UNIT V DATA NETWORKS

Data transmission in PSTN – packet switching – connection oriented and connectionless protocols – ISO – OSI architecture – TCP/IP and Internet – multiple access techniques – satellite based data networks – principles of ATM networks-IP Switching-Applications

5.1 Data transmission in PSTN

The transmission medium is the physical foundation for all the data communications. The amount of data carried across the networks crossed the voice traffic level.

5.1.1 Data Rates in PSTN

Baud rate. The maximum rate of signal transitions that can be supported by a channel is known as baud rate.

A maximum data rate that a noiseless or ideal voice channel can support can be obtained from the **Nyquist theorem**

$$\mathbf{D = 2\,B\,log_2\,L\ bps}$$

Where D = Maximum data rate (in Baud or bps)

B = Bandwidth of the channel

L = Number of discrete levels in the signals.

For higher data rates, we translate information rate into symbols per second. **A symbol is any element of an electrical signal that can be used to represent one or more binary data bits.**

Symbol rate. The rate at which symbols are transmitted is the symbol rate. This rate may be represented as a systems baud rate. Fig.5.1 illustrates the pulse representation of the binary numbers used to code the samples and representation by voltage levels (symbols) rather than pulses.

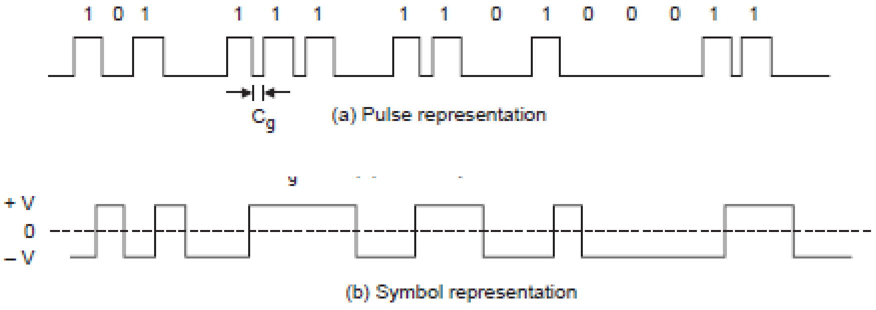

Fig. 5.1 Binary bits represented as (a) pulse and (b) symbol.

For noisy channel, data rate is calculated by

$$\mathbf{D_b = B\ log2\ (1 + S/N)}$$

Where D_b = Data rate in noisy channel (in bps)

B = Bandwidth of the channel

S/N = Signal to noise ratio.

Relation between baud rate (or symbol rate) and bps:

The baud rate and bit rate are related as

$$\mathbf{D_b = D \times \mathit{n}}$$

where *n* = number of bits required to represent signal levels.

5.2 PACKET SWITCHING

There are three types of switching used in PSTN network. The **circuit switching** and **message switching** were explained in unit-I. The **packet switching** overcomes all the limitations of message and circuit switching. Thus it is highly suitable for the data communication.

5.2.1 Packet Switching Principles

The data stream originating at the source is divided into packets of fixed or variable size. The data communication systems typically have **bursty traffic**.

Each packet contains a portion of the **user's data plus some control information**. This technique is called **store and forward technique**. Fig.5.2 illustrates the flow of packet switching.

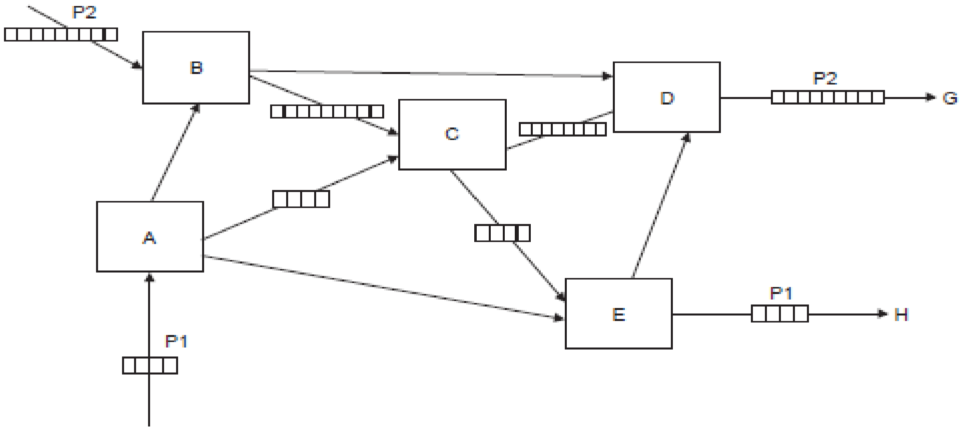

Figure 5.2 Packet switching principles

5.2.2 Routing Control

Routing control decides how the network will handle the stream of packets as it attempts to route them through the network and deliver them to the intended destination. The routing decision is determined in one of two ways. They are

1. Datagram and
2. Virtual circuit.

Datagram- In datagram, each packet within a stream is **independently routed**. A **routing table** stored in the router (switch) specifies the outgoing link for each destination. The table may be static or it may be periodically updated. In the second case, the routing depends on the router’s estimate of **the shortest path** to the destination.

Fig.5.3 shows a simple communication network where the concept of datagram is explained. The **circled one** are called the **switching nodes** whose purpose is to provide a switching facility that will move the data from node to node until they reach the destination. The **squared one** are called **the stations**. The stations may be computers, terminals, telephones or other.

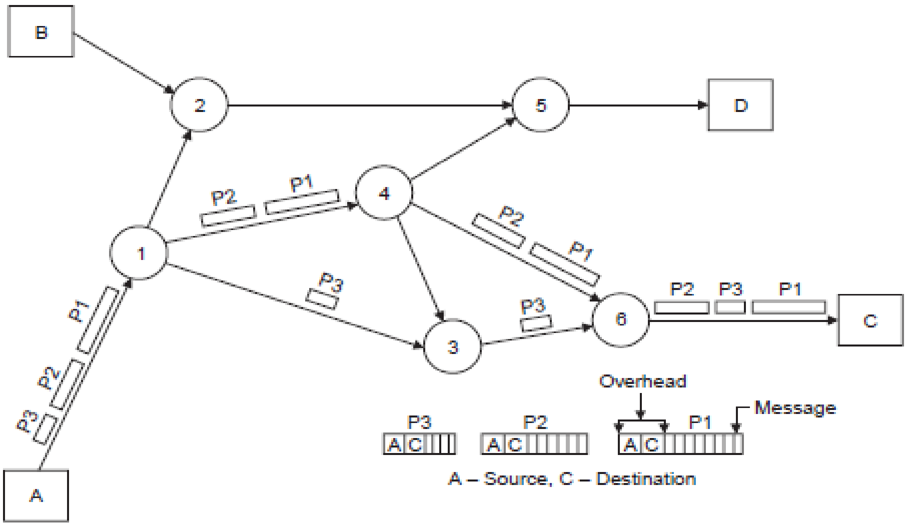

Figure 5.3 Concept of datagram.

Virtual circuit. In virtual circuit, a **fixed route** is selected before any data is transmitted in a call setup phase similar to circuit switched network. All packets belonging to the same data stream follow this **fixed route called a virtual circuit**. Packet must now contain a **virtual circuit identifier**. This bit string is usually **shorter** than the source and destination address identifiers needed for datagram. Once the virtual circuit is established, the message is transmitted in packets. Fig.5.4 shows the concept of virtual circuit.

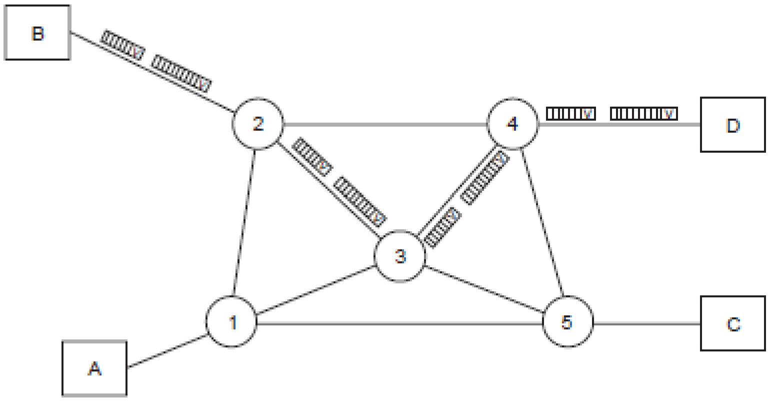

Figure 5.4 Concept of virtual circuit.

Packet size. If an organization has large amounts of data to send, then the data can be delivered to a packet assembler/disassembler (PAD). The PAD (software package) receives the data and breaks it down into manageable packets. In the data communication, a packet can be a variable length. Usually upto 128 bytes of data is in one packet.

5.2.3 Comparison of Circuit Switching and Packet Switching

There are two types of approaches in packet switching. **Datagram and virtual circuit**. The circuit switching is compared with these two approaches.

Datagram switching achieves **higher link utilization** than circuit switching especially when the traffic is bursty. No dedicated path is required as circuit switching. But the datagram have the **disadvantage** over virtual circuit wire.

1. End to end delay may be so large or so random as to preclude applications that demant guaranteed delay.

2. The overhead due to source and destination identifiers and bits needed to delimit packets may waste a significant fraction of the transmission capacity if the packet are very short.

3. A datagram switch does not have the state information to recognize if a packet belongs to a particular application. Hence the switch can not allocate resources (bandwidth and uffers) that the application may require.

Virtual circuits are more advantages and currently the packet switching network uses the virtual circuit approach. The overhead is comparable to circuit switching. As the packets arrives in sequence, no resequencing is needed.

Statistical multiplexing of packets at the router or switch can achieve better utilization than in circuit switching. Since packets contains their virtual circuit identifiers (VCI), the switch can allocate resources depending on the VCI. During the connection setup phase, the switches may be notified that a particular VCI should be given extra resources.

5.2.4 Packet Formats

The format of a packet in packet switching network can vary significantly from one network to another. Generally header includes all related control information. In some cases, control information is communicated through special control packets. Fig.5.5 shows typical packet format.

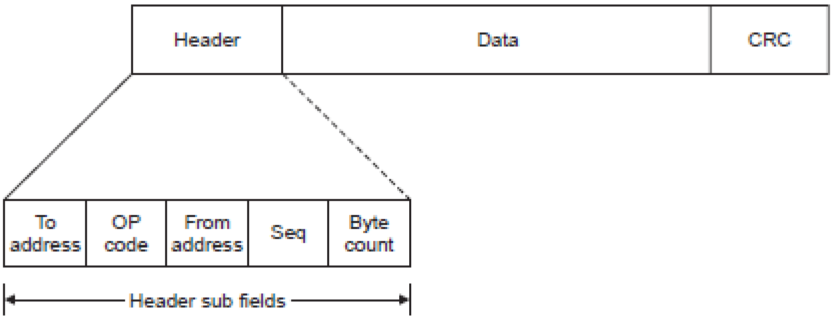

Figure 5.5 Typical packet formats.

A packet contains 3 major fields.

1. **Header.** It contains sub fields in addition to the necessary address fields. Other than the to and from address field, the following are the useful control information.
   - **Op code.** It designates whether the packet is a message (text) packet or control packet.
   - A **sequence number (Seq)** to reassemble messages at the destination node, detect faults and facilitates recovery procedures.
   - **Byte count.** Used to indicate the length of a packet.
2. **Data.** A portion of a data stream to be transferred in the data field. Some packets may not contain a message field if they are being used strictly for control purposes.
3. **CRC.** The cyclic redundancy checks (CRC) field contains a set of parity bits that cover overlapping fields of message bits. The fields overlap in such a way that small numbers of errors are always detected. The probability of not detecting the occurance of 2 large numbers of errors is 1 in 2M, where M is the number of bits in the cheek code.

(For detailed explanation https://youtu.be/3C7PhWzdWqg)

5.3 OSI MODEL

The Open System Inter connection (OSI) model was developed by the International organization for standardization (ISO). The ISO developed OSI for networking.

An open system is a set of protocols that allows two computers to communicate with each other regardless of their design, manufacturer or CPU type.

The OSI model defines seven distinct levels in its communication model. In the following paragraphs all this levels are explained in detail.

5.3.1 OSI Network Architecture

In the table 5.1 shown, the specification/functions of the layer are given briefly. The detailed explanation of each layer is given in the following sections.

Table 5.1 OSI layer specifications

LAYER	SPECIFICATIONS
7	**APPLICATION LAYER:** Performs information processing such as file transfer, e-mail and teletext. Detailed and application specific information about data being exchanged.
6	**PRESENTATION LAYER:** Defines the format of data to be sent: ASCII, data encryption, data compression and EBCDIC.
5	**SESSION LAYER:** Management of connections between programs. Sets up a session between two applications by determining the type of communication such as duplex, half duplex, synchronization etc.
4	**Transport layer:** Delivery of sequence of packets. Ensures data gets to destination. Manages error control, flow control and quality of service.
3	**NETWORK LAYER:** Format of individual data packets. Sets up connection, disconnects connection, and provides routing and multiplexing.
2	**DATA LINK LAYER:** Manages framing, error detection, and retransmission of message. Access to and control of transmission medium.
1	**PHYSICAL LAYER:** Medium and signal formed of raw bit information. Electrical interface (type of signal), Mechanical interface (type of connector), converts electrical signal to bits, transmits and receives electrical signals.

Let computer A sends a data stream of bits to computer B. Communication must move from higher layer down through the lower layers on computer A. Each layer in sending machine adds its own information to the message.

In receiving computer B, communication must move from lower layer up through the higher layers. At the receiving machine, the message is unwrapped layer by layer.

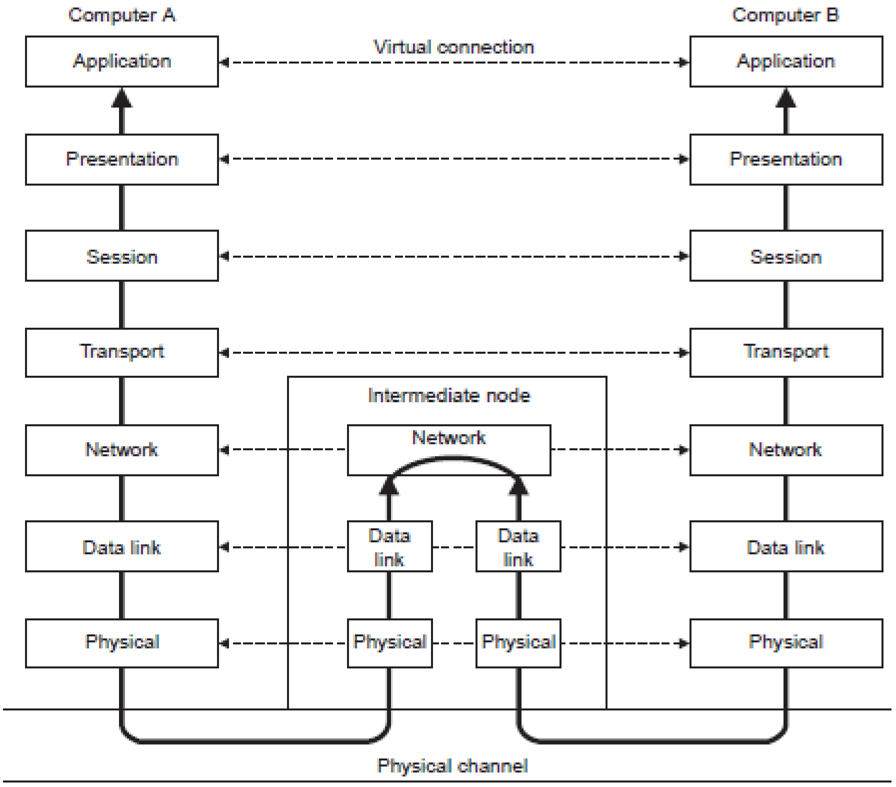

Figure5.6 OSI network architecture

The information added to the message in layers of the sending computer is in the form of **headers and trailers**. Headers are added to the message at layers **6, 5, 4, 3 and 2**. A trailer is added at layer **2**. In receiving computer, each layer removes the data meant for it and original message is recovered by the receiving computer B.

Between computers, layer *x* on one computer communicates with layer *x* on another machine. This communication is governed by certain protocols. The process on each machine at a given layer is called **pear to pear processes**.

In the following sections, all the layers are explained under three headings as network support layers, transport layer and support layers.

5.3.2. Network Support Layers

The **physical layer, data link layer and network layer** are referred as **network support layers.**

All these layers are explained below.

5.3.2.1 PHYSICAL LAYER.

It defines the mechanical, electrical, functional and procedural aspects of the physical link between networks.

5.3.2.2 DATA LINK LAYER.

- The data link layer defines the frame format such as start of frame, end of frame, size of frame and type of transmission.
- The principal service provided by the data link layer to higher layer is that of error detection and control.
- The data link layer also performs the flow control and access control.
- Two sub layers defined in the data link are the media access control (MAC) and the logical link control (LLC) layer.
    - MAC performs **address management** function.
    - LLC manages **flow and error control, automatic requests** for retransmission (APQ) and **handshake processes.**

5.3.2.3 NETWORK LAYER.

- The function of the network layer is to accomplish source to destination delivery.
- The network layer checks the logical address of each frame and forwards the frame to the next router based on a look up table.
- The network layer is responsible for translating each logic address (name address) to a physical address (MAC address).
- There are two types of virtual circuits used in the network layer.
    - In **connection oriented service**, the network layer makes a connection between source and destination, then the transmission starts.
    - In **Connectionless circuits** are also known as ‘‘bandwidth on demand’’ circuits, which establish a connection when they are needed.

5.3.3. Transport Layer

- The transport layer provides a mechanism for the exchange of data between end systems.
- Essentially, this layer is responsible for the reliable data transfer between two end nodes and is sometimes referred to as host-to host layer.
- Other processes at transport layer are :
  1. Error detection and recovery to minimize data loss and time loss due to retransmission of frames.
  2. Sets quality of service (QOS) for network layer packets to assure end-to-end message integrity.
  3. A process called blocking is employed when requested by sending station. Blocking is used to prevent specific frames to reach a particular node.

5.3.4. Support Layers

The **session layer, presentation layer and application layer** are considered as **support layers**. All these layers explained in the following paragraphs.

5.3.4.1 SESSION LAYER.

The session layer establishes a logical connection between the applications of two computers that are communicating with each other.

The session layer concerns file management and overall networking functions.

5.3.4.2 PRESENTATION LAYER.

The presentation layer receives information from the application layer and converts into ASCII or unicode or encrypts or decrypts.

This layer is concerned with the syntax and semantics of the information exchanged between two systems.

5.3.4.3 APPLICATION LAYER.

This layer enables users to access the network with applications such as e-mail, FTP and Telnet.

It provides user interfaces and support for various services.

[For detailed explanation please visit https://youtu.be/HEEnLZV2wGI]

5.4 TCP/IP

Transmission Control Protocol and Internet Protocol (TCP/IP) was developed not only to create LANs, but also for internetworking multiple LAN's. Data sharing and broadcasting are prominent features of LAN technology. TCP/IP provides three sets of services. They are :

1. **Connectionless service.** This service is described as an unreliable (delivery is not guaranteed), packet delivery service. A packet may be lost, duplicated, delayed or delivered out of order, but the service will not detect such conditions. Here each packet is considered independently.
2. **Reliable transport services.** Work with any environment.
3. **Application services.** Interfaces to most services on other architectures.

5.4.1 TCP/IP Reference Model

TCP/IP architecture is a four layer stack that deals with the equivalent seven layer architecture of OSI, SNA and DNA. Fig. 11.12 shows the TCP/IP reference model.

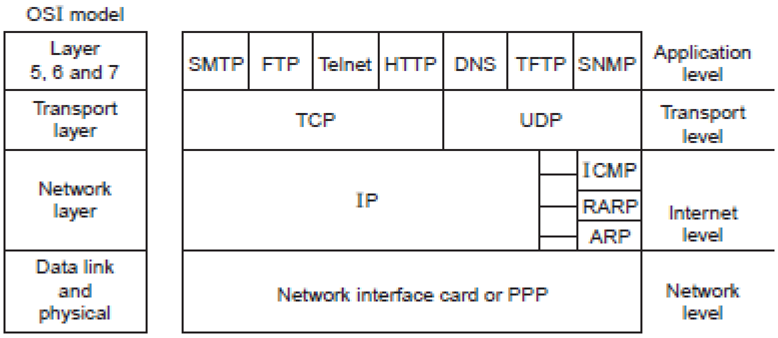

Fig.5.7 TCP/IP reference model.

Application level : Some of the internet applications are SMTP, FTP, Telnet, HTTP, DNS, TFTP, SNMP.

SMTP : Simple Mail Transfer Protocol (SMTP) is used for E-mail. It is used for transferring messages between two hosts.

Telnet : It is the most important Internet applications. It enables one computer to establish a connection to another computer.

FTP: File transfer protocol (FTP) is an internet standard for file transfer. FTP establishes a connection to a specified remote computer using an FTP remote host address.

HTTP: Hypertext Transfer Protocol (HTTP) is an advanced file retrieval program that can access distributed and linked documents on the web. HTTP is a stateless protocol that treats each transaction independently.

DNS: Domain Name System (DNS) is used to identify and locate computers connected to the internet.

SNMP: Simple Network Management Protocol (SNMP) is used by the network administrator to detect problem in the network such as router and gateway.

Transport Level Protocols : This layer consists of User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

UDP: It provides unreliable service between hosts. UDP accepts infromation from the application layer and adds a source port, destination port, UDP length and UDP checksum. The resulting packet is called UDP datagram packet.. Fig. 11.13 shows the UDP packet format.

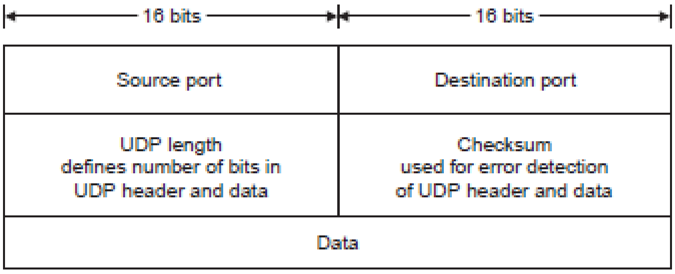

Fig.5.8 UDP packet format.

The IP protocol adds its header to the packet received from UDP and passes to LLC. MAC adds its own header and transfers the frame to the physical layer for transmission.

5.4.2 Transmission Control Protocol (TCP):

- The transmission control protocol (TCP) is a transport layer that carries application layer packets and services between two users.
- TCP offers reliable delivery of information through the internet.
- In TCP, connection between users is established before transmitting information. TCP assigns a sequence number to each packet.
- The receiving end checks the sequence number of all packets to ensure that they are received.
- When the receiving end gets a packet, it sends acknowledgment. If the sending node does not receive an acknowledgement within a given period of time, if retransmits the previous packet.

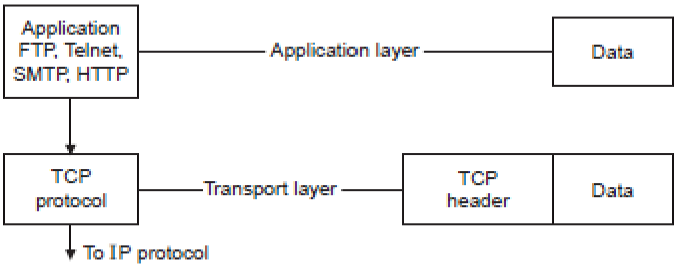

Fig.5.9 TCP operation.

The TCP header includes valuable information’s. Fig5.10 shows the TCP header.

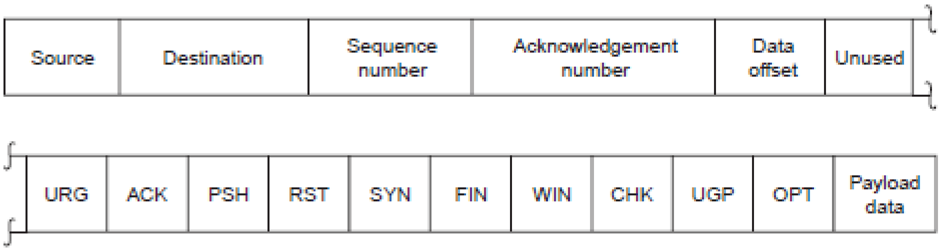

Fig.5.10 TCP header.

Source and destination. These address provides routing information for the packet.

Sequence number. It is a number label for each packet sent by the source. It is 32 bit length. The order of the packets within the completed message frame work are maintained by the use of sequence numbers.

Acknowledgment number. It acknowledges the next packet expected to be received from the source. It is 32 bits length.

Data offset. The number of 32 bit words in the header is known as the data offset number, because it indicates how much the beginning of the data is offset by the header.

URG. Urgent pointer is set to ‘1’ when the field contains urgent data. The urgent pointer indicates the offset value of the current segment and informs the receiver to find the urgent data indicated by URG.

ACK. Acknowledge flag bit is set to ‘1’ to represent that the acknowledgement number is valid.

PSIF. This field set to ‘1’ means that the receiver should push the data to an application as soon as possible.

RST. The reset bit causes the transport connection to be reset at the end of a session. It resets the connection.

SYN. A synchronization flag set to ‘1’ when a node wants to establish a connection. A SYN indication is used to establish a connection in combination with the acknowledge (ACK) bit.

SYN = 1, ACK = 0 is a connection request and

SYN = 1, ACK = 1 is a connection acknowledgement.

FIN. The FIN flage set to ‘1’ indicates that the incoming packet is the last packet. Otherwise, the final data segment is indicated by the FIN bit in the header.

WIN. The window specifies the number of data bytes the sender is willing to accept, inturn, from the host end. It is 16 bits length.

CHK. The TCP checksum is 16 bit long. It is used for error detection in TCP header and data field.

OPT. It is called option field

URG = 0 = end of option list

1 = no operation

2 = maximum segment size.

(For detailed explanation https://youtu.be/601x64peZtU?list=PLA959674DF91F95E4)

5.5 Multiple access techniques

As the spectrum is limited, Multiple access techniques are used to allow a large number of users to share the allocated spectrum in the most efficient manner.

There are several different ways to allow access to the channel. These includes mainly the following:

1) Frequency division multiple-access (FDMA)

2) Time division multiple-access (TDMA)

3) Code division multiple-access (CDMA)

4) Space Division Multiple access (SDMA)

5.5.1 Frequency division multiple-access (FDMA)

- This was the initial multiple-access technique in which each individual user is assigned a pair of frequencies while making or receiving a call as shown in Figure 5.11
- One frequency is used for downlink and one pair for uplink. This is called frequency division duplexing (FDD).

The **features of FDMA** are as follows:

- The FDMA channel carries only one phone circuit at a time.
- If an FDMA channel is not in use, then it sits idle and it cannot be used by other users to increase share capacity

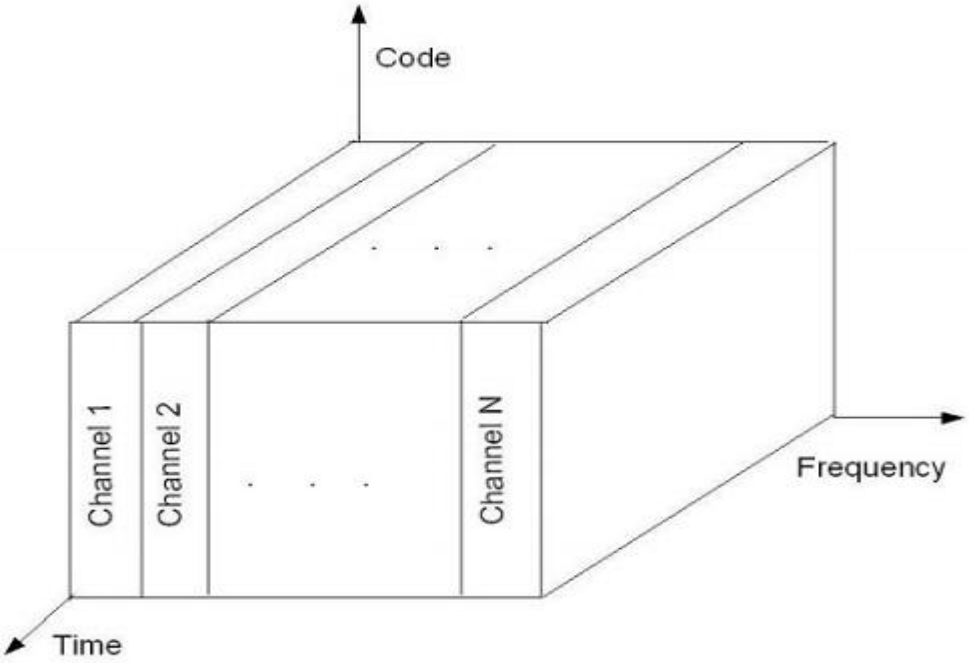

Figure 5.11 Frequency division duplexing (FDD)

5.5.2 Time Division Multiple Access

- In digital systems, continuous transmission is not required because users do not use the allotted bandwidth all the time. In such cases, TDMA is a complimentary access technique to FDMA.
- Global Systems for Mobile communications (GSM) uses the TDMA technique.
- In TDMA, the entire bandwidth is available to the user but only for a finite period of time.
- TDMA requires careful time synchronization since users share the bandwidth in the frequency domain.
- TDMA uses different time slots for transmission and reception. This type of duplexing is referred to as **Time division duplexing(TDD).**

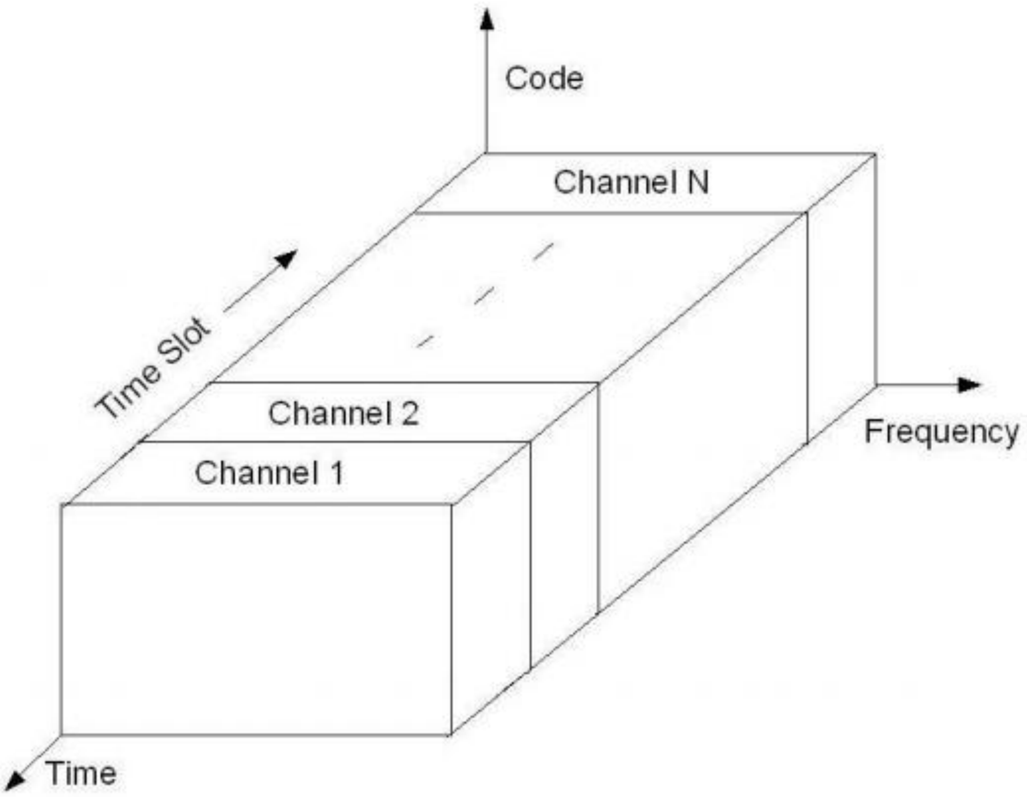

Figure 5.12 The basic concept of TDMA

5.5.3 Code Division Multiple Access

- In CDMA, the same bandwidth is occupied by all the users, however they are all assigned separate codes, which differentiates them from each other (shown in Figure 5.12).
- CDMA utilize a spread spectrum technique in which a spreading signal is used to spread the narrow band message signal.

5.5.3.1 Direct Sequence Spread Spectrum (DS-SS)

This is the most commonly used technology for CDMA. In DS-SS, the **message signal is multiplied by a Pseudo Random Noise Code**.

Each user is given his own codeword which is orthogonal to the codes of other users and in order to detect the user, the receiver must know the codeword used by the transmitter. There are, however, two problems in such systems which are discussed in the sequel.

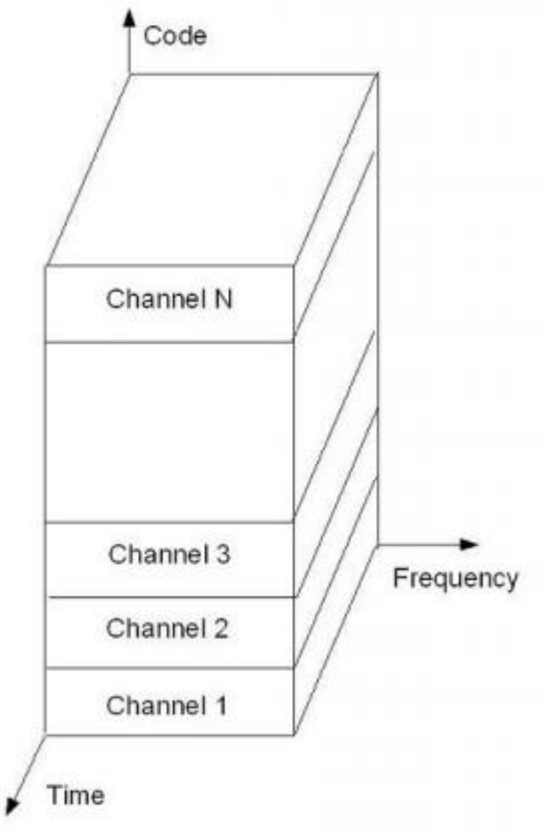

Figure 5.13 The basic concept of CDMA

5.5.3.2 CDMA and Near-Far Problem

This problem arises from the fact that signals closer to the receiver of interest are received with smaller attenuation than are signals located further away. Therefore the strong signal from the nearby transmitter will mask the weak signal from the remote transmitter.

(For detailed explanation https://youtu.be/4F_613NKUo4)

5.6 Satellite based data networks

A communication satellite functions as an overhead wireless repeater station that provides a microwave communication link between two geographically remote sites.

Due to its high altitude, satellite transmissions can cover a wide area over the surface of the earth.

Most satellites simply broadcast whatever they receive, and are often referred to as **"bent pipes".** These were traditionally used to support applications such as TV broadcasts and voice telephony.

5.6.1 Why we need satellite communication?

- Wide Area coverage of the earth's surface.
- Long transmission.
- Large Channel Bandwidth.
- Transmission costs independent of Distance.

5.6.2 Types of Satellites:

Types of Satellites

- LEO: Low Earth Orbit.
- MEO: Medium Earth Orbit.
- GEO: Geostationary Earth Orbit.

Types	Orbit Height	Time	**Merits**
LEO: Low Earth Orbit.	100-300 miles	15 min	• Lower launch costs • Very short round trip delays • Small path loss
MEO: Medium Earth Orbit.	6000-12000 miles	2-4 hrs	• Moderate launch cost • Small roundtrip delays
GEO: Geostationary Earth Orbit.	22,282 miles	24 hrs	• High launch cost • Covers 42.2% of the earth's surface • Constant view

5.6.3 Satellite Communication Configuration:

- Point-to- Point Link
- Broadcast Link

5.6.4 MAC Protocols For Satellite Links:

- ALOHA FDMA (Frequency Division Multiple Access)
- FAMA-FDMA
- DAMA-FDMA
- TDMA (Time Division Multiple Access)
- CDMA (Code Division Multiple Access)

(For details explanation www.cse.wustl.edu/~jain/cis788-97/ftp/**satellite_data**.pdf)

5.7 Principles of ATM networks

- ATM is a high Performance, cell oriented switching and multiplexing technology that utilizes fixed length packets to carry different types of traffic.
- ATM is the next generation of networking technology to be used on the information super highway.
- ATM is well suited for bursty traffic and allows communications between devices that operate at different speeds.

5.7.1 Advantages of ATM

- The most important advantages or benefits of the ATM are:
- A much wider array of information
- ATM delivers bandwidth on demand, is not dependent on applications
- The service is connection oriented, with data transferred over a virtual circuit.
- ATM switches are statistical multiplexing.
- Higher quality of service.
- Wider array of information can be handled.
- Accepts variety of transmission media such as optical fiber or twisted pair cable.
- Works with current LAN and WAN technologies and supports current protocols such as TCP/IP.

5.7.2 Concepts of ATM

5.7.2.1 Connection oriented service.

In connected oriented service, over a virtual circuit, the data stream from origin to destination follows the **same path**.

Virtual circuit (a type of packet switching) operate on the same concept as packet switching, but the routing of packet is specified before transmission.

Data from different connections is distinguished by means of virtual path identifier (VPI) and virtual channel identifier (VCI). **VPI and VCI are called connection identifiers.**

5.7.3 ATM Services. ATM forum specifies five types of services. They are:

1. **Constant bit rate (CBR).** This is used for emulating circuit switching. The cell rate is constant with time. Telephone traffic, videoconferencing and television are the examples that use CBR.

2. **Variable bit rate–non real time (VBR–NRT).** This service allows users to send traffic at a rate that varies with time depending on the availability of user information. Multimedia email is an example of VBR–NRT.

3. **Variable bit rate–real time (VBR–RT).** This service is similar to VBR–NRT, but it 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.

4. **Available bit rate (ABR).** This service provides rate based flow control and is aimed at data traffic such as file transfer and e-mail.

5. **Unspecified bit rate (UBR).** This class is widely used today for TCP/IP.

5.7.4 Two types of connection:

1. **Permanent virtual connection (PVC).** PVC is a connection that is setup and taken down manually by a network manager. A set of network switches between the ATM source and destination are programmed with predefined values for VCI/VPI.

2. **Switched virtual circuit (SVC).** SVC is a connection that is setup automatically by a signalling protocol. SVC is more widely used because it does not require manual setup, but it is not reliable.

ATM switch operation : ATM switch process cells at an extremly high rate or speed. Fig.5.14 illustrates the basic operation of ATM switch.

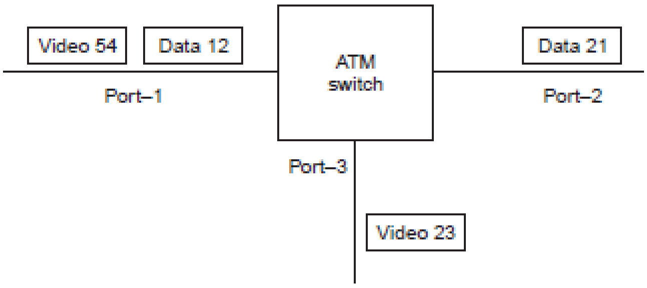

Fig.5.14 ATM switch.

Fig.5.14 shows the ATM switch with 3 ports. The cells enter the switch from port 1 and go out from the switch to ports 2 and 3 according to the routing table.

(For detailed explanation https://youtu.be/IPuLZSOye4c)

5.8 IP SWITCHING

The rapid growth of Internet and increase in real-time and multimedia applications have created a need to improve Internet routing technology in terms of bandwidth, performance, scalability and delivery of new functionalities.

Most of the current applications are based on IP and hence the success of ATM depends a lot on its capabilities to support IP and other higher layer protocols.

To counter one or more of above problems, several independent approaches have been made which can be divided into two broad categories. One is to **run IP over ATM** and other is to use the **label switching technology of ATM** for packet forwarding.

The "IP over ATM" approach tries to hide the underlying network topology from IP layer by treating the data link layer as large, opaque network cloud. However, this leads to inefficiency, complexity and duplication of functionality in the resulting network.

To construct an IP switch, a standard ATM switch is taken, the hardware is left untouched, but all the control software above AAL-5 is removed. It is replaced by standard IP routing software, a flow classifier to decide whether to switch a flow or not and a driver to control the switch hardware.

To gain the benefits of switching, a mechanism has been defined to associate IP flows with the ATM labels.

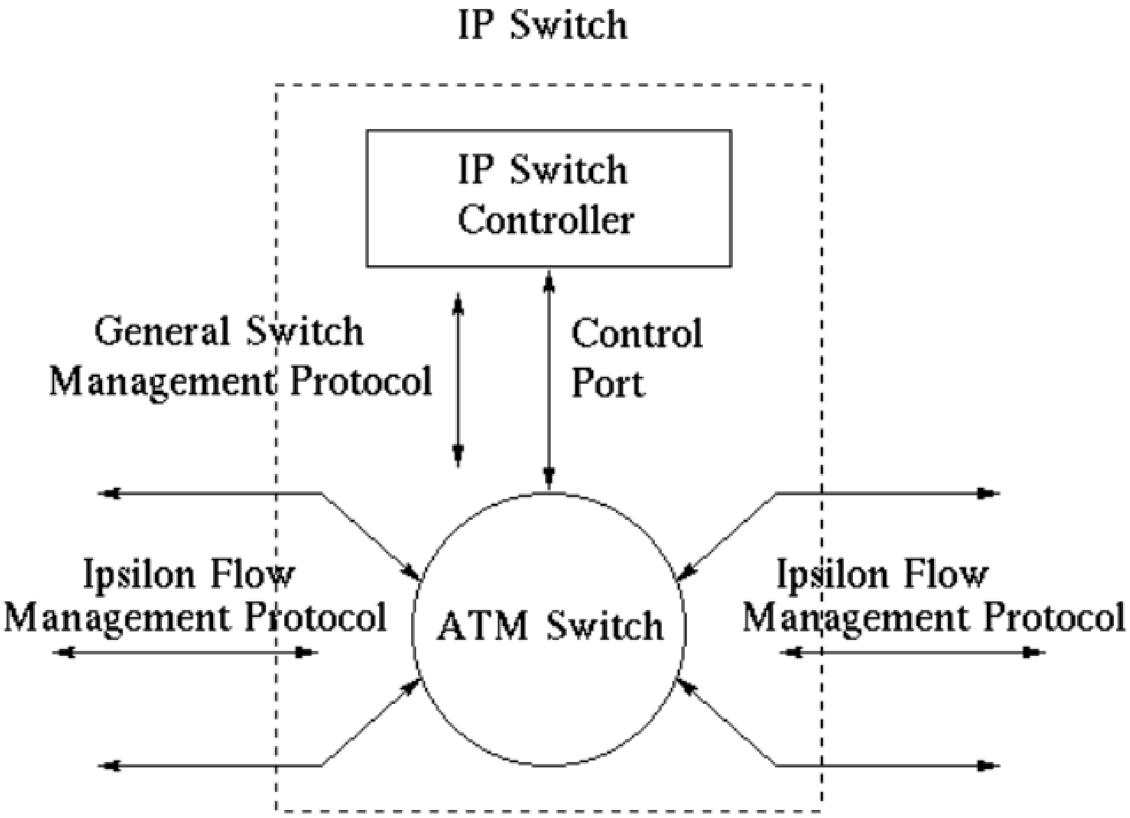
IP Switch
IP Switch Controller
General Switch Management Protocol
Control Port
Ipsilon Flow Management Protocol
ATM Switch
Ipsilon Flow Management Protocol

Figure 5.15 ATM Switch

5.8.1 IP Switching Features

Following are some important features of IP Switching

● **Point-to-Point**- IP Switching advocates point-to-point network model for ATM rather than a logical shared medium model as proposed by some competing approaches.

.● **Quality of Service-** An IP Switch can make QoS decision according to its local policy.

● **Latency** The latency in setting up of a virtual channel from source to destination can be low for connection oriented protocols like TCP.

(For detailed explanation http://www.cs.wustl.edu/~jain/cis788-97/ftp/ip_switching.pdf)

5.9 Applications

5.9.1 Economic/Industrial Telecommunications networks are making it possible for developing countries to participate in the world economy in ways that simply were not possible in the past – by enabling them to take advantage of their intellectual and cultural resources. Computer networking has taken over localised computing all over the world to allow for resources and information sharing.

5.9.2 Health Care The development of teleconferencing facilities and multi-media capabilities of telecommunications systems, which has made it possible to combine audio and video facilities, has been of immense benefit especially in healthcare delivery.

5.9.3 Education Perhaps one of the most important applications of telecom in the education sector is in the area of Distance Learning. A number of educational institutions are not only able to run courses concurrently, but lectures can also be received simultaneously, as they are being delivered, in different lecture rooms that are located in places far away from the actual point of delivery.

5.9.4 Transportation. Transportation, as a medium of establishing contact between people and of exchanging goods, is another major beneficiary of developments in telecommunications. Be it in air, sea or land transportation, telecommunications facilities have been developed to facilitate these businesses. The commercial airline industry will certainly grind to a halt without telecommunications facilities. Monitoring of travel schedules and bookings are heavily dependent on telecommunications.

5.9.5 Rural Development. In recent times, concerted efforts are being made on improving access to telecommunications services in the rural areas, hence the various Rural Telecommunications and Universal Service obligations and initiatives.

5.9.6 Disaster Warning Systems. It will never be possible to eliminate or even substantially reduce the vulnerability of large numbers of population to natural disasters such as floods, earthquakes, severe storms, etc. Consequently, the only feasible option is the dissemination of early warnings of approaching disasters. Warning of potential disasters is very dependent on effective communications systems and networks. Long-range forecasts are based on monitoring satellite observations.

For detailed explanation
ncc.gov.ng/archive/.../Practical**Applications**_of_TelecommsEVC190402.pdf