RGPVNOTES.IN

Subject Name: **Computer Network**

Subject Code: **IT-5003**

Semester: **5th**

UNIT I

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.

Computer Network: goals

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.

Computer Network: Architecture

The network architecture is the design of a communications network. It is a framework for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, as well as data formats used in its operation.

In telecommunication, the specification of a network architecture may also include a detailed description of products and services delivered via a communications network, as well as detailed rate and billing structures under which services are compensated.

The network architecture of the Internet is predominantly expressed by its use of the Internet Protocol Suite, rather than a specific model for interconnecting networks or nodes in the network, or the usage of specific types of hardware links.

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.

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.

2) Metropolitan Area network (MAN)

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.

3) Wide area Network (WAN)

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.

Layered Architecture: Protocol hierarchy, Design Issues, Interfaces and Services

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.

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.

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.

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

• 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)

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.

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. Quality of Service (QOS) although not the primary function of the network layer is available in network layer protocols such as the Internet Protocol which allows certain traffic to be prioritized over other giving it preferential treatment.

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).

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.

Protocol Data Unit: - A PDU is a specific block of information transferred over a network. It is often used in reference to the OSI model, since it describes the different types of data that are transferred from each layer. The PDU for each layer of the OSI model is listed below.

Physical layer – raw bits (1s or 0s) transmitted physically via the hardware
Data Link layer – a frame (or series of bits)
Network layer – a packet that contains the source and destination address
Transport layer – a segment that includes a TCP header and data
Session layer – the data passed to the network connection

Presentation layer – the data formatted for presentation
Application layer – the data received or transmitted by a software application

TCP/IP

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.

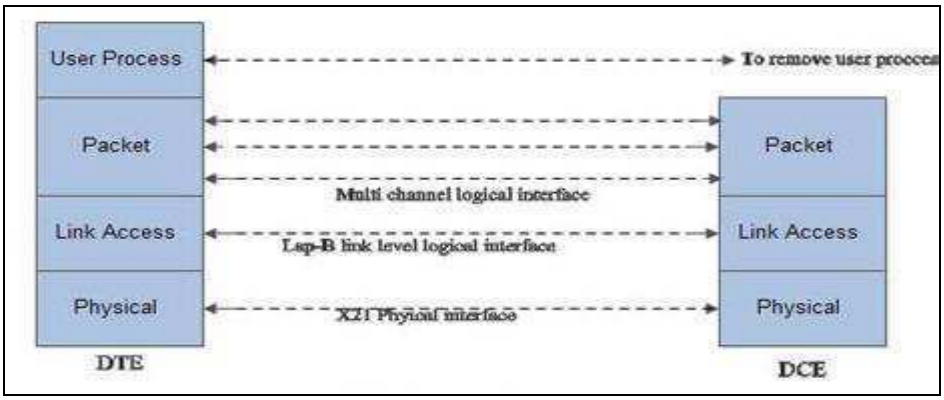
• X.25 Packet Switched networks allows remote devices to communicate with each other across high speed digital links without the expense of individual leased lines.

• 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.



UNIT II

DATA LINK LAYER:

Introduction

Data Link Layer is the second layer of OSI Layered Model. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to the upper layer as the medium to communicate.

Data link layer works between two hosts which are directly connected in some sense. This direct connection could be a point to point or broadcast. Systems on the broadcast network are said to be on the same link. The work of data link layer tends to get more complex when it is dealing with multiple hosts on single collision domain.

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 the upper layer.

Data link layer has two sub-layers:

- Logical Link Control: It deals with protocols, flow control, and error control
- Media Access Control: It deals with actual control of media

DATA LINK LAYER: SERVICES

- Encapsulation of network layer data packets into frames
- Frame synchronization
- Logical link control (LLC) sublayer:
- Error control (automatic repeat request, ARQ), in addition to ARQ
- Some transport-layer protocols, to forward error correction (FEC) techniques provided on the physical
- layer, and to error-detection and packet canceling provided at all layers, including the network layer.
- Flow control, in addition to the one provided on the transport layer. Data-link-layer error control is not used in LAN protocols such as Ethernet, but in modems and wireless networks.
- Media access control (MAC) sublayer:
- Multiple access protocols for channel access control, for example, CSMA/CD protocols for collision detection and re-transmission in Ethernet bus networks and hub networks, or the CSMA/CA protocol for collision avoidance in wireless networks.
- Physical addressing (MAC addressing)
- LAN switching (packet switching) including MAC filtering and spanning tree protocol
- Data packet queuing or scheduling

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