Department Of Electronics and Communication Engineering

NOTES ON LESSON

CLASS: III YEAR ECE

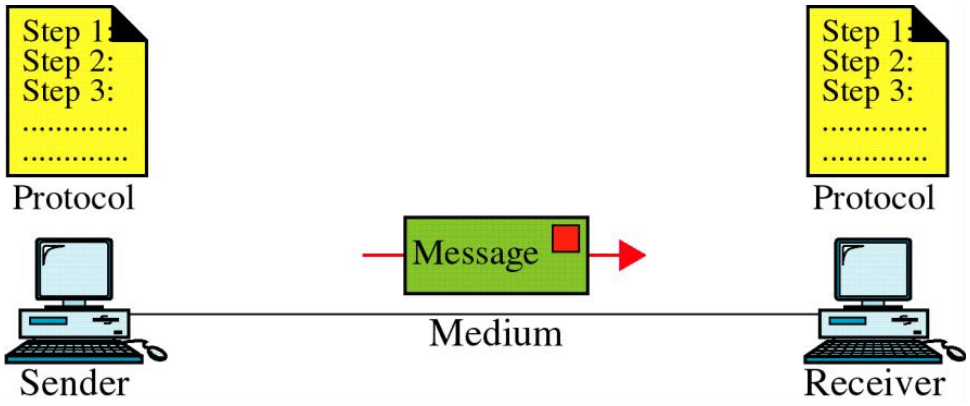
SUBJECT: COMPUTER NETWORKS CODE: EC2352

AIM:

- To introduce the concept ,terminologies and technologies used in modern data communication and computer networking.

- OBJECTIVES:
  - To introduce the students the functions of different layers.
  - To introduce IEEE standard employed in computer networking.
  - To make students to get familiarized with different protocols and network components

Data Communication System Components



Network Technologies

There is no generally accepted taxonomy into which all computer networks fit, but two dimensions stand out as important: **Transmission Technology** and **Scale**. The classifications based on these two basic approaches are considered in this section.

Classification Based on Transmission Technology

Computer networks can be broadly categorized into two types based on transmission technologies:

Broadcast networks
Point-to-point networks

Figure 2-2

Point-to-Point Line Configuration

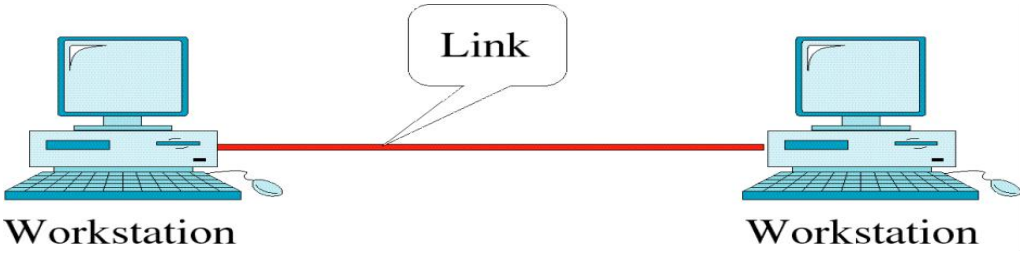
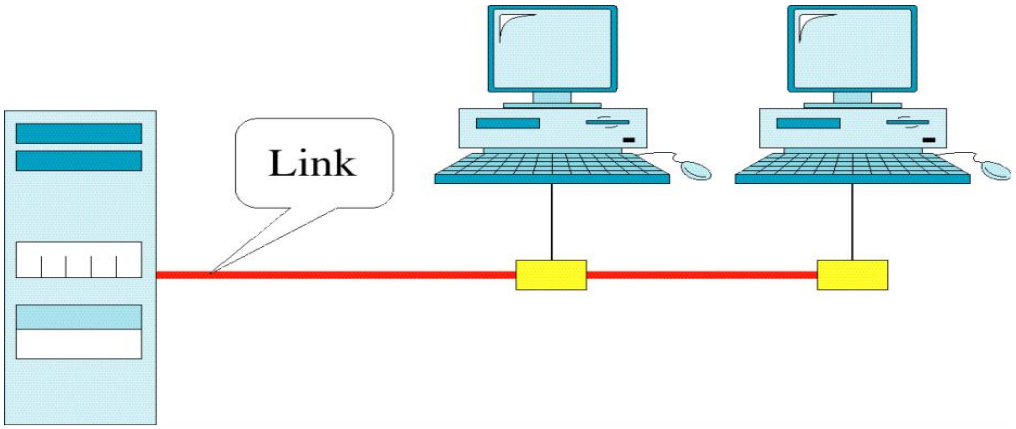


Figure 2-3

Multipoint Line Configuration



Broadcast Networks

Broadcast network have a single communication channel that is shared by all the machines on the network as shown in Figs.1.1.2 and 1.1.3. All the machines on the network receive short messages, called packets in certain contexts, sent by any machine. An address field within the packet specifies the intended recipient. Upon receiving a

packet, machine checks the address field. If packet is intended for itself, it processes the packet; if packet is not intended for itself it is simply ignored. This system generally also allows possibility of addressing the packet to all destinations(all nodes on the network). When such a packet is transmitted and received by all the machines on the network. This mode of operation is known as Broadcast Mode. Some Broadcast systems also supports transmission to a sub-set of machines, something known as Multicasting.

Point-to-Point Networks

A network based on point-to-point communication is shown in Fig. 1.1.4. The end devices that wish to communicate are called stations. The switching devices are called nodes. Some Nodes connect to other nodes and some to attached stations. It uses FDM or TDM for node-to-node communication. There may exist multiple paths between a source-destination pair for better network reliability. The switching nodes are not concerned with the contents of data. Their purpose is to provide a switching facility that will move data from node to node until they reach the destination.

As a general rule (although there are many exceptions), smaller, geographically localized networks tend to use broadcasting, whereas larger networks normally use are point-to-point communication.

Figure 2-5

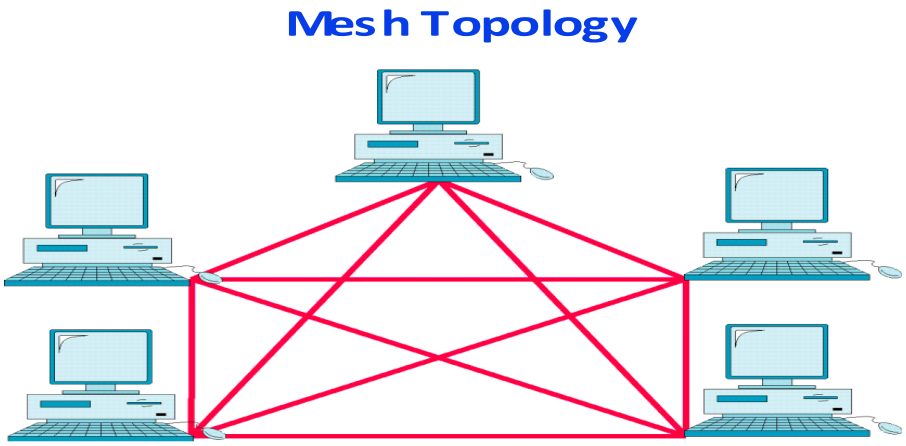


Figure 2-6

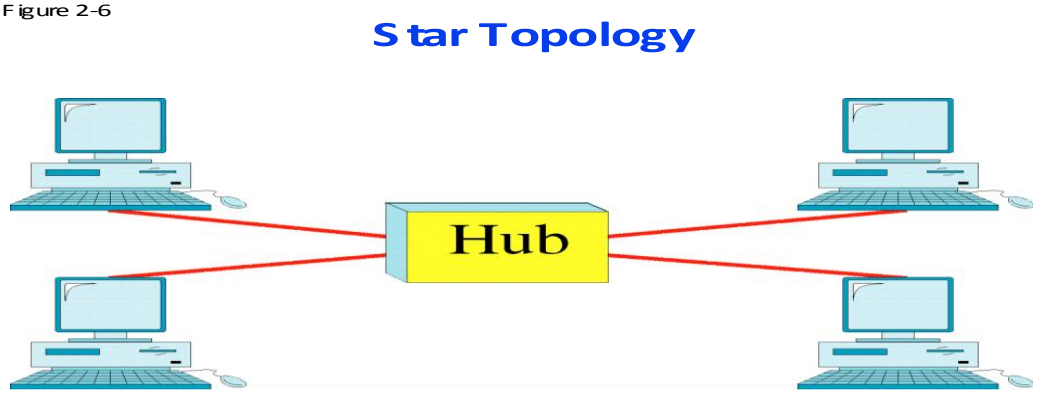
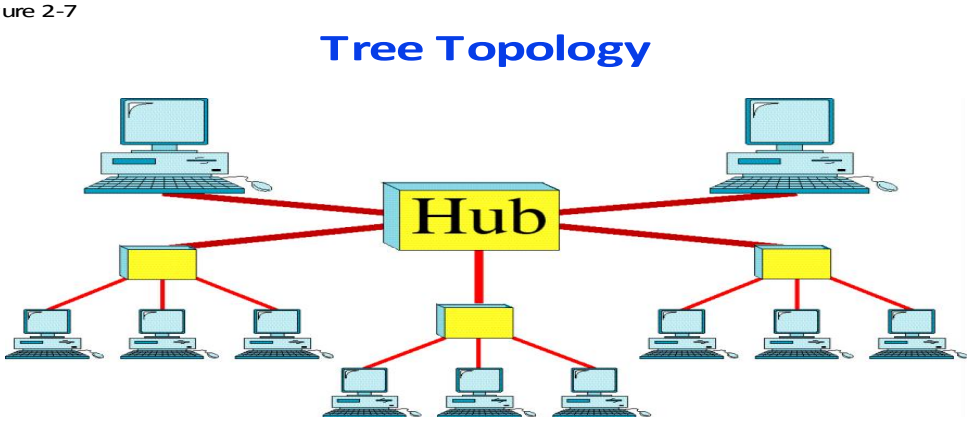


Figure 2-7

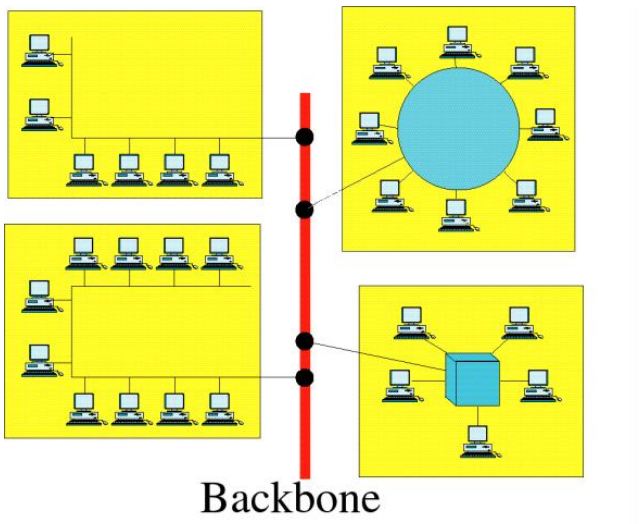


Classification based on Scale

Alternative criteria for classifying networks are their scale. They are divided into Local Area (LAN), Metropolitan Area Network (MAN) and Wide Area Networks (WAN).

Figure 2-16-continued

Local Area Network



Multiple building LAN

Figure 2-17

Metropolitan Area Network

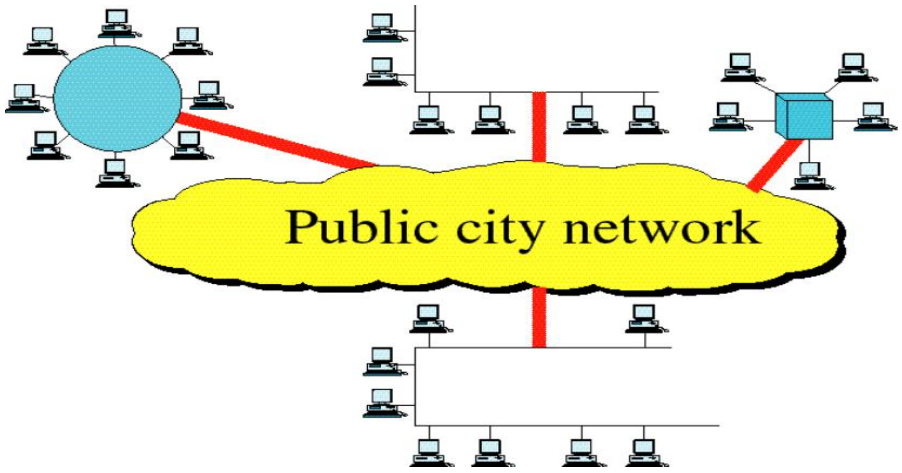
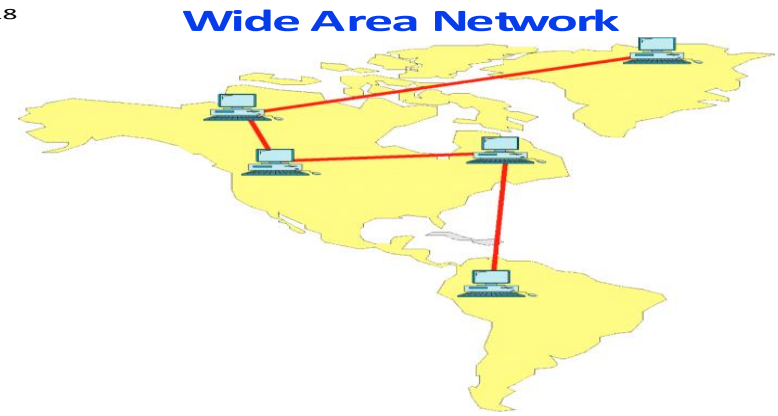


Figure 2-18



Local Area Network (LAN)

LAN is usually privately owned and links the devices in a single office, building or campus of up to few kilometers in size. These are used to share resources (may be hardware or software resources) and to exchange information. LANs are distinguished from other kinds of networks by three categories: their size, transmission technology and topology.

LANs are restricted in size, which means that their worst-case transmission time is bounded and known in advance. Hence this is more reliable as compared to MAN and WAN. Knowing this bound makes it possible to use certain kinds of design that would not otherwise be possible. It also simplifies network management.

LAN typically used transmission technology consisting of single cable to which all machines are connected. Traditional LANs run at speeds of 10 to 100 Mbps (but now much higher speeds can be achieved). The most common LAN topologies are bus, ring and star.

Metropolitan Area Networks (MAN)

MAN is designed to extend over the entire city. It may be a single network as a cable TV network or it may be means of connecting a number of LANs into a larger network so that resources may be shared as shown in Fig. 1.1.6. For example, a company can use a MAN to connect the LANs in all its offices in a city. MAN is wholly owned and operated by a private company or may be a service provided by a public **company.**

Metropolitan Area Networks (MAN)

The main reason for distinguishing MANs as a special category is that a standard has been adopted for them. It is DQDB (Distributed Queue Dual Bus) or IEEE 802.6.

Wide Area Network (WAN)

WAN provides long-distance transmission of data, voice, image and information over large geographical areas that may comprise a country, continent or even the whole world. In contrast to LANs, WANs may utilize public, leased or private communication devices, usually in combinations, and can therefore span an unlimited number of miles as shown

A WAN that is wholly owned and used by a single company is often referred to as enterprise network.

The Internet

Internet is a collection of networks or network of networks. Various networks such as LAN and WAN connected through suitable hardware and software to work in a seamless manner. Schematic diagram of the Internet is shown in Fig. 1.1.8. It allows various applications such as e-mail, file transfer, remote log-in, World Wide Web, Multimedia, etc run across the internet. The basic difference between WAN and Internet is that WAN is owned by a single organization while internet is not so. But with the time the line between WAN and Internet is shrinking, and these terms are sometimes used interchangeably.

Applications

In a short period of time computer networks have become an indispensable part of business, industry, entertainment as well as a common-man's life. These applications have changed tremendously from time and the motivation for building these networks are all essentially economic and technological.

Initially, computer network was developed for defense purpose, to have a secure communication network that can even withstand a nuclear attack. After a decade or so, companies, in various fields, started using computer networks for keeping track of inventories, monitor productivity, communication between their different branch offices located at different locations. For example, Railways started using computer networks by connecting their nationwide reservation counters to provide the facility of reservation and enquiry from any where across the country.

And now after almost two decades, computer networks have entered a new dimension; they are now an integral part of the society and people. In 1990s, computer network started delivering services to private individuals at home. These services and motivation for using them are quite different. Some of the services are access to remote information, person-person communication, and interactive entertainment. So, some of the applications of computer networks that we can see around us today are as follows:

Marketing and sales: Computer networks are used extensively in both marketing and sales organizations. Marketing professionals use them to collect, exchange, and analyze data related to customer needs and product development cycles. Sales application

includes teleshopping, which uses order-entry computers or telephones connected to order processing network, and online-reservation services for hotels, airlines and so on.

Financial services: Today's financial services are totally depended on computer networks. Application includes credit history searches, foreign exchange and investment services, and electronic fund transfer, which allow user to transfer money without going into a bank (an automated teller machine is an example of electronic fund transfer, automatic pay-check is another).

Manufacturing: Computer networks are used in many aspects of manufacturing including manufacturing process itself. Two of them that use network to provide essential services are computer-aided design (CAD) and computer-assisted manufacturing (CAM), both of which allow multiple users to work on a project simultaneously.

Directory services: Directory services allow list of files to be stored in central location to speed worldwide search operations.

Information services: A Network information service includes bulletin boards and data banks. A World Wide Web site offering technical specification for a new product is an information service.

Electronic data interchange (EDI): EDI allows business information, including documents such as purchase orders and invoices, to be transferred without using paper.

Electronic mail: probably it's the most widely used computer network application.

Teleconferencing: Teleconferencing allows conference to occur without the participants being in the same place. Applications include simple text conferencing (where participants communicate through their normal keyboards and monitor) and video conferencing where participants can even see as well as talk to other fellow participants. Different types of equipments are used for video conferencing depending on what quality of the motion you want to capture (whether you want just to see the face of other fellow participants or do you want to see the exact facial expression).

Voice over IP: Computer networks are also used to provide voice communication. This kind of voice communication is pretty cheap as compared to the normal telephonic conversation.

Video on demand: Future services provided by the cable television networks may include video on request where a person can request for a particular movie or any clip at anytime he wish to see.

Summary: The main area of applications can be broadly classified into following categories:

Scientific and Technical Computing
Client Server Model, Distributed Processing
Parallel Processing, Communication Media
Commercial
Advertisement, Telemarketing, Teleconferencing
Worldwide Financial Services
Network for the People (this is the most widely used application nowadays)
Telemedicine, Distance Education, Access to Remote Information, Person-to-Person Communication, Interactive Entertainment

Open System Interconnection Reference Model

Figure 3-1

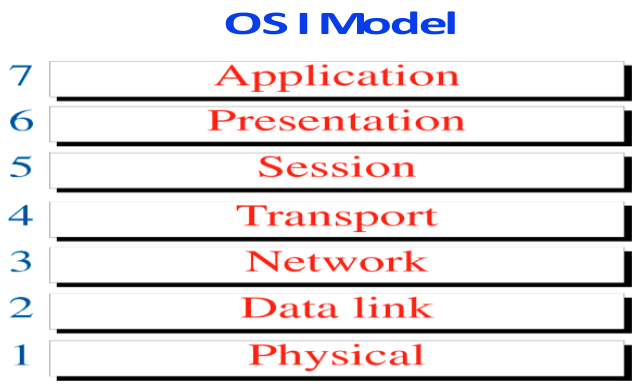


Figure 3-2

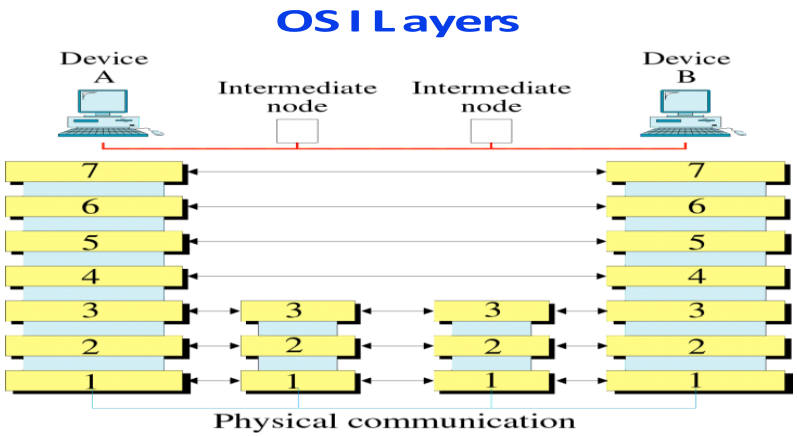


Figure 3-3

An Exchange Using the OSI Model

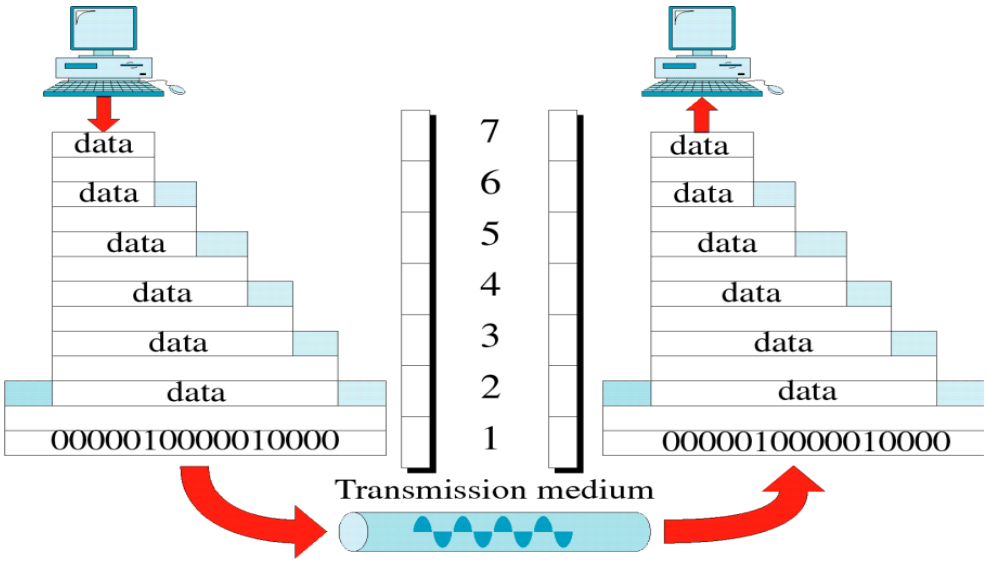


Figure 3-4

Physical Layer

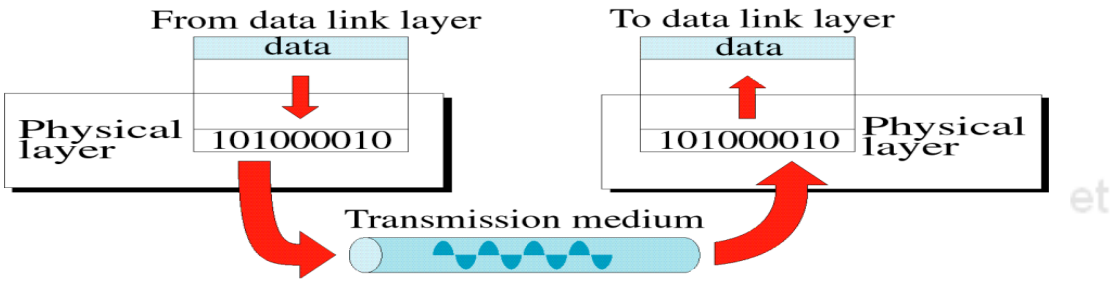


Figure 3-5

Data Link Layer

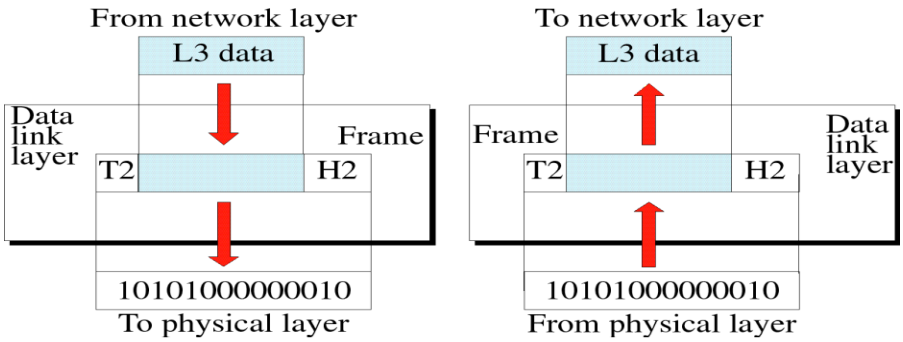


Figure 3-7

Network Layer

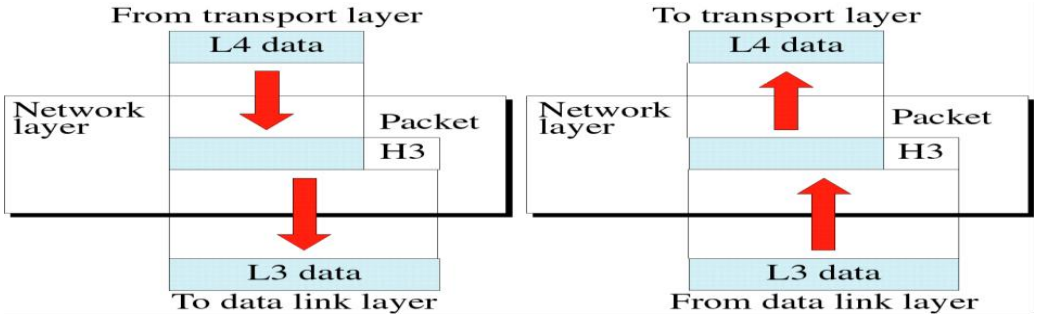


Figure 3-9

Transport Layer

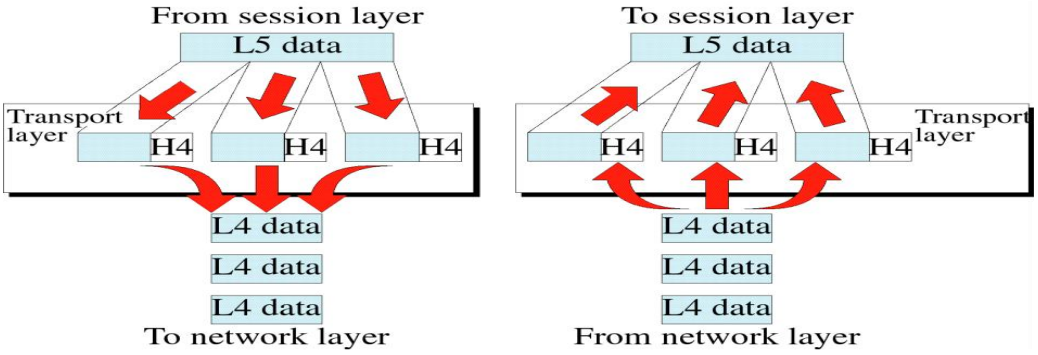


Figure 3-12

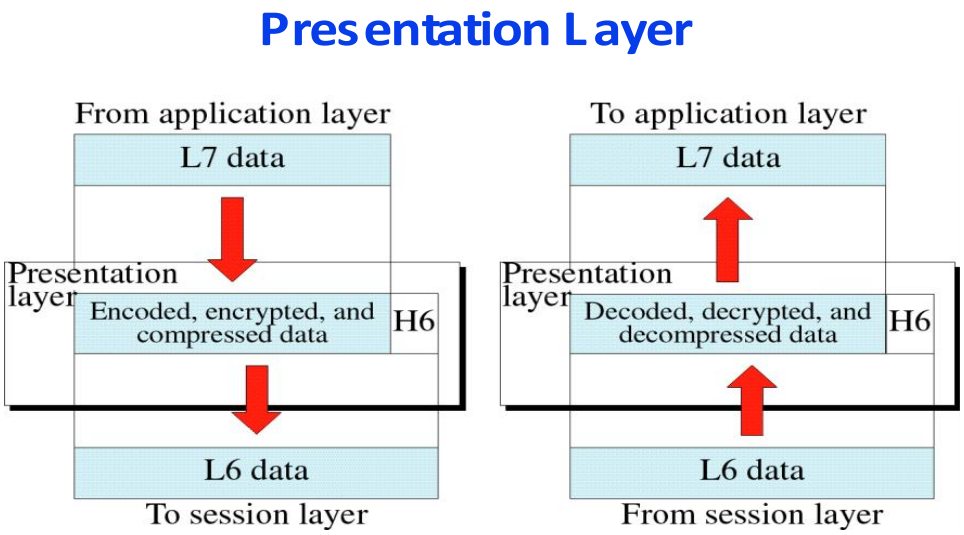
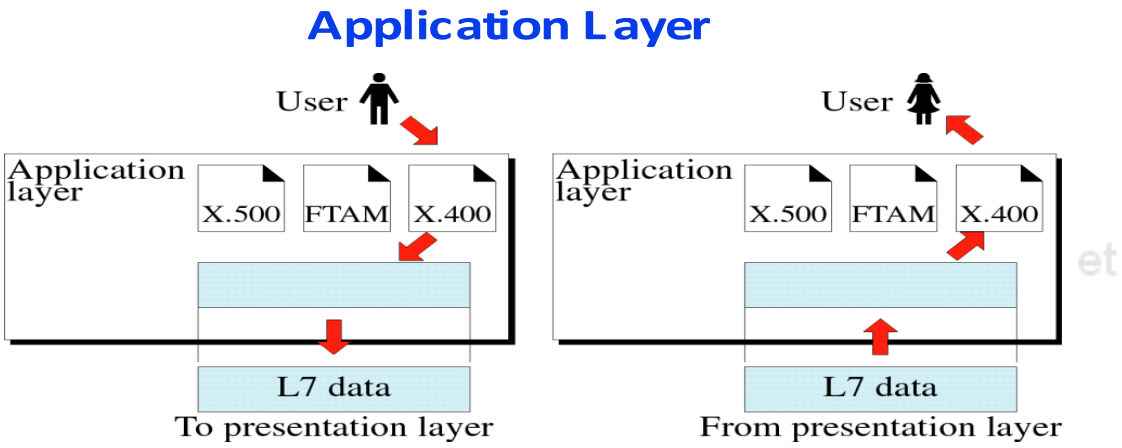


Figure 3-13



The Open System Interconnection (OSI) reference model describes how information from a software application in one computer moves through a network medium to a software application in another computer. The OSI reference model is a conceptual model composed of seven layers, each specifying particular network functions. The model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered the primary architectural model for inter-computer communications. The OSI model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. A task or group of tasks is then assigned to each of the seven OSI layers. Each layer is reasonably self-contained so that the tasks assigned to each layer can be implemented

independently. This enables the solutions offered by one layer to be updated without adversely affecting the other layers.

The OSI Reference Model includes seven layers:

7. *Application Layer*: Provides Applications with access to network services.

6. *Presentation Layer*: Determines the format used to exchange data among networked computers.

5. Session Layer: Allows two applications to establish, use and disconnect a connection between them called a session. Provides for name recognition and additional functions like security, which are needed to allow applications to communicate over the network.

4. Transport Layer: Ensures that data is delivered error free, in sequence and with no loss, duplications or corruption. This layer also repackages data by assembling long messages into lots of smaller messages for sending, and repackaging the smaller messages into the original larger message at the receiving end.

3. Network Layer: This is responsible for addressing messages and data so they are sent to the correct destination, and for translating logical addresses and names (like a machine name FLAME) into physical addresses. This layer is also responsible for finding a path through the network to the destination computer.

2. Data-Link Layer: This layer takes the data frames or messages from the Network Layer and provides for their actual transmission. At the receiving computer, this layer receives the incoming data and sends it to the network layer for handling. The Data-Link Layer also provides error-free delivery of data between the two computers by using the physical layer. It does this by packaging the data from the Network Layer into a frame, which includes error detection information. At the receiving computer, the Data-Link Layer reads the incoming frame, and generates its own error detection information based on the received frames data. After receiving the entire frame, it then compares its error detection value with that of the incoming frames, and if they match, the frame has been received correctly.

1. Physical Layer: Controls the transmission of the actual data onto the network cable. It defines the electrical signals, line states and encoding of the data and the connector types used. An example is 10BaseT.

Characteristics of the OSI Layers

The seven layers of the OSI reference model can be divided into two categories: upper layers and lower layers as shown in Fig. 1.2.2.

The upper layers of the OSI model deal with application issues and generally are implemented only in software. The highest layer, the application layer, is closest to the end user. Both users and application layer processes interact with software applications that contain a communications component. The term upper layer is sometimes used to refer to any layer above another layer in the OSI model.

The lower layers of the OSI model handle data transport issues. The physical layer and the data link layer are implemented in hardware and software. The lowest layer, the physical layer, is closest to the physical network medium (the network cabling, for example) and is responsible for actually placing information on the medium .

PROTOCOL

The OSI model provides a conceptual framework for communication between computers, but the model itself is not a method of communication. Actual communication is made possible by using communication protocols. In the context of data networking, a protocol is a formal set of rules and conventions that governs how computers exchange information over a network medium. A protocol implements the functions of one or more of the OSI layers.

A wide variety of communication protocols exist. Some of these protocols include LAN protocols, WAN protocols, network protocols, and routing protocols. LAN protocols operate at the physical and data link layers of the OSI model and define communication over various LAN media. WAN protocols operate at the lowest three layers of the OSI model and define communication over the various wide-area media. Routing protocols are network layer protocols that are responsible for exchanging information between routers so that the routers can select the proper path for network traffic. Finally, network protocols are the various upper-layer protocols that exist in a given protocol suite. Many protocols rely on others for operation. For example, many routing protocols use network protocols to exchange information between routers. This concept of building upon the layers already in existence is the foundation of the OSI model.

OSI Model and Communication between Systems

Information being transferred from a software application in one computer system to a software application in another must pass through the OSI layers. For example, if a software application in System A has information to transmit to a software application in System B, the application program in System A will pass its information to the application layer (Layer 7) of System A. The application layer then passes the information to the presentation layer (Layer 6), which relays the data to the session layer (Layer 5), and so on down to the physical layer (Layer 1). At the physical layer, the information is placed on the physical network medium and is sent across the medium to System B. The physical layer of System B removes the information from the physical medium, and then its physical layer passes the information up to the data link layer (Layer 2), which passes it to the network layer (Layer 3), and so on, until it reaches the application layer (Layer 7) of System B. Finally, the application layer of System B passes the information to the recipient application program to complete the communication process.

Interaction between OSI Model Layers

A given layer in the OSI model generally communicates with three other OSI layers: the layer directly above it, the layer directly below it, and its peer layer in other networked computer systems. The data link layer in System A, for example, communicates with the network layer of System A, the physical layer of System A, and the data link layer in System B. Figure1.2.3 illustrates this example.

Services and service access points

One OSI layer communicates with another layer to make use of the services provided by the second layer. The services provided by adjacent layers help a given OSI layer

communicate with its peer layer in other computer systems. Three basic elements are involved in layer services: the service user, the service provider, and the service access point (SAP).

In this context, the service user is the OSI layer that requests services from an adjacent OSI layer. The service provider is the OSI layer that provides services to service users. OSI layers can provide services to multiple service users. The SAP is a conceptual location at which one OSI layer can request the services of another OSI layer.

OSI Model Layers and Information Exchange

The seven OSI layers use various forms of control information to communicate with their peer layers in other computer systems. This control information consists of specific requests and instructions that are exchanged between peer OSI layers.

Control information typically takes one of two forms: headers and trailers. Headers are pretended to data that has been passed down from upper layers. Trailers are appended to data that has been passed down from upper layers. An OSI layer is not required to attach a header or a trailer to data from upper layers.

Headers, trailers, and data are relative concepts, depending on the layer that analyzes the information unit. At the network layer, for example, an information unit consists of a

Layer 3 header and data. At the data link layer, however, all the information passed down by the network layer (the Layer 3 header and the data) is treated as data.

In other words, the data portion of an information unit at a given OSI layer potentially can contain headers, trailers, and data from all the higher layers. This is known as encapsulation. Figure 1-6 shows how the header and data from one layer are encapsulated into the header of the next lowest layer.

Information Exchange Process

The information exchange process occurs between peer OSI layers. Each layer in the source system adds control information to data, and each layer in the destination system analyzes and removes the control information from that data.

If system A has data from software application to send to System B, the data is passed to the application layer. The application layer in System A then communicates any control information required by the application layer in System B by pre-pending a header to the data. The resulting information unit (a header and the data) is passed to the presentation layer, which pre-pends its own header containing control information intended for the presentation layer in System B. The information unit grows in size as each layer pre-pends its own header (and, in some cases, a trailer) that contains control information to be used by its peer layer in System B. At the physical layer, the entire information unit is placed onto the network medium.

The physical layer in System B receives the information unit and passes it to the data link layer. The data link layer in System B then reads the control information contained in the header pre-pended by the data link layer in System A. The header is then removed, and the remainder of the information unit is passed to the network layer. Each layer performs the same actions: The layer reads the header from its peer layer, strips it off, and passes the remaining information unit to the next highest layer. After the application layer

performs these actions, the data is passed to the recipient software application in System B, in exactly the form in which it was transmitted by the application in System A.

Functions of the OSI Layers

Functions of **different layers of the OSI model are presented in this section.**

Physical Layer

The physical layer is concerned with transmission of raw bits over a communication channel. It specifies the mechanical, electrical and procedural network interface specifications and the physical transmission of bit streams over a transmission medium connecting two pieces of communication equipment. In simple terns, the physical layer decides the following:

Number of pins and functions of each pin of the network connector (Mechanical)

Signal Level, Data rate (Electrical)

Whether simultaneous transmission in both directions

Establishing and breaking of connection

Deals with physical transmission

There exist a variety of physical layer protocols such as RS-232C, Rs-449 standards developed by Electronics Industries Association (EIA).

1.2.4.2 Data Link Layer

The goal of the data link layer is to provide reliable, efficient communication between adjacent machines connected by a single communication channel. Specifically:

1. Group the physical layer bit stream into units called frames. Note that frames are nothing more than ``packets'' or ``messages''. By convention, we shall use the term ``frames'' when discussing DLL packets.

2. Sender calculates the checksum and sends checksum together with data. The checksum allows the receiver to determine when a frame has been damaged in transit or received correctly.

3. Receiver recomputes the checksum and compares it with the received value. If they differ, an error has occurred and the frame is discarded.

4. Error control protocol returns a positive or negative acknowledgment to the sender. A positive acknowledgment indicates the frame was received without errors, while a negative acknowledgment indicates the opposite.

5. Flow control prevents a fast sender from overwhelming a slower receiver. For example, a supercomputer can easily generate data faster than a PC can consume it.

6. In general, data link layer provides service to the network layer. The network layer wants to be able to send packets to its neighbors without worrying about the details of getting it there in one piece.

Design Issues Below are the some of the important design issues of the data link layer:

a). Reliable Delivery:

Frames are delivered to the receiver reliably and in the same order as generated by the sender. Connection state keeps track of sending order and which frames require retransmission. For example, receiver state includes which frames have been received, which ones have not, etc.

b). Best Effort: The receiver does not return acknowledgments to the sender, so the sender has no way of knowing if a frame has been successfully delivered.

When would such a service be appropriate?

1. When higher layers can recover from errors with little loss in performance. That is, when errors are so infrequent that there is little to be gained by the data link layer performing the recovery. It is just as easy to have higher layers deal with occasional loss of packet.

2. For real-time applications requiring ``better never than late" semantics. Old data may be worse than no data.

c). Acknowledged Delivery
The receiver returns an acknowledgment frame to the sender indicating that a data frame was properly received. This sits somewhere between the other two in that the sender keeps connection state, but may not necessarily retransmit unacknowledged frames. Likewise, the receiver may hand over received packets to higher layer in the order in which they arrive, regardless of the original sending order. Typically, each frame is assigned a unique sequence number, which the receiver returns in an acknowledgment frame to indicate which frame the ACK refers to. The sender must retransmit unacknowledged (e.g., lost or damaged) frames.

d). Framing

The DLL translates the physical layer's raw bit stream into discrete units (messages) called frames. How can the receiver detect frame boundaries? Various techniques are used for this: Length Count, Bit Stuffing, and Character stuffing.

e). Error Control

Error control is concerned with insuring that all frames are eventually delivered (possibly in order) to a destination. To achieve this, three items are required: Acknowledgements, Timers, and Sequence Numbers.

f). Flow Control

Flow control deals with throttling the speed of the sender to match that of the receiver. Usually, this is a dynamic process, as the receiving speed depends on such changing factors as the load, and availability of buffer space.

Link Management In some cases, the data link layer service must be ``opened" before use:

The data link layer uses open operations for allocating buffer space, control blocks, agreeing on the maximum message size, etc.

Synchronize and initialize send and receive sequence numbers with its peer at the other end of the communications channel.

Error Detection and Correction

In data communication, error may occur because of various reasons including attenuation, noise. Moreover, error usually occurs as bursts rather than independent, single bit errors. For example, a burst of lightning will affect a set of bits for a short time after the lightning strike. Detecting and correcting errors requires redundancy (i.e., sending additional information along with the data).

There are two types of attacks against errors:

Error Detecting Codes: Include enough redundancy bits to detect errors and use ACKs and retransmissions to recover from the errors. Example: parity encoding.
• Error Correcting Codes: Include enough redundancy to detect and correct errors. Examples: CRC checksum, MD5.

Network Layer

The basic purpose of the network layer is to provide an end-to-end communication capability in contrast to machine-to-machine communication provided by the data link layer. This end-to-end is performed using two basic approaches known as connection-oriented or connectionless network-layer services.

Four issues:

1. Interface between the host and the network (the network layer is typically the boundary between the host and subnet)

2. Routing

3. Congestion and deadlock

4. Internetworking (A path may traverse different network technologies (e.g., Ethernet, point-to-point links, etc.)

Network Layer Interface

There are two basic approaches used for sending packets, which is a group of bits that includes data plus source and destination addresses, from node to node called virtual circuit and datagram methods. These are also referred to as connection-oriented and connectionless network-layer services. In virtual circuit approach, a route, which consists of logical connection, is first established between two users. During this establishment phase, the two users not only agree to set up a connection between them but also decide upon the quality of service to be associated with the connection. The well-known virtual-circuit protocol is the ISO and CCITT X.25 specification. The datagram is a self-contained message unit, which contains sufficient information for routing from the source node to the destination node without dependence on previous message interchanges between them. In contrast to the virtual-circuit method, where a fixed path is explicitly set up before message transmission, sequentially transmitted messages can follow completely different paths. The datagram method is analogous to the postal system and the virtual-circuit method is analogous to the telephone system.

Overview of Other Network Layer Issues:

The network layer is responsible for routing packets from the source to destination. The routing algorithm is the piece of software that decides where a packet goes next (e.g., which output line, or which node on a broadcast channel).

For connectionless networks, the routing decision is made for each datagram. For connection-oriented networks, the decision is made once, at circuit setup time.

Routing Issues:

The routing algorithm must deal with the following issues:

Correctness and simplicity: networks are never taken down; individual parts (e.g., links, routers) may fail, but the whole network should not.

Stability: if a link or router fails, how much time elapses before the remaining routers recognize the topology change? (Some never do.)

Fairness and optimality: an inherently intractable problem. Definition of optimality usually doesn't consider fairness. Do we want to maximize channel usage? Minimize average delay?

When we look at routing in detail, we'll consider both adaptive--those that take current traffic and topology into consideration--and non-adaptive algorithms.

Congestion The network layer also must deal with congestion:

When more packets enter an area than can be processed, delays increase and performance decreases. If the situation continues, the subnet may have no alternative but to discard packets. If the delay increases, the sender may (incorrectly) retransmit, making a bad situation even worse.

Overall, performance degrades because the network is using (wasting) resources processing packets that eventually get discarded.

Internetworking Finally, when we consider internetworking -- connecting different network technologies together -- one finds the same problems, only worse:

Packets may travel through many different networks
Each network may have a different frame format
Some networks may be connectionless, other connection oriented

Routing

Routing is concerned with the question: Which line should router J use when forwarding a packet to router K?

There are two types of algorithms:

Adaptive algorithms use such dynamic information as current topology, load, delay, etc. to select routes.
In non-adaptive algorithms, routes never change once initial routes have been selected. Also called static routing.

Obviously, adaptive algorithms are more interesting, as non-adaptive algorithms don't even make an attempt to handle failed links.

Transport Layer

The transport level provides end-to-end communication between processes executing on different machines. Although the services provided by a transport protocol are similar to those provided by a data link layer protocol, there are several important differences between the transport and lower layers:

1. User Oriented. Application programmers interact directly with the transport layer, and from the programmers perspective, the transport layer is the ``network''. Thus, the transport layer should be oriented more towards user services than simply reflect what the underlying layers happen to provide. (Similar to the beautification principle in operating systems.)

2. Negotiation of Quality and Type of Services. The user and transport protocol may need to negotiate as to the quality or type of service to be provided. Examples? A user may want to negotiate such options as: throughput, delay, protection, priority, reliability, etc.

3. Guarantee Service. The transport layer may have to overcome service deficiencies of the lower layers (e.g. providing reliable service over an unreliable network layer).

4. Addressing becomes a significant issue. That is, now the user must deal with it; before it was buried in lower levels.

Two solutions:

Use well-known addresses that rarely if ever change, allowing programs to ``wire in'' addresses. For what types of service does this work? While this works for services that are well established (e.g., mail, or telnet), it doesn't allow a user to easily experiment with new services.

Use a name server. Servers register services with the name server, which clients contact to find the transport address of a given service.

In both cases, we need a mechanism for mapping high-level service names into low-level encoding that can be used within packet headers of the network protocols. In its general form, the problem is quite complex. One simplification is to break the problem into two parts: have transport addresses be a combination of machine address and local process on that machine.

5. Storage capacity of the subnet. Assumptions valid at the data link layer do not necessarily hold at the transport Layer. Specifically, the subnet may buffer messages for a potentially long time, and an ``old'' packet may arrive at a destination at unexpected times.

6. We need a dynamic flow control mechanism. The data link layer solution of reallocating buffers is inappropriate because a machine may have hundreds of connections sharing a single physical link. In addition, appropriate settings for the flow control parameters depend on the communicating end points (e.g., Cray supercomputers vs. PCs), not on the protocol used.

Don't send data unless there is room. Also, the network layer/data link layer solution of simply not acknowledging frames for which the receiver has no space is unacceptable. Why? In the data link case, the line is not being used for anything else; thus

retransmissions are inexpensive. At the transport level, end-to-end retransmissions are needed, which wastes resources by sending the same packet over the same links multiple times. If the receiver has no buffer space, the sender should be prevented from sending data.

7. Deal with congestion control. In connectionless Internets, transport protocols must exercise congestion control. When the network becomes congested, they must reduce rate at which they insert packets into the subnet, because the subnet has no way to prevent itself from becoming overloaded.

8. Connection establishment. Transport level protocols go through three phases: establishing, using, and terminating a connection. For data gram-oriented protocols, opening a connection simply allocates and initializes data structures in the operating system kernel.

Connection oriented protocols often exchanges messages that negotiate options with the remote peer at the time a connection are opened. Establishing a connection may be tricky because of the possibility of old or duplicate packets.

Finally, although not as difficult as establishing a connection, terminating a connection presents subtleties too. For instance, both ends of the connection must be sure that all the data in their queues have been delivered to the remote application.

Session Layer

This layer allows users on different machines to establish session between them. A session allows ordinary data transport but it also provides enhanced services useful in some applications. A session may be used to allow a user to log into a remote time-

Sharing machine or to transfer a file between two machines. Some of the session related services are:

1. This layer manages Dialogue Control. Session can allow traffic to go in both direction at the same time, or in only one direction at one time.

2. Token management. For some protocols, it is required that both sides don't attempt same operation at the same time. To manage these activities, the session layer provides tokens that can be exchanged. Only one side that is holding token can perform the critical operation. This concept can be seen as entering into a critical section in operating system using semaphores.

3. Synchronization. Consider the problem that might occur when trying to transfer a 4-hour file transfer with a 2-hour mean time between crashes. After each transfer was aborted, the whole transfer has to start again and again would probably fail. To Eliminate this problem, Session layer provides a way to insert checkpoints into data streams, so that after a crash, only the data transferred after the last checkpoint have to be repeated.

Presentation Layer

This layer is concerned with Syntax and Semantics of the information transmitted, unlike other layers, which are interested in moving data reliably from one machine to other. Few of the services that Presentation layer provides are:

1. Encoding data in a standard agreed upon way.

2. It manages the abstract data structures and converts from representation used inside computer to network standard representation and back.

Application Layer

The application layer consists of what most users think of as programs. The application does the actual work at hand. Although each application is different, some applications are so useful that they have become standardized. The Internet has defined standards for:

• File transfer (FTP): Connect to a remote machine and send or fetch an arbitrary file. FTP deals with authentication, listing a directory contents, ASCII or binary files, etc.
• Remote login (telnet): A remote terminal protocol that allows a user at one site to establish a TCP connection to another site, and then pass keystrokes from the local host to the remote host.
Mail (SMTP): Allow a mail delivery agent on a local machine to connect to a mail delivery agent on a remote machine and deliver mail.
• News (NNTP): Allows communication between a news server and a news client.
• Web (HTTP): Base protocol for communication on the World Wide Web.

Transmission Media

Introduction

Transmission media can be defined as physical path between transmitter and receiver in a data transmission system. And it may be classified into two types as shown in Fig. 2.2.1.
Guided: Transmission capacity depends critically on the medium, the length, and whether the medium is point-to-point or multipoint (e.g. LAN). Examples are co-axial cable, twisted pair, and optical fiber.
Unguided: provides a means for transmitting electro-magnetic signals but do not guide them. Example wireless transmission.

Characteristics and quality of data transmission are determined by medium and signal characteristics. For guided media, the medium is more important in determining the limitations of transmission. While in case of unguided media, the bandwidth of the signal produced by the transmitting antenna and the size of the antenna is more important than the medium. Signals at lower frequencies are omni-directional (propagate in all directions). For higher frequencies, focusing the signals into a directional beam is possible. These properties determine what kind of media one should use in a particular application. In this lesson we shall discuss the characteristics of various transmission media, both guided and unguided.

Guided transmission media

In this section we shall discuss about the most commonly used guided transmission media such as twisted-pair of cable, coaxial cable and optical fiber.

Twisted Pair

In twisted pair technology, two copper wires are strung between two points:

• The two wires are typically ``twisted'' together in a helix to reduce interference between the two conductors .Twisting decreases the cross-talk interference between adjacent pairs in a cable. Typically, a number of pairs are bundled together into a cable by wrapping them in a tough protective sheath. Actually, they carry only analog signals. However, the ``analog'' signals can very closely correspond to the square waves representing bits, so we often think of them as carrying digital data. Data rates of several Mbps common. Spans distances of several kilometers. Data rate determined by wire thickness and length. In addition, shielding to eliminate interference from other wires impacts signal-to-noise ratio, and ultimately, the data rate.

Good, low-cost communication. Indeed, many sites already have twisted pair installed in offices -- existing phone lines!

Typical characteristics: Twisted-pair can be used for both analog and digital communication. The data rate that can be supported over a twisted-pair is inversely proportional to the square of the line length. Maximum transmission distance of 1 Km can be achieved for data rates up to 1 Mb/s. For analog voice signals, amplifiers are required about every 6 Km and for digital signals, repeaters are needed for about 2 Km. To reduce interference, the twisted pair can be shielded with metallic braid. This type of wire is known as Shielded Twisted-Pair (STP) and the other form is known as Unshielded Twisted-Pair (UTP).
Use: The oldest and the most popular use of twisted pair are in telephony. In LAN it is commonly used for point-to-point short distance communication (say, 100m) within a building or a room.
Base band Coaxial With ``coax'', the medium consists of a copper core surrounded by insulating material and a braided outer conductor as shown in Fig. 2.2.3. The term base band indicates digital transmission (as opposed to broadband analog).

Physical connection consists of metal pin touching the copper core. There are two common ways to connect to a coaxial cable:

1. With vampire taps, a metal pin is inserted into the copper core. A special tool drills a hole into the cable, removing a small section of the insulation, and a special connector is screwed into the hole. The tap makes contact with the copper core.
2. With a T-junction, the cable is cut in half, and both halves connect to the T-junction. A T-connector is analogous to the signal splitters used to hook up multiple TVs to the same cable wire.

Characteristics: Co-axial cable has superior frequency characteristics compared to twisted-pair and can be used for both analog and digital signaling. In baseband LAN, the data rates lies in the range of 1 KHz to 20 MHz over a distance in the range of 1 Km. Co-axial cables typically have a diameter of 3/8". Coaxial cables are used both for baseband and broadband communication. For broadband CATV application coaxial cable of 1/2" diameter and 75 Ω impedance is used. This cable offers bandwidths of 300 to 400 MHz facilitating high-speed data communication with low bit-error rate. In broadband signaling, signal propagates only in one direction, in contrast to propagation in both directions in baseband signaling. Broadband cabling uses either dual-cable scheme or single-cable scheme with a headend to facilitate flow of signal in one direction. Because

of the shielded, concentric construction, co-axial cable is less susceptible to interference and cross talk than the twisted-pair. For long distance communication, repeaters are needed for every kilometer or so. Data rate depends on physical properties of cable, but 10 Mbps is typical.

Use: One of the most popular use of co-axial cable is in cable TV (CATV) for the distribution of TV signals. Another importance use of co-axial cable is in LAN.

Broadband Coaxial

The term broadband refers to analog transmission over coaxial cable. (Note, however, that the telephone folks use broadband to refer to any channel wider than 4 kHz). The technology:

• Typically bandwidth of 300 MHz, total data rate of about 150 Mbps.
•Operates at distances up to 100 km (metropolitan area!).
• Uses analog signaling.
• Technology used in cable television. Thus, it is already available at sites such as universities that may have TV classes.
• Total available spectrum typically divided into smaller channels of 6 MHz each. That is, to get more than 6MHz of bandwidth, you have to use two smaller channels and somehow combine the signals.
• Requires amplifiers to boost signal strength; because amplifiers are one way, data flows in only one direction.

Two types of systems have emerged:

1. Dual cable systems use two cables, one for transmission in each direction:
One cable is used for receiving data. Second cable used to communicate with headend. When a node wishes to transmit data, it sends the data to a special node called the headend. The headend then resends the data on the first cable. Thus, the headend acts as a root of the tree, and all data must be sent to the root for redistribution to the other nodes.
2. Midsplit systems divide the raw channel into two smaller channels, with each sub channel having the same purpose as above. Which is better, broadband or base band? There is rarely a simple answer to such questions. Base band is simple to install, interfaces are inexpensive, but doesn't have the same range. Broadband is more complicated, more expensive, and requires regular adjustment by a trained technician, but offers more services (e.g., it carries audio and video too).

Fiber Optics

In fiber optic technology, the medium consists of a hair-width strand of silicon or glass, and the signal consists of pulses of light. For instance, a pulse of light means ``1", lack of pulse means ``0". It has a cylindrical shape and consists of three concentric sections: the core, the cladding, and the jacket as shown in Fig. 2.2.4.

The core, innermost section consists of a single solid dielectric cylinder of diameter d1 and of refractive index n1. The core is surrounded by a solid dielectric cladding of refractive index n2 that is less than n1. As a consequence, the light is propagated through multiple total internal reflection. The core material is usually made of ultra pure fused

silica or glass and the cladding is either made of glass or plastic. The cladding is surrounded by a jacket made of plastic. The jacket is used to protect against moisture, abrasion, crushing and other environmental hazards.

Three components are required:

1. Fiber medium: Current technology carries light pulses for tremendous distances (e.g., 100s of kilometers) with virtually no signal loss.
2.Light source: typically a Light Emitting Diode (LED) or laser diode. Running current through the material generates a pulse of light.
3. A photo diode light detector, which converts light pulses into electrical signals.

Advantages:

1. Very high data rate, low error rate. 1000 Mbps (1 Gbps) over distances of kilometers common. Error rates are so low they are almost negligible.
2. Difficult to tap, which makes it hard for unauthorized taps as well. This is responsible for higher reliability of this medium. How difficult is it to prevent coax taps? Very difficult indeed, unless one can keep the entire cable in a locked room!
3. Much thinner (per logical phone line) than existing copper circuits. Because of its thinness, phone companies can replace thick copper wiring with fibers having much more capacity for same volume. This is important because it means that aggregate phone capacity can be upgraded without the need for finding more physical space to hire the new cables.
4. Not susceptible to electrical interference (lightning) or corrosion (rust).
5. Greater repeater distance than coax.

Disadvantages:

• Difficult to tap. It really is point-to-point technology. In contrast, tapping into coax is trivial. No special training or expensive tools or parts are required.
• One-way channel. Two fibers needed to get full duplex (both ways) communication.
Optical Fiber works in three different types of modes (or we can say that we have 3 types of communication using Optical fiber). Optical fibers are available in two varieties; Multi-Mode Fiber (MMF) and Single-Mode Fiber (SMF). For multi-mode fiber the core and cladding diameter lies in the range 50-200µm and 125-400µm, respectively. Whereas in single-mode fiber, the core and cladding diameters lie in the range 8-12µm and 125µm, respectively. Single-mode fibers are also known as Mono-Mode Fiber. Moreover, both single-mode and multi-mode fibers can have two types; step index and graded index. In the former case the refractive index of the core is uniform throughout and at the core cladding boundary there is an abrupt change in refractive index. In the later case, the refractive index of the core varies radially from the centre to the core-cladding boundary from n1 to n2 in a linear manner. Fig. 2.2.5 shows the optical fiber transmission modes.
Figure 2.2.5 Schematics of three optical fiber types, (a) Single-mode step-index, (b) Multi-mode step-index, and (c) Multi-mode graded-index
Characteristics: Optical fiber acts as a dielectric waveguide that operates at optical frequencies (1014 to 1015 Hz). Three frequency bands centered around 850,1300 and 1500 nanometers are used for best results. When light is applied at one end of the optical fiber core, it reaches the other end by means of total internal reflection because of the choice of refractive index of core and cladding material (n1 > n2). The light source can

be either light emitting diode (LED) or injection laser diode (ILD). These semiconductor devices emit a beam of light when a voltage is applied across the device. At the receiving end, a photodiode can be used to detect the signal-encoded light. Either PIN detector or APD (Avalanche photodiode) detector can be used as the light detector.

In a multi-mode fiber, the quality of signal-encoded light deteriorates more rapidly than single-mode fiber, because of interference of many light rays. As a consequence, single-mode fiber allows longer distances without repeater. For multi-mode fiber, the typical maximum length of the cable without a repeater is 2km, whereas for single-mode fiber it is 20km.

Fiber Uses: Because of greater bandwidth (2Gbps), smaller diameter, lighter weight, low attenuation, immunity to electromagnetic interference and longer repeater spacing, optical fiber cables are finding widespread use in long-distance telecommunications. Especially, the single mode fiber is suitable for this purpose. Fiber optic cables are also used in high-speed LAN applications. Multi-mode fiber is commonly used in LAN.

- Long-haul trunks-increasingly common in telephone network (Sprint ads)
- Metropolitan trunks-without repeaters (average 8 miles in length)
- Rural exchange trunks-link towns and villages
- Local loops-direct from central exchange to a subscriber (business or home)
- Local area networks-100Mbps ring networks.

Unguided Transmission

Unguided transmission is used when running a physical cable (either fiber or copper) between two end points is not possible. For example, running wires between buildings is probably not legal if the building is separated by a public street.

Infrared signals typically used for short distances (across the street or within same room),

Microwave signals commonly used for longer distances (10's of km). Sender and receiver use some sort of dish antenna as shown in Fig. 2.2.6.

Difficulties:

1. Weather interferes with signals. For instance, clouds, rain, lightning, etc. may adversely affect communication.
2. Radio transmissions easy to tap. A big concern for companies worried about competitors stealing plans.
3. Signals bouncing off of structures may lead to out-of-phase signals that the receiver must filter out.

Satellite Communication

Satellite communication is based on ideas similar to those used for line-of-sight. A communication satellite is essentially a big microwave repeater or relay station in the sky. Microwave signals from a ground station is picked up by a transponder, amplifies the signal and rebroadcasts it in another frequency, which can be received by ground stations at long distances as shown in Fig. 2.2.7.

To keep the satellite stationary with respect to the ground based stations, the satellite is placed in a geostationary orbit above the equator at an altitude of about 36,000 km. As the spacing between two satellites on the equatorial plane should not be closer than 40, there can be 360/4 = 90 communication satellites in the sky at a time. A satellite can be used for point-to-point communication between two ground-based stations or it

can be used to broadcast a signal received from one station to many ground-based stations as shown in Fig. 2.2.8. Number of geo-synchronous satellites limited (about 90 total, to minimize interference). International agreements regulate how satellites are used, and how frequencies are allocated. Weather affects certain frequencies. Satellite transmission differs from terrestrial communication in another important way: One-way propagation delay is roughly 270 ms. In interactive terms, propagation delay alone inserts a 1 second delay between typing a character and receiving its echo.

Characteristics: Optimum frequency range for satellite communication is 1 to 10 GHz. The most popular frequency band is referred to as 4/6 band, which uses 3.7 to 4.2 GHz for down link and 5.925 to 6.425 for uplink transmissions. The 500 MHz bandwidth is usually split over a dozen transponders, each with 36 MHz bandwidth. Each 36 MHz bandwidth is shared by time division multiplexing. As this preferred band is already saturated, the next highest band available is referred to as 12/14 GHz. It uses 14 to 14.5GHz for upward transmission and 11.7 to 12.2 GHz for downward transmissions. Communication satellites have several unique properties. The most important is the long communication delay for the round trip (about 270 ms) because of the long distance (about 72,000 km) the signal has to travel between two earth stations. This poses a number of problems, which are to be tackled for successful and reliable communication. Another interesting property of satellite communication is its broadcast capability. All stations under the downward beam can receive the transmission. It may be necessary to send encrypted data to protect against piracy.

Use: Now-a-days communication satellites are not only used to handle telephone, telex and television traffic over long distances, but are used to support various internet based services such as e-mail, FTP, World Wide Web (WWW), etc. New types of services, based on communication satellites, are emerging.

Comparison/contrast with other technologies:

1. Propagation delay very high. On LANs, for example, propagation time is in nanoseconds -- essentially negligible.
2. One of few alternatives to phone companies for long distances.
3. Uses broadcast technology over a wide area - everyone on earth could receive a message at the same time!
4. Easy to place unauthorized taps into signal.

Satellites have recently fallen out of favor relative to fiber.

However, fiber has one big disadvantage: no one has it coming into their house or building, whereas anyone can place an antenna on a roof and lease a satellite channel.

Introduction

In the previous module we have discussed various encoding and modulation techniques, which are used for converting data in to signal. To send signal through the transmission media, it is necessary to develop suitable mechanism for interfacing data terminal equipments (DTEs), which are the sources of data, to the data circuit terminating equipments (DCEs), which converts data to signal and interfaces with the transmission media. The way it takes place is shown in Fig. 3.1.2. The link between the two devices is known as *interface*. But, before we discuss about the interface we shall introduce various modes of communication in Sec. 3.1.2. Various aspects of framing and synchronization for bit-oriented framing have been presented in Sec. 3.1.3. Character-oriented framing

has discussed in Sec. 3.1.4. Finally, We shall discuss about the interface in detail along with some standard interfaces in Sec. 3.1.5.

Possible Modes of communication

Transmission of digital data through a transmission medium can be performed either in serial or in parallel mode. In the serial mode, one bit is sent per clock tick, whereas in parallel mode multiple bits are sent per clock tick. There are two subclasses of transmission for both the serial and parallel modes, as shown in Fig 3.1.3

Different modes of transmission

Parallel Transmission

Parallel transmission involves grouping several bits, say n, together and sending all the n bits at a time. This can be accomplishes with the help of eight wires bundled together in the form of a cable with a connector at each end. Additional wires, such as request (req) and acknowledgement (ack) are required for asynchronous transmission.

Primary advantage of parallel transmission is higher speed, which is achieved at the expense of higher cost of cabling. As this is expensive for longer distances, parallel transmission is feasible only for short distances.

Figure 3.1.4 Parallel mode of communication with n = 8

Serial Transmission

Serial transmission involves sending one data bit at a time. Figure 3.1.5 shows how serial transmission occurs. It uses a pair of wire for communication of data in bit-serial form. Since communication within devices is parallel, it needs parallel-to-serial and serial-to-parallel conversion at both ends.

Serial mode of communication widely used because of the following advantages:

• Reduced cost of cabling: Lesser number of wires is required as compared to parallel connection

• Reduced cross talk: Lesser number of wires result in reduced cross talk

• Availability of suitable communication media

• Inherent device characteristics: Many devices are inherently serial in nature

• Portable devices like PDAs, etc use serial communication to reduce the size of the connector

However, it is slower than parallel mode of communication.

There are two basic approaches for serial communication to achieve synchronization of data transfer between the source-destination pair. These are referred to as – asynchronous and synchronous. In the first case, data are transmitted in small sizes, say character by character, to avoid timing problem and make data transfer self-synchronizing, as discussed later. However, it is not very efficient because of large overhead. To overcome this problem, synchronous mode is used. In synchronous mode, a block with large number of bits can be sent at a time. However, this requires tight synchronization between the transmitter and receiver clocks.

Direction of data flow:

There are three possible modes in serial communication: simplex, full duplex and half duplex. In simplex mode, the communication is unidirectional, such as from a computer to a printer, as shown in Fig. 3.1.6(a). In full-duplex mode both the sides can communicate simultaneously, as shown in Fig. 3.1.6 (b). On the other hand, in half-

duplex mode of communication, each station can both send and receive data, But, when one is sending, the other one can only receive and vice versa.

Why Framing and Synchronization?

Normally, units of data transfer are larger than a single analog or digital encoding symbol. It is necessary to recover clock information for both the signal (so we can recover the right number of symbols and recover each symbol as accurately as possible), and obtain synchronization for larger units of data (such as data words and frames). It is necessary to recover the data in words or blocks because this is the only way the receiver process will be able to interpret the data received; for a given bit stream. Depending on the byte boundaries, there will be seven or eight ways to interpret the bit stream as ASCII characters, and these are likely to be very different. So, it is necessary to add other bits to the block that convey control information used in the data link control procedures. The data along with preamble, postamble, and control information forms a frame. This framing is necessary for the purpose of synchronization and other data control functions.

Synchronization

Data sent by a sender in bit-serial form through a medium must be correctly interpreted at the receiving end. This requires that the beginning, the end and logic level and duration of each bit as sent at the transmitting end must be recognized at the receiving end. There are three synchronization levels: Bit, Character and Frame. Moreover, to achieve synchronization, two approaches known as asynchronous and synchronous transmissions are used. Frame synchronization is the process by which incoming frame alignment signals (i.e., distinctive bit sequences) are identified, i.e. distinguished from data bits, permitting the data bits within the frame to be extracted for decoding or retransmission. The usual practice is to insert, in a dedicated time slot within the frame, a non-information bit that is used for the actual synchronization of the incoming data with the receiver.

In order to receive bits in the first place, the receiver must be able to determine how fast bits are being sent and when it has received a signal symbol. Further, the receiver needs to be able to determine what the relationship of the bits in the received stream have to one another, that is, what the logical units of transfer are, and where each received bit fits into the logical units. We call these logical units frames. This means that in addition to bit (or transmission symbol) synchronization, the receiver needs word and frame synchronization.

Synchronous communication (bit-oriented)

Timing is recovered from the signal itself (by the carrier if the signal is analog, or by regular transitions in the data signal or by a separate clock line if the signal is digital). Scrambling is often used to ensure frequent transitions needed. The data transmitted may be of any bit length, but is often constrained by the frame transfer protocol (data link or MAC protocol). Bit-oriented framing only assumes that bit synchronization has been achieved by the underlying hardware, and the incoming bit stream is scanned at all possible bit positions for special patterns generated by the sender. The sender uses a special pattern (a flag pattern) to delimit frames (one flag at each end), and has to provide for data transparency by use of bit stuffing (see below). A commonly used flag pattern is HDLC's 01111110 flag as shown in Fig. 3.1.7. The bit sequence 01111110 is used for

both preamble and postamble for the purpose of synchronization. A frame format for bit-oriented synchronous frame is shown in Fig. 3.1.8. Apart from the flag bits there are control fields. This field contains the commands, responses and sequences numbers used to maintain the data flow accountability of the link, defines the functions of the frame and initiates the logic to control the movement of traffic between sending and receiving stations.

Specific pattern to represent start of frame

Specific pattern to represent end of frame

Summary of the approach:

- Initially 1 or 2 synchronization characters are sent
- Data characters are then continuously sent without any extra bits
- At the end, some error detection data is sent

Advantages:

- Much less overhead
- No overhead is incurred except for synchronization characters

Disadvantages:

- No tolerance in clock frequency is allowed

- The clock frequency should be same at both the sending and receiving ends

Bit stuffing: If the flag pattern appears anywhere in the header or data of a frame, then the receiver may prematurely detect the start or end of the received frame. To overcome this problem, the sender makes sure that the frame body it sends has no flags in it at any position (note that since there is no character synchronization, the flag pattern can start at any bit location within the stream). It does this by bit stuffing, inserting an extra bit in any pattern that is beginning to look like a flag. In HDLC, whenever 5 consecutive 1's are encountered in the data, a 0 is inserted after the 5th 1, regardless of the next bit in the data as shown in Fig. 3.1.9. On the receiving end, the bit stream is piped through a shift register as the receiver looks for the flag pattern. If 5 consecutive 1's followed by a 0 is seen, then the 0 is dropped before sending the data on (the receiver destuffs the stream). If 6 1's and a 0 are seen, it is a flag and either the current frame are ended or a new frame is started, depending on the current state of the receiver. If more than 6 consecutive 1's are seen, then the receiver has detected an invalid pattern, and usually the current frame, if any, is discarded.

a). 1101111111110011111111000111111000

b). 01111110 1101111101111001111101110001111101100 0 01111110

0’s stuffed after every five 1’s

With bit stuffing, the boundary between two frames can be unambiguously recognized by the flag pattern. Thus, if receiver loses track of where it is, all it has to do is to scan the input for flag sequence, since they can only occur at frame boundaries and never within data. In addition to receiving the data in logical units called frames, the receiver should have some way of determining if the data has been corrupted or not. If it has been

corrupted, it is desirable not only to realize that, but also to make an attempt to obtain the correct data. This process is called error detection and error correction, which will be discussed in the next lesson.

Asynchronous communication (word-oriented)

In asynchronous communication, small, fixed-length words (usually 5 to 9 bits long) are transferred without any clock line or clock is recovered from the signal itself. Each word has a start bit (usually as a 0) before the first data bit of the word and a stop bit (usually as a 1) after the last data bit of the word, as shown in Fig. 3.1.10. The receiver's local clock is started when the receiver detects the 1-0 transition of the start bit, and the line is sampled in the middle of the fixed bit intervals (a bit interval is the inverse of the data rate). The sender outputs the bit at the agreed-upon rate, holding the line in the appropriate state for one bit interval for each bit, but using its own local clock to determine the length of these bit intervals. The receiver's clock and the sender's clock may not run at the same speed, so that there is a relative clock drift (this may be caused by variations in the crystals used, temperature, voltage, etc.). If the receiver's clock drifts too much relative to the sender's clock, then the bits may be sampled while the line is in transition from one state to another, causing the receiver to misinterpret the received data. There can be variable amount of gap between two frames as shown in Fig. 3.1.11.

Advantages of asynchronous character oriented mode of communication are summarized below:

- Simple to implement
- Self synchronization; Clock signal need not be sent
- Tolerance in clock frequency is possible
- The bits are sensed in the middle hence ± ½ bit tolerance is provided

This mode of data communication, however, suffers from high overhead incurred in data transmission. Data must be sent in multiples of the data length of the word, and the two or more bits of synchronization overhead compared to the relatively short data length causes the effective data rate to be rather low. For example, 11 bits are required to transmit 8 bits of data. In other words, baud rate (number of signal elements) is higher than data rate.

Character Oriented Framing

The first framing method uses a field in the header to specify the number of characters in the frame. When the data link-layer sees the character count, it knows how many characters follow, and hence where the end of the frame is. The trouble with this algorithm is that the count can be garbled by a transmission error. Even if the checksum is incorrect so the destination knows that the frame is bad, it still had no way of telling where the next frame starts. Sending a frame back to the source and asking for retransmission does not help either, since the destination doesn't know how many characters to skip over to the start of retransmission. For this reason the character count method is rarely used. Character-oriented framing assumes that character synchronization has already been achieved by the hardware. The sender uses special characters to indicate the start and end of frames, and may also use them to indicate header boundaries and to assist the receiver gain character synchronization. Frames must be of an integral character length.

Character stuffing

When a DLE character occurs in the header or the data portion of a frame, the sender must somehow let the receiver know that it is not intended to signal a control character. The sender does this by inserting an extra DLE character after the one occurring inside the frame, so that when the receiver encounters two DLEs in a row, it immediately deletes one and interpret the other as header or data.

The main disadvantage of this method is that it is closely tied to 8-bit characters in general and the ASCII character code in particular. As networks grow, this disadvantage of embedding the character code in framing mechanism becomes more and more obvious, so a new technique had to be developed to allow arbitrary sized character. Bit-oriented frame synchronization and bit stuffing is used that allow data frames to contain an arbitrary number of bits and allow character code with arbitrary number of bits per character.

Data Rate Measures

• The raw data rate (the number of bits that the transmitter can per second without formatting) is only the starting point. There may be overhead for synchronization, for framing, for error checking, for headers and trailers, for retransmissions, etc.

• Utilization may mean more than one thing. When dealing with network monitoring and management, it refers to the fraction of the resource actually used (for useful data and for overhead, retransmissions, etc.). In this context, utilization refers to the fraction of the channel that is available for actual data transmission to the next higher layer. It is the ratio of data bits per protocol data unit (PDU) to the total size of the PDU, including synchronization, headers, etc. In other words, it is the ratio of the time spent actually sending useful data to the time it takes to transfer that data and its attendant overhead. The effective data rate at a layer is the net data rate available to the next higher layer. Generally this is the utilization times the raw data rate.

DTE-DCE Interface

As two persons intending to communicate must speak in the same language, for successful communication between two computer systems or between a computer and a peripheral, a natural understanding between the two is essential. In case of two persons a common language known to both of them is used. In case of two computers or a computer and an appliance, this understanding can be ensured with the help of a standard, which should be followed by both the parties. Standards are usually recommended by some International bodies, such as, Electronics Industries Association (EIA), The Institution of Electrical and Electronic Engineers (IEEE), etc. The EIA and ITU-T have been involved in developing standards for the DTE-DCE interface known as EIA-232, EIA-442, etc and ITU-T standards are known as V series or X series. The standards should normally define the following four important attributes:

Mechanical: The mechanical attribute concerns the actual physical connection between the two sides. Usually various signal lines are bundled into a cable with a terminator plug, male or female at each end. Each of the systems, between which communication is to be established, provide a plug of opposite gender for connecting the terminator plugs of the cable, thus establishing the physical connection. The mechanical part specifies cables and connectors to be used to link two systems

Electrical: The Electrical attribute relates to the voltage levels and timing of voltage changes. They in turn determine the data rates and distances that can be used for

communication. So the electrical part of the standard specifies voltages, Impedances and timing requirements to be satisfied for reliable communication

Functional: Functional attribute pertains to the function to be performed, by associating meaning to the various signal lines. Functions can be typically classified into the broad categories of data control, timing and ground. This component of standard specifies the signal pin assignments and signal definition of each of the pins used for interfacing the devices

Procedural: The procedural attribute specifies the protocol for communication, i.e. the sequence of events that should be followed during data transfer, using the functional characteristic of the interface.

A variety of standards exist, some of the most popular interfaces are presented in this section

Flow Control and Error Control

Introduction

As we have mentioned earlier, for reliable and efficient data communication a great deal of coordination is necessary between at least two machines. Some of these are necessary because of the following constraints:

- Both sender and receiver have limited speed
- Both sender and receiver have limited memory

It is necessary to satisfy the following requirements:

- A fast sender should not overwhelm a slow receiver, which must perform a certain amount of processing before passing the data on to the higher-level software.
- If error occur during transmission, it is necessary to devise mechanism to correct it

The most important functions of Data Link layer to satisfy the above requirements are **error control** and **flow control**. Collectively, these functions are known as **data link control**, as discussed in this lesson.

Flow Control is a technique so that transmitter and receiver with different speed characteristics can communicate with each other. Flow control ensures that a transmitting station, such as a server with higher processing capability, does not overwhelm a receiving station, such as a desktop system, with lesser processing capability. This is where there is an orderly flow of transmitted data between the source and the destination.

Error Control involves both error detection and error correction. It is necessary because errors are inevitable in data communication, in spite of the use of better equipment and reliable transmission media based on the current technology. In the preceding lesson we have already discussed how errors can be detected. In this lesson we shall discuss how error control is performed based on retransmission of the corrupted data. When an error is detected, the receiver can have the specified frame retransmitted by the sender. This process is commonly known as **Automatic Repeat Request (ARQ).**

For example, Internet's Unreliable Delivery Model allows packets to be discarded if network resources are not available, and demands that ARQ protocols make provisions for retransmission.

Flow Control

Modern data networks are designed to support a diverse range of hosts and communication mediums. Consider a 933 MHz Pentium-based host transmitting data to a 90 MHz 80486/SX. Obviously, the Pentium will be able to drown the slower processor with data. Likewise, consider two hosts, each using an Ethernet LAN, but with the two Ethernets connected by a 56 Kbps modem link. If one host begins transmitting to the other at Ethernet speeds, the modem link will quickly become overwhelmed. In both cases, flow control is needed to pace the data transfer at an acceptable speed.

Flow Control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver. The flow of data should not be allowed to overwhelm the receiver. Receiver should also be able to inform the transmitter before its limits (this limit may be amount of memory used to store the incoming data or the processing power at the receiver end) are reached and the sender must send fewer frames. Hence, Flow control refers to the set of procedures used to restrict the amount of data the transmitter can send before waiting for acknowledgment.

There are two methods developed for flow control namely Stop-and-wait and Sliding-window. Stop-and-wait is also known as Request/reply sometimes. Request/reply (Stop-and-wait) flow control requires each data packet to be acknowledged by the remote host before the next packet is sent. This is discussed in detail in the following subsection. Sliding window algorithms, used by TCP, permit multiple data packets to be in simultaneous transit, making more efficient use of network Stop-and-Wait

This is the simplest form of flow control where a sender transmits a data frame. After receiving the frame, the receiver indicates its willingness to accept another frame by sending back an ACK frame acknowledging the frame just received. The sender must wait until it receives the ACK frame before sending the next data frame.This is sometimes referred to as ping-pong behavior, request/reply is simple to understand and easy to implement, but not very efficient. In LAN environment with fast links, this isn't much of a concern, but WAN links will spend most of their time idle, especially if several hops are required.

The blue arrows show the sequence of data frames being sent across the link from the sender (top to the receiver (bottom). The protocol relies on two-way transmission (full duplex or half duplex) to allow the receiver at the remote node to return frames acknowledging the successful transmission. The acknowledgements are shown in green in the diagram, and flow back to the original sender. A small processing delay may be introduced between reception of the last byte of a Data PDU and generation of the corresponding ACK.

Major drawback of Stop-and-Wait Flow Control is that only one frame can be in transmission at a time, this leads to inefficiency if propagation delay is much longer than the transmission delay.

Stop-and Wait protocol	Some protocols pretty much require stop-and-wait behavior. For example, Internet's Remote Procedure Call (RPC) Protocol is used to implement subroutine calls from a program on one machine to library routines on another machine. Since most programs are single threaded, the sender has little choice but to wait for a reply before continuing the program and possibly sending another request.

Link Utilization in Stop-and-Wait Let us assume the following:
Transmission time: The time it takes for a station to transmit a frame (normalized to a value of 1).
Propagation delay: The time it takes for a bit to travel from sender to receiver (expressed as a).
a < 1 :The frame is sufficiently long such that the first bits of the frame arrive at the destination before the source has completed transmission of the frame.
– a > 1: Sender completes transmission of the entire frame before the leading bits of the frame arrive at the receiver.
– The link utilization U = 1/(1+2a),
a = Propagation time / transmission time

It is evident from the above equation that the link utilization is strongly dependent on the ratio of the propagation time to the transmission time. When the propagation time is small, as in case of LAN environment, the link utilization is good. But, in case of long propagation delays, as in case of satellite communication, the utilization can be very poor. To improve the link utilization, we can use the following (sliding-window) protocol instead of using stop-and-wait protocol.

Sliding Window

With the use of multiple frames for a single message, the stop-and-wait protocol does not perform well. Only one frame at a time can be in transit. In stop-and-wait flow control, if a > 1, serious inefficiencies result. Efficiency can be greatly improved by allowing multiple frames to be in transit at the same time. Efficiency can also be improved by making use of the full-duplex line. To keep track of the frames, sender station sends sequentially numbered frames. Since the sequence number to be used occupies a field in the frame, it should be of limited size. If the header of the frame allows k bits, the

sequence numbers range from 0 to 2k – 1. Sender maintains a list of sequence numbers that it is allowed to send (sender window). The size of the sender's window is at most 2k – 1. The sender is provided with a buffer equal to the window size. Receiver also maintains a window of size 2k – 1. The receiver acknowledges a frame by sending an ACK frame that includes the sequence number of the next frame expected. This also explicitly announces that it is prepared to receive the next N frames, beginning with the

number specified. This scheme can be used to acknowledge multiple frames. It could receive frames 2, 3, 4 but withhold ACK until frame 4 has arrived. By returning an ACK with sequence number 5, it acknowledges frames 2, 3, 4 in one go. The receiver needs a buffer of size 1.

Sliding window algorithm is a method of flow control for network data transfers. TCP, the Internet's stream transfer protocol, uses a sliding window algorithm.

A sliding window algorithm places a buffer between the application program and the network data flow. For TCP, the buffer is typically in the operating system kernel, but this is more of an implementation detail than a hard-and-fast requirement.	Buffer in sliding window

Data received from the network is stored in the buffer, from where the application can read at its own pace. As the application reads data, buffer space is freed up to accept more input from the network. The window is the amount of data that can be "read ahead" - the size of the buffer, less the amount of valid data stored in it. Window announcements are used to inform the remote host of the current window size.

Sender sliding Window: At any instant, the sender is permitted to send frames with sequence numbers in a certain range (the sending window)
Receiver sliding Window: The receiver always maintains a window of size 1 as shown in It looks for a specific frame (frame 4 as shown in the figure) to arrive in a specific order. If it receives any other frame (out of order), it is discarded and it needs to be resent. However, the receiver window also slides by one as the specific frame is received and accepted as shown in the figure. The receiver acknowledges a frame by sending an ACK frame that includes the sequence number of the next frame expected. This also explicitly announces that it is prepared to receive the next N frames, beginning with the number specified. This scheme can be used to acknowledge multiple frames. It could receive frames 2, 3, 4 but withhold ACK until frame 4 has arrived. By returning an ACK with sequence number 5, it acknowledges frames 2, 3, 4 at one time. The receiver needs a buffer of size 1.
Receiver sliding window

On the other hand, if the local application can process data at the rate it's being transferred; sliding window still gives us an advantage. If the window size is larger than the packet size, then multiple packets can be outstanding in the network, since the sender knows that buffer space is available on the receiver to hold all of them. Ideally, a steady-state condition can be reached where a series of packets (in the forward direction) and window announcements (in the reverse direction) are constantly in transit. As each new window announcement is received by the sender, more data packets are transmitted. As the application reads data from the buffer (remember, we're assuming the application can

keep up with the network), more window announcements are generated. Keeping a series of data packets in transit ensures the efficient use of network resources.

The link utilization in case of Sliding Window Protocol
U = 1, for N > 2a + 1
N/(1+2a), for N < 2a + 1
Where N = the window size,
and a = Propagation time / transmission time

Error Control Techniques

When an error is detected in a message, the receiver sends a request to the transmitter to retransmit the ill-fated message or packet. The most popular retransmission scheme is known as Automatic-Repeat-Request (ARQ). Such schemes, where receiver asks transmitter to re-transmit if it detects an error, are known as reverse error correction techniques.

Stop-and-Wait ARQ

In Stop-and-Wait ARQ, which is simplest among all protocols, the sender (say station A) transmits a frame and then waits till it receives positive acknowledgement (ACK) or negative acknowledgement (NACK) from the receiver (say station B). Station B sends an ACK if the frame is received correctly, otherwise it sends NACK. Station A sends a new frame after receiving ACK; otherwise it retransmits the old frame, if it receives a NACK.
Stop-And-Wait ARQ technique
To tackle the problem of a lost or damaged frame, the sender is equipped with a timer. In case of a lost ACK, the sender transmits the old frame. In the Fig. 3.3.7, the second PDU of Data is lost during transmission. The sender is unaware of this loss, but starts a timer after sending each PDU.

In this case no ACK is received, and the timer counts down to zero and triggers retransmission of the same PDU by the sender. The sender always starts a timer following transmission, but in the second transmission receives an ACK PDU before the timer expires, finally indicating that the data has now been received by the remote node.
Retransmission due to lost frame
The receiver now can identify that it has received a duplicate frame from the label of the frame and it is discarded

To tackle the problem of damaged frames, say a frame that has been corrupted during the transmission due to noise, there is a concept of NACK frames, i.e. Negative Acknowledge frames. Receiver transmits a NACK frame to the sender if it founds the received frame to be corrupted. When a NACK is received by a transmitter before the time-out, the old frame is sent again
Retransmission due to damaged frame

The main advantage of stop-and-wait ARQ is its simplicity. It also requires minimum buffer size. However, it makes highly inefficient use of communication links, particularly when ‘a’ is large.

Go-back-N ARQ

The most popular ARQ protocol is the go-back-N ARQ, where the sender sends the frames continuously without waiting for acknowledgement. That is why it is also called as continuous ARQ. As the receiver receives the frames, it keeps on sending ACKs or a NACK, in case a frame is incorrectly received. When the sender receives a NACK, it retransmits the frame in error plus all the succeeding frames as shown in Fig.3.3.9. Hence, the name of the protocol is go-back-N ARQ. If a frame is lost, the receiver sends NAK after receiving the next frame as shown in Fig. 3.3.10. In case there is long delay before sending the NAK, the sender will resend the lost frame after its timer times out. If the ACK frame sent by the receiver is lost, the sender resends the frames after its timer times out Assuming full-duplex transmission, the receiving end sends piggybacked acknowledgement by using some number in the ACK field of its data frame. Let us assume that a 3-bit sequence number is used and suppose that a station sends frame 0 and gets back an RR1, and then sends frames 1, 2, 3, 4, 5, 6, 7, 0 and gets another RR1.This might either mean that RR1 is a cumulative ACK or all 8 frames were damaged. This ambiguity can be overcome if the maximum window size is limited to 7, i.e. for a k-bit sequence number field it is limited to 2k-1. The number N (=2k-1) specifies how many frames can be sent without receiving acknowledgement.

If no acknowledgement is received after sending N frames, the sender takes the help of a timer. After the time-out, it resumes retransmission. The go-back-N protocol also takes care of damaged frames and damaged ACKs. This scheme is little more complex than the previous one but gives much higher throughput.

Assuming full-duplex transmission, the receiving end sends piggybacked acknowledgement by using some number in the ACK field of its data frame. Let us assume that a 3-bit sequence number is used and suppose that a station sends frame 0 and gets back an RR1, and then sends frames 1, 2, 3, 4, 5, 6, 7, 0 and gets another RR1.This might either mean that RR1 is a cumulative ACK or all 8 frames were damaged. This ambiguity can be overcome if the maximum window size is limited to 7, i.e. for a k-bit sequence number field it is limited to 2k-1. The number N (=2k-1) specifies how many frames can be sent without receiving acknowledgement. If no acknowledgement is received after sending N frames, the sender takes the help of a timer. After the time-out, it resumes retransmission. The go-back-N protocol also takes care of damaged frames and damaged ACKs. This scheme is little more complex than the previous one but gives much higher throughput.

Selective-Repeat ARQ

The selective-repetitive ARQ scheme retransmits only those for which NAKs are received or for which timer has expired, This is the most efficient among the ARQ schemes, but the sender must be more complex so that it can send out-of-order frames. The receiver also must have storage space to store the post-NAK frames and processing power to reinsert frames in proper sequence.

HDLC

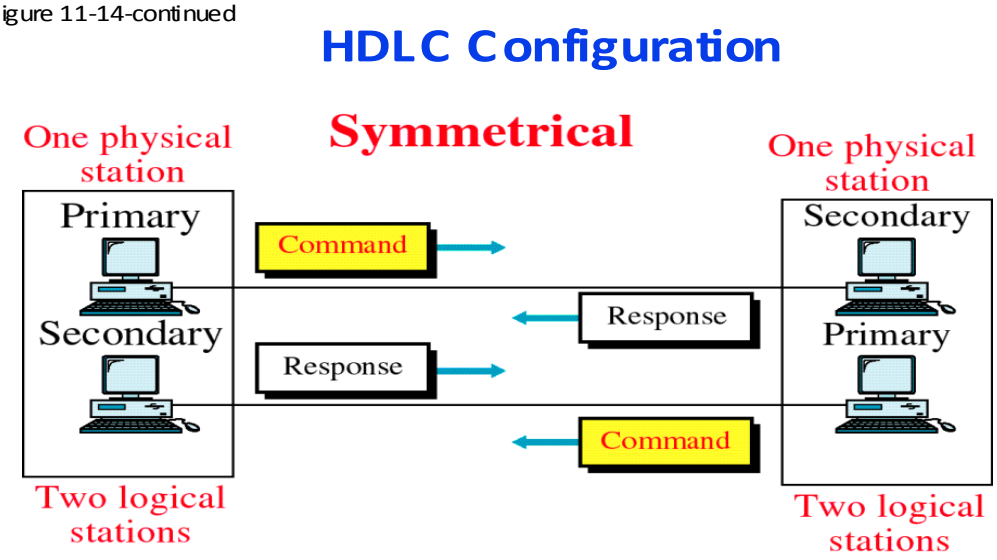
Introduction

HDLC is a bit-oriented protocol. It was developed by the International Organization for Standardization (ISO). It falls under the ISO standards ISO 3309 and ISO 4335. It specifies a packitization standard for serial links. It has found itself being used throughout the world. It has been so widely implemented because it supports both half-duplex and

full-duplex communication lines, point-to-point (peer to peer) and multi-point networks, and switched or non-switched channels. HDLC supports several modes of operation, including a simple sliding-window mode for reliable delivery. Since Internet provides retransmission at higher levels (i.e., TCP), most Internet applications use HDLC's unreliable delivery mode, Unnumbered Information.

Other benefits of HDLC are that the control information is always in the same position, and specific bit patterns used for control differ dramatically from those in representing data, which reduces the chance of errors. It has also led to many subsets. Two subsets widely in use are Synchronous Data Link Control (SDLC) and Link Access Procedure-Balanced (LAP-B).

Figure 11-14-continued



In this lesson we shall consider the following aspects of HDLC:

- Stations and Configurations
- Operational Modes
- Non-Operational Modes
- Frame Structure
- Commands and Responses
- HDLC Subsets (SDLC and LAPB)

HDLC Stations and Configurations

HDLC specifies the following three types of stations for data link control:

- Primary Station
- Secondary Station
- Combined Station

Primary Station

Within a network using HDLC as its data link protocol, if a configuration is used in which there is a primary station, it is used as the controlling station on the link. It has the

responsibility of controlling all other stations on the link (usually secondary stations). A primary issues commands and secondary issues responses. Despite this important aspect of being on the link, the primary station is also responsible for the organization of data flow on the link. It also takes care of error recovery at the data link level (layer 2 of the OSI model).

Secondary Station

If the data link protocol being used is HDLC, and a primary station is present, a secondary station must also be present on the data link. The secondary station is under the control of the primary station. It has no ability, or direct responsibility for controlling the link. It is only activated when requested by the primary station. It only responds to the primary station. The secondary station's frames are called responses. It can only send response frames when requested by the primary station. A primary station maintains a separate logical link with each secondary station.

Combined Station

A combined station is a combination of a primary and secondary station. On the link, all combined stations are able to send and receive commands and responses without any permission from any other stations on the link. Each combined station is in full control of itself, and does not rely on any other stations on the link. No other stations can control any combined station.

HDLC also defines three types of configurations for the three types of stations. The word configuration refers to the relationship between the hardware devices on a link.

Following are the three configurations defined by HDLC:

• Unbalanced Configuration
• Balanced Configuration
• Symmetrical Configuration

Unbalanced Configuration

The unbalanced configuration in an HDLC link consists of a primary station and one or more secondary stations. The unbalanced condition arises because one station controls the other stations. In an unbalanced configuration, any of the following can be used:

• Full-Duplex or Half-Duplex operation
• Point to Point or Multi-point networks

Balanced Configuration

The balanced configuration in an HDLC link consists of two or more combined stations. Each of the stations has equal and complimentary responsibility compared to each other. Balanced configurations can use only the following:

• Full - Duplex or Half - Duplex operation
• Point to Point networks

Symmetrical Configuration

This third type of configuration is not widely in use today. It consists of two independent point-to-point, unbalanced station configurations. In this configuration, each station has a primary and secondary status. Each station is logically considered as two stations.

HDLC Operational Modes

A mode in HDLC is the relationship between two devices involved in an exchange; the mode describes who controls the link. Exchanges over unbalanced configurations are

always conducted in normal response mode. Exchanges over symmetric or balanced configurations can be set to specific mode using a frame design to deliver the command. HDLC offers three different modes of operation. These three modes of operations are:

• Normal Response Mode (NRM)
• Asynchronous Response Mode (ARM)
• Asynchronous Balanced Mode (ABM)

Normal Response Mode

This is the mode in which the primary station initiates transfers to the secondary station. The secondary station can only transmit a response when, and only when, it is instructed to do so by the primary station. In other words, the secondary station must receive explicit permission from the primary station to transfer a response. After receiving permission from the primary station, the secondary station initiates its transmission. This transmission from the secondary station to the primary station may be much more than just an acknowledgment of a frame. It may in fact be more than one information frame. Once the last frame is transmitted by the secondary station, it must wait once again from explicit permission to transfer anything, from the primary station. Normal Response Mode is only used within an unbalanced configuration.

Asynchronous Response Mode

In this mode, the primary station doesn't initiate transfers to the secondary station. In fact, the secondary station does not have to wait to receive explicit permission from the primary station to transfer any frames. The frames may be more than just acknowledgment frames. They may contain data, or control information regarding the status of the secondary station. This mode can reduce overhead on the link, as no frames need to be transferred in order to give the secondary station permission to initiate a transfer. However, some limitations do exist. Due to the fact that this mode is asynchronous, the secondary station must wait until it detects and idle channel before it can transfer any frames. This is when the ARM link is operating at half-duplex. If the ARM link is operating at full duplex, the secondary station can transmit at any time. In this mode, the primary station still retains responsibility for error recovery, link setup, and link disconnection.

Synchronous Balanced Mode

`This mode is used in case of combined stations. There is no need for permission on the part of any station in this mode. This is because combined stations do not require any sort of instructions to perform any task on the link.

Normal Response Mode is used most frequently in multi-point lines, where the primary station controls the link. Asynchronous Response Mode is better for point-to-point links, as it reduces overhead. Asynchronous Balanced Mode is not used widely today. The "asynchronous" in both ARM and ABM does not refer to the format of the data on the link. It refers to the fact that any given station can transfer frames without explicit permission or instruction from any other station.

HDLC Non-Operational Modes

HDLC also defines three non-operational modes. These three non-operational modes are:

• Normal Disconnected Mode (NDM)

• Asynchronous Disconnected Mode (ADM)
• Initialization Mode (IM)

The two disconnected modes (NDM and ADM) differ from the operational modes in that the secondary station is logically disconnected from the link (note the secondary station is not physically disconnected from the link). The IM mode is different from the operations modes in that the secondary station's data link control program is in need of regeneration or it is in need of an exchange of parameters to be used in an operational mode.

HDLC Frame Structure

There are three different types of frames as shown in Fig. 3.4.4 and the size of different fields are shown Table 3.4.1.

Table 3.4.1 Size of different fields

Field Name	Size(in bits)
Flag Field(F)	8 bits
Address Field(A)	8 bits
Control Field(C)	8 or 16 bits
Information Field(I) OR Data	Variable; Not used in some frames
Frame Check Sequence(FCS)	16 or 32 bits
Closing Flag Field(F)	8 bits

The Flag field

Every frame on the link must begin and end with a flag sequence field (F). Stations attached to the data link must continually listen for a flag sequence. The flag sequence is an octet looking like 01111110. Flags are continuously transmitted on the link between frames to keep the link active. Two other bit sequences are used in HDLC as signals for the stations on the link. These two bit sequences are:

• Seven 1's, but less than 15 signal an abort signal. The stations on the link know there is a problem on the link.
• 15 or more 1's indicate that the channel is in an idle state.

The time between the transmissions of actual frames is called the interframe time fill. The interframe time fill is accomplished by transmitting continuous flags between frames. The flags may be in 8 bit multiples.

HDLC is a code-transparent protocol. It does not rely on a specific code for interpretation of line control. This means that if a bit at position N in an octet has a specific meaning, regardless of the other bits in the same octet. If an octet has a bit sequence of 01111110, but is not a flag field, HLDC uses a technique called bit-stuffing to differentiate this bit sequence from a flag field as we have discussed in the previous lesson.

At the receiving end, the receiving station inspects the incoming frame. If it detects 5 consecutive 1's it looks at the next bit. If it is a 0, it pulls it out. If it is a 1, it looks at the 8th bit. If the 8th bit is a 0, it knows an abort or idle signal has been sent. It then proceeds to inspect the following bits to determine appropriate action. This is the manner in which

HDLC achieves code-transparency. HDLC is not concerned with any specific bit code inside the data stream. It is only concerned with keeping flags unique.

The Address field

The address field (A) identifies the primary or secondary stations involvement in the frame transmission or reception. Each station on the link has a unique address. In an unbalanced configuration, the A field in both commands and responses refer to the secondary station. In a balanced configuration, the command frame contains the destination station address and the response frame has the sending station's address.

The Control field

HDLC uses the control field (C) to determine how to control the communications process. This field contains the commands, responses and sequences numbers used to maintain the data flow accountability of the link, defines the functions of the frame and initiates the logic to control the movement of traffic between sending and receiving stations. There three control field formats:

• Information Transfer Format: The frame is used to transmit end-user data between two devices.

• Supervisory Format: The control field performs control functions such as acknowledgment of frames, requests for re-transmission, and requests for temporary suspension of frames being transmitted. Its use depends on the operational mode being used.

• Unnumbered Format: This control field format is also used for control purposes. It is used to perform link initialization, link disconnection and other link control functions.

The Poll/Final Bit (P/F)

The 5th bit position in the control field is called the poll/final bit, or P/F bit. It can only be recognized when it is set to 1. If it is set to 0, it is ignored. The poll/final bit is used to provide dialogue between the primary station and secondary station. The primary station uses P=1 to acquire a status response from the secondary station. The P bit signifies a poll. The secondary station responds to the P bit by transmitting a data or status frame to the primary station with the P/F bit set to F=1. The F bit can also be used to signal the end of a transmission from the secondary station under Normal Response Mode.

The Information field or Data field

This field is not always present in a HDLC frame. It is only present when the Information Transfer Format is being used in the control field. The information field contains the actually data the sender is transmitting to the receiver in an I-Frame and network management information in U-Frame.

The Frame check Sequence field

This field contains a 16-bit, or 32-bit cyclic redundancy check bits. It is used for error detection.

HDLC Commands and Responses

The set of commands and responses in HDLC is summarized in Table 3.4.2.

Information transfer format command and response (I-Frame)

The function of the information command and response is to transfer sequentially numbered frames, each containing an information field, across the data link.

Supervisory format command and responses (S-Frame)

Supervisory (S) commands and responses are used to perform numbered supervisory functions such as acknowledgment, polling, temporary suspension of information transfer, or error recovery. Frames with the S format control field cannot contain an information field. A primary station may use the S format command frame with the P bit set to 1 to request a response from a secondary station regarding its status. Supervisory Format commands and responses are as follows:

• Receive Ready (RR) is used by the primary or secondary station to indicate that it is ready to receive an information frame and/or acknowledge previously received frames.

• Receive Not Ready (RNR) is used to indicate that the primary or secondary station is not ready to receive any information frames or acknowledgments.

• Reject (REJ) is used to request the retransmission of frames.

• Selective Reject (SREJ) is used by a station to request retransmission of specific frames. An SREJ must be transmitted for each erroneous frame; each frame is treated as a separate error. Only one SREJ can remain outstanding on the link at any one time.

TABLE 3.4.2 HDLC Commands and Responses

Information Transfer Format Commands	Information Transfer Format Responses
I - Information	I - Information
Supervisory Format Commands	Supervisory Format Responses
RR - Receive ready	RR - Receive ready
RNR - Receive not ready	RNR - Receive not ready
REJ - Reject	REJ - Reject
SREJ - Selective reject	SREJ - Selective reject
Unnumbered Format Commands	Unnumbered Format Commands
SNRM - Set Normal Response Mode	UA - Unnumbered Acknowledgment
SARM - Set Asynchronous Response Mode	DM - Disconnected Mode
SABM - Set Asynchronous Balanced Mode	RIM - Request Initialization Mode
DISC - Disconnect	RD - Request Disconnect
SNRME - Set Normal Response Mode Extended	UI - Unnumbered Information
SARME - Set Asynchronous Response Mode Extended	XID - Exchange Identification
SABME - Set Asynchronous Balanced Mode Extended	FRMR - Frame Reject
SIM - Set Initialization Mode	TEST - Test
UP - Unnumbered Poll	
UI - Unnumbered Information	
XID - Exchange identification	
RSET - Reset	

TEST - Test

Unnumbered Format Commands and responses (U-Frame)

The unnumbered format commands and responses are used to extend the number of data link control functions. The unnumbered format frames have 5 modifier bits, which allow for up to 32 additional commands and 32 additional response functions. Below, 13 command functions, and 8 response functions are described.

• Set Normal Response Mode (SNRM) places the secondary station into NRM. NRM does not allow the secondary station to send any unsolicited frames. Hence the primary station has control of the link.

• Set Asynchronous Response Mode (SARM) allows a secondary station to transmit frames without a poll from the primary station.

• Set Asynchronous Balanced Mode (SABM) sets the operational mode of the link to ABM.

• Disconnect (DISC) places the secondary station in to a disconnected mode.

• Set Normal Response Mode Extended (SNRME) increases the size of the control field to 2 octets instead of one in NRM. This is used for extended sequencing. The same applies for SARME and SABME.

• Set Initialization Mode (SIM) is used to cause the secondary station to initiate a station-specific procedure(s) to initialize its data link level control functions.

• Unnumbered Poll (UP) polls a station without regard to sequencing or acknowledgment.

• Unnumbered Information (UI) is used to send information to a secondary station.

• Exchange Identification (XID) is used to cause the secondary station to identify itself and provide the primary station identifications characteristics of itself.

• Reset (RSET) is used to reset the receive state variable in the addressed station.

• Test (TEST) is used to cause the addressed secondary station to respond with a TEST response at the first response opportunity. It performs a basic test of the data link control.

• Unnumbered Acknowledgment (UA) is used by the secondary station to acknowledge the receipt and acceptance of an SNRM, SARM, SABM, SNRME, SARME, SABME, RSET, SIM, or DISC commands.

•

Disconnected Mode (DM) is transmitted from a secondary station to indicate it is in disconnected mode(non-operational mode.)

• Request Initialization Mode (RIM) is a request from a secondary station for initialization to a primary station. Once the secondary station sends RIM, it can only respond to SIM, DSIC, TEST or XID commands.

• Request Disconnect (RD) is sent by the secondary station to inform the primary station that it wishes to disconnect from the link and go into a non-operational mode(NDM or ADM.

• Frame Reject (FRMR) is used by the secondary station in an operation mode to report that a condition has occurred in transmission of a frame and retransmission of the frame will not correct the condition.

HDLC Subsets

Many other data link protocols have been derived from HDLC. However, some of them reach beyond the scope of HDLC. Two other popular offsets of HDLC are Synchronous Data Link Control (SDLC), and Link Access Protocol, Balanced (LAP-B). SDLC is used and developed by IBM. It is used in a variety of terminal to computer applications. It is

also a part of IBM's SNA communication architecture. LAP-B was developed by the ITU-T. It is derived mainly from the asynchronous response mode (ARM) of HDLC. It is commonly used for attaching devices to packet-switched networks.

• Combined Station: A combined station is a combination of a primary and secondary station. On the link, all combined stations are able to send and receive commands and responses without any permission from any other stations on the link.

Switched Communication Networks

Lesson

1 Switching Techniques: Circuit Switching

Specific Instructional Objectives

At the end of this lesson the student will be able to:

• Understand the need for circuit switching
• Specify the components of a switched communication network
• Explain how circuit switching takes place
• Explain how switching takes place using space-division and time-division switching
• Explain how routing is performed
• Explain how signalling in performed

Introduction

When there are many devices, it is necessary to develop suitable mechanism for communication between any two devices. One alternative is to establish point-to-point communication between each pair of devices using mesh topology. However, mesh topology is impractical for large number of devices, because the number of links increases exponentially (n(n-1)/2, where n is the number of devices) with the number of devices. A better alternative is to use switching techniques leading to switched communication network. In the switched network methodology, the network consists of a set of interconnected nodes, among which information is transmitted from source to destination via different routes, which is controlled by the switching mechanism. A basic model of a switched communication is shown in Fig. 4.1.1. The end devices that wish to communicate with each other are called stations. The switching devices are called nodes. Some nodes connect to other nodes and some are to connected to some stations. Key features of a switched communication network are given below:

• Network Topology is not regular.
• Uses FDM or TDM for node-to-node communication.
• There exist multiple paths between a source-destination pair for better network reliability.
• The switching nodes are not concerned with the contents of data.

• Their purpose is to provide a switching facility that will move data from node to node until they reach the destination.

The switching performed by different nodes can be categorized into the following three types:

• Circuit Switching
• Packet Switching
• Message Switching

Figure 14-1

Switched Network

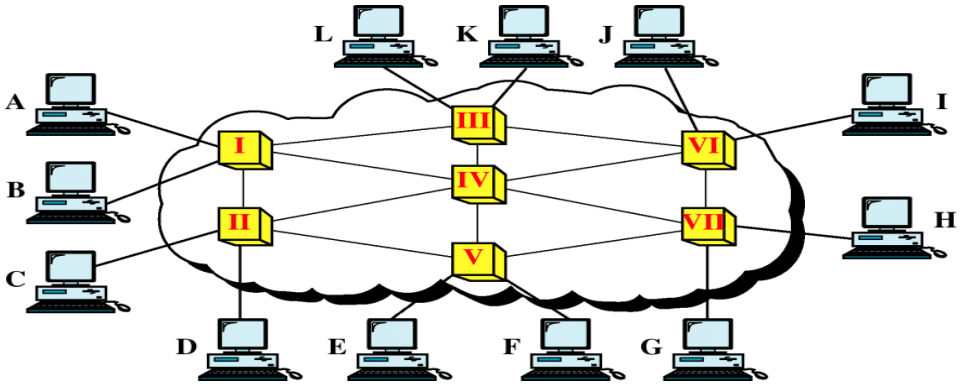


Figure 14-3

Circuit-Switched Network

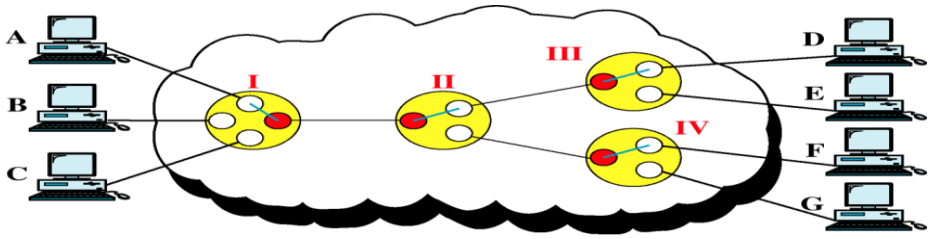


Figure 14-14

Datagram Approach

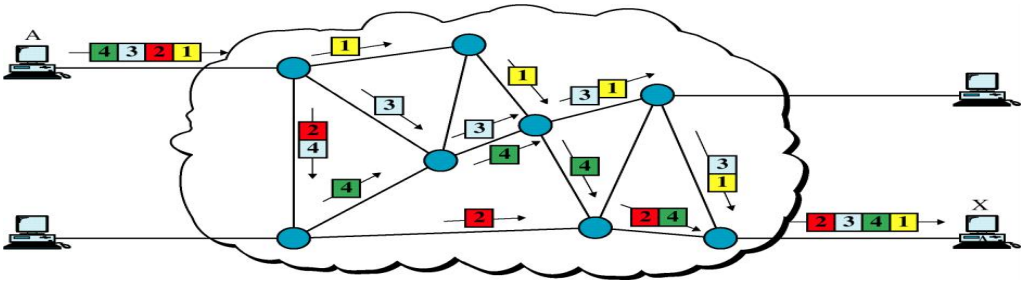
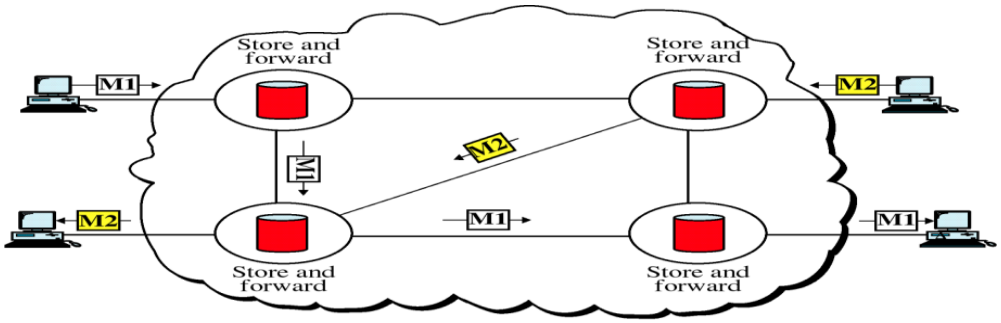


Figure 14-17

Message Switching



Circuit switching Technique

Communication via circuit switching implies that there is a dedicated communication path between the two stations. The path is a connected through a sequence of links between network nodes. On each physical link, a logical channel is dedicated to the connection. Circuit switching is commonly used technique in telephony, where the caller sends a special message with the address of the callee (i.e. by dialling a number) to state its destination. It involved the following three distinct steps,

Circuit Establishment: To establish an end-to-end connection before any transfer of data. Some segments of the circuit may be a dedicated link, while some other segments may be shared.

Data transfer:

- Transfer data is from the source to the destination.
- The data may be analog or digital, depending on the nature of the network.
- The connection is generally full-duplex.

Circuit disconnect:

- Terminate connection at the end of data transfer.

- Signals must be propagated to deallocate the dedicated resources.

Thus the actual physical electrical path or circuit between the source and destination host must be established before the message is transmitted. This connection, once established, remains exclusive and continuous for the complete duration of information exchange and the circuit becomes disconnected only when the source wants to do so.

Switching Node

Let us consider the operation of a single circuit switched node comprising a collection of stations attached to a central switching unit, which establishes a dedicated path between any two devices that wish to communicate.

Major elements of a single-node network are summarized below:

• Digital switch: That provides a transparent (full-duplex) signal path between any pair of attached devices.

• Network interface: That represents the functions and hardware needed to connect digital devices to the network (like telephones).

• Control unit: That establishes, maintains, and tears down a connection.

The simplified schematic diagram of a switching node is shown in Fig. 4.1.3. An important characteristic of a circuit-switch node is whether it is blocking or non-blocking. A blocking network is one, which may be unable to connect two stations because all possible paths between them are already in use. A non-blocking network permits all stations to be connected (in pairs) at once and grants all possible connection requests as long as the called party is free. For a network that supports only voice traffic, a blocking configuration may be acceptable, since most phone calls are of short duration. For data applications, where a connection may remain active for hours, non-blocking configuration is desirable.

Circuit switching uses any of the three technologies: Space-division switches, Time-division switches or a combination of both. In Space-division switching, the paths in the circuit are separated with each other spatially, i.e. different ongoing connections, at a same instant of time, uses different switching paths, which are separated spatially. This was originally developed for the analog environment, and has been carried over to the digital domain. Some of the space switches are crossbar switches, Multi-stage switches (e.g. Omega Switches). A crossbar switch is shown in Fig. 4.1.4. Basic building block of the switch is a metallic crosspoint or semiconductor gate that can be enabled or disabled by a control unit.

• The number of crosspoints grows with the square of the number of attached stations.

• Costly for a large switch.

• The failure of a crosspoint prevents connection between the two devices whose lines intersect at that crosspoint.

• The crosspoints are inefficiently utilized.

• Only a small fraction of crosspoints are engaged even if all of the attached devices are active.

Some of the above problems can be overcome with the help of multistage space division switches. By splitting the crossbar switch into smaller units and interconnecting them, it is possible to build multistage switches with fewer crosspoints.

Three-stage space division switch: In this case the number of crosspoints needed goes down from 64 to 40. There is more than one path through the network to connect two

endpoints, thereby increasing reliability. Multistage switches may lead to blocking. The problem may be tackled by increasing the number or size of the intermediate switches, which also increases the cost. The blocking feature is illustrated in Fig. 4.1.6. after setting up connections for 1-to-3 and 2-to-4, the switch cannot establish connections for 3-to-6 and 4-to-5.

Time Division Switching

Both voice and data can be transmitted using digital signals through the same switches. All modern circuit switches use digital time-division multiplexing (TDM) technique for establishing and maintaining circuits. Synchronous TDM allows multiple low-speed bit streams to share a high-speed line. A set of inputs is sampled in a round robin manner. The samples are organized serially into slots (channels) to form a recurring frame of slots. During successive time slots, different I/O pairings are enabled, allowing a number of connections to be carried over the shared bus. To keep up with the input lines, the data rate on the bus must be high enough so that the slots recur sufficiently frequently. For 100 full-duplex lines at 19.200 Kbps, the data rate on the bus must be greater than 1.92 Mbps. The source-destination pairs corresponding to all active connections are stored in the control memory. Thus the slots need not specify the source and destination addresses. Schematic diagram of time division switching.

Time-division switching uses time-division multiplexing to achieve switching, i.e. different ongoing connections can use same switching path but at different interleaved time intervals. There are two popular methods of time-division switching namely, Time-Slot Interchange (TSI) and the TDM bus. TSI changes the ordering of the slots based on desired connection and it has a random-access memory to store data and flip the time slots as shown in Fig. 4.1.8. The operation of a TSI is depicted in Fig. 4.1.9. As shown in the figure, writing can be performed in the memory sequentially, but data is read selectively. In TDM bus there are several input and outputs connected to a high-speed bus. During a time slot only one particular output switch is closed, so only one connection at a particular instant of time

Public Switched Telephone Networks

Public switched telephone network (PSTN) is an example of circuit-switched network. It's also known as Plain Old Telephone Service (POTS). The switching centres used for the switching are organised in different levels, namely: Regional offices (class 1), Section offices (class 2), primary offices (class 3), Toll offices (class 4) and finally End offices (class 5). Level 1 is at the highest level and Level 5 is the lowest level. Subscribers or the customers are directly connected to these end offices. And each office is connected directly to a number of offices at a level below and mostly a single office at higher level. Subscriber Telephones are connected, through Local Loops to end offices (or central offices). A small town may have only one end office, but large cities have several end offices. Many end offices are connected to one Toll office, which are connected to primary offices. Several primary offices are connected to a section office, which normally serves more than one state. All regional offices are connected using mesh topology. Accessing the switching station at the end offices is accomplished through dialling. In the past, telephone featured rotary or pulse dialling, in which digital signals were sent to the end office for each dialled digit. This type of dialling was prone to errors due to inconsistency in humans during dialling. Presently, dialling is accomplished by Touch-

Tone technique. In this method the user sends a small burst of frequency called dual tone, because it is a combination of two frequencies. This combination of frequencies sent depends on the row and column of the pressed pad.
The connections are multiplexed when have to send to a switching office, which is one level up. For example, Different connections will be multiplexed when they are to be forwarded from an end-office to Toll office.

Frame Relay

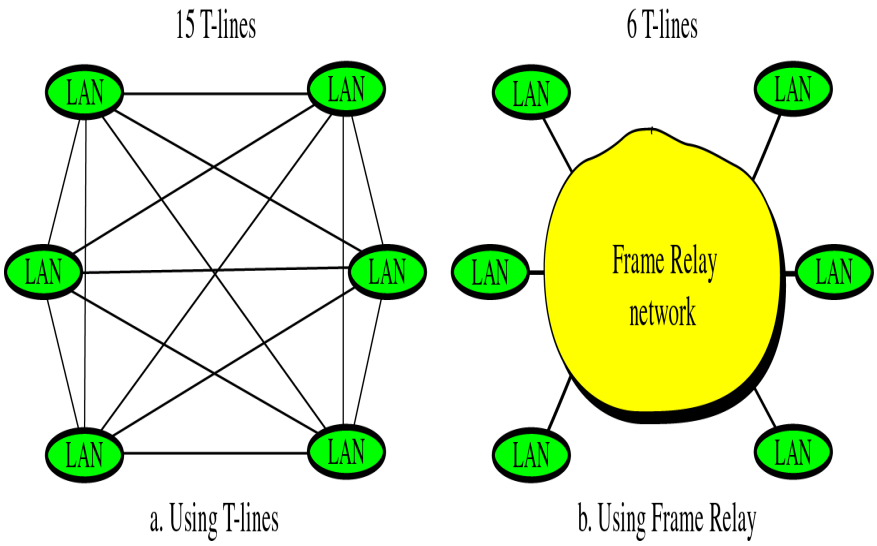


Figure 18-14

Frame Relay Frame

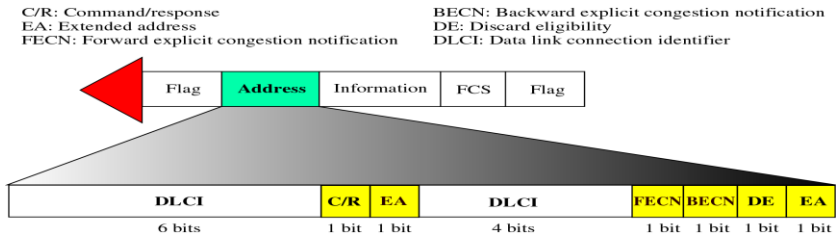
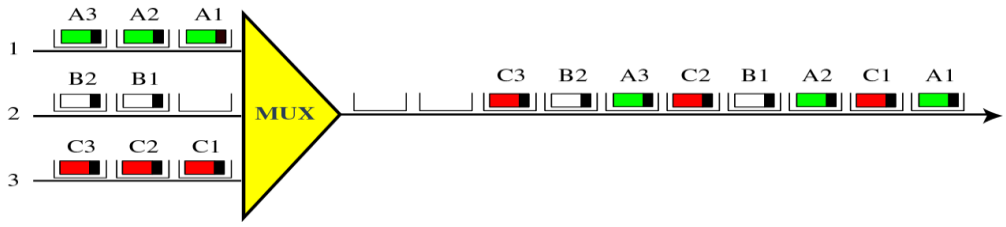


Figure 19-3

ATM Multiplexing



Introduction

Frame Relay is a high-performance WAN protocol that operates at the physical and data link layers of the OSI reference model. Frame Relay originally was designed for use across Integrated Services Digital Network (ISDN) interfaces. Today, it is used over a variety of other network interfaces as well. Frame Relay is a simplified form of Packet Switching, similar in principle to X.25, in which synchronous frames of data are routed to different destinations depending on header information. The biggest difference between Frame Relay and X.25 is that X.25 guarantees data integrity and network managed flow control at the cost of some network delays. Frame Relay switches packets end to end much faster, but there is no guarantee of data integrity at all.

As line speeds have increased from speeds below 64kbps to T1/E1 and beyond, the delays inherent in the store-and-forward mechanisms of X.25 become intolerable. At the same time, improvements in digital transmission techniques have reduced line errors to the extent that node-to-node error correction throughout the network is no longer necessary. The vast majority of Frame Relay traffic consists of TCP/IP or other protocols that provide their own flow control and error correction mechanisms. Much of this traffic is fed into the Internet, another packet switched network without any built-in error control.

Because Frame Relay does not 'care' whether the frame it is switching is error-free or not, a Frame Relay node can start switching traffic out onto a new line as soon as it has read the first two bytes of addressing information at the beginning of the frame. Thus a frame of data can travel end-to-end, passing through several switches, and still arrive at its destination with only a few bytes' delay. These delays are small enough that network latency under Frame Relay is not noticeably different from direct leased line connections. As a result, the performance of a Frame Relay network is virtually identical to that of a leased line, but because most of the network is shared, costs are lower.

Frame Relay is an example of a packet-switched technology. Packet-switched networks enable end stations to dynamically share the network medium and the available bandwidth. The following two techniques are used in packet-switching technology:

- Variable-length packets
- Statistical multiplexing

Variable-length packets are used for more efficient and flexible data transfers. These packets are switched between the various segments in the network until the destination is reached.

Statistical multiplexing techniques control network access in a packet-switched network. The advantage of this technique is that it accommodates more flexibility and more efficient use of bandwidth. Most of today's popular LANs, such as Ethernet and Token Ring, are packet-switched networks.

Frame Relay Devices

Devices attached to a Frame Relay WAN fall into the following two general categories:

- Data terminal equipment (DTE)
- Data circuit-terminating equipment (DCE)

DTEs generally are considered to be terminating equipment for a specific network and typically are located on the premises of a customer. In fact, they may be owned by the customer. Examples of DTE devices are terminals, personal computers, routers, and bridges.

DCEs are carrier-owned internetworking devices. The purpose of DCE equipment is to provide clocking and switching services in a network, which are the devices that actually transmit data through the WAN. In most cases, these are packet switches.

The connection between a DTE device and a DCE device consists of both a physical layer component and a link layer component. The physical component defines the mechanical, electrical, functional, and procedural specifications for the connection between the devices. One of the most commonly used physical layer interface specifications is the recommended standard (RS)-232 specification. The link layer component defines the protocol that establishes the connection between the DTE device, such as a router, and the DCE device, such as a switch.

Virtual Circuits

Frame Relay is a virtual circuit network, so it doesn't use physical addresses to define the DTEs connected to the network. Frame Relay provides connection-oriented data link layer communication. This means that a defined communication exists between each pair of devices and that these connections are associated with a connection identifier. However, virtual circuit identifiers in Frame relay operate at the data link layer, in contrast with X.25, where they operate at the network layer. This service is implemented by using a Frame Relay virtual circuit, which is a logical connection created between two data terminal equipment (DTE) devices across a Frame Relay packet-switched network (PSN).

Virtual circuits provide a bidirectional communication path from one DTE device to another and are uniquely identified by a data-link connection identifier (DLCI). A number of virtual circuits can be multiplexed into a single physical circuit for transmission across the network. This capability often can reduce the equipment and network complexity required to connect multiple DTE devices.

A virtual circuit can pass through any number of intermediate DCE devices (switches) located within the Frame Relay PSN. Before going into the details of DLCI let us first have a look at the two types of Frame Relay Circuits, namely: switched virtual circuits (SVCs) and permanent virtual circuits (PVCs).

Switched virtual circuits (SVCs) are temporary connections used in situations requiring only sporadic data transfer between DTE devices across the Frame Relay network. A communication session across an SVC consists of the following four operational states:

- Call setup—The virtual circuit between two Frame Relay DTE devices is established.
- Data transfer—Data is transmitted between the DTE devices over the virtual circuit.
- Idle—The connection between DTE devices is still active, but no data is transferred. If an SVC remains in an idle state for a defined period of time, the call can be terminated.
- Call termination—The virtual circuit between DTE devices is terminated.

After the virtual circuit is terminated, the DTE devices must establish a new SVC if there is additional data to be exchanged. It is expected that SVCs will be established, maintained, and terminated using the same signaling protocols used in ISDN.

Permanent Virtual Circuits

Permanent virtual circuits (PVCs) are permanently established connections that are used for frequent and consistent data transfers between DTE devices across the Frame Relay network. Communication across PVC does not require the call setup and termination states that are used with SVCs. PVCs always operate in one of the following two operational states:

- Data transfer: Data is transmitted between the DTE devices over the virtual circuit.
- Idle: The connection between DTE devices is active, but no data is transferred.

Unlike SVCs, PVCs will not be terminated under any circumstances when in an idle state. DTE devices can begin transferring data whenever they are ready because the circuit is permanently established.

Data-Link Connection Identifier (DLCI)

Frame Relay virtual circuits are identified by data-link connection identifiers (DLCIs). DLCI values typically are assigned by the Frame Relay service provider (for example, the telephone company). Frame Relay DLCIs have local significance, which means that their values are unique in the LAN, but not necessarily in the Frame Relay WAN. The local DTEs use this DLCI to send frames to the remote DTE.

DLCIs are not only used to define the virtual circuit between a DTE and a DCE, but also to define the virtual circuit between two DCEs (switches) inside the network. A switch assigns a DLCI to each virtual connection in an interface. This means that two different connections belonging to two different interfaces may have the same DLCIs (as shown in the above figure). In other words, DLCIs are unique for a particular interface.

A connection between DTE A and DTE D has been shown in this figure, DLCI assigned inside the Frame Relay network is also shown in the network. DCEs inside the network use incoming interface – DLCI combination to decide the outgoing interface – DLCI combination to switch out the frame, from that DCE.

Each switch in a Frame relay network has a table to route frames The table matches the incoming interface- DLCI combination with an outgoing interface-DLCI combination.

Frame Relay Layers

Frame Relay has only 2 layers, namely Physical layer and Data Link layer. And as compared to other layer of packet switching network such as X.25, frame relay has only 1.5 layers whereas X.25 has 2 layers. Frame Relay eliminates all network layer functions and a portion of conventional data-link layer functions.

Physical Layer

No specific protocol is defined for physical layer in frame relay. Frame relay supports any one of the protocols recognized by ANSI, and thus the choice of physical layer protocol is up to the implementer.

Data Link Layer

At Data-link Layer Frame employs a simpler version of HDLC. Simpler version is used because HDLC provides extensive error and flow control fields that are not needed in frame relay.

To understand much of the functionality of Frame Relay, it is helpful to understand the structure of the Frame Relay frame. Figure 4.5.4 depicts the basic format of the Frame Relay frame. Flags indicate the beginning and end of the frame. Three primary components make up the Frame Relay frame: the header and address area, the user-data portion, and the frame check sequence (FCS). The address area, which is 2 bytes in length, is comprised of 10 bits representing the actual circuit identifier and 6 bits of fields related to congestion management. This identifier commonly is referred to as the data-link connection identifier (DLCI).

• Flags—Delimits the beginning and end of the frame. The value of this field is always the same and is represented either as the hexadecimal number 7E or as the binary number 01111110.

• Address—Contains the following information:

DLCI—The 10-bit DLCI is the essence of the Frame Relay header. This value represents the virtual connection between the DTE device and the switch. Each virtual connection that is multiplexed onto the physical channel will be represented by a unique DLCI. The DLCI values have local significance only, which means that they are unique only to the physical channel on which they reside. Therefore, devices at opposite ends of a connection can use different DLCI values to refer to the same virtual connection. The first 6-bits of the first byte make up part 1 of the DLCI, and second part of DLCI uses the first 4-bits of second byte.

Extended Address (EA)—The EA is used to indicate whether the byte in which the EA value is 1 is the last addressing field. If the value is 1, then the current byte is determined to be the last DLCI octet. Although current Frame Relay implementations all use a two-octet DLCI, this capability does allow longer DLCIs to be used in the future. The eighth bit of each byte of the Address field is used to indicate the EA.

C/R—The C/R is the bit that follows the most significant DLCI byte in the Address field. The C/R bit is not currently defined.

Congestion Control—This consists of the 3 bits that control the Frame Relay congestion-notification mechanisms. These are the FECN, BECN, and DE bits, which are the last 3 bits in the Address field.

Forward-explicit congestion notification (FECN) is a single-bit field that can be set to a value of 1 by a switch to indicate to an end DTE device, such as a router, that congestion was experienced in the direction of the frame transmission from source to destination as shown in Fig. 4.5.5. The primary benefit of the use of the FECN and BECN fields is the capability of higher-layer protocols to react intelligently to these congestion indicators. Today, DECnet and OSI are the only higher-layer protocols that implement these capabilities.

Backward-explicit congestion notification (BECN) is a single-bit field that, when set to a value of 1 by a switch, indicates that congestion was experienced in the network in the direction opposite of the frame transmission from source to destination.

Discard eligibility (DE) is set by the DTE device, such as a router, to indicate that the marked frame is of lesser importance relative to other frames being transmitted. Frames that are marked as "discard eligible" should be discarded before other frames in a congested network. This allows for a basic prioritization mechanism in Frame Relay networks.

Backward-explicit congestion notification

•Data—Contains encapsulated upper-layer data. Each frame in this variable-length field includes a user data or payload field that will vary in length up to 16,000 octets. This field serves to transport the higher-layer protocol packet (PDU) through a Frame Relay network.

•Frame Check Sequence—Ensures the integrity of transmitted data. This value is computed by the source device and verified by the receiver to ensure integrity of transmission.

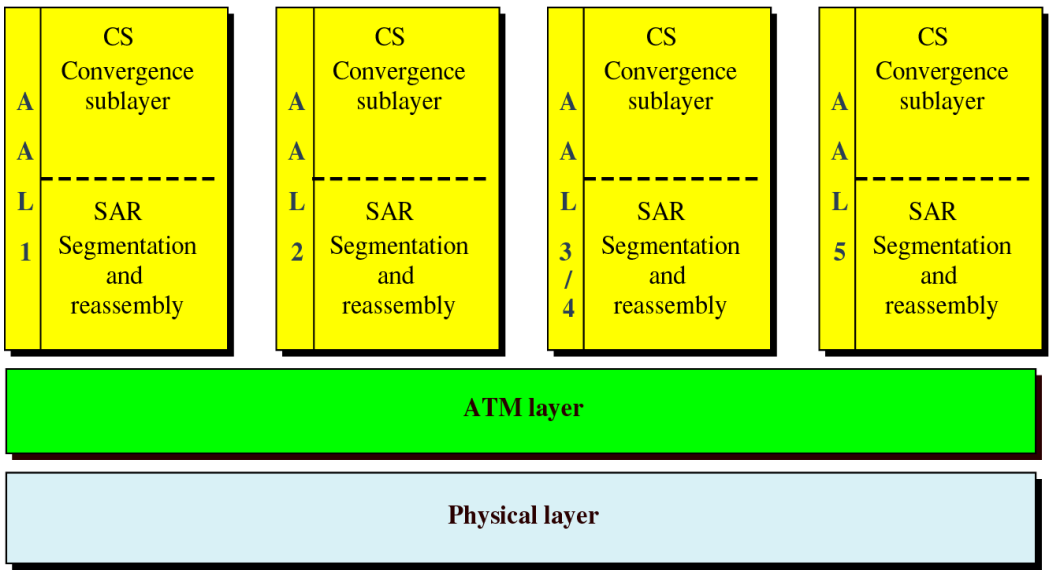
Summary

• Frame relay operates only in data link and physical layer.
• Frame Relay allows bursty traffic.
• It allows frame size of 9000 bytes, which can accommodate all local area network frames.
• Frame relay is less expensive then other traditional WANs.
• Frame relay provides both Permanent and switched connections.
• Frame relay allow variable-length frames, this may create varying delays for different users. Due to variable delay it is not suitable for real-time communication

Asynchronous Transfer Mode Switching (ATM)

Figure 19-22

AAL Types



Introduction

Asynchronous Transfer Mode (ATM) is an International Telecommunication Union-Telecommunications Standards Section (ITU-T) standard for cell relay wherein information for multiple service types, such as voice, video, or data, is conveyed in small, fixed-size cells. ATM networks are connection-oriented. Asynchronous transfer mode (ATM) is a technology that has its history in the development of broadband ISDN in the 1970s and 1980s. Technically, it can be viewed as an evolution of packet switching. Like packet switching protocols for data (e.g., X.25, frame relay, Transmission Control Protocol and Internet protocol (TCP IP]), ATM integrates the multiplexing and switching functions, is well suited for bursty traffic (in contrast to circuit switching), and allows communications between devices that operate at different speeds. Unlike packet switching, ATM is designed for high-performance multimedia networking. ATM technology has been implemented in a very broad range of networking devices. The most basic service building block is the ATM virtual circuit, which is an end-to-end connection that has defined end points and routes but does not have bandwidth dedicated to it. Bandwidth is allocated on demand by the network as users have traffic to transmit. ATM also defines various classes of service to meet a broad range of application needs. This lesson provides an overview of ATM protocols, services, and operation.

Benefits of ATM

The high-level benefits delivered through ATM services deployed on ATM technology using international ATM standards can be summarized as follows:

• **Dynamic bandwidth for bursty traffic** meeting application needs and delivering high utilization of networking resources; most applications are or can be viewed as inherently

bursty, for example voice is bursty, as both parties are neither speaking at once nor all the time; video is bursty, as the amount of motion and required resolution varies over time.

• **Smaller header** with respect to the data to make the efficient use of bandwidth.

• **Can handle Mixed network traffic very efficiently:** Variety of packet sizes makes traffic unpredictable. All network equipments should incorporate elaborate software systems to manage the various sizes of packets. ATM handles these problems efficiently with the fixed size cell.

• **Cell network:** All data is loaded into identical cells that can be transmitted with complete predictability and uniformity.

• Class-of-service support for multimedia traffic allowing applications with varying throughput and latency requirements to be met on a single network.

• Scalability in speed and network size supporting link speeds of T1/E1 to OC–12 (622 Mbps).

• Common LAN/WAN architecture allowing ATM to be used consistently from one desktop to another; traditionally, LAN and WAN technologies have been very different, with implications for performance and interoperability. But ATM technology can be used either as a LAN technology or a WAN technology.

• International standards compliance in central-office and customer-premises environments allowing for multivendor operation.

ATM Devices and the Network Environment

ATM is a cell-switching and multiplexing technology that combines the benefits of circuit switching (guaranteed capacity and constant transmission delay) with those of packet switching (flexibility and efficiency for intermittent traffic). It provides scalable bandwidth from a few megabits per second (Mbps) to many gigabits per second (Gbps). Because of its asynchronous nature, ATM is more efficient than synchronous technologies, such as time-division multiplexing (TDM).

With TDM, each user is assigned to a time slot, and no other station can send in that time slot as shown in Fig. 4.6.1. If a station has much data to send, it can send only when its time slot comes up, even if all other time slots are empty. However, if a station has nothing to transmit when its time slot comes up, the time slot is sent empty and is wasted.

Because ATM is asynchronous, time slots are available on demand with information identifying the source of the transmission contained in the header of each ATM cell. Figure 4.6.2 shows how cells from 3 inputs have been multiplexed. At the first clock tick input 2 has no data to send, so multiplexer fills the slot with the cell from third input. When all cells from input channel are multiplexed then output slot are empty.

ATM Devices

An ATM network is made up of an ATM switch and ATM endpoints. An ATM switch is responsible for cell transit through an ATM network. The job of an ATM switch is well defined. It accepts the incoming cell from an ATM endpoint or another ATM switch. It then reads and updates the cell header information and quickly switches the cell to an output interface towards its destination. An ATM endpoint (or end system) contains an ATM network interface adapter. Examples of ATM endpoints are workstations, routers, digital service units (DSUs), LAN switches, and video coder-decoders (Codec's).

ATM Network Interfaces

An ATM network consists of a set of ATM switches interconnected by point-to-point ATM links or interfaces. ATM switches support two primary types of interfaces: UNI and NNI as shown in Fig. 4.6.3. The UNI (User-Network Interface) connects ATM end systems (such as hosts and routers) to an ATM switch. The NNI (Network-Network Interface) connects two ATM switches. Depending on whether the switch is owned and located at the customer's premises or is publicly owned and operated by the telephone company, UNI and NNI can be further subdivided into public and private UNIs and NNIs. A private UNI connects an ATM endpoint and a private ATM switch. Its public counterpart connects an ATM endpoint or private switch to a public switch. A private NNI connects two ATM switches within the same private organization. A public one connects two ATM switches within the same public organization.

ATM transfers information in fixed-size units called cells. Each cell consists of 53 octets, or bytes as shown in Fig. 4.6.4. The first 5 bytes contain cell-header information, and the remaining 48 contain the payload (user information). Small, fixed-length cells are well suited to transfer voice and video traffic because such traffic is intolerant to delays that result from having to wait for a large data packet to download, among other things.

Header	Payload

An ATM cell header can be one of two formats: UNI or NNI. The UNI header is used for communication between ATM endpoints and ATM switches in private ATM networks. The NNI header is used for communication between ATM switches. Figure 4.6.5 depicts the ATM UNI cell header format, and the ATM NNI cell header format. Unlike the UNI, the NNI header does not include the Generic Flow Control (GFC) field. Additionally, the NNI header has a Virtual Path Identifier (VPI) field that occupies the first 12 bits, allowing for larger trunks between public ATM switches.

5 bytes

48 bytes

Figure 4.6.4 ATM cell Format

GFC	VPI
VPI	VCI
VPI	PT
VCI	CLP
PT	HEC
CLP	Payload
HEC	(48 bytes)
Payload	
(48 bytes)	

ATM Cell Header Fields

The following descriptions summarize the ATM cell header fields shown in Fig. 4.6.5.

• Generic Flow Control (GFC)—Provides local functions, such as identifying multiple stations that share a single ATM interface. This field is typically not used and is set to its default value of 0 (binary 0000).
• Virtual Path Identifier (VPI)—In conjunction with the VCI, identifies the next destination of a cell as it passes through a series of ATM switches on the way to its destination.
• Virtual Channel Identifier (VCI)—In conjunction with the VPI, identifies the next destination of a cell as it passes through a series of ATM switches on the way to its destination.
• Payload Type (PT)—Indicates in the first bit whether the cell contains user data or control data. If the cell contains user data, the bit is set to 0. If it contains control data, it is set to 1. The second bit indicates congestion (0 = no congestion, 1 = congestion), and

the third bit indicates whether the cell is the last in a series of cells that represent a single AAL5 frame (1 = last cell for the frame).
• Cell Loss Priority (CLP)—Indicates whether the cell should be discarded if it encounters extreme congestion as it moves through the network. If the CLP bit equals 1, the cell should be discarded in preference to cells with the CLP bit equal to 0.
• Header Error Control (HEC)—Calculates checksum only on the first 4 bytes of the header. HEC can correct a single bit error in these bytes, thereby preserving the cell rather than discarding it.

ATM Virtual Connections
ATM standard defines two types of ATM connections: virtual path connections (VPCs), which contain virtual channel connections (VCCs) as shown in Fig. 4.6.6. A virtual channel connection (or virtual circuit) is the basic unit, which carries a single stream of cells, in order, from user to user. A collection of virtual circuits can be bundled together into a virtual path connection. A virtual path connection can be created from end-to-end across an ATM network. In this case, the ATM network does not route cells belonging to a particular virtual circuit. All cells belonging to a particular virtual path are routed the same way through the ATM network, thus resulting in faster recovery in case of major failures. In this case, all the switches within the ATM network are only VP switches, i.e. they switch the cells only on the basis of VPIs. Only the switches, which are connected to the subscribers are VP/VC switches, i.e. they use both VPIs and VCIs to switch the cell. This configuration is usually followed so that the intermediate switches can do switching much faster.

Virtual channel connections of ATM

An ATM network also uses virtual paths internally for the purpose of bundling virtual circuits together between switches. Two ATM switches may have many different virtual channel connections between them, belonging to different users. These can be bundled by two ATM switches into a virtual path connection. This can serve the purpose of a virtual trunk between the two switches. This virtual trunk can then be handled as a single entity by perhaps, multiple intermediate virtual paths cross connects between the two virtual circuit switches.

ATM Switching Operations

The basic operation of an ATM switch is straightforward: The cell is received across a link with a known VPI/VCI value. The switch looks up the connection value in a local translation table to determine the outgoing port (or ports) of the connection and the new VPI/VCI value of the connection on that link. The switch then retransmits the cell on that outgoing link with the appropriate connection identifier.

Incoming		Outgoing		
VPI	VCI	VPI	VCI	Interface
10	122	11	41	1
121	213	10	158	1

12	11	211	111	2
11	151	321	210	2

A VP/VC ATM switch table

Because all VCIs and VPIs have only local significance across a particular link, these values are remapped, as necessary, at each switch. Figure 4.6.7 and Fig. 4.6.8 shows a VP-VC switch and an only VP switch, respectively. Usually the intermediate switches are only VPI switches while switches connected to the users are VPI/VCI switches.

Incoming	Outgoing	
VPI	VPI	Interface
22	65	1
121	99	2
312	201	1
11	21	2

VP ATM switch table

To make the switching more efficient, ATM uses two types of switches namely, VP switch and VP-VC switch. A VP switch route cells only on the basis of VPI, here VPIs change but VCIs remain same during switching. On the other hand, VP-VC switch uses the complete identifier, i.e. both VPI and VCI to route the cell. We can think of a VP-VC switch as a combination of Only VP and Only VC switch.

4.6.6 ATM Reference Model

The ATM architecture uses a logical model to describe the functionality that it supports. ATM functionality corresponds to the physical layer and part of the data link layer of the OSI reference model.

The ATM reference model, as shown in Fig. 4.6.9, consists of the following planes, which span all layers:

• Control—This plane is responsible for generating and managing signaling requests.
• User—This plane is responsible for managing the transfer of data.
• Management—This plane contains two components:

Layer management manages layer-specific functions, such as the detection of failures and protocol problems.

Plane management manages and coordinates functions related to the complete system.

The ATM reference model consists of the following ATM layers:

• Physical layer—Analogous to the physical layer of the OSI reference model, the ATM physical layer manages the medium-dependent transmission.

• ATM layer—Combined with the ATM adaptation layer, the ATM layer is roughly analogous to the data link layer of the OSI reference model. The ATM layer is responsible for the simultaneous sharing of virtual circuits over a physical link (cell multiplexing) and passing cells through the ATM network (cell relay). To do this, it uses the VPI and VCI information in the header of each ATM cell.
• ATM adaptation layer (AAL)—Combined with the ATM layer, the AAL is roughly analogous to the data link layer of the OSI model. The AAL is responsible for isolating higher-layer protocols from the details of the ATM processes. The adaptation layer prepares user data for conversion into cells and segments the data into 48-byte cell payloads.

Finally, the higher layers residing above the AAL accept user data, arrange it into packets, and hand it to the AAL.

The ATM Physical Layer

The main functions of the ATM physical layer are as follows:

• Cells are converted into a bit stream,
• The transmission and receipt of bits on the physical medium are controlled,
• ATM cell boundaries are tracked,
• Cells are packaged into the appropriate types of frames for the physical medium.

The ATM physical layer is divided into two parts: the physical medium-dependent (PMD) sub layer and the transmission convergence (TC) sub layer.

The PMD sub layer provides two key functions.

• It synchronizes transmission and reception by sending and receiving a continuous flow of bits with associated timing information.
• It specifies the physical media for the physical medium used, including connector types and cable.

The TC sub layer has four functions:

• Cell delineation, it maintains ATM cell boundaries, allowing devices to locate cells within a stream of bits.
• Generates and checks the header error control code to ensure valid data.
• Cell-rate decoupling, maintains synchronization and inserts or suppresses idle (unassigned) ATM cells to adapt the rate of valid ATM cells to the payload capacity of the transmission system.
• Transmission frame adaptation packages ATM cells into frames acceptable to the particular physical layer implementation.

ATM Layer

The ATM layer provides routing, traffic management, switching and multiplexing services. It processes outgoing traffic by accepting 48-byte segment from the AAL sub-layers and transforming them into 53-byte cell by addition of a 5-byte header. Adaptation Layers

ATM adaptation layers allow existing packet networks to connect to ATM facilities. AAL Protocol accepts transmission from upper layer services (e.g.: packet data) and map them into fixed-sized ATM cells. These transmissions can be of any type, variable or fixed data rate. At the receiver, this process is reversed and segments are reassembled into their original formats and passed to the receiving services. Instead of one protocol for all types of data, the ATM standard divides the AAL layer into categories, each supporting the requirements of different types of applications. There are four types of data streams that are identified: Constant-bit rate, variable bit-rate, connection oriented packet data transfer, connectionless packet data transfer. In addition to dividing AAL by category (AAL1, AAL2 and so on), ITU-T also divides it on the basis of functionality. Each AAL layer is actually divided into two layers: the convergence sub-layer and Segmentation and reassembly (SAR) sub-layer. Table below gives a brief description of these data streams and various ATM adaptation layers which are used for each of them.

Table Mapping of various data types and ATM adaptation layers

Service Class	Quality of Service Parameter	ATM Adaptation layers
Constant Bit rate (CBR)	This class is used for emulating circuit switching. The cell rate is constant with time. CBR applications are quite sensitive to cell-delay variation. Examples of applications that can use CBR are telephone traffic (i.e., nx64 kbps), videoconferencing, and television.	AAL1: AAL1, a connection-oriented service, is suitable for handling constant bit rate sources (CBR), such as voice and videoconferencing. AAL1 requires timing synchronization between the source and the destination. For this reason, AAL1 depends on a medium, such as SONET, that supports clocking. The AAL1 process prepares a cell for transmission in three steps. First, synchronous samples (for example, 1 byte of data at a sampling rate of 200 microseconds) are inserted into the Payload field. Second, Sequence Number (SN) and Sequence Number Protection (SNP) fields are added to provide information that the receiving AAL1 uses to verify that it has received cells in the correct order. Third, the remainder of the

		Payload field is filled with enough single bytes to equal 48 bytes.

Variable Bit Rate - non-real time (VBR–NRT)	This class allows users to send traffic at a rate that varies with time depending on the availability of user information. Statistical multiplexing is provided to make optimum use of network resources. Multimedia e-mail is an example of VBR–NRT.	AAL 2: The AAL2 process uses 44 bytes of the cell payload for user data and reserves 4 bytes of the payload to support the AAL2 processes. VBR traffic is characterized as either real-time (VBR-RT) or as non-real-time (VBR-NRT). AAL2 supports both types of VBR traffic.
Variable bit rate–real time (VBR–RT)	This class is similar to VBR–NRT but is designed for applications that are sensitive to cell-delay variation. Examples for real-time VBR are voice with speech activity detection (SAD) and interactive compressed video.	

Connection oriented packet transfer or available bit rate (ABR)	This class of ATM services provides rate-based flow control and is aimed at data traffic such as file transfer and e-mail. Although the standard does not require the cell transfer delay and cell-loss ratio to be guaranteed or minimized, it is desirable for switches to minimize delay and loss as much as possible. Depending upon the state of congestion in the network, the source is required to control its rate. The users are allowed to declare a minimum cell rate, which is guaranteed to the connection by the network.	AAL3/4: AAL3/4 supports both connection-oriented and connectionless data. AAL3/4 prepares a cell for transmission in four steps. First, the convergence sub layer (CS) creates a protocol data unit (PDU) by prepending a beginning/end tag header to the frame and appending a length field as a trailer. Second, the segmentation and reassembly (SAR) sub layer fragments the PDU and prepends a header to it. Then the SAR sub layer appends a CRC-10 trailer to each PDU fragment for error control. Finally, the completed SAR PDU becomes the Payload field of an ATM cell to which the ATM layer prepends the standard ATM header. AAL 5: AAL5 is the primary AAL for data and supports both connection-oriented and connectionless data. It is used to transfer most non-SMDS data, such as classical IP over ATM and LAN Emulation (LANE). AAL5 also is known as the simple and efficient adaptation layer (SEAL)
Connectionless data transfer or unspecified bit rate (UBR)	This class is the catch-all, other class and is widely used today for TCP/IP.	

ATM Applications

ATM is used in both LANs and WANs; let's have a look at few of the possible applications.

ATM WANs: ATM is basically a WAN technology that delivers cell over long distances. Here ATM is mainly used to connect LANs or other WANs together. A router between ATM network and the other network serves as an end point. This router has two stacks of protocols: one belonging to ATM and other belonging to other protocol.

ATM LANs: High data rate (155 and 622 Mbps) of ATM technology attracted designers to think of implementing ATM technology in LANs too. At the surface level, to implement an ATM LAN ATM switch will replace the traditional Ethernet switch, in a

switched LAN. But few things have to be kept in mind and software modules would be needed to map the following differences between the two technologies:
• Connectionless versus connection-oriented: ATM is a virtual connection oriented technology, while traditional Ethernet uses connectionless protocols.
• Physical address versus virtual circuit identifier: In the Traditional LAN packets are routed based on the source and destination addresses, while in ATM cells are routed based on the virtual circuit identifiers (VPI-VCI pair).

Multimedia virtual private networks and managed services: Service providers are building on their ATM networks to offer a broad range of services. Examples include managed ATM, LAN, voice and video services (these being provided on a per-application basis, typically including customer-located equipment and offered on an end-to-end basis), and full-service virtual private-networking capabilities (these including integrated multimedia access and network management).

Frame-relay backbones: Frame-relay service providers are deploying ATM backbones to meet the rapid growth of their frame-relay services to use as a networking infrastructure for a range of data services and to enable frame relay to ATM service internetworking services.

Internet backbones: Internet service providers are likewise deploying ATM backbones to meet the rapid growth of their frame-relay services, to use as a networking infrastructure for a range of data services, and to enable Internet class-of-service offerings and virtual private intranet services.
Residential broadband networks: ATM is the networking infrastructure of choice for carriers establishing residential broadband services, driven by the need for highly scalable solutions.
Carrier infrastructures for the telephone and private-line networks: Some carriers have identified opportunities to make more-effective use of their SONET/SDH fiber infrastructures by building an ATM infrastructure to carry their telephony and private-line traffic.

Network Topology

Introduction

Topology refers to the way in which the network of computers is connected. Each topology is suited to specific tasks and has its own advantages and disadvantages. The choice of topology is dependent upon type and number of equipment being used, planned applications and rate of data transfer required, response time, and cost. Topology can also be defined as the *geometrically interconnection pattern* by which the stations (nodes/computers) are connected using suitable transmission media (which can be point-to-point and broadcast). Various commonly used topologies are discussed in the following sections.

Mesh Topology

In this topology each node or station is connected to every other station The key characteristics of this topology are as follows:

Key Characteristics:
- Fully connected
- Robust – Highly reliable
- Not flexible
- Poor expandability

Two nodes are connected by dedicated point-point links between them. So the total number of links to connect n nodes = n(n-1)/2; which is proportional to n^2 . Media used for the connection (links) can be twisted pair, co-axial cable or optical fiber. With this topology there is no need to provide any additional information, that is from where the packet is coming, along with the packet because two nodes have a point-point dedicated link between them. And each node knows which link is connected to which node on the other end.

Mesh Topology is not flexible and has a poor expandability as to add a new node n links have to be laid because that new node has to be connected to each of the existing nodes via dedicated link as shown in Fig. 5.1.2. For the same reason the cost of cabling will be very high for a larger area. And due to these reasons this topology is rarely used in practice.

Bus Topology

In Bus Topology, all stations attach through appropriate hardware interfacing known as a tap, directly to a linear transmission medium, or bus as shown in Fig. 5.1.3. Full-duplex operation between the station and the tap allows data to be transmitted onto the bus and received from the bus. A transmission from any station propagates the length of the medium in both directions and can be received by all other stations. At each end of the bus there is a terminator, which absorbs any signal, preventing reflection of signal from the endpoints. If the terminator is not present, the endpoint acts like a mirror and reflects the signal back causing interference and other problems.

Figure 5.1.3 Bus Topology

Key Characteristics of this topology are:

o Flexible
o Expandable
o Moderate Reliability
o Moderate performance

A shared link is used between different stations. Hence it is very cost effective. One can easily add any new node or delete any node without affecting other nodes; this makes this topology easily expandable.

some extra information about the desired destination, i.e. to explicitly specify the destination in the packet, as compared to mesh topology. This is because the same medium is shared among many nodes. As each station has a unique address in the network, a station copies a packet only when the destination address of the packet matches with the self-address. This is how data communications take place among the stations on the bus.

As there are dedicated links in the mess topology, there is a possibility of transferring data in parallel. But in bus topology, only one station is allowed to send data at a time and all other stations listen to it, as it works in a broadcast mode. Hence, only one station can transfer the data at any given time. Suitable medium access control technique should be used so as to provide some way to decide "who" will go next to send data? Usually a distributed medium access control technique, as discussed in the next lesson, is used for this purpose.

As the distance through which signal traverses increases, the attenuation increases. If the sender sends data (signal) with a small strength signal, the farthest station will not be able to receive the signal properly. While on the other hand if the transmitter sends the signal with a larger strength (more power) then the farthest station will get the signal properly but the station near to it may face over-drive. Hence, delay and signal unbalancing will force a maximum length of shared medium, which can be used in bus topology.

STAR Topology

In the star topology, each station is directly connected to a common central node Typically, each station attaches to a central node, referred to as the star coupler, via two point-to-point links, one for transmission and one for reception.

Key features:
- o High Speed
- o Very Flexible
- o High Reliability
- o High Maintainability

In general, there are two alternatives for the operation of the central node.

o One approach is for the central node to operate in a broadcast fashion. A transmission of a frame from one station to the node is retransmitted on all of the

outgoing links. In this case, although the arrangement is physically a star, it is logically a bus; a transmission from any station is received by all other stations, and only one station at a time may successfully transmit. In this case the central node acts as a repeater.

o Another approach is for the central node to act as a frame-switching device. An incoming frame is buffered in the node and then retransmitted on an outgoing link to the destination station. In this approach, the central node acts as a switch and performs the switching or routing function. This mode of operation can be compared with the working of a telephone exchange, where the caller party is connected to a single called party and each pair of subscriber who needs to talk have a different connection.

Very High speeds of data transfer can be achieved by using star topology, particularly when the star coupler is used in the switch mode. This topology is the easiest to maintain, among the other topologies. As the number of links is proportional to n, this topology is very flexible and is the most preferred topology.

Ring topology

In the ring topology, the network consists of a set of repeaters joined by point-to-point links in a closed loop. The repeater is a comparatively simple device, capable of receiving data on one link and transmitting them, bit by bit, on the other link as fast as they are received, with no buffering at the repeater. The links are unidirectional; that is data are transmitted in one direction only and all are oriented in the same way. Thus, data circulate around the ring in one direction (clockwise or counterclockwise).

Ring Topology

Each station attaches to the network at a repeater and can transmit data onto the network through that repeater. As with the bus and tree, data are transmitted in frames.

As a frame circulates past all the other stations, the destination station recognizes its address and copies the frame into a local buffer as it goes by. The frame continues to circulate until it returns to the source station, where it is removed. Because multiple stations share the ring, medium access control is needed to determine at what time each station may insert frames.

How the source knows whether it has to transmit a new packet and whether the previous packet has been received properly by the destination or not. For this, the destination change a particular bit (bits) in the packet and when the receiver sees that packet with the changed bit, it comes to know that the receiver has received the packet.

This topology is not very reliable, because when a link fails the entire ring connection is broken. But reliability can be improved by using wiring concentrator, which helps in bypassing a faulty node and somewhat is similar to star topology.

Repeater works in the following three modes:

• Listen mode: In this mode, the station listens to the communication going over the shared medium

Transmit mode: In this mode the station transmit the data over the network

• By-Pass mode: When the node is faulty then it can be bypassed using the repeater in bypass mode, i.e. the station doesn't care about what data is transmitted through the network, as shown in Fig. 5.1.8. In this mode there is no delay introduced because of this repeater.

Tree Topology

This topology can be considered as an extension to bus topology. It is commonly used in cascading equipments. For example, you have a repeater box with 8-port, as far as you have eight stations, this can be used in a normal fashion. But if you need to add more stations then you can connect two or more repeaters in a hierarchical format (tree format) and can add more stations. In the Fig. 5.1.9, R1 refers to repeater one and so on and each repeater is considered to have 8-ports.

Tree Topology

This tree topology is very good in an organization as incremental expansion can be done in this way. Main features of this topology are scalability and flexibility. This is

because, when the need arises for more stations that can be accomplished easily without affecting the already established network.

Unconstrained Topology

All the topologies discussed so far are symmetric and constrained by well-defined interconnection pattern. However, sometimes no definite pattern is followed and nodes are interconnected in an arbitrary manner using point-to-point links Unconstrained topology allows a lot of configuration flexibility but suffers from the complex routing problem. Complex routing involves unwanted overhead and delay.

Combination of topology and transmission media

Topology and transmission media are interrelated. For example, all the important criteria of a network such as reliability, expandability and performance depend on both the topology and the transmission media used in the network. As a consequence, these two aspects are interrelated. Let us have a look at the various transmission media, which are used for different topologies.

Internetworking Devices

Introduction

HILI subcommittee (IEEE802.1) of the IEEE identified the following possible internetworking scenarios.

- A single LAN
- Two LANs connected together (LAN-LAN)
- A LAN connected to a WAN (LAN-WAN)
- Two LANs connected through a WAN (LAN-WAN-LAN)

Various internetworking devices such as hubs, bridges, switches, routers and gateways are required to link them together. These internetworking devices are introduced in this lesson.

Repeaters

A single Ethernet segment can have a maximum length of 500 meters with a maximum of 100 stations (in a cheapernet segment it is 185m). To extend the length of the network, a *repeater* may be used. Functionally, a repeater can be considered as two transceivers joined together and connected to two different segments of coaxial cable. The repeater passes the digital signal bit-by-bit in both directions between the two segments. As the signal passes through a repeater, it is amplified and regenerated at the other end. The repeater does not isolate one segment from the other, if there is a collision on one segment, it is regenerated on the other segment. Therefore, the two segments form a single LAN and it is transparent to rest of the system. Ethernet allows five segments to be used in cascade to have a maximum network span of 2.5 km. With reference of the ISO model, a repeater is considered as a *level-1 relay* .It simply repeats, retimes and amplifies the bits it receives. The repeater is merely used to extend the span of a single LAN.

Important features of a repeater are as follows:

- A repeater connects different segments of a LAN
- A repeater forwards every frame it receives

• A repeater is a regenerator, not an amplifier
• It can be used to create a single extended LAN

Hubs

Hub is a generic term, but commonly refers to a multiport repeater. It can be used to create multiple levels of hierarchy of stations. The stations connect to the hub with RJ-45 connector having maximum segment length is 100 meters. This type of interconnected set of stations is easy to maintain and diagnose. Figure 6.1.3 shows how several hubs can be connected in a hierarchical manner to realize a single LAN of bigger size with a large number of nodes.

Bridges

The device that can be used to interconnect two separate LANs is known as a bridge. It is commonly used to connect two similar or dissimilar LANs. The bridge operates in layer 2, that is data-link layer and that is why it is called level-2 relay with reference to the OSI model. It links similar or dissimilar LANs, designed to store and forward frames, it is protocol independent and transparent to the end stations. The flow of information through a bridge. Use of bridges offer a number of advantages, such as higher reliability, performance, security, convenience and larger geographic coverage. But, it is desirable that the quality of service (QOS) offered by a bridge should match that of a single LAN. The parameters that define the QOS include availability, frame mishaps, transit delay, frame lifetime, undetected bit errors, frame size and priority. Key features of a bridge are mentioned below:

• A bridge operates both in physical and data-link layer
• A bridge uses a table for filtering/routing
• A bridge does not change the physical (MAC) addresses in a frame
• Types of bridges:
    o Transparent Bridges
o Source routing bridges

A bridge must contain addressing and routing capability. Two routing algorithms have been proposed for a bridged LAN environment. The first, produced as an extension of IEEE 802.1 and applicable to all IEEE 802 LANs, is known as transparent bridge. And the other, developed for the IEEE 802.5 token rings, is based on source routing approach. It applies to many types of LAN including token ring, token bus and CSMA/CD bus.

Transparent Bridges

The transparent bridge uses two processes known as bridge forwarding and bridge learning. If the destination address is present in the forwarding database already created, the packet is forwarded to the port number to which the destination host is attached. If it is not present, forwarding is done on all parts (flooding). This process is known as bridge forwarding. Moreover, as each frame arrives, its source address indicates where a particular host is situated, so that the bridge learns which way to forward frames to that address. This process is known as bridge learning. Key features of a transparent bridge are:

• The stations are unaware of the presence of a transparent bridge
• It performs two functions: o Forwar
o Learning to create th

Bridge Forwarding

Bridge forwarding operation is explafunctions of the bridge forwarding ar
• Discard the frame if source and destination addresses are same • Forward the frame if the source and destination

Loop Problem

Forwarding and learning processes work without any problem as long as there is no redundant bridge in the system. On the other hand, redundancy is desirable from the viewpoint of reliability, so that the function of a failed bridge is taken over by a redundant bridge. The existence of redundant bridges creates the so-called loop problem. Assuming that after initialization tables in both the bridges are empty let us consider the following steps:
Step 1. Station-A sends a frame to Station-B. Both the bridges forward the frame to LAN Y and update the table with the source address of A.
Step 2. Now there are two copies of the frame on LAN-Y. The copy sent by Bridge-a is received by Bridge-b and vice versa. As both the bridges have no information about Station B, both will forward the frames to LAN-X.
Step 3. Again both the bridges will forward the frames to LAN-Y because of the lack of information of the Station B in their database and again Step-2 will be repeated, and so on. So, the frame will continue to loop around the two LANs indefinitely.

Spanning Tree

As redundancy creates loop problem in the system, it is very undesirable. To prevent loop problem and proper working of the forwarding and learning processes, there must be only one path between any pair of bridges and LANs between any two segments in the entire bridged LAN. The IEEE specification requires that the bridges use a special topology. Such a topology is known as spanning tree (a graph where there is no loop) topology.
Source Routing Bridges
The second approach, known as source routing, where the routing operation is performed by the source host and the frame specifies which route the frame is to follow. A host can discover a route by sending a discovery frame, which spreads through the entire network using all possible paths to the destination. Each frame gradually gathers addresses as it goes. The destination responds to each frame and the source host chooses an appropriate route from these responses. For example, a route with minimum hop-count can be chosen. Whereas transparent bridges do not modify a frame, a source routing bridge adds a routing information field to the frame. Source routing approach provides a shortest path at the cost of the proliferation of discovery frames, which can put a serious extra burden on the network. Figure 6.1.11 shows the frame format of a source routing bridge.
Switches
A switch is essentially a fast bridge having additional sophistication that allows faster processing of frames. Some of important functionalities are:
• Ports are provided with buffer
• Switch maintains a directory: #address - port#
• Each frame is forwarded after examining the #address and forwarded to the proper port#

• Three possible forwarding approaches: Cut-through, Collision-free and Fully-buffered as briefly explained below.

Cut-through: A switch forwards a frame immediately after receiving the destination address. As a consequence, the switch forwards the frame without collision and error detection.
Collision-free: In this case, the switch forwards the frame after receiving 64 bytes, which allows detection of collision. However, error detection is not possible because switch is yet to receive the entire frame.
Fully buffered: In this case, the switch forwards the frame only after receiving the entire frame. So, the switch can detect both collision and error free frames are forwarded.

Comparison between a switch and a hub

Although a hub and a switch apparently look similar, they have significant differences. both can be used to realize physical star topology, the hubs works like a logical bus, because the same signal is repeated on all the ports. On the other hand, a switch functions like a logical star with the possibility of the communication of separate signals between any pair of port lines. As a consequence, all the ports of a hub belong to the same collision domain, and in case of a switch each port operates on separate collision domain. Moreover, in case of a hub, the bandwidth is shared by all the stations connected to all the ports. On the other hand, in case of a switch, each port has dedicated bandwidth. Therefore, switches can be used to increase the bandwidth of a hub-based network by replacing the hubs by switches.

Routers

A router is considered as a layer-3 relay that operates in the network layer, that is it acts on network layer frames. It can be used to link two dissimilar LANs. A router isolates LANs in to subnets to manage and control network traffic. However, unlike bridges it is not transparent to end stations. A router has four basic components: Input ports, output ports, the routing processor and the switching fabric. The functions of the four components are briefly mentioned below.

• Input port performs physical and data-link layer functions of the router. As shown in
• Output ports, as shown in Fig. 6.1.14(b), perform the same functions as the input ports, but in the reverse order.
• The routing processor performs the function of the network layer. The process involves table lookup.
• The switching fabric, shown in Fig. 6.1.15, moves the packet from the input queue to the output queue by using specialized mechanisms. The switching fabric is realized with the help of multistage interconnection networks.
• Communication of a frame through a router is shown in Fig. 6.1.16.

Gateways

A gateway works above the network layer, such as application layer As a consequence, it is known as a Layer-7 relay. The application level gateways can look into the content application layer packets such as email before forwarding it to the other side. This property has made it suitable for use in Firewalls discussed in the next module.

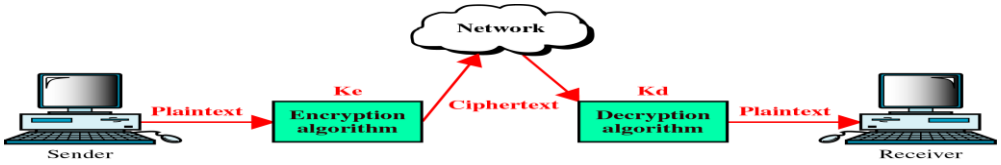
A Simple Internet

A simple internet comprising several LANs and WANs linked with the help of routers

Network Security

Figure 23-7

Concept of Encryption and Decryption



Specific Instructional Objectives On completion, the students will be able to: State the need for secured communication Explain the requirements for secured communication Explain the following cryptographic algorithms: Symmetric-key Cryptography • Traditional ciphers • Monoalphabetic Substitution • Polyalphabetic Substitution • Transpositional Cipher • Block ciphers Public-key Cryptography • The RSA Algorithm Introduction The word **cryptography** has come from a Greek word, which means *secret writing*. In the present day context it refers to the tools and techniques used to make messages secure for communication between the participants and make messages immune to attacks by hackers. For private communication through public network, cryptography plays a very crucial role. The role of cryptography can be illustrated with the help a simple model of cryptography as shown in Fig. 8.1.1. The message to be sent through an unreliable medium is known as **plaintext**, which is encrypted before sending over the medium. The encrypted message is known as **ciphertext**, which is received at the other end of the medium and decrypted to get back the original plaintext message. In this lesson we shall discuss various cryptography algorithms, which can be divided into two broad categorize - **Symmetric key cryptography** and **Public key cryptography.**

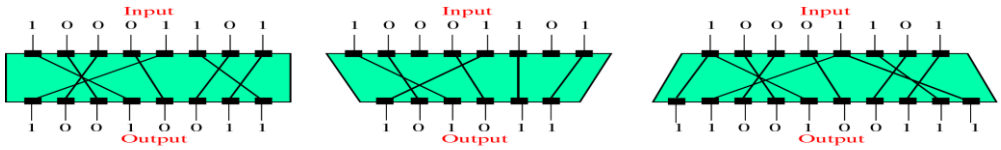
Symmetric Key Cryptography The cipher, an algorithm that is used for converting the plaintext to ciphertex, operates on a **key**, which is essentially a specially generated number (value). To decrypt a secret message (ciphertext) to get back the original message (plaintext), a decrypt algorithm uses a decrypt key. In symmetric key cryptography, same key is shared, i.e. the same key is used in both encryption and decryption. The algorithm used to decrypt is just the inverse of the algorithm used for encryption. For example, if addition and division is used for encryption, multiplication and subtraction are to be used for decryption. Symmetric key cryptography algorithms are simple requiring lesser execution time. As a consequence, these are commonly used for long messages. However, these algorithms suffer from the following limitations: Requirement of large number of unique keys. For example for n users the number of keys required is n(n-1)/2. Distribution of keys among the users in a secured manner is difficult

Monoalphabetic Substitution One simple example of symmetric key cryptography is the *Monoalphabetic substitution*. In this case, the relationship between a character in the plaintext and a character in the ciphertext is always one-to-one. An example Monoalphabetic substitution is the Caesar cipher. In this approach a character in the ciphertext is substituted by another character shifted by three places, e.g. A is substituted by D. Key feature of this approach is that it is very simple but the code can be attacked very easily. Polyalphabetic Substitution This is an improvement over the Caesar cipher. Here the relationship between a character in the plaintext and a character in the ciphertext is always one-to-manyExample of polyalphabetic substitution is the Vigenere cipher. In this case, a particular character is substituted by different characters in the ciphertext depending on its position in the plaintext. Here the top row shows different characters in the plaintext and the characters in different bottom rows show the characters by which a particular character is to be replaced depending upon its position in different rows from row-0 to row-25. • Key feature of this approach is that it is more complex and the code is harder to attack successfully. Transpositional Cipher The transpositional cipher, the characters remain unchanged but their positions are changed to create the ciphertext. The characters are arranged in two-dimensional matrix and columns are interchanged according to a key is shown in the middle portion of the diagram. The key defines which columns are to be swapped. As per the key shown in the figure, character of column is to be swapped to column 3, character of column 2 is to be swapped to column 6, and so on. Decryption can be done by swapping in the reverse order using the same key. Transpositional cipher is also not a very secure approach. The attacker can find the plaintext by trial and error utilizing the idea of the frequency of occurrence of characters. Block Ciphers Block ciphers use a block of bits as the unit of encryption and decryption. To encrypt a 64-bit block, one has to take each of the 264 input values and map it to one of the 264 output values. The mapping should be one-to-one. Encryption and decryption operations of a block cipher are shown in Fig. 8.1.6. Some operations, such as permutation and substitution, are performed on the block of bits based on a key (a secret number) to produce another block of bits. The permutation and substitution operations. In the decryption process, operations are performed in the reverse order based on the same key to get back the original block of bits.

Transformations in Block Ciphers **Permutation:**, the permutation is performed by a permutation box at the bit-level, which keeps the number of 0s and 1s same at the input and output. Although it can be implemented either by a hardware or a software, the hardware implementation is faster. Permutation operation used in Block Ciphers **Substitution:** the substitution is implemented with the help of three building blocks – a decoder, one p-box and an encoder. For an n-bit input, the decoder produces an 2_n bit output having only one 1, which is applied to the P-box. The P-box permutes the output of the decoder and it is applied to the encoder. The encoder, in turn, produces an n-bit output. For example, if the input to the decoder is 011, the output of the decoder is 00001000. Let the permuted output is 01000000, the output of the encoder is 011. It performs the following steps: **Step-2:** Substitute each 8-bit based on **Step-3:** Permute the bits based on the key A

Figure 23-13

Permutation



a. Straight permutation b. Compressed permutation c. Expanded permutation

Figure 23-14

Substitution

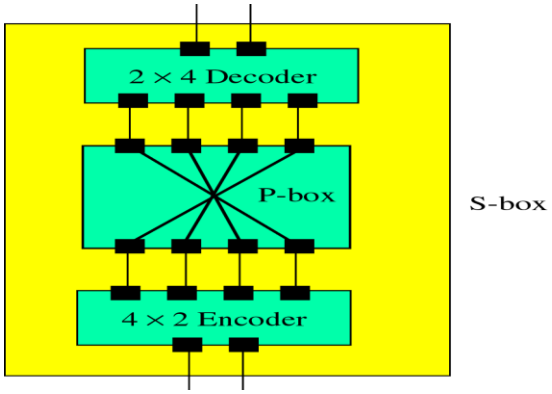


Figure 23-21

Public Key Encryption

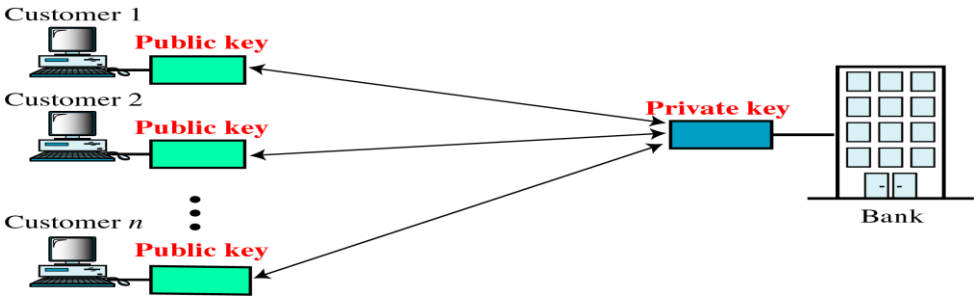


Figure 27-3

Public key encryption

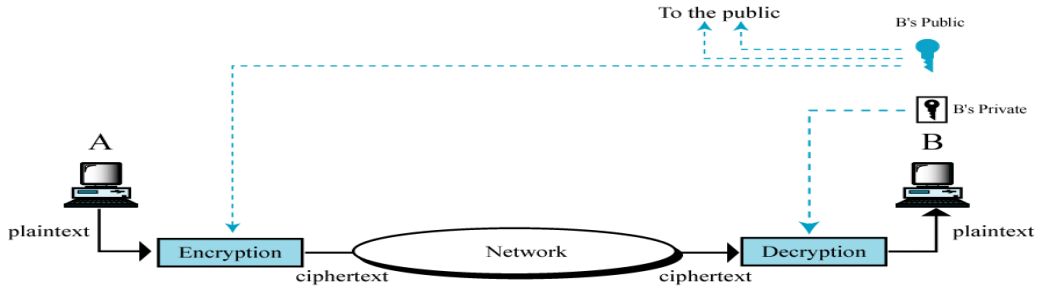


Figure 23-25

Signature Authentication

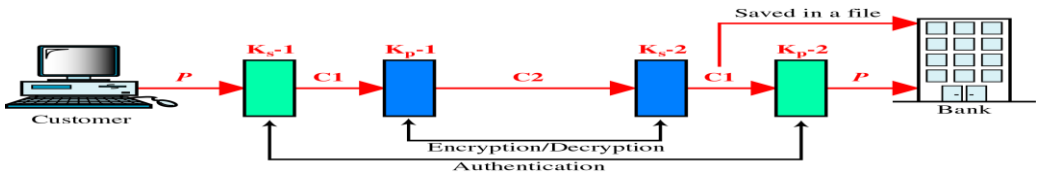
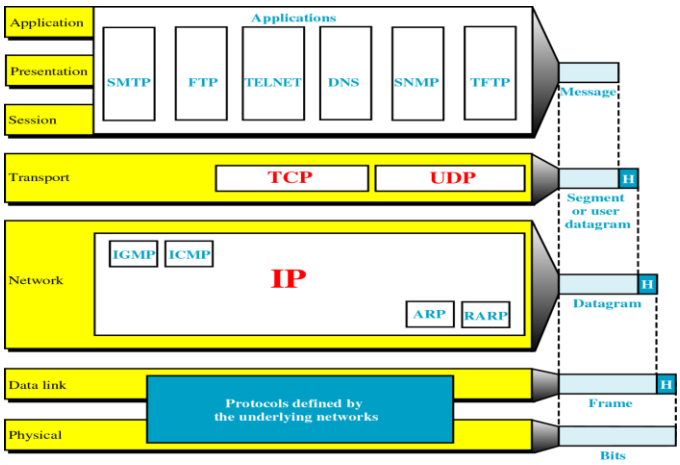


Figure 24-2

TCP/IP and the OSI Model



Encryption Standard (DES) One example of the block cipher is the Data Encof the DES algorithm are given below: • A monoalphabetic substitution c• It has 19 distinct stages • Although the input key fonly 56 bits in length. • The decryption can be carried out in reverse order. • DES has 16 rounds, meaning the ciphertext. • As the number oexponentially. • Once the key scactual encryption or decryption is performed with the

help of the main DES algorithm **Caining (CBC)** In this mode of operation, encrypted ciphernext plaintext block to be encrypted, thus making all the blocks dependent on all the previous blocksCipher Feedback Mode (CFB) encryption technique **Output Feedback Mode (OFB)** The encryption technique of Output Feedback Mode (OFB) is shown in Fig. 8.1.14. Key features of this mode are mentioned below: • OFB is also a stream cipher • Encryption is performed by XORing the message with the one-time pad • One-time pad can be generated in advance • If some bits of the ciphertext get garbled, only those bits of plaintext get garbled • The message can be of any arbitrary size • Less secure than other modes

Triple DES Tincreasing the key length. Its operation is explained below: • Each block of plaintext is subjected to enencryption by K1 in a sequen• CBC is used to turn the block encryption scheme into a stream encryption

Public key Cryptography

In public key cryptography, there are two keys: a private key and a public key. The public key is announced to the public, where as the private key is kept by the receiver. The sender uses the public key of the receiver for encryption and the receiver uses his private key for decryption

• Advantages: ○ The pair of keys can be used with any other entity The number of keys required is small ○• Disadvantages: It is not efficient for long messages

Figure 27-5

Signing the whole document

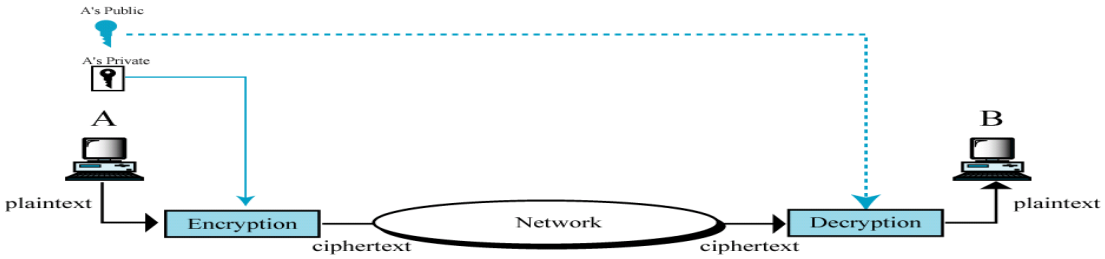


Figure 27-6

Signing the digest

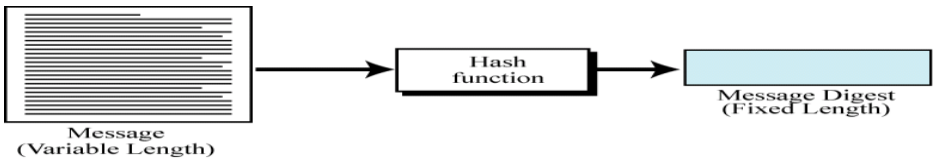
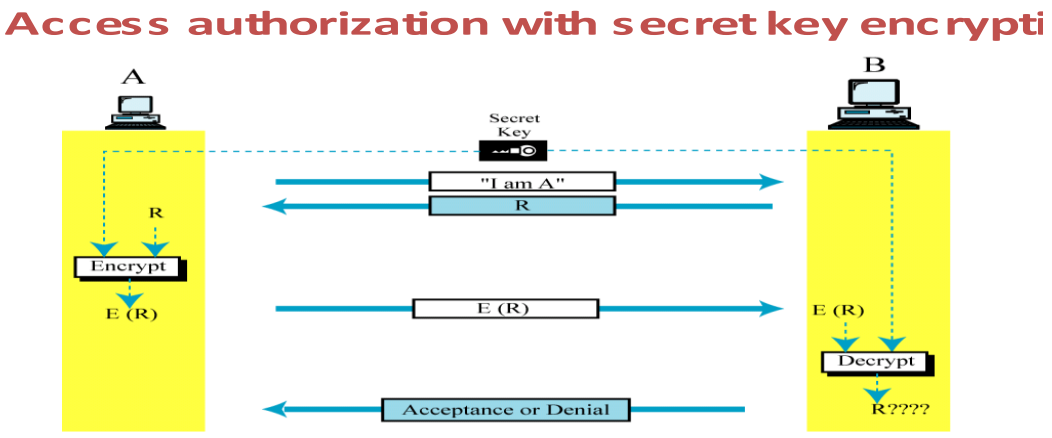


Figure 25-11



TEXT BOOKS

1. Behrouz A. Foruzan, "Data communication and Networking", Tata McGraw-Hill, 2006: Unit I-IV
2. Andrew S. Tannenbaum, "Computer Networks", Pearson Education, Fourth Edition, 2003: Unit V

REFERENCES

1. Wayne Tomasi, "Introduction to Data Communication and Networking", 1/e, Pearson Education.
2. James .F. Kurouse & W. Rouse, "Computer Networking: A Topdown Approach Featuring",3/e, Pearson Education
3. C.Sivaram Murthy, B.S.Manoj, "Ad hoc Wireless Networks – Architecture and Protocols", Second Edition, Pearson Education.
4. Greg Tomshon, Ed Tittel, David Johnson. "Guide to Networking Essentials", fifth edition, Thomson India Learning, 2007.
5. William Stallings, "Data and Computer Communication", Eighth Edition, Pearson Education, 2000.