RGPVNOTES.IN

Program : **B.Tech**

Subject Name: **Computer Network**

Subject Code: **IT-502**

Semester: **5th**

Department of Information Technology

Sub: Computer **Sub Code :IT-502**

UNIT I

Subject Introduction

A computer network or data network is a telecommunications network which allows computers to exchange data. In computer networks, networked computing devices pass data to each other along data connections (network links). Data is transferred in the form of packets. The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet.

Network computer devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices are said to be networked together when one device can exchange information with the other device, whether or not they have a direct connection to each other.

Importance of computer networks

Computer networks allow the user to access remote programs and remote databases either of the same organization or from other enterprises or public sources. Computer networks provide communication possibilities faster than other facilities and also have following capabilities.

1. Resource and load sharing
2. Programs do not need to run on a single machine
3. Reduced cost
4. Several machines can share printers, tape drives, etc.
5. High reliability
6. If a machine goes down, another can take over
7. Mail and communication

Computer Network: components

Computer networks share common devices, functions, and features including servers, clients, transmission media, shared data, shared printers and other hardware and software resources, network interface card(NIC), the local operating system(LOS), and the network operating system (NOS).

Servers - Servers are computers that hold shared files, programs, and the network operating system. Servers provide access to network resources to all the users of the network. There are many different kinds of servers, and one server can provide several functions. For example, there are file servers, print servers, mail servers, communication servers, database servers, print servers, fax servers and web servers, to name a few.

Clients - Clients are computers that access and use the network and shared network resources. Client computers are basically the customers (users) of the network, as they request and receive services from the servers.

Transmission Media - Transmission media are the facilities used to interconnect computers in a network, such as twisted-pair wire, coaxial cable, and optical fiber cable. Transmission media are sometimes called channels, links or lines.

Shared data - Shared data are data that file servers provide to clients such as data files, printer access programs, and e-mail.

Shared printers and other peripherals - Shared printers and peripherals are hardware resources provided to the users of the network by servers. Resources provided include data files, printers, software, or any other items used by clients on the network.

Network Interface Card - Each computer in a network has a special expansion card called a network interface card (NIC). The NIC prepares (formats) and sends data, receives data, and controls data flow between the computer and the network. On the transmit side, the NIC passes frames of data on to the physical layer, which transmits the data to the physical link. On the receiver's side, the NIC processes bits received from the physical layer and processes the message based on its contents. Local Operating System - A local operating system allows personal computers to access files, print to a local printer, and have and use one or more disk and CD drives that are Located on the computer. Examples are MS-DOS, UNIX, Linux, Windows 2000, Windows 98, and Windows XP etc.

Network Operating System - The network operating system is a program that runs on computers and servers and allows the computers to communicate over the network.

Hub - Hub is a device that splits a network connection into multiple computers. It is a distribution center. When a computer request information from a network or a specific computer, it sends the request to the hub through a cable. The hub will receive the request and transmit it to the entire network. Each computer in the network should then figure out whether the broadcast data is for them or not.

Switch - Switch is a telecommunication device grouped as one of computer network components. The switch is like a Hub but built in with advanced features. It uses physical device addresses in each incoming message so that it can deliver the message to the right destination or port.

Like a hub, the switch doesn't broadcast the received message to the entire network; rather before sending it checks to which system or port should the message be sent.

Broadcast and point to point networks

Broadcast links and point-to-point links are two types of transmission technologies that are in widespread use. Point-to-point links is a connection between individual pairs of machines. In this connection, a short message from the source to the destination is called a “packet”.

This packet may have to visit one or more intermediate machines before returning to the destination, therefore finding good routes within the network is important in point-to-point.

A point-to-point transmission with one sender and one receiver is called unicasting. Broadcast links is in contrast a communication channel that is shared by all the machines in the network. The difference between point-to-point and broadcast, is that in broadcast networks, the packets(/the message) is sent by any machine and received by all the other machines.

Point-to-Point Connection

The point-to-point is a kind of line configuration which describes the method to connect two communication devices in a link. The point-to-point connection is a unicast connection. There is a dedicated link between an individual pair of sender and receiver. The capacity of the entire channel is reserved only for the transmission of the packet between the sender and receiver.

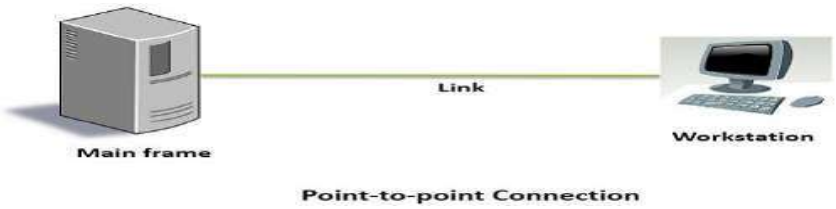

Fig 1.1 Point to Point connection

Multipoint Connection

The multipoint connection is a connection established between more than two devices. The multipoint connection is also called multidrop line configuration. In multipoint connection, a single link is shared by multiple devices. So, it can be said that the channel capacity is shared temporarily by every device connecting to the link. If devices are using the link turn by turn, then it is said to be time shared line configuration.

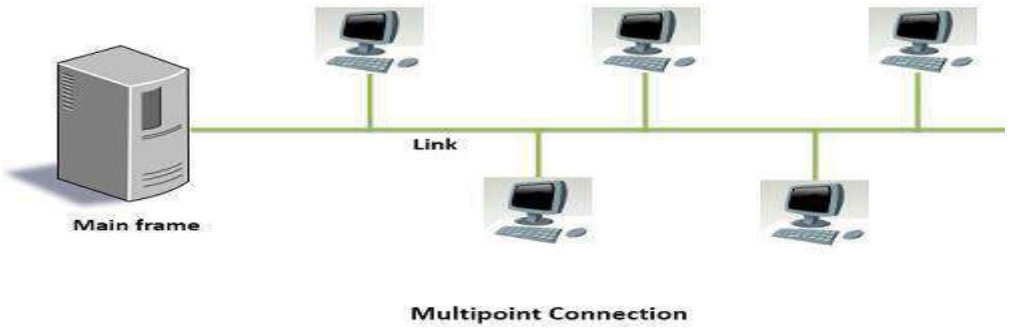

Fig 1.2 Multipoint Connection

Computer Network: Classifications & Types

Computer Network: Classifications & Types. There are three types of network classification

1) LAN (Local area network)
2) MAN (Metropolitan Area network)
3) WAN (Wide area network)

1) Local area network (LAN)

LAN is a group of the computers placed in the same room, same floor, or the same building so they relate to each other to form a single network to share their resources such as disk drives, data, CPU, modem etc. LAN is limited to some geographical area less than 2 km. Most of LAN is used widely is an Ethernet system of the bus topology.

Fig 1.3 Local Area Network

Characteristics of LAN

- LAN connects the computer in a single building; block and they are working in any limited area.
- Media access control methods in a LAN, the bus based Ethernet, token ring.
- This is private networks, not for the subject to tariffs or regulatory controls.
- LAN is a wireless there is an additional in some countries.

Advantages of local area network (LAN)

1. **Sharing of resources:**

All the resources are attached to one network and if any computer needs any resources then it can be shared with the required computer. Types of resources are the DVD drive, printers, scanners, modems and hard drives. So there is no need to purchase separate resources for each computer and it saves money.

2. **Client and server relationship:**

All the data from attached computers can be stored in one server. If any computer (Client) needs data then that computer user can simply log in and access the data from the server. For example movies and songs can be stored on the server and can be accessed by any authorized user (Client computer).

3. **Sharing of the internet:**

In offices and net cafes, we can see that one internet connection is shared between all computers. This is also the type of LAN technology in which main internet cable is attached to one server and distributed amoung attached computers by the operating system.

4. **Software program sharing:**

Software programs can also be shared on the LAN. You can use single licensed software and any user can use it in the network. It is expensive to buy a license for each user in the network so sharing software program is easy and cost-effective.

5. **Securing of data:**

Keeping data on the server is more secure. And if you want to change or remove any data you can do it easily on one server computer and other computers can access updated data. You can also give access or revoke access to specific users so that only authorized users can access the data in the network.

6. **Communication is easy, fast, and time-saving**

In LAN computers can exchange data and messages in the easy and fast way. It also saves time and makes our work fast. Every user can share messages and data with any other user on LAN. The user can log in from any computer on the network and access the same data placed on the server.

7. **Computer identification:**

Each computer is given a MAC address and is temporarily stored in the switch or router during communication. All computers on the LAN are identified by MAC addresses which are used to send and receive messages and data. Note that MAC address is stored in the network adapter that is attached in the motherboard of each computer. In old computers, network adapters were not built in with motherboards but in modern computers, they come built-in with motherboards.

Disadvantages of local area network (LAN)

1. **Data security problem:**

If the server computer is not set up correctly and there is a leak in security then unauthorized users can access the data also. So there should be privacy policy and rules set up correctly on the server.

2. **Limitation of distance:**

Local area networks are usually made within a building or nearby building and cannot extend to the wider area.

3. **Server crashes may affect all computers:**

If any file on the server is corrupted or hard drive fails then all the attached computers face problems in functioning properly.

4. **Setting up a LAN is expensive:**

It is expensive to set up LAN because there is special software required to make a server. Also, communication devices like hubs, switches, routers, cables are costly. The special administrator is required to maintain and troubleshoot LAN for a large office.

2) Metropolitan Area network (MAN)

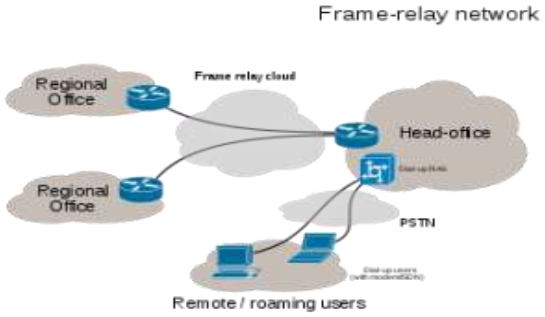

Fig.1.2 Metropolitan Area network

The metropolitan area network is a large computer network that expands a Metropolitan area or campus. It is geographic area between WAN and LAN. It's expand around 50km devices used are modem and wire/cable.

Characteristics of MAN

- Its covers the towns and cities (50km)
- It is developed in the 1980s.
- MAN is used by the communication medium for optical fiber cables, it also used for other media

Advantages of a metropolitan area network (MAN)

1. **Less expensive:**

It is less expensive to attach MAN with WAN. MAN gives the good efficiency of data. In MAN data is easily managed in a centralized way.

2. **Sending local emails:**

On MAN you can send local emails fast and free.

3. **High speed than WAN:**

MAN uses fiber optics so the speed of data can easily reach upon 1000 Mbps. Files and databases can be transferred fast.

4. **Sharing of the internet:**

In some installation of MANs, users can share their internet connection. So multiple users can get the same high-speed internet.

5. **Conversion from LAN to MAN is easy:**

MAN is a faster way to connect two fast LANs together. This is due to the fast configuration of links.

6. **High Security:**

MAN has a high-security level than WAN.

Disadvantages of metropolitan area network (MAN)

1. **Difficult to manage:**

If MAN becomes bigger then it becomes difficult to manage it. This is due to a security problem and other extra configuration.

2. **Internet speed difference:**

MAN cannot work on traditional phone copper wires. If MAN is installed on copper wires then there will be very low speed. So it required the high cost to set up fiber optics for the first time.

3. **Hackers attack:**

In MAN there are high chances of attacking hackers on the network compared to LAN. So data may be leaked. Data can be secured but it needs high trained staff and security tools.

4. **Technical people required to set up:**

To setup MAN it requires technical people that can correctly setup MAN. The technical people are network administrators and troubleshooters.

5. **More wires required:**

In MAN additional cables are required to connect two LAN which is another problem.

3. Wide area Network (WAN)

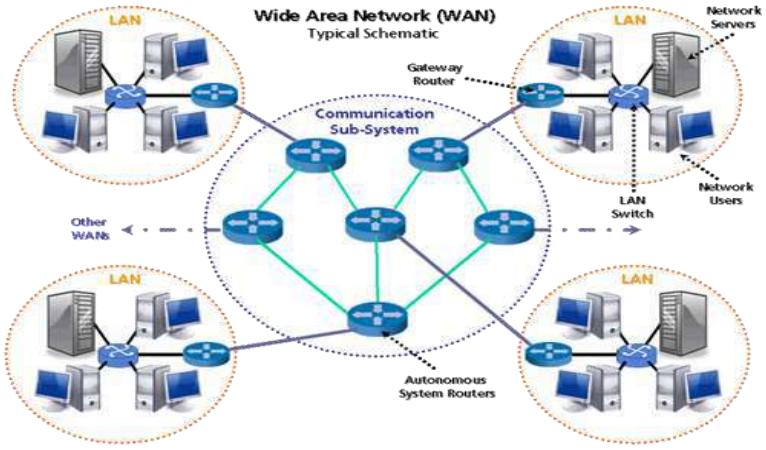

Fig. 1.3 Wide area Network

The wide area network is a network which connects the countries, cities or the continents; it is a public communications links. The most popular example of a WAN is the internet. WAN is used to connect LAN so the users and the computer in the one location can communicate with each other.

Characteristics of WAN

- It covers the large distances.
- Communication medium used are a satellite, telephones which are connected by the routers.

Advantages of WANS

If your company has branches in several locations, a wide area network is a viable option to boost productivity and increase internal communications. Below are some of the more critical business advantages to establishing a WAN:

- **Centralizes IT infrastructure** — Many consider this WAN's top advantage. A WAN eliminates the need to buy email or file servers for each office. Instead, you only have to set up one at your head office's data center. Setting up a WAN also simplifies server management, since you won't have to support, back-up, host, or physically protect several units. Also, setting up a WAN provides significant economies of scale by providing a central pool of IT resources the whole company can tap into.

- **Boosts your privacy** — Setting up a WAN allows you to share sensitive data with all your sites without having to send the information over the Internet. Having your WAN encrypt your data before you send it adds an extra layer of protection for any confidential material you may be transferring. With so many hackers out there just dying to steal sensitive corporate data, a business needs all the protection it can get from network intrusions.

- **Increases bandwidth** — Corporate WANS often use leased lines instead of broadband connections to form the backbone of their networks. Using leased lines offers several pluses for a company, including higher upload speeds than your typical broadband connections. Corporate WANS also generally offer unlimited monthly data transfer limits, so you can use these links as much as you like without boosting costs. Improved communications not only increase efficiency but also boost productivity.

- **Eliminates Need for ISDN** — WANs can cut costs by eliminating the need to rent expensive ISDN circuits for phone calls. Instead, you can have your WAN carry them. If your WAN provider "prioritizes voice traffic," you probably won't see any drop off in voice quality, either. You may also benefit from much cheaper call rates when compared to calls made using ISDN circuits. Some companies use a hybrid approach. They have inbound calls come over ISDN and outbound calls go over the WAN. This approach won't save you as much money, but it will still lower your bill.

- **Guaranteed uptime** — Many WAN providers offer business-class support. That means you get a specific amount of uptime monthly, quarterly, or yearly as part of your SLA. They may also offer you round the clock support. Guaranteed uptime is a big plus no matter what your industry. Let's face it. No company can afford to be down for any length of time in today's business environment given the stringent demands of modern customers.

- **Cuts costs, increase profits** — In addition to eliminating the need for ISDN, WANs can help you cut costs and increase profits in a wide variety of other ways. For example, WANS eliminate or significantly reduce the costs of gathering teams from different offices in one location. Your marketing team in the United States can work closely with your manufacturing team in Germany

using video conferencing and email. Saving on the travel costs alone could make investing in a WAN a viable option for you.

WANS also provide some key technical advantages as well. In addition to providing support for a wide variety of applications and a large number of terminals, WANs allow companies to expand their networks through plug-in connections over locations and boost interconnectivity by using gateways, bridges, and routers. Plus, by centralizing network management and monitoring of use and performance, WANS ensure maximum availability and reliability.

Disadvantages of WANS

While WANS provide numerous advantages, they have their share of disadvantages. As with any technology, you need to be aware of these downsides to make an informed decision about WANS. The three most critical downsides are high setup costs, security concerns, and maintenance issues.

- **High setup costs** — WANs are complicated and complex, so they are rather expensive to set up. Obviously, the bigger the WAN, the costlier it is to set up. One reason that the setup costs are high is the need to connect far-flung remote areas. However, by using public networks, you can set up a WAN using just software (SD-WAN), which reduces setup costs. Keep in mind also that the price/performance ratio of WANs is better now than a decade or so ago.

- **Security Concerns** —WANs open the way for certain types of internal security breaches, such as unauthorized use, information theft, and malicious damage to files. While many companies have some security in place when it comes to the branches, they deploy the bulk of their security at their data centers to control and manage information sent to their locations. This strategy reduces management costs but limits the company's ability to deal directly with security breaches at their locations. Some companies also have a hard time compressing and accelerating SSL traffic without significantly increasing security vulnerabilities and creating new management challenges.

- **Maintenance Issues** — Maintaining a WAN is a challenge, no doubt about it. Guaranteeing that your data center will be up and operating 24/7 is the biggest maintenance challenge of all. Data center managers must be able to detect failures before they occur and reduce data center downtime as much as possible, regardless of the reasons. Downtime is costly, in fact, a study done by infinities Research estimates that medium and large businesses in North America lose as much as $100 million annually to IT and communication technology downtime.

Layered Architecture: Interfaces and Services Protocol hierarchy, Design Issues

To tackle with the design complexity most of the networks are organize as a set of layers or levels. The fundamental idea of layered architecture is to divide the divide the design into small pieces. The layering provides modularity to the network design. The main duty of each layer is to provide offer services to higher layers and provide abstraction. The main benefits of layered architecture are modularity and clear interfaces. The basic elements of a layered model are services, protocols, and Interfaces.
A service is a set of functions that a layer offers to another layer (usually to upper layer) we know that

protocol is a set of rules. Here the protocols are used to exchange information with a peer layer. Peers means layers at the same level. The protocol consists several rules that deals with the content and the order or structure of the messages exchanged.

Five Layered Network

Layered architectures have several advantages. Some of them are

- Modularity and clear interface
- Provide flexibility to modify network services
- Ensure independence of layers
- Management of network architecture is easy
- Each layer can be analyzed and tested independently of other layers

The benefits to layering networking protocol specifications are many including Interoperability. Layering promotes greater interoperability between devices from different manufacturers and even between different generations of the same type of device from the same manufacturer.

Greater Compatibility - One of the greatest of all the benefits of using a hierarchal or layered approach to networking and communications protocols is the greater compatibility between devices, systems, and networks that this delivers.

Better Flexibility - Layering and the greater compatibility that it delivers goes a long way to improving the flexibility; particularly in terms of options and choices, that network engineers and administrators alike crave so much.

Flexibility and Peace of Mind - Peace of mind in knowing that if worst comes to worst and a key core network device; suddenly and without warning decides to give up the ghost, you can rest assured that a replacement or temporary stand-by can be readily put to work with the highest degree of confidence that it will do the job.

Increased Life Expectancy - Increased product working life expectancies as backward compatibility is made considerably easier. Devices from different technology generations can co-exist thus the older units do not get discarded immediately newer technologies are adopted.

Scalability- Experience has shown that a layered or hierarchal approach to networking protocol design and implementation scales better than the horizontal approach. Mobility - Greater mobility is more readily delivered whenever we adopt the layered and segmented strategies into our architectural design Value **Cost Effective Quality** - The layered approach has proven time and time again to be the most economical way of developing and implementing any system(s) be they small, simple, large or complex makes no difference.

Modularity - I am sure that you have come across plug-ins and add-ons. These are common and classical examples of the benefits to be derived from the use of a hierarchal (layered) approach to design.

Standardization and Certification - The layered approach to networking protocol Specifications facilitates a more streamlined and simplified standardization and certification process; particularly from an "industry" point of view.

Compartmentalization of Functionality - The compartmentalization or layering of processes, procedures and communications functions gives developers the freedom to concentrate on a specific layer or specific functions within that layer's realm of responsibility without the need for great concern or modification of any other layer.

Side-Kicks - The development of "Helper" protocols or side- kicks is much easier when a layered approach to networking protocols is embraced. This is especially so when it comes to the development of "helper"

protocols that are developed as after-thoughts because the need arose.

Time - The time spent debugging can be greatly reduced as a direct result of taking the layered approach to developing network protocols because debugging is made easier and faster when using the layered approach as opposed to not using it.

Promotion of Multi-Vendor Development - Layering allows for a more precise identification and delineation of task, process, and methodology. This permits a clearer definition of what needs to be done, where it needs to be done, when it needs to be done, how it needs to be done and what or who will do it.

Easier Binding Implementation – The principle of binding is far easier to implement in layered, tiered, and hierarchal systems. Humans also tend to understand this form easier than the flat model.

Enhanced Troubleshooting and Fault Identification - Troubleshooting and fault identification are made considerably easier thus resolution times are greatly reduced. Layering allows for examination in isolation of subcomponents as well as the whole.

Enhanced Communications Flow and Support - Adopting the layered approach allows for improved flow and support for communication between diverse systems, networks, hardware, software, and protocols.

Support for Disparate Hosts - Communications between disparate hosts is supported seamlessly thus Unix, PC, MAC & Linux to name but a few can freely interchange data. Reduction of the Domino Effect - Another very important advantage of a layered protocol system is that it helps to prevent changes in one layer from affecting other layers. This helps to expedite technology development. Rapid Application Development (RAD) - Workloads can be evenly distributed which means that multiple activities can be conducted in parallel thereby reducing the time taken to develop, debug, optimize and package new technologies ready for production implementation.

ISO-OSI Reference Model: Principle, Model, Descriptions of various layers

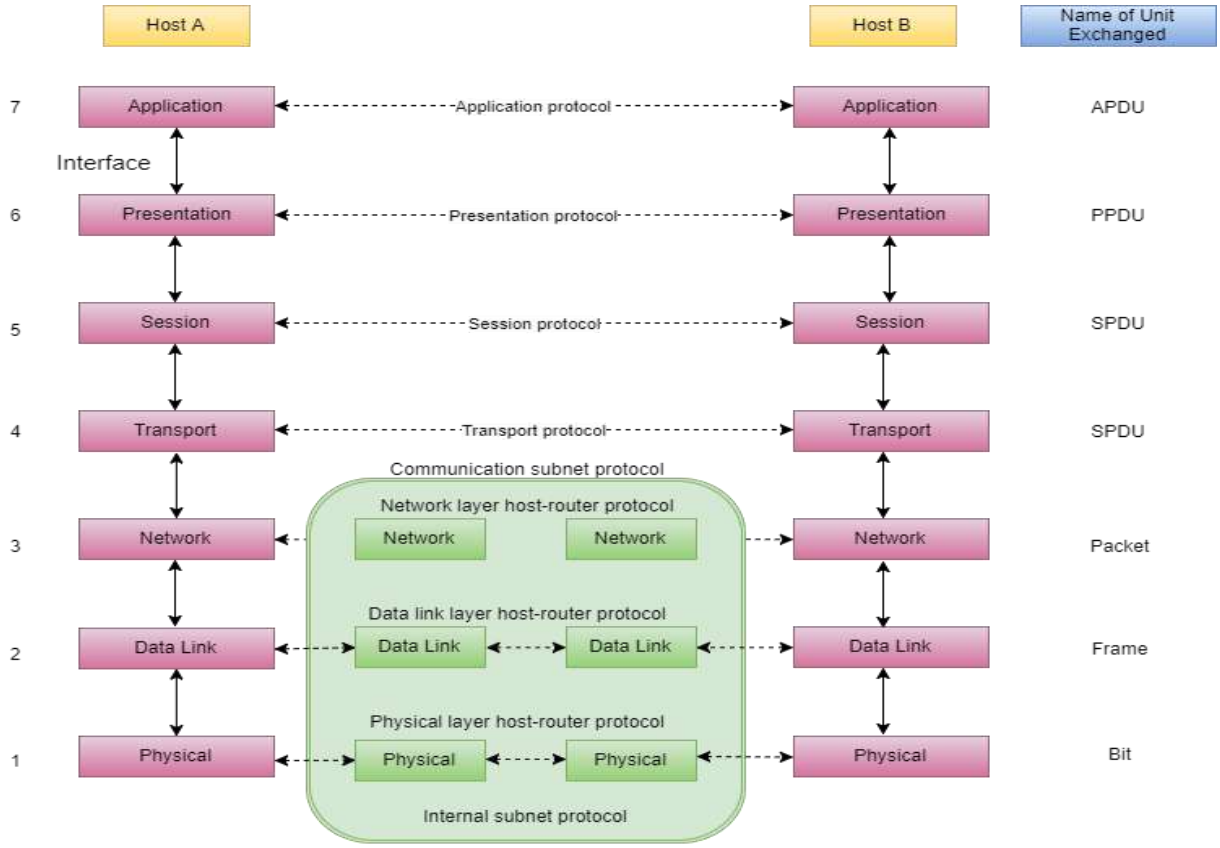

Fig. 1.4 OSI Reference Model

• Helps users understand the big picture of networking
• Helps users understand how hardware and software elements function together
• Makes troubleshooting easier by separating networks into manageable pieces
• Defines terms that networking professionals can use to compare basic functional relationships on different networks
• Helps users understand new technologies as they are developed
• Aids in interpreting vendor explanations of product functionality

The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1. The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal connection on that layer. The recommendation X.200 describes seven layers, labeled 1 to 7. Layer 1 is the lowest layer in this model.

Layer 1: Physical layer

The physical layer has the following major functions:

- It defines the electrical and physical specifications of the data connection. It defines the relationship between a device and a physical transmission medium (e.g., a copper or fiber optical cable). This includes the layout of pins, voltages, line impedance, cable specifications, signal timing, hubs, repeaters, network adapters, host bus adapters (HBA used in storage area networks) and more.
- It defines the protocol to establish and terminate a connection between two directly connected nodes over a communications medium.
- It may define the protocol for flow control.
- It defines transmission mode i.e. simplex, half duplex, full duplex.
- It defines the topology.
- It defines a protocol for the provision of a (not necessarily reliable) connection between two directly connected nodes, and the modulation or conversion between the representation of digital data in user Equipment and the corresponding signals transmitted over the physical communications channel.

• Cabling system components
• Adapters that connect media to physical interfaces
• Connector design and pin assignments
• Hub, repeater, and patch panel specifications
• Wireless system components
• Parallel SCSI (Small Computer System Interface)
• Network Interface Card (NIC)

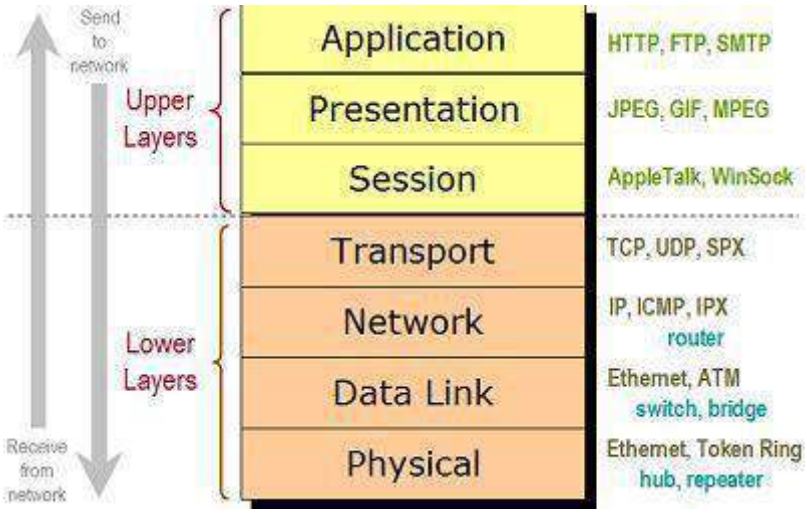

Fig.1.5 Protocols

Layer 2: Data link layer

The data link layer provides node-to-node data transfer - A reliable link between two directly connected nodes, by detecting and possibly correcting errors that may occur in the physical layer. The data link layer is divided into two sublayers:

- Media Access Control (MAC) layer - Responsible for controlling how devices in a network gain access to data and permission to transmit it.
- Logical Link Control (LLC) layer - Controls error checking and packet synchronization.

The Point-to-Point Protocol (PPP) is an example of a data link layer in the TCP/IP protocol stack.

The ITU-T standard, which provides high-speed local area networking over existing wires (power lines, phone lines and coaxial cables), includes a complete data link layer that provides both error correction and flows control by means of a selective-repeat sliding- window protocol.

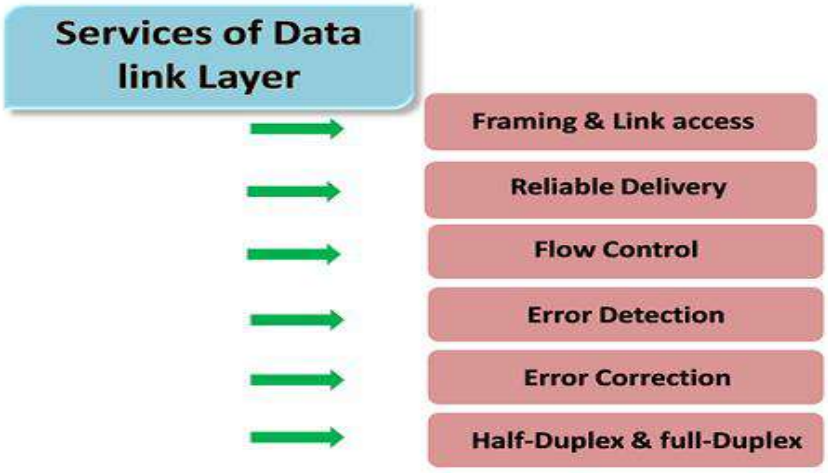

Fig . 1.6 Services are provided by the Data Link Layer

- **Framing & Link access:** Data Link Layer protocols encapsulate each network frame within a Link layer frame before the transmission across the link. A frame consists of a data field in which network layer datagram is inserted and a number of data fields. It specifies the structure of the frame as well as a channel access protocol by which frame is to be transmitted over the link.

- **Reliable delivery:** Data Link Layer provides a reliable delivery service, i.e., transmits the network layer datagram without any error. A reliable delivery service is accomplished with transmissions and acknowledgements. A data link layer mainly provides the reliable delivery service over the links as they have higher error rates and they can be corrected locally, link at which an error occurs rather than forcing to retransmit the data.
- **Flow control:** A receiving node can receive the frames at a faster rate than it can process the frame. Without flow control, the receiver's buffer can overflow, and frames can get lost. To overcome this problem, the data link layer uses the flow control to prevent the sending node on one side of the link from overwhelming the receiving node on another side of the link.
- **Error detection:** Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a mechanism to detect one or more errors. This is achieved by adding error detection bits in the frame and then receiving node can perform an error check.
- **Error correction:** Error correction is similar to the Error detection, except that receiving node not only detect the errors but also determine where the errors have occurred in the frame.
- **Half-Duplex & Full-Duplex:** In a Full-Duplex mode, both the nodes can transmit the data at the same time. In a Half-Duplex mode, only one node can transmit the data at the same time.

Basic Functions

• Allows a device to access the network to send and receive messages
• Offers a physical address so a device's data can be sent on the network
• Works with a device's networking software when sending and receiving messages
• Provides error-detection capability

Common networking components that function at layer 2 include:

• Network interface cards
• Ethernet and Token Ring switches
• Bridges

Layer 3: Network layer

- The network layer provides the functional and procedural means of transferring variable length data sequences (called datagrams) from one node to another connected to the same network.
- It translates logical network address into physical machine address.
- Routing is also one of the main functions of the Network Layer, routing is the process of selecting paths in a network over which to send packets.
- Internet Control Message Protocol (ICMP) is network layer protocol and one of the main protocols of the Internet Protocol suite and is used for error handling and diagnostic purposes.

  The main functions performed by the network layer are:

  - **Routing:** When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.
  - **Logical Addressing:** The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.

- **Internetworking:** This is the main role of the network layer that it provides the logical connection between different types of networks.
- **Fragmentation:** The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.

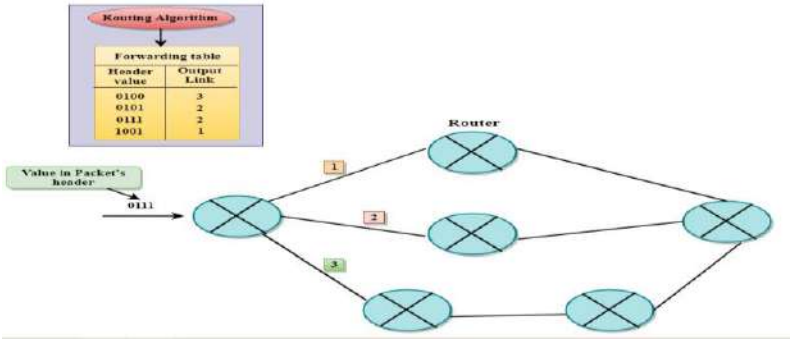

Fig1.7 Routing forwarding table

Services Provided by the Network Layer

- **Guaranteed delivery:** This layer provides the service which guarantees that the packet will arrive at its destination.
- **Guaranteed delivery with bounded delay:** This service guarantees that the packet will be delivered within a specified host-to-host delay bound.
- **In-Order packets:** This service ensures that the packet arrives at the destination in the order in which they are sent.
- **Guaranteed max jitter:** This service ensures that the amount of time taken between two successive transmissions at the sender is equal to the time between their receipt at the destination.
- **Security services:** The network layer provides security by using a session key between the source and destination host. The network layer in the source host encrypts the payloads of datagrams being sent to the destination host. The network layer in the destination host would then decrypt the payload. In such a way, the network layer maintains the data integrity and source authentication services.

Layer 4: Transport layer

The transport layer provides the functional and procedural means of transferring variable- length data sequences from a source to a destination host via one or more networks while maintaining the quality of service functions.

An example of a transport-layer protocol in the standard Internet stack is Transmission Control Protocol (TCP), usually built on top of the Internet Protocol (IP).

Some of the functions offered by the transport layer include:

• Application identification
• Client-side entity identification
• Confirmation that the entire message arrived intact
• Segmentation of data for network transport
• Control of data flow to prevent memory overruns
• Establishment and maintenance of both ends of virtual circuits

• Transmission-error detection
• Realignment of segmented data in the correct order on the receiving side
• Multiplexing or sharing of multiple sessions over a single physical link
The most common transport layer protocols are the connection-oriented TCP Transmission Control Protocol (TCP) and the connectionless UDP User Datagram Protocol (UDP).

Services provided by the Transport Layer

The services provided by the transport layer are similar to those of the data link layer. The data link layer provides the services within a single network while the transport layer provides the services across an internetwork made up of many networks. The data link layer controls the physical layer while the transport layer controls all the lower layers.

The services provided by the transport layer protocols can be divided into five categories:

- End-to-end delivery
- Flow control
- Multiplexing
- Addressing
- Reliable delivery

Layer 5: Session layer
The session layer controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application.
It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures. This session layer allows applications functioning on devices to establish, manage, and terminate a dialog through a network. Session layer functionality includes:
• Virtual connection between application entities
• Synchronization of data flow
• Creation of dialog units
• Connection parameter negotiations
• Partitioning of services into functional groups
• Acknowledgements of data received during a session
• Retransmission of data if it is not received by a device
Layer 6: Presentation layer
The presentation layer, is responsible for how an application formats the data to be sent out onto the network. The presentation layer basically allows an application to read (or understand) the message.
Examples of presentation layer functionality include:
• Encryption and decryption of a message for security
• Compression and expansion of a message so that it travels efficiently
• Graphics formatting
• Content translation
• System-specific translation
Layer 7: Application layer

The application layer, provides an interface for the end user operating a device connected to a network. This layer is what the user sees, in terms of loading an application (such as Web browser or e-mail. Examples of application layer functionality include:

• Support for file transfers
• Ability to print on a network
• Electronic mail
• Electronic messaging
• Browsing the World Wide Web

Some examples of application layer implementations include:

- On OSI stack:
- FTAM File Transfer and Access Management Protocol
- X.400 Mail
- Common Management Information Protocol (CMIP)
- On TCP/IP stack:
- Hypertext Transfer Protocol (HTTP),
- File Transfer Protocol (FTP),
- Simple Mail Transfer Protocol (SMTP),
- Simple Network Management Protocol (SNMP), etc.

TCP/IP reference model

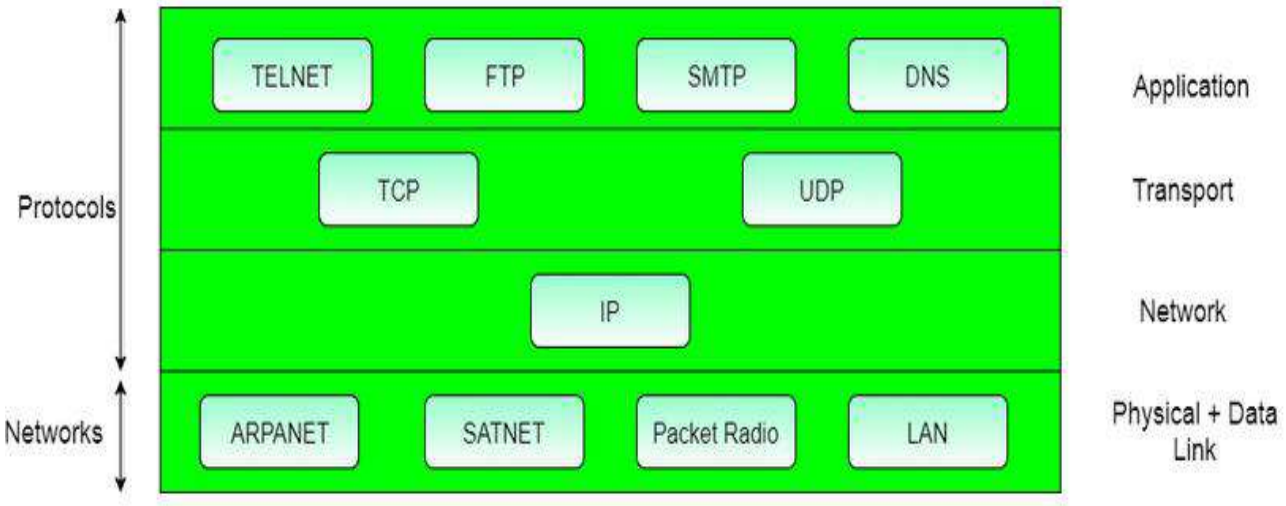

Fig .1.8 TCP/IP reference model

The TCP/IP reference model is the network model used in the current Internet architecture. It is considered as the grandfather of the Internet the ARPANET. The reference model was named after two of its main protocols, TCP (Transmission control Protocol) and IP (Internet Protocol).

There are versions of this model with four layers and with five layers. The original four-layer version of the model is shown below.

Layer 4: Process Layer or Application Layer: This is where the "higher level" protocols such as FTP, HTTP, etc. Operate. The original TCP/IP specification described many different applications that fit into the top

layer of the protocol stack. These applications include Telnet, FTP, SMTP, and DNS.

Layer 3: Host-To-Host (Transport) Layer: This is where flow-control and connection protocols exist, such as TCP. This layer deals with opening and maintaining a connection, ensuring that packet is in fact received the transport layer is the interface between the application layer and the complex hardware of the.

Two modes are an available, full-duplex and half-duplex. In full-duplex operation, both sides can transmit and receive data simultaneously, whereas, in half duplex, a side can only send or receive at one time.

Layer 2: Internet or Internetworking Layer: This layer defines IP addresses, with many routing schemes for navigating packets from one IP address to another. The job of the network layer is to inject packets into any network and have them travel independently to the destination. Packet routing is a major job of this protocol.

Layer 1: Networking Access Layer: This layer describes the physical equipment necessary for communications, such as twisted pair cables, the signaling used on that equipment, and the low-level protocols using that signaling. That Host-to-Network layer interfaces the TCP/IP protocol stack to the physical network.

TCP/IP Protocol Suite:

The TCP/IP protocol suite has two sets of protocols at the Internet layer:

- IPv4, also known as IP, is the Internet layer in common use today on private intranets and the Internet.
- IPv6 is the new Internet layer that will eventually replace the existing IPv4 Internet layer.

X.25 is a standard used by many older public networks specially outside the U.S.

• This was developed in 1970s by CCITT for providing an interface between public packet-switched network and their customers.

• The packet switching networks use X.25 protocol. The X.25 recommendations were first prepared in 1976 and then revised in 1978, 1980 and 1984.

• X.25 was developed for computer connections, used for terminal/timesharing connection.

• This protocol is based on the protocols used in early packet switching networks such as ARPANET, DATAPAC, and TRANSPAC etc.

• X.25 Packet Switched networks allows remote devices to communicate with each other across high speed digital links without the expense of individual leased lines.

• A protocol X.21 which is a physical layer protocol is used to specify the physical electrical and procedural interface between the host and network.

• The problem with this standard is that it needs digital signal rather than analog signals on telephone lines.

• So not many networks support this standard. Instead RS 232 standard is defined.

• The data link layer standard has a number of variations. It is designed for error detection and corrections.

• The network layer protocol performs the addressing, flow control, delivery confirmation etc.

• It allows the user to establish virtual circuits and send packets on them. These packets are delivered to the destination reliably and in order.

• X.25 is a connection oriented service. It supports switched virtual circuits as well as the permanent circuits.

• Packet Switching is a technique whereby the network routes individual packets of HDLC data between different destinations based on addressing within each packet.

• A switched virtual circuit is established between a computer and network when the computer sends a

packet to the network requesting to make a call to another computer.
• Packets can then be sent over this connection from sender to receiver.
• X.25 provides the flow control, to avoid a fast sender overriding a slow or busy receiver.
• A permanent virtual circuit is analogous to-a leased line. It is set up in advance with a mutual agreement between the users.
• Since it is always present, no call set up is required for its use.
• In order to allow the computers which do not use the X.25 to communicate with the X.25 network a packet assembler disassembler (PAD) is used.
• PAD is required to be installed along with each computer which does not use X.25.
• X.25 defines the interface for exchange of packets between a DTE and switch data subnetwork node.

Three Layers of X.25:

The X.25 interface is defined at three levels:
The three levels are:
(i) Physical layer (level 1)
(ii) Data link layer (level 2)
(iii) Packet layer (level 3).
• These three layers correspond to the three lower most layers of the ISO-OSI reference model. The physical layer takes care of the interface between a computer terminal and the link which attaches it to the packet switching node.
• The X.25 defines the interface for exchange of packets between the user's machine (DTE) and the packet switching node to which this DTE is attached which is called as DCE.
• The three layers of X.25 interface are as shown in below figure.
• At the physical level X.21 physical interface is being used which is defined for circuit switched data network. At the data link level, X.25 specifies the link access procedure-B (LAP-B) protocol which is a subset of HDLC protocol.

Protocol data unit (PDU)

In telecommunications, a protocol data unit (PDU) is a single unit of information transmitted among peer entities of a computer network. A PDU is composed of protocol specific control information and user data. In the layered architectures of communication protocol stacks, each layer implements protocols tailored to the specific type or mode of data exchange. For example, the Transmission Control Protocol (TCP) implements a connection-oriented transfer mode, and the PDU of this protocol is called a segment, while the User Datagram Protocol (UDP) uses datagram's as protocol data unit for connection-less transfer. A layer lower in the Internet protocol suite, at the Internet layer, the PDU is called a packet, irrespective of its payload type.

For application data to travel uncorrupted from one host to another, header (or control data),which contains control and addressing information, is added to the data as it moves down the layers. The process of adding control information as it passes through the layered model is called encapsulation. De capsulation is the process of removing the extra information and sending only the original application data up to the destination application layer.

Each layer adds control information at each step. The generic term for data at each level is protocol data unit (PDU), but a PDU is different at each layer. For example, a PDU at the internetwork layer is different from the PDU at the transport layer, because in network layer data has been added to the transport layer data. The different names for PDUs at each layer are listed below.

Data---------→Application layer PDU

Segment----→Transport layer PDU

Packet------→Internetwork Layer PDU

Frame ------→Network Access Layer PDU

Bits---------→PDU used for the physical transmission of binary data over media

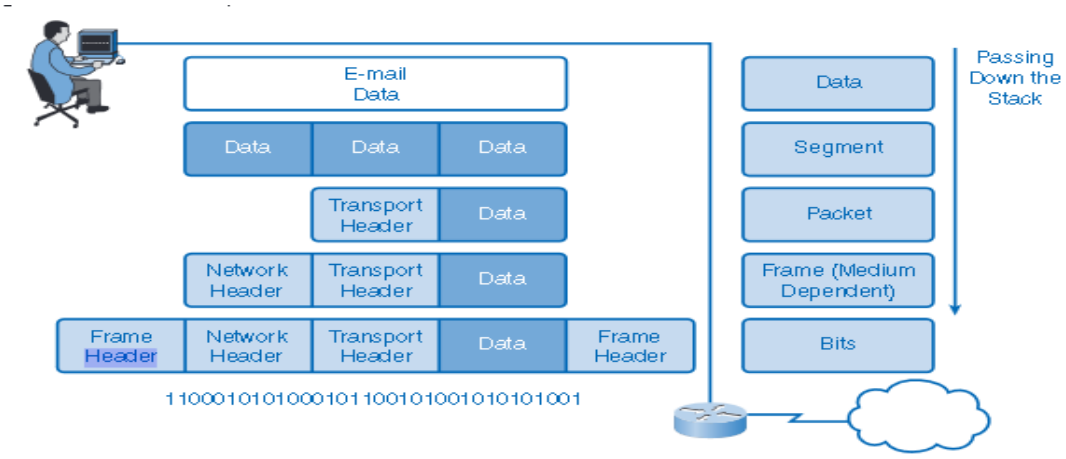

Fig 1.9 PDU Encapsulation

Connection Oriented & Connectionless Services, Service primitives, Design issues & its functionality

Connection-oriented communication is a network communication mode in telecommunications and computer networking, where a communication session or a semi- permanent connection is established before any useful data can be transferred, and where a stream of data is delivered in the same order as it was sent.

- **Connection-oriented**

There is a sequence of operation to be followed by the users of connection-oriented service. They are:

1. Connection is established
2. Information is sent
3. Connection is released

In connection-oriented service we must establish a connection before starting the communication. When connection is established we send the message or the information. Then we release the connection.

Connection oriented service is more reliable than connectionless service. Example of connection oriented is TCP (Transmission Control Protocol) protocol.

- **Connectionless**

It is similar to postal services, as it carries the full address where the message (letter) is to be carried. Each message is routed independently from source to destination. The order of message sent can be different from the order received.

In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message. Authentication is not needed in this. Example of Connectionless service is UDP (User Datagram Protocol) protocol.

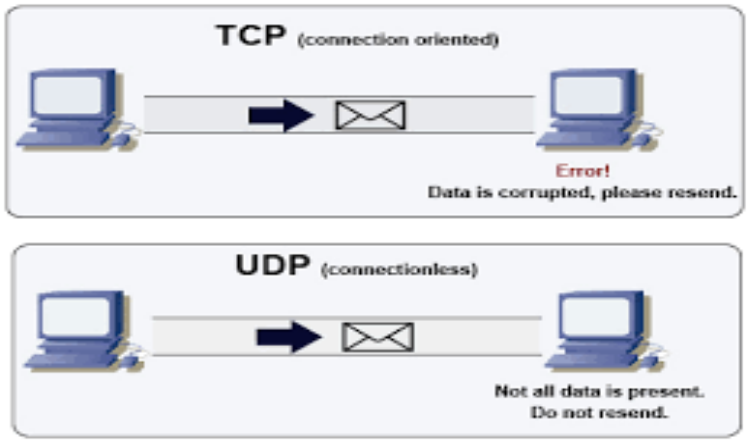

Fig. 1.10 Connection Oriented & Connectionless Services

#Service Primitives

Connection Oriented Service Primitives

LISTEN	Block waiting for an incoming connection
CONNECTION	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Sending a message to the peer
DISCONNECT	Terminate a connection

Connectionless Service Primitives

UNIDATA	This primitive sends a packet of data
FACILITY, REPORT	Primitive for enquiring about the performance of the network, like delivery statistics.

Design issues & its functionality

- **Justifying a Network**: - Some applications may be best satisfied by individual point to point connections to handle very specific communication requirements.
- **Scope**: - The scope of the network is viewed as bounded on one side by the offerings of the common carriers who provide communication facilities from which the network is built and on the other side by the application on which it is interconnected.

- **Network Architecture**: - While designing the network architecture, network may be a single homogeneous mesh comprised of a single type of node and a single type of link. Network architecture might be hierarchical network with one type link riding on another.
- **Switch Mode**: - For data transmission, different types of switching methods are possible. These are packet switching, circuit switching and hybrid switching.
- **Node Placement and sizing**: - A fundamental problem in the topological optimization of a network is the selection of the network node sites and where to place multiplexers, hubs and switch.
- **Link Topology and sizing**: - It involves selecting the specific links interconnecting nodes. At the highest level, that is where the architecture of the network is derived. Thus a hierarchy that include a backbone as well as LAN'S may be defined. It is possible to permit the backbone to be a mesh while LAN is constrained to be trees.
- **Routing**: - It involves selecting paths for each requirements. At higher level, this involves selecting the routing procedure itself.

Criteria	Connection-Oriented	Connection-Less
Connection	Prior connection needs to be established.	No prior connection is established.
Resource Allocation	Resources need to be allocated.	No prior allocation of resource is required.
Reliability	It ensures reliable transfer of data.	Reliability is not guaranteed as it is a best effort service.
Congestion	Congestion is not at all possible.	Congestion can occur likely.
Transfer mode	It can be implemented either using Circuit Switching or VCs.	It is implemented using Packet Switching.
Retransmission	It is possible to retransmit the lost data bits.	It is not possible.
Suitability	It is suitable for long and steady communication.	It is suitable for bursty transmissions.
Signaling	Connection is established through process of signaling.	There is no concept of signaling.
Packet travel	In this packets travel to their destination node in a sequential manner.	In this packets reach the destination in a random manner.
Delay	There is more delay in transfer of information, but once connection established faster delivery.	There is no delay due absence of connection establishment phase.

Address Resolution Protocol (ARP)

Address Resolution Protocol is a communication protocol used for discovering physical address associated with given network address. Typically, ARP is a network layer to data link layer mapping process, which is used to discover MAC address for given Internet Protocol Address.

In order to send the data to destination, having IP address is necessary but not sufficient; we also need the

physical address of the destination machine. ARP is used to get the physical address (MAC address) of destination machine.

Before sending the IP packet, the MAC address of destination must be known. If not so, then sender broadcasts the ARP-discovery packet requesting the MAC address of intended destination. Since ARP-discovery is broadcast, every host inside that network will get this message but the packet will be discarded by everyone except that intended receiver host whose IP is associated. Now, this receiver will send a unicast packet with its MAC address (ARP-reply) to the sender of ARP-discovery packet. After the original sender receives the ARP-reply, it updates ARP-cache and start sending unicast message to the destination.

If a machine talks to another machine in the same network, it requires its physical or MAC address. But ,since the application has given the destination's IP address it requires some mechanism to bind the IP address with its MAC address.This is done through Address Resolution protocol (ARP).IP address of the destination node is broadcast and the destination node informs the source of its MAC address.

1. Assume broadcast nature of LAN
2. Broadcast IP address of the destination
3. Destination replies it with its MAC address.
4. Source maintains a cache of IP and MAC address bindings

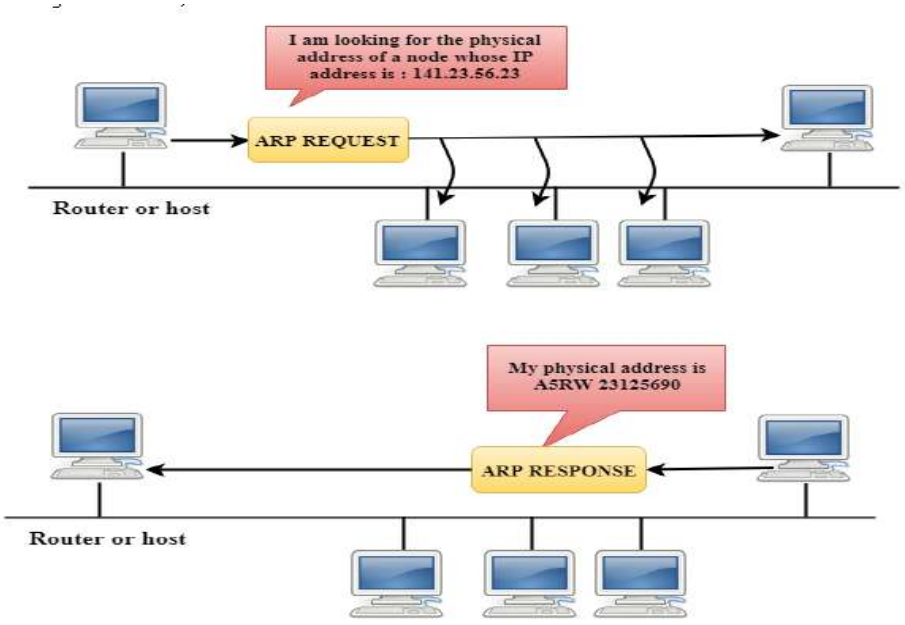

Fig.11 ARP Request and Response

But this means that every time machine A wants to send packets to machine B, A has to send an ARP packet to resolve the MAC address of B and hence this will increase the traffic load too much, so to reduce the communication cost computers that use ARP maintains a cache of recently acquired IP_ to_ MAC address bindings, i.e. they don't have to use ARP repeatedly. ARP Refinements Several refinements of ARP are possible: When machine A wants to send packets to machine B, it is possible that machine B is going to send packets to machine A in the near future .So to avoid ARP for machine B, A should put its IP_ to _MAC address binding in the special packet while requesting for the MAC address of B. Since A broadcasts its initial

request for the MAC address of B, every machine on the network should extract and store in its cache the IP_ to _MAC address binding of A When a new machine appears on the network (e.g. when an operating system reboots) it can broadcast its IP _to_ MAC address binding so that all other machines can store it in their caches. This will eliminate a lot of ARP packets by all other machines, when they want to communicate with this new machine.

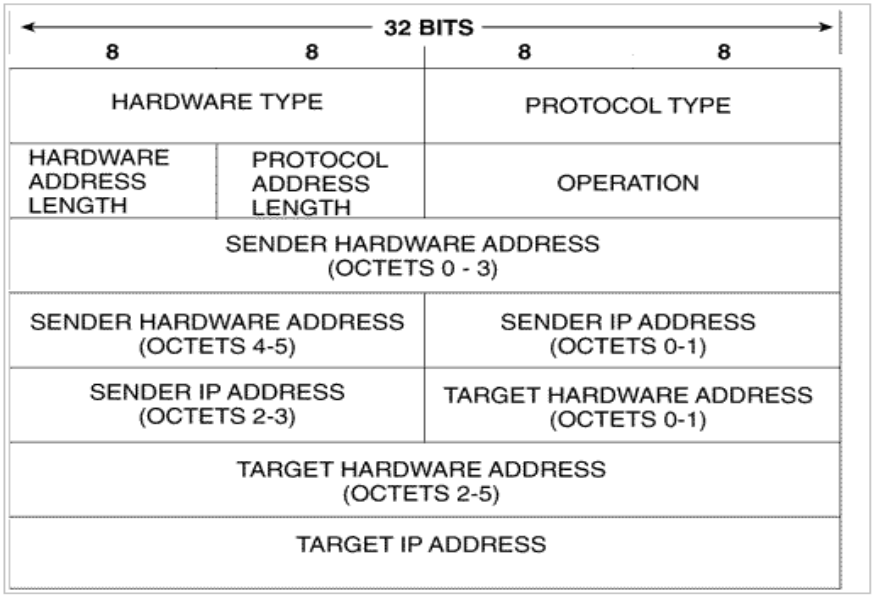

Fig 1.12 ARP Packet Format

Packet Format Description

Hardware type 16 bits.

Hardware Type: Hardware Type field in the Address Resolution Protocol (ARP) Message specifies the type of hardware used for the local network transmitting the Address Resolution Protocol (ARP) message. Ethernet is the common Hardware Type and he value for Ethernet is 1. The size of this field is 2 bytes.

Protocol type 16 bits.

Value	Description
0x800	IP.

Hardware addresses length 8 bits.
Length of the hardware address in bytes.

Protocol addresses length 8 bits.
Length of the protocol address in bytes.

Opcode 16 bits.

Value	Description	References
0	Reserved	RFC 5494
1	Request.	RFC 826
2	Reply.	RFC 826, 1868 5227
3	Request Reverse.	RFC 903
4	Reply Reverse.	

Table No. 01 Packet Format Description

Source hardware address Variable length.

Source protocol address Variable length.

Destination hardware address Variable length.

Destination protocol address Variable length.

Reverse Address Resolution Protocol (RARP)

Reverse ARP is a networking protocol used by a client machine in a local area network to request its Internet Protocol address (IPv4) from the gateway-router's ARP table. The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address.
When a new machine is setup or any machine which don't have memory to store IP address, needs an IP address for its own use. So the machine sends a RARP broadcast packet which contains its own MAC address in both sender and receiver hardware address field.

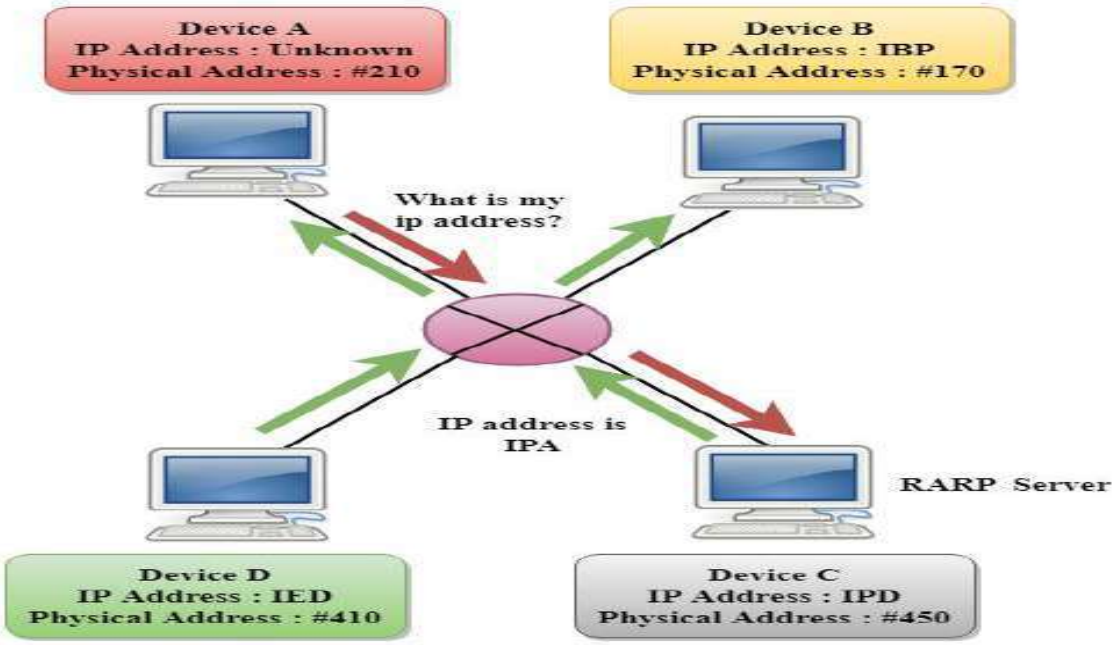

Fig. 13 Reverse Address Resolution Protocol

A special host configured inside the local area network, called as RARP-server is responsible to reply for these kind of broadcast packets. Now the RARP server attempt to find out the entry in IP to MAC address mapping table. If any entry matches in table, RARP server send the response packet to the requesting device along with IP address.

- LAN technologies like Ethernet, Ethernet II, Token Ring and Fiber Distributed Data Interface (FDDI) support the Address Resolution Protocol.
- RARP is not being used in today's networks. Because we have much great featured protocols like BOOTP (Bootstrap Protocol) and DHCP(Dynamic Host Configuration Protocol).

RARP is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution Protocol table or cache. This is needed since the machine may not have permanently attacded disk where it can store its IP address permanently. A network administrator creates a table in a local area network's gateway router that maps the physical machine (or Medium Access Control - MAC) addresses to corresponding Internet Protocol addresses. When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.

Detailed Mechanism

Both the machine that issues the request and the server that responds use physical network addresses during their brief communication. Usually, the requester does not know the physical address. So, the request is broadcasted to all the machines on the network. Now, the requester must identify is self uniquely to the server. For this either CPU serial number or the machine's physical network address can be used. But using the physical address as a unique id has two advantages.

- These addresses are always available and do not have to be bound into bootstrap code.
- Because the identifying information depends on the network and not on the CPU vendor, all machines on a given network will supply unique identifiers.

Request:

Like an ARP message, a RARP message is sent from one machine to the another encapsulated in the data portion of a network frame. An Ethernet frame carrying a RARP request has the usual preamble, Ethernet source and destination addresses, and packet type fields in front of the frame. The frame contains the value 8035 (base 16) to identify the contents of the frame as a RARP message. The data portion of the frame contains the 28-octet RARP message. The sender broadcasts a RARP request that specifies itself as both the sender and target machine, and supplies its physical network address in the target hardware address field. All machines on the network receive the request, but only those authorized to supply the RARP services process the request and send a reply, such machines are known informally as RARP servers. For RARP to succeed, the network must contain at least one RARP server.

Reply:

Servers answers request by filling in the target protocol address field, changing the message type from request to reply, and sending the reply back directly to the machine making the request.

Timing RARP Transactions

Since RARP uses the physical network directly, no other protocol software will time the response or retransmit the request. RARP software must handle these tasks. Some workstations that rely on RARP to boot, choose to retry indefinitely until the receive a response. Other implementations announce failure after only a few tries to avoid flooding the network with unnecessary broadcast.

Multiple RARP Servers

Advantage: More reliability. Disadvantage: Overloading may result when all servers respond. So, to get away with disadvantage we have primary and secondary servers. Each machine that makes RARP request is assigned a primary server. Normally, the primary server responds but if it fails, then requester may time out and rebroadcast the request. Whenever a secondary server receives a second copy of the request within a short time of the first, it responds. But, still there might be a problem that all secondary servers respond, thus overloading the network. So, the solution adopted is to avoid having all secondary servers transmit responses simultaneously. Each secondary server that receives the request computes a random delay and then sends a response.

RARP Packet Format :

00	**01**	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
Hardware type																Protocol type															
Hardware address length								Protocol address length								Opcode															
Source hardware address																															
Source protocol address																															
Destination hardware address																															
Destination protocol address																															

Fig 1.14 RARP Packet Format

Hardware type 16 bits.

Protocol type 16 bits.

Protocol	**Description**
0x800	IP.

Hardware addresses length 8 bits.
Length of the hardware address in bytes.

Protocol addresses length 8 bits.
Length of the protocol address in bytes.

Opcode 8 bits.

Opcode	Description	References
3	Request Reverse.	RFC 903
4	Reply Reverse.	RFC 903

Source hardware addresses Variable length.

Source protocol addresses Variable length.

Destination hardware addresses Variable length.

Destination protocol addresses Variable length.

ARP Encapsulation :

An ARP is directly encapsulate in data link frame Type field indicates that data carried by the frame is ARP packet

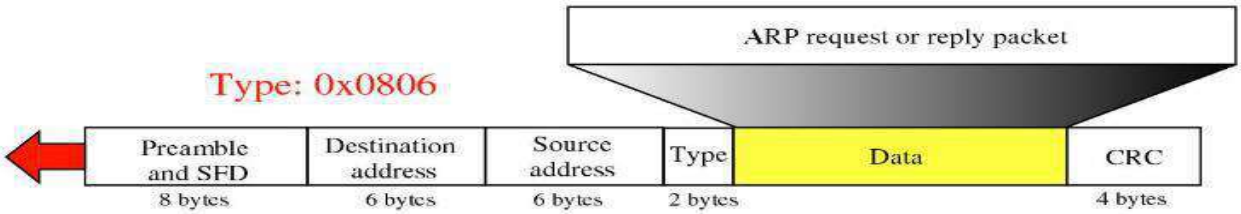

Fig 1.15 Encapsulation of ARP

Drawbacks of RARP

- Since it operates at low level, it requires direct address to the network which makes it difficult for an application programmer to build a server.
- It doesn't fully utilizes the capability of a network like Ethernet which is enforced to send a minimum packet size since the reply from the server contains only one small piece of information, the 32-bit internet address.

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in