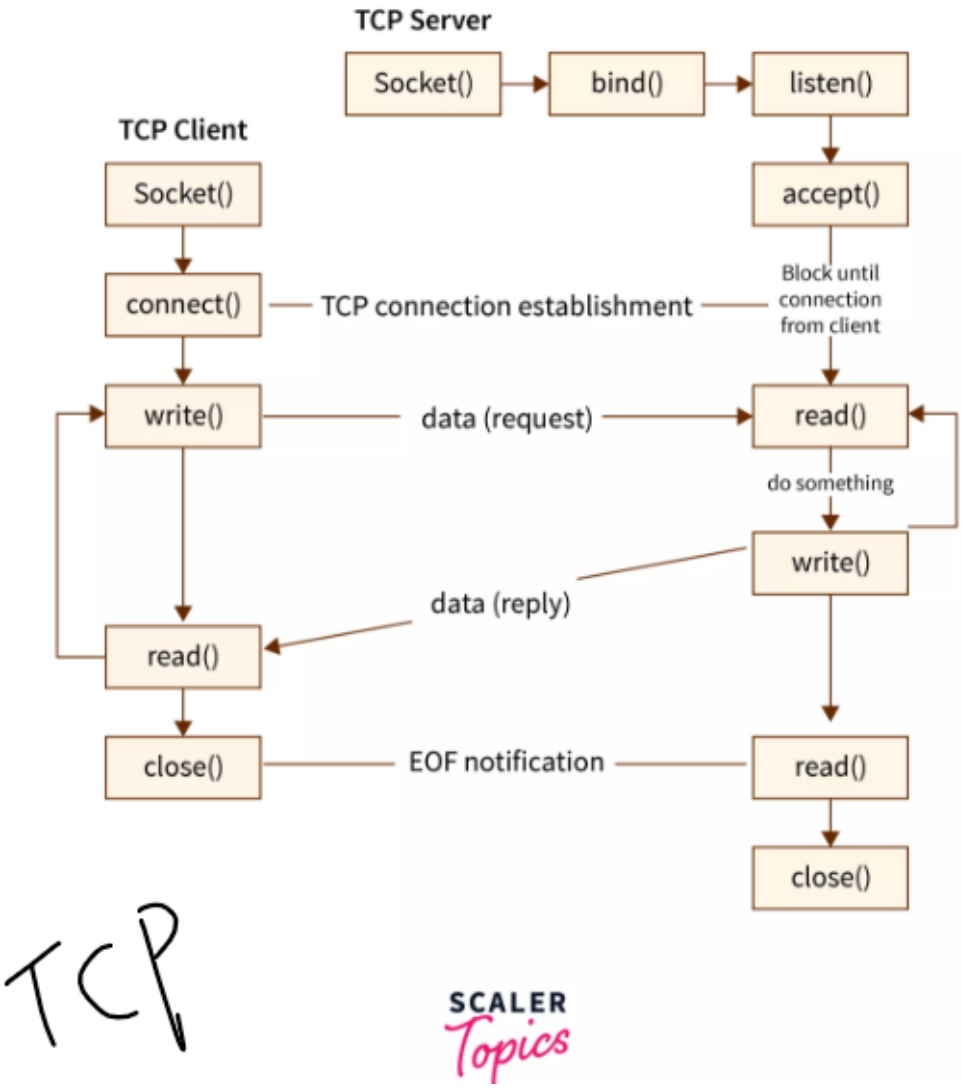
The steps involved in establishing a socket on the ***server*** side are as follows:

- Create a socket with the socket() system call
- Bind the socket to an address using the bind() system call. For a server socket on the Internet, an address consists of a port number on the host machine.
- Listen for connections with the listen() system call
- Accept a connection with the accept() system call. This call typically blocks until a client connects with the server.
- Send and receive data.



UDP

SCALER Topics



▼ Exp 5: FTP

- FTP is TCP for uploading and downloading files between computers
- Works on client-server model.
- Server is called an FTP daemon. It continuously listens for FTP requests from remote clients
- When request is received, it manages the login and set up the connection
- PORT → 20 and 21
- Two ways to access FTP server
  - Anonymous

        - Default user called “anonymous” or “ftp” and sending email address as password
    - Authenticated
        - must have account
        - permissions defined for the account used to login
        - FTP daemon Hide root directory and change it to FTP home directory
        - Also hide rest of the file system from remote session

▼ Steps

1. install vsftpd by running command `sudo apt-get install vsftpd`
2. make copy of original file `cp /etc/vsftpd.conf /etc/vsftpd.conforignal`
3. Configure vsftpd using gedit `gedit /etc/vsftpd.conf`

   uncomment following lines

   local_enable=YES

   write_enable=YES
4. restart vsftpd `/etc/init.d restart`
5. Add user with command `adduser <username>` fill the details
6. navigate to ftp://localhost using any browser and enter login username and password
7. After successful authentication files can be transfer and access using ftp

▼ FTP commands

? → help about FTP commands

bye → exit FTP

cd → change directory

close → terminate connection with another computer

delete → remove file from remote directory

get → copy file from remote to local machine

mget → copy multiple files

mput → copy multiple files from local to remote

put → copy one file from local to remoter

lcd → change directory on local machine

mkdri → make new directory in remote directory

ls, pwd, rmdir → all related to remote directory

▼ Exp 6: Telnet

- Terminal Emulation program for TCP/IP network that allows access another computer
- client-server protocol connects to port 23 of TCP
- use to check open pots on a remote system, test or troubleshoot remote web or mail servers

▼ Steps

1. Install telnet daemon `sudo apt-get install telnetd`
2. restart inetd using command `sudo /etc/init.d/openbsd-inetd restart`
3. Connect with remote client use command `telnet <hostip>` for example, `telnet 122.175.140.221`
4. Provide username and password

FTP is used for file transferring and TELNET is used for remote login for a system

> Telnet poses high-security risks due to lack of encryption SSH is recommended protocol when connecting to remote systems

▼ Theory

- Interconnection of computers to form a network is called computer network
- Goal
  - For companies → resource sharing, providing high reliability, save money, provide powerful communication medium
  - For people → access remote information, communication, entertainment
- Transmission
  - Transmission means sending a signal from one location to another.
  - Transmission technologies refer to the physical layer protocol.

    ▼ Broadcast networks

    - Single communication channel is shared and used by all the machines on the network.
    - Messages called packets sent by any machine are received by all others.
    - Use special code in address field for addressing a packet to all the concerned computers. This mode of operation is called broadcasting.
    - Upon receiving a packet, machine checks the address field if the packet is addressed to it then the packet is processed, other wise packet is ignored.

    ### ▼ Advantages

    1. Multicasting
    2. Better utilization of all resource available

    ### ▼ Disadvantages

    1. Cannot accommodate huge number of devices
    2. Doesn’t allow personalized messages

    ▼ Point-to-Point networks (P2P)

    - Many connections between individual pairs of machines.

- Packet has to follow multiple routes of different length.
- Routing algorithm are very important in P2P network

▼ Advantages

1. Speed is guaranteed
2. Better security

▼ Disadvantages

1. Can connect only 2 sites
2. Expensive for distant locations

▼ Network devices

- Five types based on level of operation
  - below physical → passive hub
  - at physical → active hub, repeater
  - at physical and data link → bridge
  - at physical, data link and network → router
  - all layers → gateway
- Passive hub
  - no need of power connection just act as a connector
  - do not amplify or regenerate signal
- Repeater
  - Receive signal before it becomes too weak or corrupted regenerates original bit pattern then sends refreshed signal
  - Extends physical length of LAN
  - It has no filtering capacity and forwards every frame
  - Regenerator not amplifier
- Active hub
  - create connection between stations in start topology
  - amplify incoming signals

- Bridges
  - Operates in both physical and data link layer
  - As physical layer device, regenerates signal it receives
  - As data link layer device, check physical addresses contained in frame
- Routers
  - Routes packets based on their logical address (host-to-host addressing)
  - connects LANs and WANs
  - has routing table that is used for making decision about the route
  - normally dynamic and updates using routing protocol
- Gateway
  - Takes application message, read and interprets it
  - can be used as connecting device between two internetworks that use different models
  - Gateways can provide security

- Protocols are rules and procedures set up to send and receive digital data

▼ Types of communication

1. Simplex
   a. One directional information transfer
   b. Example → Radio and TV broadcasting
2. Half Duplex
   a. bidirectional
   b. transmit and receive data but not simultaneously
   c. When one device is sending, other one is receiving & vice versa. At a time either transmit or receive
   d. Example → Walky-talky

3. Full Duplex
    a. Bidirectional
    b. allow communication simultaneously
    c. Signal going in either direction share full capacity of link.
    d. Example → Telephone

▼ Network classification

Based on geographical area network covers

- PAN
    - Personal Area network
    - range of a person
    - Example, Bluetooth connection
- LAN
    - Local area network
    - small physical area
    - Example, office, factory
    - 100 Mbps
- MAN
    - Metropolitan Area Network
    - extends LAN to an entire city
    - Example, Cable operator
- WAN
    - Wide Area Network
    - For large distance
    - using satellite or telephone links
    - cheap to use telephone links
    - transfer large block of data between users
    - Example, Airline reservation
- GAN

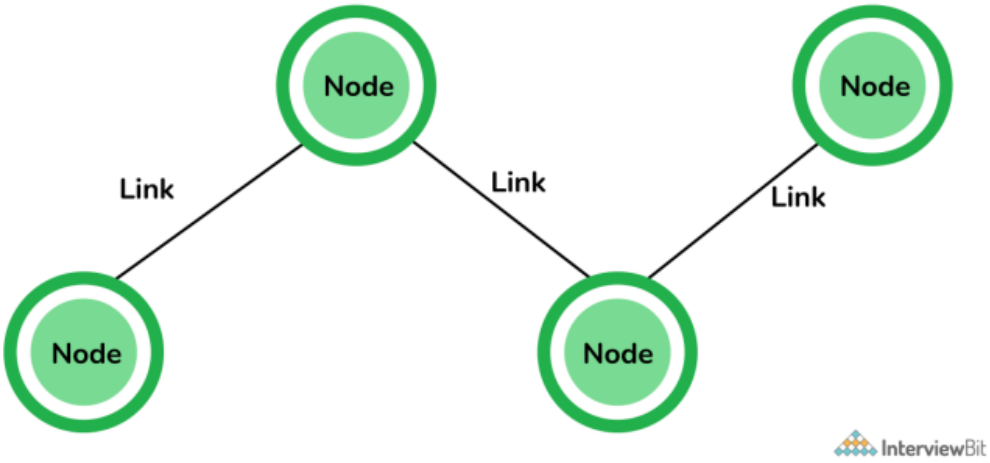
- Global Area Network
- also known as Internet

▼ Network Topology

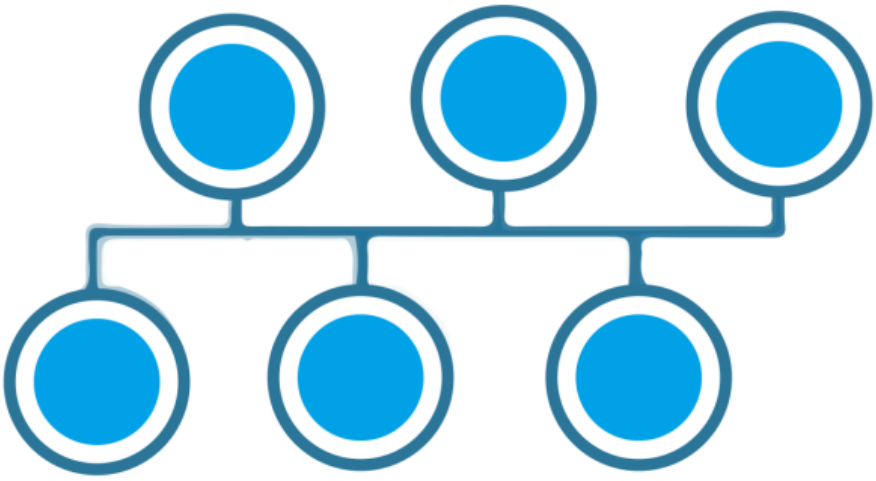
How network is physically laid out

Node → Any communicating device in a network. Examples are computers, laptops, printers, servers, modems

Link → connectivity between two nodes. Includes type and protocols used for inter-node communication

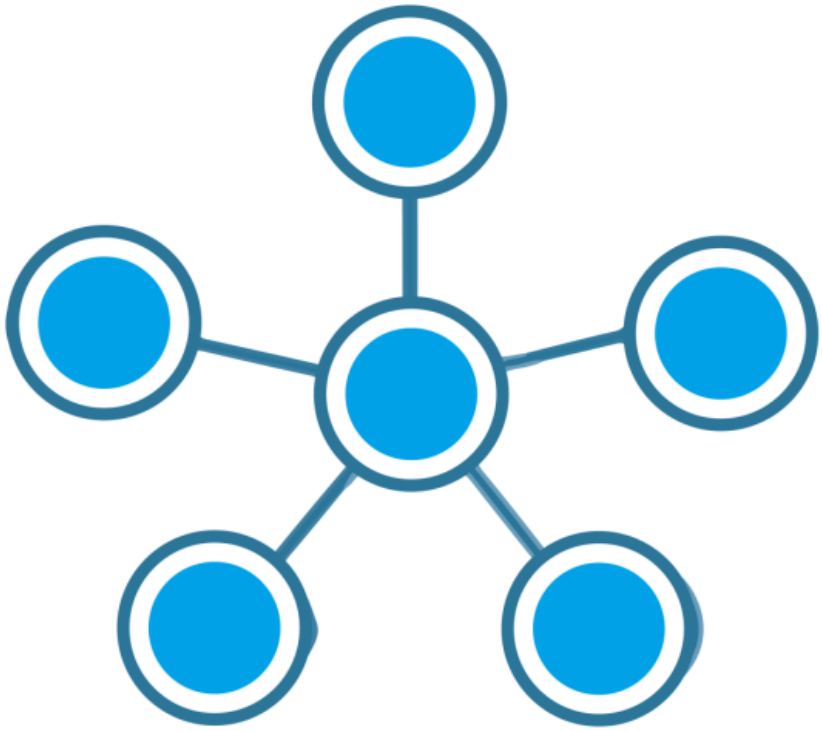


- Bus Topology

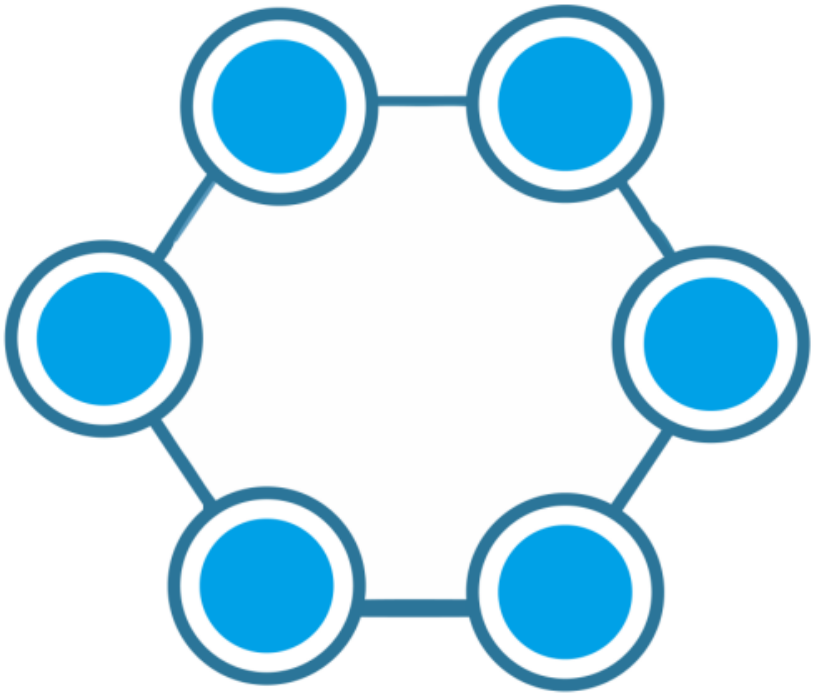


- All nodes are connected using central link known as bus

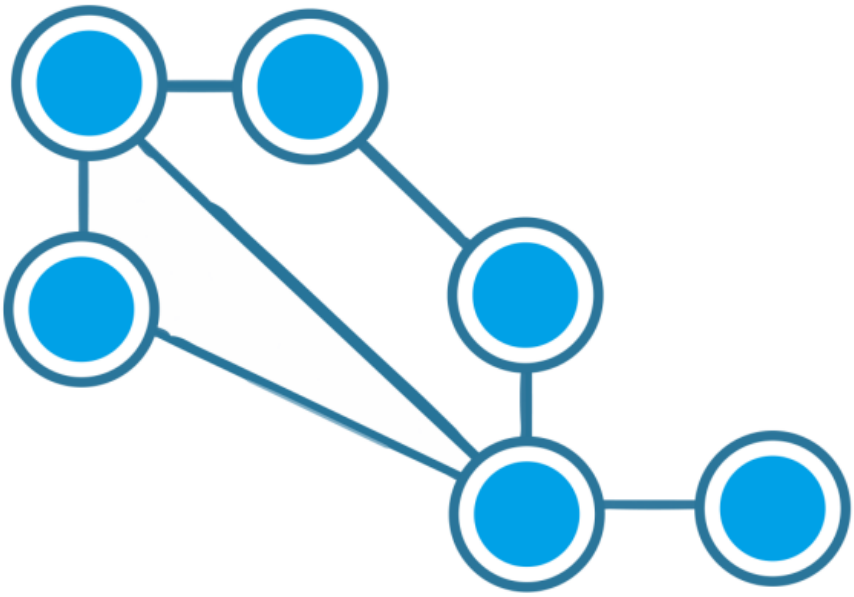
    - Useful for smaller number of devices
    - If main cable gets damaged, whole network down
- Star Topology



    - All nodes are connected to one signal node known as central node
    - easy to troubleshoot mainly used in home and office network
    - central node fails whole network down
- Ring Topology

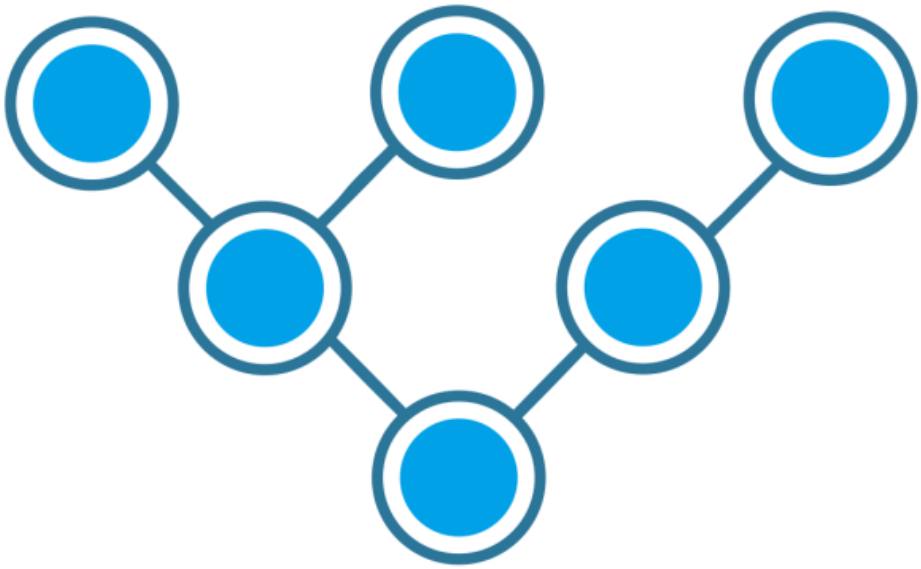


    - Each node is connected to exactly two node forming ring structure
    - used very rarely
    - expensive and hard to install and manage
    - If one node damage whole network down
- Mesh Topology



- Each node is connected to one or many nodes
- rarely used as installation and management are difficult
- Failure in one link only disconnects that node

- Tree topology



- combination of bus and star

    - smaller star networks connected to single bus
    - main bus fails whole network down
- Hybrid
    - combination of different topologies
    - Helps to ignore drawbacks of particular topology and pick the strengths from other

▼ Ipv4

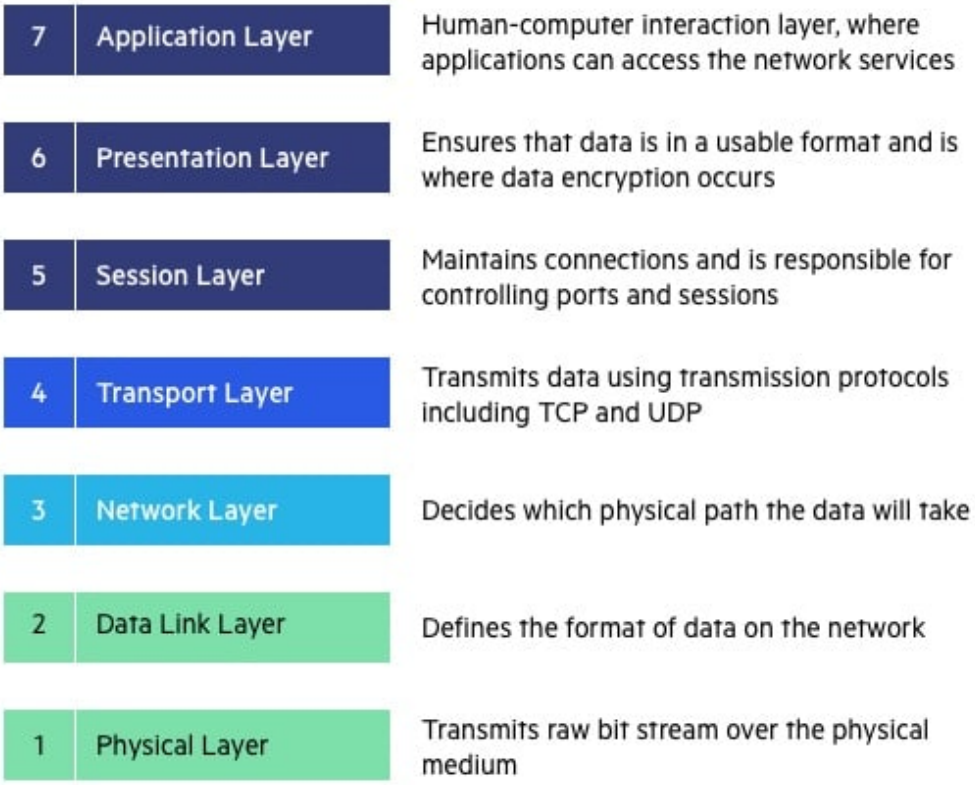
- 32 bit dynamic address of a node
- 4 octets and 8-bit each number with value of 255
- classes are differentiated based on number of hosts it supports
- five types of IPv4 classes

Five Different Classes of IPv4 Addresses

Class	First Octet decimal (range)	First Octet binary (range)	IP range	Subnet Mask	Hosts per Network ID	# of networks
Class A	0 – 127	0XXXXXXX	0.0.0.0-127.255.255.255	255.0.0.0	$2^{24}-2$	2^{7}
Class B	128 – 191	10XXXXXX	128.0.0.0-191.255.255.255	255.255.0.0	$2^{16}-2$	2^{14}
Class C	192 – 223	110XXXXX	192.0.0.0-223.255.255.255	255.255.255.0	$2^{8}-2$	2^{21}
Class D (Multicast)	224 – 239	1110XXXX	224.0.0.0-239.255.255.255			
Class E (Experimental)	240 – 255	1111XXXX	240.0.0.0-255.255.255.255			

▼ OSI

- open system interconnection
- network architecture model based on ISO standards



Layer	Functional Description
Application (7)	Refers to interfaces between network and application software. Also includes authentication services.
Presentation (6)	Defines the format and organization of data. Includes encryption.
Session (5)	Establishes and maintains end-to-end bidirectional flows between endpoints. Includes managing transaction flows.
Transport (4)	Provides a variety of services between two host computers, including connection establishment and termination, flow control, error recovery, and segmentation of large data blocks into smaller parts for transmission.
Network (3)	Refers to logical addressing, routing, and path determination.
Data link (2)	Formats data into frames appropriate for transmission onto some physical medium. Defines rules for when the medium can be used. Defines means by which to recognize transmission errors.
Physical (1)	Defines the electrical, optical, cabling, connectors, and procedural details required for transmitting bits, represented as some form of energy passing over a physical medium.

▼ TCP/IP

- Compressed version of OSI with only 4 layers

▼ TCP vs IP

OSI Vs TCP/IP

OSI Reference Model	TCP/IP Reference Model
7 layered architecture	4 layered architecture
Fixed boundaries and functionality for each layer	Flexible architecture with no strict boundaries between layers
Low Reliability	High Reliability
Vertical Layer Approach	Horizontal Layer Approach

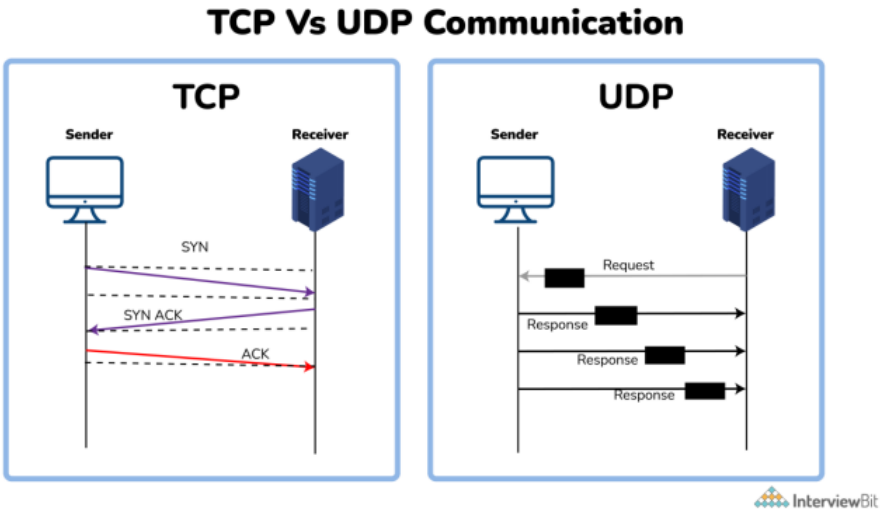
- TCP/IP is a functional model designed to solve specific communication problems, and which is based on specific, standard protocols. OSI is a generic, protocol-independent model intended to describe all forms of network communication.
- In TCP/IP, most applications use all the layers, while in OSI simple applications do not use all seven layers. Only layers 1, 2 and 3 are mandatory to enable any data communication.
- OSI model, the transport layer is only connection-oriented. A layer of the TCP/IP model is both connection-oriented and connectionless.
- OSI is more reliable
- OSI → ISO (International Standard Organization) TCP/IP → ARPANET (Advance Research Project Agency Network)
- OSI 7 layers TCP/IP 4 layers
- OSI follows vertical approach TCP/IP follows Horizontal approach

- Protocols
  - HTTP/HTTPS
    - How information can be transmitted on WWW
    - Stateless protocol
    - It is an application layer built on TCP
    - HHTPS is advanced secured version of HTTP
    - SSL/TSL protocol is used to provide security
    - Enables secure transaction by encrypting communication and also helps identify network servers securely
    - Default ports: HTTP → 80 | HTTPS → 443

- SMTP
  - Simple Mail Transfer Protocol
  - how communication between mail servers
  - always listening mode on port 25
- TCP
  - Transmission Control Protocol
  - Connection oriented
  - how computer connects to the Internet and how data transmission will be take place
  - creates virtual network where three way handshake model to establish the connection
  - more reliable but slow
- UDP
  - User Datagram Protocol based on datagrams
  - Mainly used for multicasting and broadcasting
  - No hand-shaking hence less reliable but fast

23. Compare between TCP and UDP

TCP/IP	UDP
Connection-Oriented Protocol	Connectionless Protocol
More Reliable	Less Reliable
Slower Transmission	Faster Transmission
Packets order can be preserved or can be rearranged	Packets order is not fixed and packets are independent of each other
Uses three ways handshake model for connection	No handshake for establishing the connection
TCP packets are heavy-weight	UDP packets are light-weight
Offers error checking mechanism	No error checking mechanism
Protocols like HTTP, FTP, Telnet, SMTP, HTTPS, etc use TCP at the transport layer	Protocols like DNS, RIP, SNMP, RTP, BOOTP, TFTP, NIP, etc use UDP at the transport layer



- DNS
  - Domain name system
  - translates domain names (URL) to corresponding IP
- ICMP
  - Internet Control Message Protocol
  - Used for error handling
  - used by network devices like router for diagnosing network connection issues
  - Default port 7
- DHCP
  - Dynamic Host Configuration Protocol

        - Application layer protocol used to auto-configure devices on IP networks enabling them to use TCP and UDP based protocols.
        - DHCP servers auto assign IPs and other network configuration to the devices individually which enables them to communicate over IP
        - Helps to get subnet mask, IP address and resolve DNS
        - Default port 67
    - ARP
        - Address resolution protocol
        - network layer protocol
        - convert logical address (IP) to physical address (MAC)
        - can also be used to get MAC of devices when they are trying to communicate over local network
    - FTP
        - File transfer Protocol
        - used to transfer files and data reliably between hosts
        - download files from remote servers
        - Default port 27
- MAC
    - Media Access Control
    - 48 or 64 bit unique identifier in network
    - also called as physical address embedded with Network Interface Card used at data link layer

MAC Address	IP Address
Media Access Control Address	Internet Protocol Address
6 or 8-byte hexadecimal number	4 (IPv4) or 16 (IPv6) Byte address
It is embedded with NIC	It is obtained from the network
Physical Address	Logical Address
Operates at Data Link Layer	Operates at Network Layer.
Helps to identify the device	Helps to identify the device connectivity on the network.

- Subnet is a network achieved by process called subnetting. Subnetting is smaller networks which are divided from bigger network to maintain the security

31. Compare the hub vs switch

Hub	Switch
Operates at Physical Layer	Operates at Data Link Layer
Half-Duplex transmission mode	Full-Duplex transmission mode
Ethernet devices can be connectedsend	LAN devices can be connected
Less complex, less intelligent, and cheaper	Intelligent and effective
No software support for the administration	Administration software support is present
Less speed up to 100 MBPS	Supports high speed in GBPS
Less efficient as there is no way to avoid collisions when more than one nodes sends the packets at the same time	More efficient as the collisions can be avoided or reduced as compared to Hub

32. What is the difference between the ipconfig and the ifconfig?

ipconfig	ifconfig
Internet Protocol Configuration	Interface Configuration
Command used in Microsoft operating systems to view and configure network interfaces	Command used in MAC, Linux, UNIX operating systems to view and configure network interfaces
Used to get the TCP/IP summary and allows to changes the DHCP and DNS settings	

-