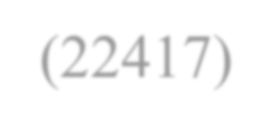
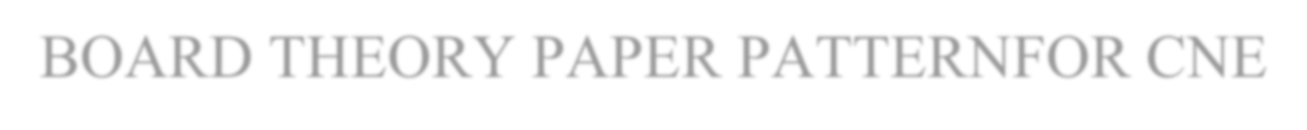
***Subject: - Computer Network (22417)***



|  |  |  |  |
| --- | --- | --- | --- |
| **Chapter No.** | **Name of chapter** |  | **Marks** |
| **1** | Fundamentals Of Computer Network |  | 14 |
| **2** | Network Components & Topologies |  | 16 |
| **3** | Reference Models for Computer Network |  | 16 |
| **4** | TCP/IP Protocol Suite |  | 12 |
| **5** | Addressing |  | 12 |
|  | | **Total Marks: -** | **70** |

BOARD THEORY PAPER PATTERN FOR CNE



(22417)

|  |  |  |
| --- | --- | --- |
| **Q.1** |  | **Attempt any TWO 7\*2=14** |
|  | a) | Fundamental of Computer Network |
|  | b) | Network Components and Topologies |
|  | c) | TCP/IP Protocol Suite |
|  | d) | Fundamental of Computer Network |
|  | e) | IP Addressing |
|  | f) | IP Addressing |
|  | g) | Reference Model for computer Network |
| **Q.2** |  | **Attempt any THREE 4\*4=16** |
|  | a) | Network Topologies |
|  | b) | Reference models |
|  | c) | Reference models |
|  | d) | TCP/IP Protocol suite |
| **Q.3** |  | **Attempt any TWO** **4\*4=16** |
|  | a) | Fundamental of Computer Network |
|  | b) | Network components |
|  | c) | Reference models |
|  | d) | TCP/IP Protocol suite |
| **Q.4** |  | Attempt any TWO **5\*4=20** |
|  | a) | Fundamental of Computer Network |
|  | b) | Network Topologies |
|  | c) | Fundamental of Computer Network |
|  | d) | IP Addressing |
|  | e) | TCP/IP Protocol Suite |
| **Q.5** |  | **Attempt any TWO 3\*6=18** |
|  | a) | TCP/IP Protocol suite |
|  | b) | IP Addressing |
|  | c) | Network Components |
| **Q.6** |  | **Attempt any TWO 3\*6=18** |
|  | a) | Reference models |
|  | b) | IP Addressing |
|  | c) | Network Topologies |

# UNIT-I

**Fundamental of Computer Network**

1.**List advantages & disadvantages of Computer Network.**

**Advantages of Computer Network:**

1. Resource sharing
2. Information Sharing
3. High reliability communication
4. Cost effective
5. Powerful communication medium
6. Centralised management 6. Data Backup
7. Increased Storage capacity

**Disadvantages of Computer Network:**

1. Social issues regarding privacy of data, information etc..
2. Broadcasting of anonymous messages
3. Security threats
4. Need for efficient handler
5. Lack of Robustness

**2. State features of Nos.**

**Features of NOS (Network Operating System).:**

A network operating systems salient features are:

* Basic support for operating systems like protocol and processor support, hardware detection and multiprocessing.
* Printer and application sharing.
* Common file system and database sharing.
* Network security capabilities such as user authentication and access control.
* Directory Services
* Backup and web services.
* Internetworking of various resources connected in the network
* Providing access to remote printers, managing which users are using which printers when, managing how print jobs are queued, and recognizing when devices aren't available to the network.
* Enabling and managing access to files on remote systems, and determining who can access what—and who can't.  Granting access to remote applications and resources, such as the Internet, and making those resources seem like local resources to the user (the network is ideally transparent to the user).
* Providing routing services, including support for major networking protocols, so that the operating system knows what data to send where.
* Monitoring the system and security, so as to provide proper security against viruses, hackers, and data corruption.  Providing basic network administration utilities (such as SNMP, or Simple Network Management Protocol), enabling an administrator to perform tasks involving managing network resources and users.

**3.Define host and access point in computer network.**

Host: Host is the end system of WAN which contains a collection of machines intended for running user (application) programs.

OR

Host is an end device such a computer which is connected for communication.

**Access point:** Access point is the system in network which allows user to use application programs stored at HOST machine.

OR

An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building.

OR

An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area.

**4.State Computer topology. Give its importance**.

**Computer topology** is the network configuration. The term „topology‟ refers to the way a network is laid out either physically or logically.

OR

The topology of network is the geometric representation of the relationship of all the links and linked devices usually called nodes to each other.

OR

Network Topology is the way in which the devices and connected to each other in a computer network. **Importance of Topology**:

1. Better Understanding of the network
2. Effective use of resources
3. Easier error detection
4. Effective management of cost of network
5. Easy to upgrade/change in the network

**5.Define protocol. State its significance.**

Protocols: Protocols are the rules and conventions used in the exchange of information between two machines in various layers of a network.

**Significance of protocol**:

* Protocols control the sending and receiving of the information with in a network.
* The peer entities communicate using these protocols. Each protocol belongs to one of the layers and is distributed among the network entities that implement this protocol.

1. **List any four application layer protocols.**

**(Note: Any other application layer protocol shall be considered**).

**Protocols used at application layer are**:

1.TELNET (Terminal Network)

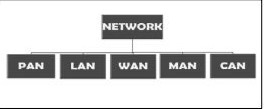
* 1. FTP (File Transfer Protocol)
  2. SMTP (Simple Mail Transfer Protocol)
  3. DNS (Domain Name System)
  4. HTTP (Hyper Text Transfer Protocol)
  5. SNMP (Simple Network Management Protocol)
  6. DHCP (Dynamic Host Configuration Protocol)

1. **Explain the logical address and physical address in computer network.**

**Logical Address:** -Logical Address is network layer generated 32 bit address (for IPv4) interpreted by protocol handler. Logical addresses are used by networking software to allow packets to travel through WAN (Internet). It makes packets to travel independently.

**Physical Address: -**Physical address is 48 bit MAC address of system. This is hardware level address used by “Ethernet” interface to communicate on LAN (Local Area Network) NIC card carries this address. This address is specified by the manufacturer of NIC.

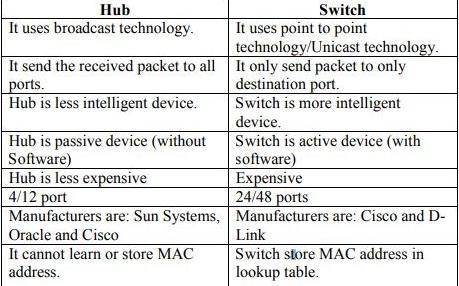
**8.List network classification based on network geographic area**



Personal Area Network

* + Local Area Network
  + Wide Area Network
  + Metropolitan Area Network
  + Campus Area Network

**9.State any two differences between switch and hub**.



**10.Define meaning of layered approach**

**Layered Approach**: The complex task of communication is broken into simpler subtask or modules. Each layer performed a subset of the required communication function.

**11.State the application of computer network**

* + Marketing and sales
  + Financial services
  + Information services
  + Banking
  + Television
  + E-mail
  + Electronic data interchange(EDI)

Teleconferencing**.**

**12.List any four application layer protocol**.

* + SMTP-Simple mail transfer protocol.
  + POP- Post office protocol
  + HTTP- Hypertext transfer protocol.  FTP- File transfer protocol.
  + TELNET-Terminal Network
  + DNS- Domain Name system BOOTP-BOOT protocol

**13.Define IP address. State IP addresses classes**

IP address: An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.

Or

An IP address is an address used to uniquely identify a device on an IP network.. **Classes:** Class A

Class B

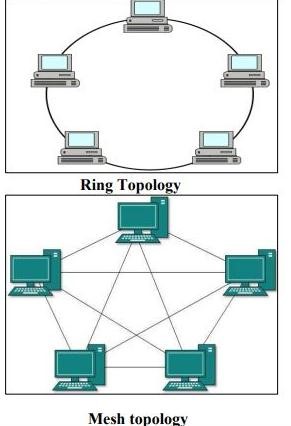
Class C

Class D

Class E

**14.Draw following topology with five Host:**

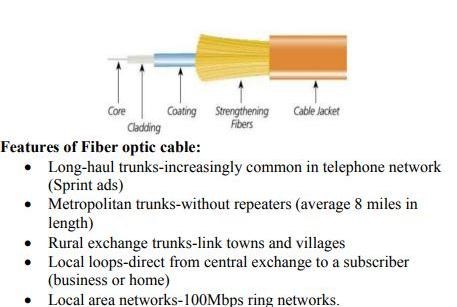
1. **Ring**
2. **Mesh Topology**



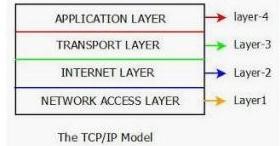
# UNIT-II

**Network Components and Topologies**.

**1.Draw constructional structure of fiber optic cable. Write any four features**.



**2.Draw TCP/IP reference model. Write the function of each layer.**



TCP/IP Reference Model is a four-layered suite of co mmunication protocols.

**The four layers in the TCP/IP protocol suite are:**

* **Host-to- Network Layer:** It is the lowest layer that is concerned with the physical transmission of data. TCP/IP does not specifically define any protocol here but supports all the standard protocols
* **Internet Layer:** It defines the protocols for logical transmission of data over the network. The main protocol in this layer is Internet Protocol (IP) and it is supported by the protocols ICMP, IGMP, RARP, and ARP.
* **Transport Layer:** It is responsible for error-free end-to-end delivery of data. The protocols defined here are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)
* **Application Layer**: This is the topmost layer and defines the interface of host programs with the transport layer services. This layer includes all high-level protocols like Telnet, HTTP, FTP, SMTP, etc.

**3.Describe the working of following OSI Model:**

**(i)Data Link layer (ii) Network layer**

**Data link layer**: Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals assembles them in a recognizable frame format, and hands over to upper layer. **Function of data link layer**:

* **Framing**: Data-link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver‟ end, data link layer picks up signals from hardware and assembles them into frames.
* **Addressing**: Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.
* **Synchronization**: When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.
* **Error Control**: Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.
* **Flow Control**: Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machines to exchange data on same speed.  Multi-Access: When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple Systems.

**Network layer**: The network layer (Layer 3) controls the source to destination delivery of data packets across multiple hops (nodes). It controls the operation of the subnet.

**The main functions of the network layer are as follows:**

* It is responsible for routing packets from the source host to the destination host. The routes can be based upon static tables that are rarely changed, or they can be automatically updated depending upon network conditions.
* The data link layer assigns the physical address locally. When the data packets are routed to remote locations, a logical addressing scheme is required to differentiate between the source system and the destination system. This is provided by the network layer.
* This layer also provides mechanisms for congestion control.
* The network layer tackles issues like transmission delays, transmission time, avoidance of jitters, etc.

**4.Describe the Host –to –network layer protocol Slip and PPP**

SLIP means Serial Line Internet Protocol. SLIP is the result of the integration of modem protocols prior to the suite of TCP/IP protocols. It is a simple Internet link protocol conducting neither address nor error control, which is the reason that it is quickly becoming obsolete in comparison to PPP. Data transmission with SLIP is very simple: this protocol sends a frame composed only of data to be sent followed by an end of transmission character (i.e. the END character, the ASCII code 192). A SLIP frame looks like this:

|  |  |
| --- | --- |
| **Data To Be Transmitted** | **END** |

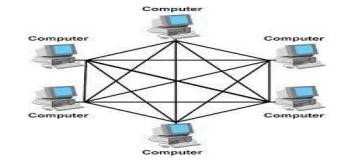
PPP means **Point to Point Protocol**. It is a much more developed protocol than SLIP (which is why it is replacing it), insofar as it can transfer additional data and is better suited to data transmission over the Internet. (The addition of data in a frame is mainly due to the increasing bandwidth). In reality, PPP is a collection of three protocols: a datagram encapsulation protocol; an **LCP, or Link Control Protocol**, enabling testing and communication configuration; a collection of **NCPs, or Network Control Protocols**, allowing integration control of PPP within the protocols of the upper layers. Data encapsulated in a PPP frame is called a **packet**. These packets are generally datagrams, but they can also be different (hence the specific designation of packet instead of datagram). As such, one field of the frame is reserved for the type of protocol to which the packet belongs. A PPP frame looks like this:

|  |  |  |
| --- | --- | --- |
| **Protocol (1-2 bytes)** | **Data To Be Transmitted** | **Padding Data** |

The padding data is used to adapt the length of the frame for certain protocols. A PPP session (from opening to closure) takes place as follows. Upon connection, an LCP packet is sent. In the event of an authentication request from the server, a packet relating to an authentication protocol may be sent i.e. PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), or Kerberos. Once communication is established, PPP sends configuration information using the NCP protocol. Datagrams to be sent are transmitted as packets. Upon disconnection, an LCP packet is sent to end the session

**5.Describe working of Mesh topology. Give its advantages and disadvantages**.

**Mesh topology:** In mesh topology there are multiple paths between / nodes. Mesh networks are most commonly employed for long distance transmission of data between nodes, which act as message switch, circuit switch or packet switch. A fully connected mesh, linking „n‟ nodes requires n (n-1) / 2 links but it is unusual for all possible or connections to be provided



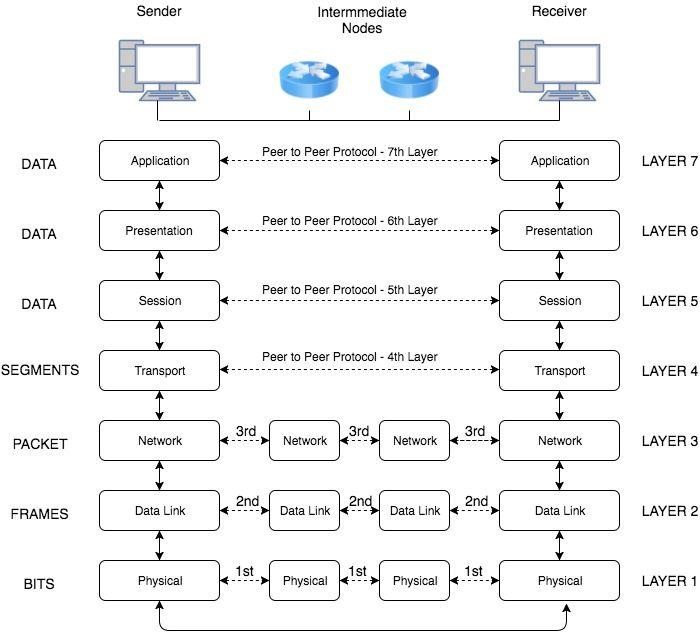
**Advantages:**

1. Avoids traffic problem
2. Robust topology since if one node fails, it does not affect the other nodes.
3. Point to point connection makes it easier to detect errors.
4. More security and Privacy in connections.

**Disadvantages:**

1. More cables are required than other topologies.
2. Cost of the network is high since more number of cables are used.
3. Installation and re-configuration is difficult.
4. Setup and maintenance of the topology is difficult.
5. Through put and transmission quantity depends on media and capacity of switching nodes.

**6.Draw OSI model. State function of each layer**.



OSI model has following 7 layers as **Physical layer, Data link layer, Network layer, Transport layer, Session layer, Presentation layer, Application layer**.

Following are the functions performed by the above layer

1. **Physical layer**: it deals with the mechanical and electrical specification of the interface and transmission medium.
   * Physical characteristics of interfaces and medium.
   * Representation of bits or signals.
   * Data rate
   * Synchronization of bit
   * Line configuration or connection type.  Physical topology
   * Transmission mode.
2. **Data link layer**: It performs node to node delivery of the data. It is responsible for transmitting group of bits between the adjacent nodes. The group of bits is called as frame.
   * Framing
   * Physical addressing
   * Flow control
   * Error control
   * Media access control
   * Node to node delivery
3. **Network layer:** It is responsible for routing the packets within the subnet i.e. from source to destination. It is responsible for source to destination delivery of individual packets across multiple networks. It ensures that packet is delivered from point of origin to destination
   * . Logical addressing
   * Routing
   * . Congestion control
   * Accounting and billing
   * Address transformation
   * Source host to destination host error free delivery of packet.
4. **Transport layer**: Responsibility of process to process delivery of message ensures that whole message arrives in order.
   * Service point addressing
   * Segmentation and reassembly
   * Connection control
   * Flow control is performed end to end
   * Error control
5. **Session layer**: Establishes, maintains, and synchronizes the interaction among communication systems It is responsible for dialog control and synchronization.
   * Dialog control
   * Synchronization
   * Token Management
   * Activity Management
   * Data Exchange
6. **Presentation layer:** It is concerned with syntax, semantics of information exchanged between the two systems
   * Translation: Presentation layer is responsible for converting various formats into required format of the recipient
   * Encryption: Data encryption and decryption is done by presentation layer for security.
   * Compression and Decompression: data is compressed while sending and decompress while receiving for reducing time of transmission.
7. **Application layer**: It enables user to access the network. It provides user interfaces and support for services like email, remote file access. Functions of Application layer:

* Network virtual terminal
* File transfer access and management  Mail services and directory services.

7.**Describe design issue for layering in computer network.**

**Design issue for layering in computer network:**

**Reliability**: Network channels and components may be unreliable, resulting in loss of bits while data transfer. So, an important design issue is to make sure that the information transferred is not distorted.

**Scalability**: Networks are continuously evolving. The sizes are continually increasing leading to congestion. Also, when new technologies are applied to the added components, it may lead to incompatibility issues. Hence, the design should be done so that the networks are scalable and can accommodate such additions and alterations.

**Addressing**: At a particular time, innumerable messages are being transferred between large numbers of computers. So, a naming or addressing system should exist so that each layer can identify the sender and receivers of each message.

**Error Control**: Unreliable channels introduce a number of errors in the data streams that are communicated. So, the layers need to agree upon common error detection and error correction methods so as to protect data packets while they are transferred.

**Flow Control**: If the rate at which data is produced by the sender is higher than the rate at which data is received by the receiver, there are chances of overflowing the receiver. So, a proper flow control mechanism needs to be implemented.

**Resource Allocation**: Computer networks provide services in the form of network resources to the end users. The main design issue is to allocate and deallocate resources to processes. The allocation/ deallocation should occur so that minimal interference among the hosts occurs and there is optimal usage of the resources.

**Statistical Multiplexing**: It is not feasible to allocate a dedicated path for each message while it is being transferred from the source to the destination. So, the data channel needs to be multiplexed, so as to allocate a fraction of the bandwidth or time to each host.

**Routing**: There may be multiple paths from the source to the destination. Routing involves choosing an optimal path among all possible paths, in terms of cost and time. There are several routing algorithms that are used in network systems.

**Security**: A major factor of data communication is to defend it against threats like eavesdropping and surreptitious alteration of messages. So, there should be adequate mechanisms to prevent unauthorized access to data through authentication and cryptography.

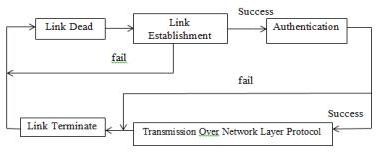
8. **Describe working of SLIP protocol and PPP protocol.**

**SLIP (Serial Line Internet Protocol):**

SLIP (Serial Line Internet Protocol) is designed to work over serial ports and routers with TCP/IP suit. It is a simple protocol which provides communication between machines which are previously configured for direct communication with each other. E.g Telephone lines to be use for computer networks SLIP transmission has a very simple format comprising of payload and a flag that act as an end delimiter. The flag in generally a special character equivalent to decimal 192. If the flag is present in data then an escape sequence precedes it, so that the receiver does not consider it as the end of frame

|  |  |
| --- | --- |
| **Data** | **END Flag** |

**PPP (Point to Point protocol):**



PPP (Point to Point protocol) is a layer 2 or data link layer protocol which is used to establish a direct communication between two nodes in network. This protocol is used to create a simple link between two peers in a network to transmit packets. It provides authentication, encryption and compression.

PPP links are full duplex and deliver packets in order. PPP works in 5 phases.

1. Link Dead Phase: PPP begin with Link Dead phase. At this phase link establishment initiates.
2. Link Establishment Phase: Configured packets with link control protocol are handed over to Network Layer. 3) Authentication Phase: PPP link needs authentication before exchange packets which network layer. Two types of authentication protocols used
   1. Password Authentication Protocol
   2. Challenge Handshake Authentication Protocol.
3. Link Transmission Phase: PPP packets travels over network layer with IP, IPX and other Network Layer

Protocol

1. Line Termination Phase: Closing the link is the task at this phase. PPP packet is configured to instruct network layer for proper termination.

# UNIT-III

**Reference model for Computer Network**

1. **State the classification of network based on:**

**i) Transmission technology ii) Network Relationship**

**Classification of networks based on transmission technology**:

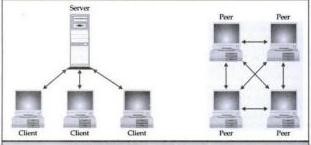
**The can be categorized broadly into two types**:

* **Broadcast networks**: Broadcast networks have a single communication channel that is shared or used by all the machines on the network. Short messages called packets sent by any machine are received by all the others. Broadcast systems generally use a special code in the address field for addressing a packet to all the concerned computers. This mode of operation is called broadcasting.
* **Point-to-point networks**: Point to point networks consists of many connections between individual pairs of machines. To go from the source to the destination a packet on these types of network may have to go through intermediate computers before they reach the desired computer.

**Classification of networks based on Network Relationship:**

**i)Client Server network ii) Peer to Peer network**

**Client Server Network**: In this network, a centralized computer, server is used for sharing the resources and providing services to other computers, clients. Thus the name Client Server. The servers stores all the network's shared files and applications programs, such as word processor documents, compilers, database applications, spreadsheets, and the network operating system. Client will send request to access information from the server. Based on the request, server will send the required information to the client.

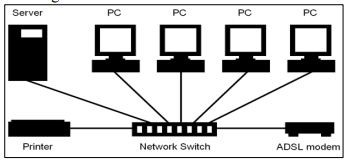


**Peer to Peer network: In** this type of network, each computer/node shares its resources using its own file system. There are no servers required in this network. Thus there is no centralized management, but each system owns its resources and services to be shared with other computers.

2.**Write any two specifications of following:**

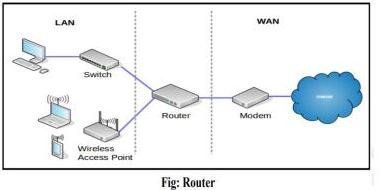
**i)Switch ii)Router Switch:**

* A switch is a multi-port bridge with a buffer and a design that can boost its efficiency (large number of ports implies less traffic) and performance.
* Switch is data link layer device. Switch can perform error checking before forwarding data that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.
* In other words, switch divides collision domain of hosts, but broadcast domain remains same.
* The basic function that any switch is supposed to perform is to receive information from any source connected to it and dispatch that information to the appropriate destination only. This thing differentiates switches from hubs.



**Router**:

* Router is network layer device that routes packets based on their logical address (host to host address).  Router normally connects LAN and WANS in the internet using route information stored in routing table Routing table of router is tabular database which stores information about destination and path (next Hop address through with to reach) information routing table is updated dynamically depending on changes in network.
* Messages are stored in the routers before re-transmission, routers are said to implement a store-andforward technique.



**Two types of routers are**:

1. Static routers: A router with manually configured routing tables is known as a static router.
2. Dynamic routers: A router with dynamically configured routing tables is known as a dynamic router. Dynamic routing consists of routing tables that are built and maintained automatically through an ongoing communication between routers.

3.**Describe major functions of Transport layer in TCP/IP model.Functions of**

**Transport Layer**

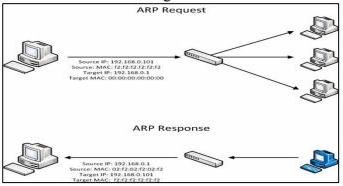
1. **Service Point Addressing**: Transport Layer header includes service point address which is port address. This layer gets the message to the correct process on the computer unlike Network Layer, which gets each packet to the correct computer.
2. **Segmentation and Reassembling**: A message is divided into segments; each segment contains sequence number, which enables this layer in reassembling the message. Message is reassembled correctly upon arrival at the destination and replaces packets which were lost in transmission.
3. **Connection Control**: It includes 2 types:
   * **Connectionless Transport Layer**: Each segment is considered as an independent packet and delivered to the transport layer at the destination machine.
   * **Connection Oriented** Transport Layer: Before delivering packets, connection is made with transport layer at the destination machine.
4. **Flow Control**: In this layer, flow control is performed end to end.
5. **Error Control**: Error Control is performed end to end in this layer to ensure that the complete message arrives at the receiving transport layer without any error. Error Correction is done through retransmission

**4.Describe the function of ARP with suitable diagram**

* Address Resolution Protocol (ARP)  ARP is a network-layer protocol.
* ARP maps IP address to its corresponding MAC address.
* The sender knows the IP address of the target; and it wants to know the hardware address of the target.  So, the sender creates an ARP request message in which it fills the following fields:

o Sender Hardware Address o Sender IP address o Target IP Address

* „Target Hardware Address‟ field is filled with 0‟s since it does not know that.  This ARP request message is broadcast to all hosts on the network.
* All hosts on the network receive and process the ARP packet. Only the host whose IP address matches with the value in the „Target IP address‟ field sends an ARP reply.
* The ARP reply message sent by the target machine contains its hardware address. This ARP reply is unicast.
* The sender receives this reply message and now it knows the hardware address of the target machine



**4.Describe the classification of networks based on transmission technology.**

The Computer networks can be classified on the basis of transmission technology used by them.

There are two types of Computer networks in this category:

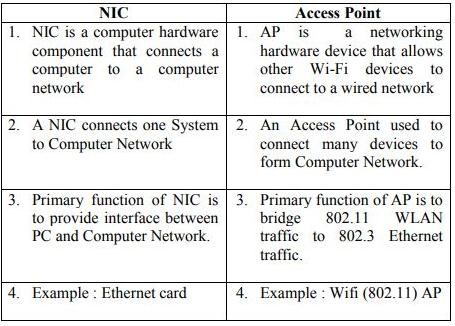
1. **Broadcast Networks:** In broadcast networks, a single communication channel is shared among all the computers of the network. This means, all the data transportation occurs through this shared channel. The data is transmitted in the form of packets. The packets transmitted by one computer are received by all others in the network. The destination of packet is specified by coding the address of destination computer in the address field of packet header. On receiving a packet, every computer checks whether it is intended for it or not. If the packet is intended for it, it is processed otherwise, it is discarded. There is another form of broadcast networks in which the packets transmitted by a computer are received by a particular group of computers. This is called as "Multicasting".
2. **Point to Point or Store and Forward Networks**: The store and forward networks consist of several interconnected computers and networking devices. The data is transmitted in the form of packets. Each packet has its own source and destination address. 1

To go from a source to a destination, a packet on this type of network may first have to visit one or more intermediate devices or computers that are generally called as "routers". The packets are stored on an intermediate router unless the output line is free. When the output line is free, it is forwarded to the next router. The routing algorithms are used to find a path from the source to destination. The routing algorithms play a very important role in this type of network.

5.**State NIC and Access Point. How it differs?**

**NIC :** A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter. **Access Point** : An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building. An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area.

For example, if you want to enable Wi-Fi access in your company's reception area but don‟t have a router within range, you can install an access point near the front desk and run an Ethernet cable through the ceiling back to the server room.



6. **Describe working of TCP/IP model. How it differs from OSI**.

**Working of TCP/IP Model** :

TCP/IP uses the client/server model of communication in which a user or machine (a client) is provided a service (like sending a webpage) by another computer (a server) in the network. Collectively, the TCP/IP suite of protocols is classified as stateless, which means each client request is considered new because it is unrelated to previous requests. Being stateless frees up network paths so they can be used continuously.

The transport layer itself, however, is stateful. It transmits a single message, and its connection remains in place until all the packets in a message have been received and reassembled at the destination.

TCP/IP model layers

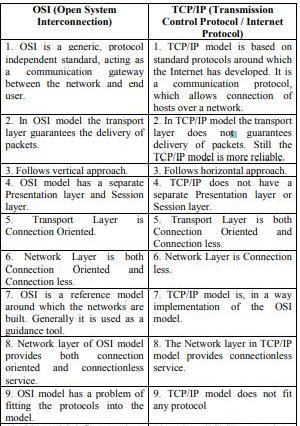
TCP/IP functionality is divided into four layers, each of which include specific protocols.

The application layer provides applications with standardized data exchange. Its protocols include the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol 3 (POP3), Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP).

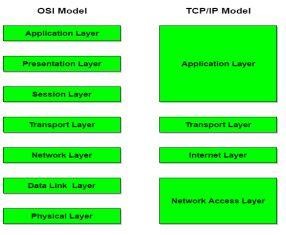
The transport layer is responsible for maintaining end-to-end communications across the network. TCP handles communications between hosts and provides flow control, multiplexing and reliability. The transport protocols include TCP and User Datagram Protocol (UDP), which is sometimes used instead of TCP for special purposes.

The Network layer, also called the Internet layer, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are the IP and the Internet Control Message Protocol (ICMP), which is used for error reporting.

The physical layer consists of protocols that operate only on a link -- the network component that interconnects nodes or hosts in the network. The protocols in this layer include Ethernet for local area networks (LANs) and the Address Resolution Protocol (ARP).



Diagrammatic Comparison between OSI Reference Model and TCP/IP Reference Model



**7.Explain working of ARP and RARP to assign IP addresses**.

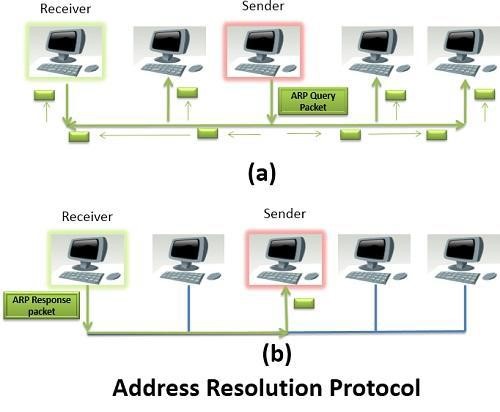
ARP :

ARP (Address Resolution Protocol) is a network layer protocol. As ARP is a dynamic mapping protocol, each host in the network knows the Logical address of another host. Now, suppose a host needs to send the IP datagram to another host. But, the IP datagram must be encapsulated in a frame so that it can pass through the physical network between sender and receiver. Here, the sender needs the physical address of the receiver so that it is being identified that to which receiver the packet belong to when the packet travel in the physical network.

For retrieving the physical address of the receiver the sender performs the following action.

1. The sender sends the ARP query packet on the network which is broadcasted to all the other host or router present in the network.
2. The ARP query packet contains the logical and physical address of the sender and the logical address of the receiver. iii. All the host and router receiving the ARP query packet process it but, only the intended receiver identifies its logical address present in the ARP query packet. iv. The receiver then sends ARP response packet which contains the logical (IP) address and physical address of the receiver.

v. The ARP response packet is unicast message sent directly to the sender whose physical address is present in the ARP query packet



# UNIT-IV

**TCP/IP Protocol Suite**

**1.List and describe any four benefits of Computer network.**

1. **File sharing:** -files can be centrally stored and used by multiple users. Shared directory or diskdrive is used. If many users access same file on network and make changes at same time and conflict occurs. Network operating system performs file sharing and provides
2. **Printer sharing**: Printer connected in a network can be shared inmany ways. Use printerqueues on server. Here printer is connected to server. Each work station can access printerdirectly. Printer can be connected to server. Connect a printer to a computer in a network andrun special print server software. Use built in print server. Use dedicated print server. Byprinter sharing reduces no. of printers needed. Share costly and high quality printers.
3. **Application services**: Share application on a network. When applications are centralized,amount of memory required on disk of work station is reduced. It is easier to administer anapplication. It is more secure and reliable. It is faster and convenient.
4. **E-mail services**. Two types of email systems are available:
5. File based system: Files are stored in shared location on server. Server provides access to file. Gate way server connects from file based email system to internet.

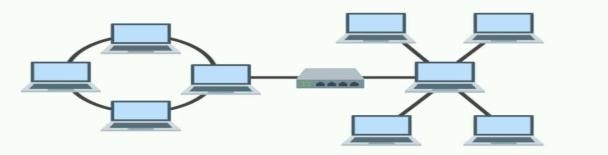
1. Client server e-mail system: E-mail server contains message and handles e-mailinterconnections. E-mail client functions (also consider other e-mail functions): read mail,send, compose, forward, delete.

E-mail protocols: SMTP, POP etc.

5. **Remote access**: Set up remote access service on network operating system. Setup VPN (virtualprivate network) on internet terminal services (T ELNET). User can access files from remotelocation. User can access centralized application or share files on LAN. security to sharefiles.

2 **Draw and describe graphical representation of Hybrid topology. Give it significance**.

Hybrid topology is an interconnection of two or more basic network topologies, each of which contains its own nodes. The resulting interconnection allows the nodes in a given basic topology to communicate with other nodes in the same basic topology as well as those in other basic topologies within the hybrid topology. Advantages of a hybrid network include increased flexibility as new basic topologies can easily be added or existing ones removed and increased fault tolerance.



Significance:

1. There are many reasons why hybrid topologies are used but they all have one thing in common: flexibility.

2.There are few constraints on the structure that a hybrid topology cannot accommodate, and you can incorporate ring, bus, mesh, and star topologies into one hybrid setup.

3.Hybrid topologies are very scalable. Their scalability makes them well-suited to larger networks.

**3.Define Interfaces, Services, Packets & Layer.**

**Interfaces :**

In OSI Reference Model, the mechanism for communication between adjacent layers in the model is called an interface. Interface refers to the process by which data is passed between layer N of the model and layer N-1 or layer N+1.

**Services:** A service is a set of actions that a layer offers to another (higher) layer.A service is what the layer provides to the layer above it through an interface. A service is a set of primitives (operations) that a layer provides to the layer above it.

**Packet :**

A packet is a small amount of data sent over a network, such as a LAN or the Internet. Similar to a real-life package, each packet includes a source and destination as well as the content (or data) being transferred. When the packets reach their destination, they are reassembled into a single file or other contiguous block of data. A typical packet includes two sections — a header and payload. Information about the packet is stored in the header.

**Layer :**

In layered architecture of Network Model, one whole network process is divided into small tasks. Each small task is then assigned to a particular layer which works dedicatedly to process the task only. Every layer does only specific work. In layered communication system, one layer of a host deals with the task done by or to be done by its peer layer at the same level on the remote host. The task is either initiated by layer at the lowest level or at the top most level.

4.**Give class & subnet address for following IP address:**

1. **191.168.0.1**
2. **221.45.14.68**
3. **245.32.14.24 (iv) 10.145.14.68**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr.**  **No.** | **IP Address Class Subnet** | **IP Address Class Subnet** | **IP Address Class Subnet** |
| **1** | 191.168.0.1 | Class B | 191.168.0.0 |
| **2** | 221.45.14.68 | Class C | 221.45.14.0 |
| **3** | 245.32.14.24 | Class E | Reserved |
| **4** | 10.145.14.68 | Class A | 10.0.0.0 |

**5.Describe working of Nos. State its salient features.**

**Working of NOS :**

A network operating system (NOS) is a computer operating system (OS) that is designed primarily to support workstations, personal computers and, in some instances, older terminals that are connectedon a local area network (LAN). The software behind a NOS allows multiple devices within a network to communicate and share resources with each other. The composition of hardware that typically uses a NOS includes a number of personal computers, a printer, a server and file server with a local network that connects them together. The role of the NOS is to. then provide basic network services and features that support multiple input requests simultaneously in a multiuser environment.

Types of network operating systems

There are two basic types of network operating systems, the peer-to peer peer NOS and the client/server NOS: **Features of network operating systems**

Features of network operating systems are typically associated with user administration, system maintenance and resource management functionality.

This includes:

* Basic support for operating systems like protocol and processor  support, hardware detection and multiprocessing.
* Printer and application sharing.
* Common file system and database sharing.
* Network security capabilities such as user authentication and access control.  Directory Services
* Backup and web services.
* Internetworking of various resources connected in the network

Providing access to remote printers, managing which users are using which printers when, managing how print jobs are queued, and recognizing when devices aren't available to the network. Enabling and managing access to files on remote systems, and determining who can access what—and who can't.

* Granting access to remote applications and resources, such as the Internet, and making those resources seem like local resources to the user (the network is ideally transparent to the user).
* Providing routing services, including support for major networking protocols, so that the operating system knows what data to send where.
* Monitoring the system and security, so as to provide proper security against viruses, hackers, and data corruption.
* Providing basic network administration utilities (such as SNMP, or Simple Network

Management Protocol), enabling an administrator to perform tasks involving managing network

**UNIT-V**

# Addressing

**1.Describe working of DNS and SMTP protocols with suitable example.**

***(Note: Any other diagram showing the DNS concept shall also be considered).***

**DNS:**

The Domain Name System (DNS) is a client/server application that identifies each host on the Internet with a unique userfriendly name.

DNS organizes the name space in a hierarchical structure to decentralize the responsibilities involved in naming.

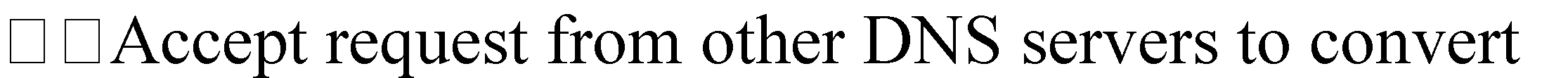
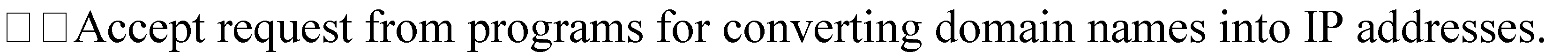
Each node in the tree has a domain name.

A domain is defined as any subtree of the domain name space.

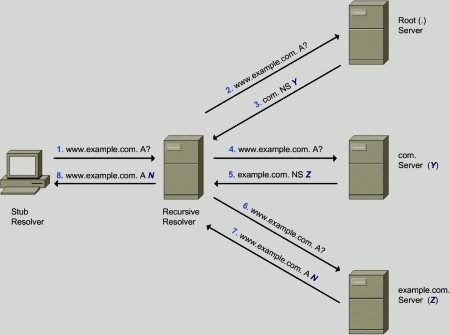
Domain Name system has top level domains such as .edu, .org, .com etc The name space information is distributed among DNS servers.

A domain name server is simply a computer that contains the database and the software of mapping between domain names and IP addresses.

Functions of DNS:



domain names into IP addresses.



As shown in Diagram Stub receiver wants to access www.example.com; this request is forwarded to Recursive resolver. The Recursive resolver forwards the request to all connected machines with request via its IP address. Server which is connected to specified IP address will respond back with said request

**SMTP:**

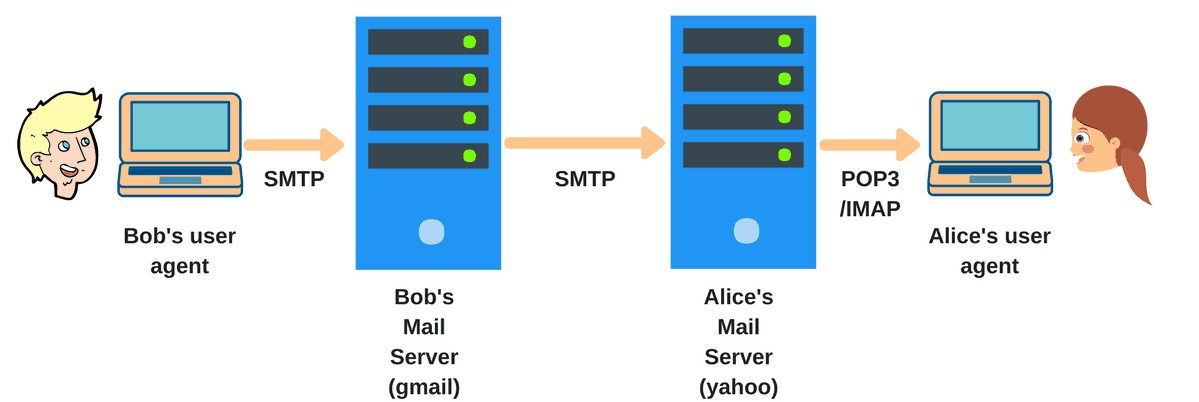
SMTP is simple mail transfer protocol.

It is connection-orientedtext-based protocol in which sender communicates with receiver using a command and supplying data over reliable TCP connection.

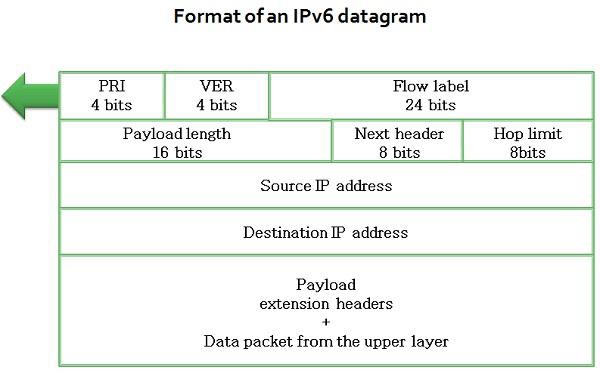
SMTP is standard application layer protocol for delivery of email over TCP/IP network.

SMTP establish a TCP connection between Sender And port number 25 of receiver.

It is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server



**2.Draw & explain structure of IPV6 address. Highlights major enhancement w.r.f. IPV4.**



**Version:** This four-bit field specifies the version of the IP, i.e., 6 in this case.

**Priority:** It defines the priority of the packet concerning traffic congestion.

**Flow label:** The reason for designing this protocol is to facilitate with special controlling for a certain flow of data.

**Payload length:** It defines the total length of the IP datagram excepting the base header.

**Next header:** It‟s an eight-bit field describe the header that trails the base header in the datagram. The next header is one of the optional extension headers which IP uses or the header for an upper layer protocol such as UDP or TCP.

**Hop limit:** This eight-bit hop limit field assist with the same functions at the TTL field in IPv4.

**Source address:** It is a 16 bytes internet address identifies the source of the datagram.

**Destination address:** This is 16-byte internet address that generally describes the final destination of the datagram.

Major enhancement in IPv6.

1. IPv4 has 32-bit address length whereas IPv6 has 128-bit address length.
2. IPv4 addresses represent the binary numbers in decimals. On the other hand, IPv6 addresses express binary numbers in hexadecimal.
3. IPv6 uses end-to-end fragmentation while IPv4 requires an intermediate router to fragment any datagram that is too large.
4. Header length of IPv4 is 20 bytes. In contrast, header length of IPv6 is 40 bytes.
5. IPv4 uses checksum field in the header format for handling error checking. On the contrary, IPv6 removes the header checksum field.
6. In IPv4, the base header does not contain a field for header length, and 16-bit payload length field replaces it in the IPv6 header.
7. The option fields in IPv4 are employed as extension headers in IPv6.
8. The Time to live field in IPv4 refers to as Hop limit in IPv6.
9. The header length field which is present in IPv4 is eliminated in IPv6 because the length of the header is fixed in this version.
10. IPv4 uses broadcasting to transmit the packets to the destination computers while IPv6 uses multicasting and anycasting.
11. IPv6 provides authentication and encryption, but IPv4 doesn‟t provide it.

**3.Differentiate between peer-to-peer, client server and distributed modes of computing.**

**(Any four points).**

|  |  |  |  |
| --- | --- | --- | --- |
| **BASIS FOR**  **COMPA RISON** | **PEER-TOPEER** | **CLIENTSERVER** | **DISTRIBUTED**  **MODES** |
| Basic | Clients and server are not distinguished; each node act as client and server. | There is a specific server and specific clients connected to the server. | All nodes are kept at different/distributed location |
| Service | Each node can request for services and can also provide the services. | The client request for service and server respond with the service. | Each node is capable to accept input and produce result. |
| Focus | Connectivity. | Sharing the information. | Sharing Resources and performing dedicated task |
| Data | Each peer has its own data. | The data is stored in a centralized server. | Data is stored at local and over network as well. |
| Server | As the services are provided by several servers distributed in the peer-topeer system, a server in not bottlenecked. | When several clients request for the services simultaneously, a server can get bottlenecked | Each node can act as dedicated server if required |
| Expense | Peer-to-peer Are less expensive to implement. | The client server are Expensive to implement. | This is very expensive architecture as it requires special hardware |
| Stability | Peer-toPeer suffers if the number of peers increases in the system. | Client-Server is more stable and scalable. | Extremely stableand scalable. |

**1.Enlist steps to share a printer in a network and share a scanner within two computers.**

1. **Install the printer drivers:** In order to share a printer, it must be installed on the computer it is connected to. Most modern printers connect via USB and will install automatically when they are connected.
2. **Open the Control Panel:** You can access the Control Panel in Windows 7 by clicking the Start menu and selecting Control Panel. In Windows, press Win+X and select Control Panel from the menu.
3. **Open the Network and Sharing Center:** If your Control Panel is in Category view, click "Network and Internet", and then select "Network and Sharing Center". Click on "Network and Internet".

If your Control Panel is in Icon view, click the "Network and Sharing Center" icon.

1. **Click the "Change advanced sharing settings" link.** This is located in the left navigation pane of the Network and Sharing Center.
2. **Expand the profile you need to change.** You will see three different options when you open the "Advanced share settings": Private, Guest or Public, and All Networks. If you are on a Home network, expand the Private section.
3. **Enable "File and printer sharing".** Toggle this on to allow other devices to connect to your printer.

This will also allow you to share files and folders with other computers on the network.

1. **Toggle the password protection.** You can decide whether or not you want to enable password protection for your printer. If it is turned on, only users who have a user account on your computer will be able to access the printer. You can toggle password protection in the "All Networks" section.
2. **Share the printer.** Now that file and printer sharing has been turned on, you will need to share the printer itself. To do this, go back to the Control Panel and open the Devices and Printers option. Rightclick on the printer you want to share and click "Printer properties". Click the Sharing tab, and then check the "Share this printer" box.

**Sharing Scanner within two machine:**

1. Open the Start menu and select "Control Panel."
2. Type "network" in the search box
3. Find the scanner in the list of devices, right-click it, then select "Install."
4. Follow the on-screen instructions to finish adding the scanner.

**2.Elaborate the procedure to divide networks into subnets. Divide given network address in four equal part to hold maximum 50 devices in each subnet. IP address 192.168.14.14/25**

***(Note: The problem is solved considering the given address as Host address with class C type and 2 bits considered for subnetting. Any other correct solution shall be considered).***

1. Convert to binary: Convert given IP address and Subnet mask into binary equivalent values.
2. Calculate the subnet address: To calculate the subnet address perform a bit-wise AND operation (1 .1=1, 1 . 0 or 0 . 1 =0, 0 . 0=0) on the host IP address and subnet mask. The result is the subnet address in which the host is situated.
3. Find host range.The Subnet address is identified by all 0 bits in the Host part of the address. The first host within the subnet is identified by all 0s and a 1. The last host is identified by all 1s and a 0. The broadcast address is the all 1s.
4. Calculate the total number of subnets and the hosts per subnet. Knowing the number of Subnet and Host bits we can now calculate the total number of possible subnets and the total number of hosts per subnet. We assume in our calculations that all-zeros and all-ones subnets can be used. Step 1:

|  |  |
| --- | --- |
| IP Address (Decimal) | 192.168.14.14 |
| IP Address (Binary) | 11000000 .10101000 .00001110. 00001110 |
| Subnet Mask (Decimal) | 255. 255. 255.192 |
| Subnet Mask (Binary) | 11111111 . 11111111. 11111111. 10000000 |

Since we need 4 subnet works subnet mask of 25 will not work because with subnet mask of 25 one can divide network in two parts. So we borrow a bit from host bit.

|  |  |
| --- | --- |
| IP Address (Decimal) | 192.168.14.14 |
| IP Address (Binary) | 11000000 .10101000 .00001110. 00001110 |
| Subnet Mask (Decimal) | 11111111. 11111111. 11111111. 11000000 |
| Subnet Mask (Binary) | 11000000 .10101000. 00001110. 00000000 |
| Subnet Address (Decimal) | 192.168.14.0 |

Step 3:

We know already that for sub netting this Class C address we have borrowed 2 bits from the Host field. These 2 bits are used to identify the subnets. The remaining 6 bits are used for defining hosts within a particular subnet. Step 4:

|  |  |  |
| --- | --- | --- |
| **Network Address** | **Usable Host Range** | **Broadcast Address:** |
| 192.168.14.0 | 192.168.14.1 - 192.168.14.62 | 192.168.14.63 |
| 192.168.14.64 | 192.168.14.65 - 192.168.14.126 | 192.168.14.127 |
| 192.168.14.128 | 192.168.14.129 -192.168.14.190 | 192.168.14.191 |
| 192.168.14.192 | 192.168.14.193 -192.168.14.254 | 192.168.14.255 |

Since we want 50 in each subnetwork we can adjust it as follows.

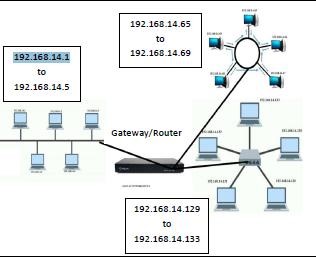
|  |  |  |
| --- | --- | --- |
| **Network Address** | **Usable Host Range** | **Broadcast Address:** |
| 192.168.14.0 | 192.168.14.1 - 192.168.14.50 | 192.168.14.63 |
| 192.168.14.64 | 192.168.14.65 - 192.168.14.114 | 192.168.14.127 |
| 192.168.14.128 | 192.168.14.129 -192.168.14.178 | 192.168.14.191 |
| 192.168.14.192 | 192.168.14.193 -192.168.14.242 | 192.168.14.255 |

**3.Design a network with 15 host divided into 3 equal size sub networks each with different network topology. i.e. bus, star and ring. Connect these sub-networks with suitable network device.**

**Specify IP address to each sub-network with its Broadcast and Network address.**

***(Note: Any other Class of IP address with different set of subnets shall be considered).* List of available IP Address, Broadcast and Network Address:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Network Topology** | **Network Address** | **Broadcast Address:** | **Usable Host Range** |
| BUS | 192.168.14.0 | 192.168.14.63 | 192.168.14.1 - 192.168.14.5 |
| RING | 192.168.14.64 | 192.168.14.127 | 192.168.14.65 - 192.168.14.69 |
| STAR | 192.168.14.128 | 192.168.14.191 | 192.168.14.129 -192.168.14.133 |



**4.Differentiate between OSI Model and TCP/IP Model.**

|  |  |
| --- | --- |
| **OSI** | **TCP/IP** |
| OSI is a generic, protocol independent standard, acting as a communication gateway  between the network and end  User | TCP/IP model is based on standard  Protocols around which the  Internet has developed. It is a communication protocol, which allows connection of hosts over a network. |
| In OSI model the transport layer Guarantees the delivery of packets. | In TCP/IP model the transport layer does not guarantee delivery of packets. Still the TCP/IP model is more reliable. |
| Follows vertical approach. | Follows horizontal approach. |
| OSI model has a separate Presentation layer and Session layer. | TCP/IP does not have a separate Presentation layer or Session layer. |
| OSI is a reference model around Which the networks are built. Generally, it is used as a  guidance Tool. | TCP/IP model is, in a way implementation of the OSI model. |
| Network layer of OSI model provides both connection oriented  And connectionless service. | The Network layer in TCP/IP model  Provides connectionless service. |
| OSI model has a problem of fitting the protocols into model. | TCP/IP model does not fit any protocol |

**5.a.State difference between IPv4 and IPv6.**

|  |  |
| --- | --- |
| **IPv4** | **IPv6** |
| Source and Destination addresses are 32 bits in length. | Source and Destination addresses are 128 bits in length. |
| IPv4 addresses are binary numbers represented in decimals. | IPv6 addresses are binary numbers represented in hexadecimals. |
| IPsec supports in optional | IPsec support is required. |
| Security is dependent on application. | IPsec is inbuilt in IPv6 protocol. |
| No packet flow identification. | Packet flow identification is available within the IPv6 header using flow label field |
| Header includes a checksum. | Header does not include a checksum |
| Encryption and Authentication is not provided.. | Encryption and Authentication is provided. |
| Must be configured either manually or through DHCP | Does not require manual configuration or DHCP. |
| Header includes options. | All optional data is moved to IPv6extension headers |
| Most support a 576 byte packet size.(Usually fragmented) | Must support 1280 byte packet size(Without Fragmentation |

**b.Write step wise procedure to configure DHCP server.**

**Steps to configure DHCP server:**

1.When the client detects it has connected to the DHCP server, it send the DHCPDISCOVER request.

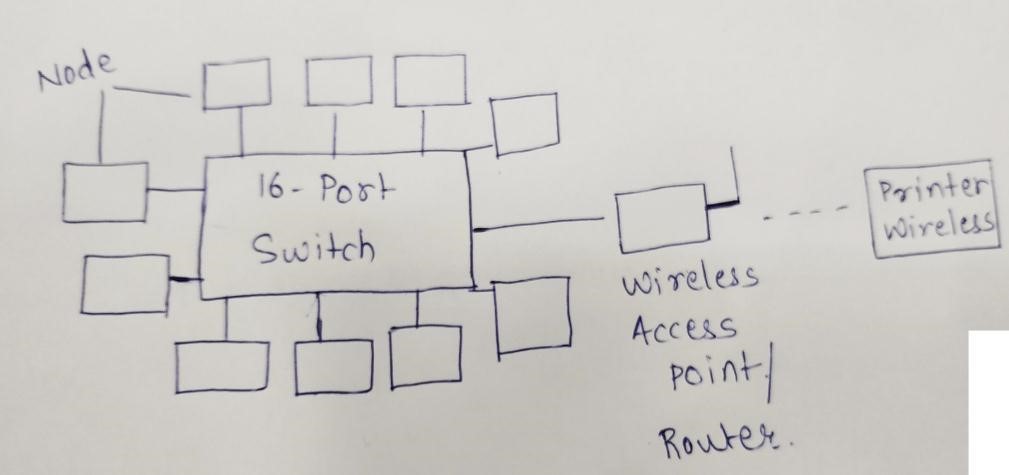
2.The router either receives the request or redirects it to the appropriate DHCP server.

3.If the server accepts the new device, it will send a DHCPOFFER message back to the client which contains the client device‟s MAC address and the IP address being offered.

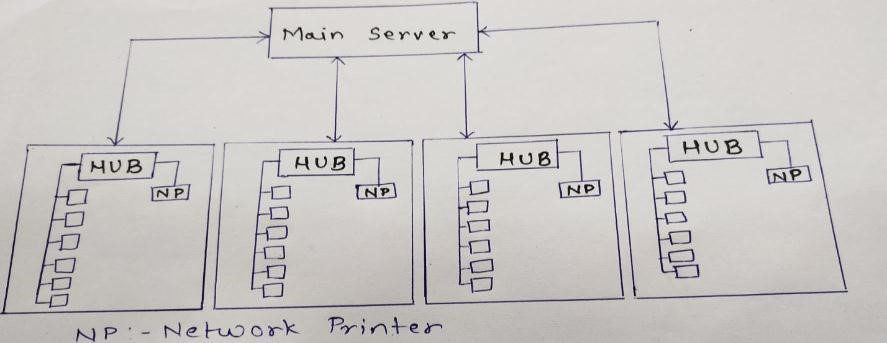
4.The client returns the DHCPREQUEST message to the server confirming it will use the IP Address.

5.Finally, server responds with a DHCPACK acknowledgement message that confirms the client has been given access for a certain amount of time.

**6.Draw Suitable network layout with star topology for a computer lab with 10 hosts and a wireless printer. List all components in the layout.**



**7.Design suitable network layout for an organization with four departments (6 users each), shared print server and network printer.**



**8.Design a network class ‘c’ with network address 192.156.5.0 with 2 subnet. State the subnet mask and subnet address.**

In Binary IP Address:

11000000 10011100 0000001 00000000

We will use class C address which takes 1 bit from Host field for sub netting and leaves 7 bits for defining hosts. Having 7 bits available for defining subnets means we have up to 2(21) different subnets.

8 bits 8 bits 8 bits

8 bits

|  |  |  |  |
| --- | --- | --- | --- |
| **N/W** | **N/W** | **N/W** | **N/W** |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 bits  7 bit |  | 8 bits | | 8 bits | |  | 1 bit | |
| **N/W** | **N/W** |  |  | **N/W** |  | **Subnet** |  | **Host** |

Let‟s use IP address 192.156.5.0 with subnet mask 255.255.255.128 **Step 1: convert to binary**

192 156 5 0

11000000 10011100 00000101 00000000

255 255 255 128

11111111 11111111 11111111 100000000

**Subnet Mask is: 255.255.255.128**

**Step 2: Calculate subnet address**

To calculate the subnets IP address you need to perform bit wise AND operation (1+1=1, 1+0=0 or 0+1=0,

0+0=0) on the host IP address and subnet mask:

IP address

11000000 10011100 00000101 00000000

AND

11111111 11111111 11111111 10000000

11000000 10011100 00000101 00000000

**Subnet Address is: 192.156.5.0**