Bandwidth Limited Signals

A signal is said to be band-limited or bandwidth-limited if it can be represented by a finite number of harmonics. Engineers limit the bandwidth of signals to enable multiple signals to share the same channel with minimal interference. A key result that pertains to bandwidth-limited signals is Nyquist's sampling theorem, which states that a signal of bandwidth B can be reconstructed by taking $2B$ samples every second. In 1924, Harry Nyquist derived the following formula for the maximum data rate that can be achieved in a noiseless channel:Maximum Data Rate = $2\ B\ \log_2 V$ bits per second,where B is the bandwidth of the channel and V is the number of discrete signal levels used in the channel. For example, to send only zeros and ones requires two signal levels. It is possible to envision any number of signal levels, but in practice the difference between signal levels must get smaller, for a fixed bandwidth, as the number of levels increases. And as the differences between signal levels decrease, the effect of noise in the channel becomes more pronounced.

Bandwidth

There are three frequently used definitions of bandwidth in the context of Information Technology (IT) and general business.

1) In computer networks, bandwidth is used as a synonym for data transfer rate, the amount of data that can be carried from one point to another in a given time period (usually a second). Network bandwidth is usually expressed in bits per second (bps); modern networks typically have speeds measured in the millions of bits per second (megabits per second, or Mbps) or billions of bits per second (gigabits per second, or Gbps).

Note that bandwidth is not the only factor that affects network performance: There is also packet loss, latency and jitter, all of which degrade network throughput and make a link perform like one with lower bandwidth. A network path usually consists of a succession of links, each with its own bandwidth, so the end-to-end bandwidth is limited to the bandwidth of the lowest speed link (the bottleneck).

Different applications require different bandwidths. An instant messaging conversation might take less than 1,000 bits per second (bps); a voice over IP (VoIP) conversation requires 56 kilobits per second (Kbps) to sound smooth and clear. Standard definition video (480p) works at 1 megabit per second (Mbps), but HD video (720p) wants around 4 Mbps, and HDX (1080p), more than 7 Mbps.

Effective bandwidth -- the highest reliable transmission rate a path can provide -- is measured with a bandwidth test. This rate can be determined by repeatedly measuring the time required for a specific file to leave its point of origin and successfully download at its destination.

2) Bandwidth is the range of frequencies -- the difference between the highest-frequency signal component and the lowest-frequency signal component -- an electronic signal uses on a given transmission medium. Like the frequency of a signal, bandwidth is measured in hertz (cycles per second). This is the original

meaning of bandwidth, although it is now used primarily in discussions about cellular networks and the spectrum of frequencies that operator's license from various governments for use in mobile services.

3) In business, bandwidth is sometimes used as a synonym for capacity or ability. In this sense, bandwidth usually refers to having time or staffing available to tackle something, e.g. "We just don't have the bandwidth to take on mobile app development, we're already short-staffed on developers."

Latency

- AAA

Latency is the delay from input into a system to desired outcome; the term is understood slightly differently in various contexts and latency issues also vary from one system to another.

Latency greatly affects how usable and enjoyable electronic and mechanical devices as well as communications are.

Latency in communication is demonstrated in live transmissions from various points on the earth as the communication hops between a ground transmitter and a satellite and from a satellite to a receiver each take time. People connecting from distances to these live events can be seen to have to wait for responses. This latency is the wait time introduced by the signal travelling the geographical distance as well as over the various pieces of communications equipment. Even fiber optics are limited by more than just the speed of light, as the refractive index of the cable and all repeaters or amplifiers along their length introduce delays.

Types of latency

Network latency is an expression of how much time it takes for a packet of data to get from one designated point to another. In some environments (for example, AT&T), latency is measured by sending a packet that is returned to the sender; the round-trip time is considered the latency. Ideally latency is as close to zero as possible.

The contributors to network latency include:

- Propagation: This is simply the time it takes for a packet to travel between one place and another at the speed of light.
- Transmission: The medium itself (whether optical fiber, wireless, or some other) introduces some delay, which varies from one medium to another. The size of the packet introduces delay in a round trip since a larger packet will take longer to receive and return than a short one. Also, when signals must be boosted by a repeater, this too introduces additional latency.
- Router and other processing: Each gateway node takes time to examine and possibly change the header in a packet (for example, changing the hop count in the time-to-livefield).
- Other computer and storage delays: Within networks at each end of the journey, a packet may be subject to storage and hard disk access delays at intermediate devices such as switches and bridges. (In backbone statistics, however, this kind of latency is probably not considered.)

Internet latency is just a special case of network latency - the Internet is a very large wide-area network (WAN). The same factors as above determine latency on the Internet. However, distances in the transmission medium, the number of hops over equipment and servers are all greater than for smaller networks. Internet latency measurement would generally start at the exit of a network and end on the return of the requested data from an Internet resource.

WAN latency itself can be an important factor in determining Internet latency. A WAN that is busy directing other traffic will produce a delay whether a resource is being requested from a server on the LAN, another computer on that network or elsewhere on the Internet. LAN users will also experience delay when the WAN is busy. In either of these examples the delay would still exist even if the rest of the hops -- including the server where the desired data was located -- were entirely free of traffic congestion.

Audio latency is the delay between sound being created and heard. In sound created in the physical world, this delay is determined by the speed of sound, which varies slightly depending on the medium the sound wave travels through. Sound travels faster in denser mediums: It travels faster through solids, less quickly through liquids and slowest through air. We generally refer to the speed of sound as measured in dry air at room temperature, which is 796 miles-per-hour. In electronics, audio latency is the cumulative delay from audio input to audio output. How long this delay is depends on the hardware and even software used, such as the operating system and drivers used in computer audio. Latencies of 30milliseconds are generally noticed by an individual as a separate production and arrival of sound to the ear.

Operational latency can be defined as the sum time of operations, when performed in linear workflows. In parallel workflows, the latency is determined by the slowest operation performed by a single task worker.

Mechanical latency is the delay from input into a mechanical system or device to the desired output. This delay is determined by Newtonian physics-based limits of the mechanism (excepting quantum mechanics). An example would be the delay in time to shift a gear from the time the shift lever of a gear box or bicycle shifter was actuated.

Computer and operating system latency is the combined delay between an input or command and the desired output. In a computer system, latency is often used to mean any delay or waiting that increases real or perceived response time beyond what is desired. Specific contributors to computer latency include mismatches in data speed between the microprocessor and input/output devices, inadequate data buffers and the performance of the hardware involved, as well as its drivers. The processing load of the computer can also add significant latency.

From the user's perspective, latency issues are usually a perceived lag between an action and a response to it. In 3D VR simulation, for example, in using a helmet that provides stereoscopic vision and head tracking, latency is the time between the computer's detection of head motion to the time it displays motion in the image. In multiplayer networked or Internet gaming, low latency is critical for best gameplay and enjoyability. Control is difficult with significant latency as the player is lagging behind the real-time events in the game, due to delays in the information getting to their computer.

Latency issues are noticeable for an individual, generally increasing user annoyance and impacting productivity as the level increases above 30ms. The severity of the effect varies from one application to another, as do mitigating tactics. However, games can often be enjoyable up to around 90ms latency. In communications, delays can be a result of heavy traffic, hardware problems, incorrect set up and/or configuration.

Latency testing:

Latency testing can vary from application to application. In some applications, measuring latency requires special and complex equipment or knowledge of special computer commands and programs; in other cases, latency can be measured with a stop watch. In networking, an estimated latency to equipment or servers can be determined by running a ping command; information about latency through all the hops can be gathered with a trace route command. High-speed cameras might be used to capture the minute differences in response times for input to various mechanical and electronic systems.

Reducing latency:

Reducing latency is a function of tuning, tweaking and upgrading both computer hardware and software and mechanical systems. Within a computer, latency can be removed or hidden by such techniques as prefetching (anticipating the need for data input requests) andmultithreading or by using parallelism across multiple execution threads. Other steps to reduce latency and increase performance include uninstalling unnecessary programs, optimizing networking and software configurations and upgrading or overclocking hardware.

Jitter

Jitter is any deviation in, or displacement of, the signal pulses in a high-frequency digitalsignal. The deviation can be in terms of amplitude, phase timing or the width of the signal pulse. Among the causes of jitter are electromagnetic interference (EMI) and crosstalk with other signals. Jitter can cause a display monitor to flicker, affect the ability of theprocessor in a desktop or server to perform as intended, introduce clicks or other undesired effects in audio signals, and loss of transmitted data between network devices. The amount of allowable jitter is highly dependent on the application.

Jitter in IP networks is the variation in thelatency on a packet flow between two systems, when some packets take longer to travel from one system to the other. Jitter results from network congestion, timing drift and route changes.

Jitter is especially problematic in real-time communications like IP telephony and video conferencing. It is also a serious problem for hosted desktops and virtual desktop infrastructure (VDI). Jitter can lead to audio and video artifacts (unintended deviation or inconsistency) that degrade the quality of communications.

A jitter buffer (or de-jitter buffer) can mitigate the effects of jitter, either in the network on a router or switch, or on a computer. The application consuming the network packets essentially receives them from the buffer instead of directly. They are fed out of the buffer at a regular rate, smoothing out the variations in timing of packets flowing into the buffer.

Other techniques for mitigating jitter where multiple pathways for traffic are available is to selectively route traffic along the most stable paths, or to always pick the path that can come closest to the targeted packet delivery rate.

II

Data Link protocols - II Unit.

Chapter 4

The Point to Point Protocol (PPP)

This chapter gives an overview of the PPP, explains the various stages, some packet formats, implementation details and options, and discusses the PPP implementation on the WMI™.

4.1 Introduction to PPP

Much help was acquired from Internet Request-For-Comments (RFC) documents on the details of the point-to-point protocol. PPP is a protocol that can be used to establish communication between any two communicating devices that need to exchange information. Information is exchanged in the form of structured data packets. The point-to-point links that utilize this protocol should be able to support full-duplex communication.

PPP can be fragmented into three parts:

1. Encapsulation
2. Link Control Protocol (LCP)
3. Network Control Protocol (NCP)

4.2 Encapsulation

Encapsulation is provided by PPP so that different protocols at the network layer can be supported simultaneously. Data is sent in frames whose general structure is shown in Figure 4.1 [2]. Data is transmitted from the left to right.

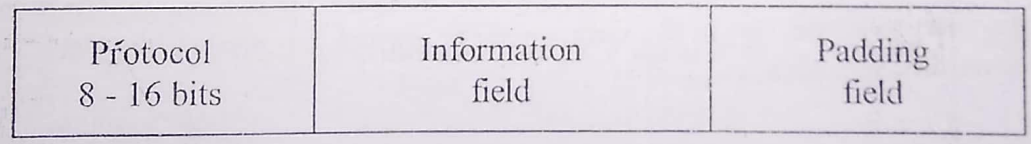


Figure 4.1: Encapsulation of PPP packets

4.2.1 Protocol field

This field is one or two bytes and it identifies the data being sent in the information field. All protocol values are odd numbers. The least significant bit of the lower byte is always set to "1" and that of the most significant bit is always set to "0". Frames that violate these rules are treated as unrecognized protocols.

Some examples of protocol field values are:

0xC021 for Link control protocol
0xC023 for Password Authentication Protocol
0x8021 for Internet Protocol Control Protocol

4.2.2 Information field

This field is zero or more bytes long. It has a maximum length (including padding and excluding the protocol field) of 1500 bytes. This limit is termed as the Maximum Receive Unit (MRU) at the receiving end and Maximum Transmit Unit (MTU) at the transmitting end. The default field length is also 1500 bytes. Negotiations are possible between peers as to the MRU values.

4.2.3 Padding

This is an optional field. The information field may be padded with as many bytes as needed to reach the MRU. However, both peers should be able to recognize the padding bytes from the true data.

4.3 Block diagram

To establish communication between two peers, LCP packets must first be sent both ways to configure the link. Any peer may request validation after link configuration. This phase is optional when there is no such request made. Figure 4.2 shows the phase diagram that the link passes through in order to support PPP [2].

The end of the link establishment phase (or the authentication phase as the case may be) triggers the next phase - the network phase. In this stage a Network Control Protocol (NCP) is first selected and then the link can proceed to obey the rules of sending/receiving NCP packets. Some of the available Network Layer Protocols (NLP) are ATCP (AppleTalk Control Protocol), IPCP (Internet Protocol Control Protocol), Novell IPX Control Protocol, etc. These protocols are similar to the LCP in message format, with varying details. It is at this layer, that messages can be sent to select IP addresses.

The link remains open for communications until special LCP/NCP packets are sent to close down the link or other events trigger a shutdown (time out, human intervention, etc.).

4.4 PPP phases

4.4.1 Link Dead phase

The link starts and stops in this phase. The detection of a carrier signal at the peer triggers the link to proceed to the next phase. Disconnecting from the modem line should bring the link back to this phase.

4.4.2 Link Establishment phase

Once the presence of the peer is detected, the link proceeds to this phase. In this phase, the LCP establishes a healthy connection by exchanging configuration packets. After the link configuration has been consented upon, **Configure-Ack** packets are sent and received [2].

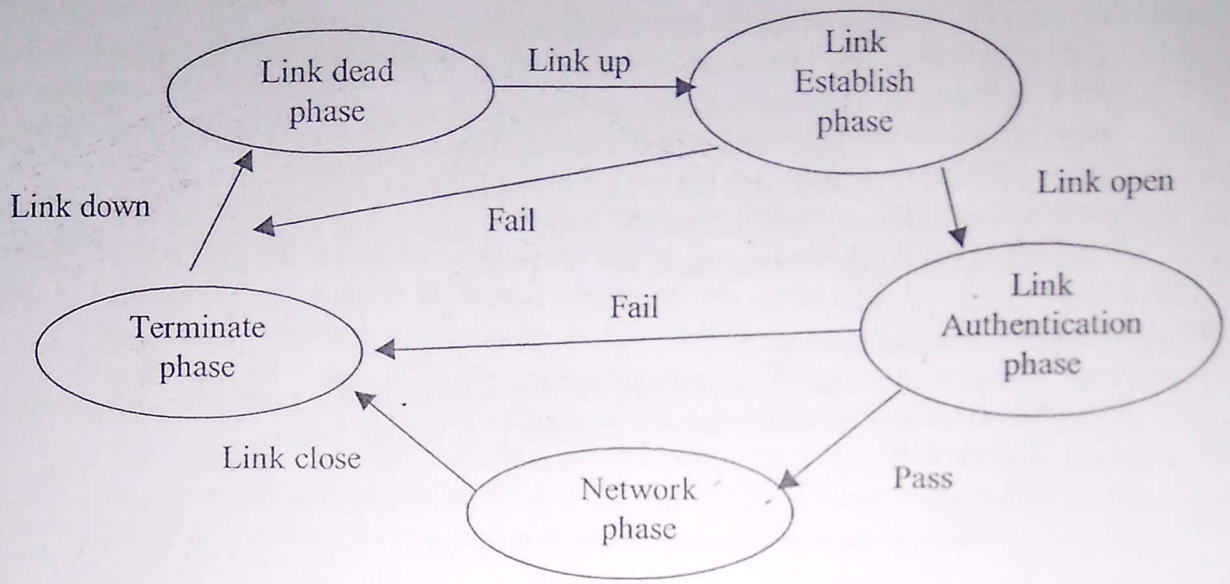


Figure 4.2: Different phases of PPP

Configuration options have defined default values, which can be modified during this phase. These options are independent of the network layer protocol being implemented. These options are negotiated between the peers based on the hardware and software abilities at both the ends.

Any non-LCP packets received during this phase should be discarded and logged. When the link is in the network layer protocol (NLP) phase, receiving a **Configure-Request** packet causes the link to move back to the Link Establishment phase [2].

The end of this phase indicates the LCP open state.

4.4.3 Authentication phase

This is an optional phase. Before proceeding to the NLP, a peer may request authentication or validation by the other peer. By default, this phase is optional. If a peer requests authentication, a request must be issued during the link establishment process where configuration options are negotiated. If requested, this phase must be entered as soon as link establishment is complete. It is possible that link quality determination may occur during this phase. If link quality determination needs to be performed while in the authentication phase, appropriate priority levels should be given to the quality determination process.

Entering the NLP, requires passing the authentication phase. Failing at validation necessitates the link to move to the termination phase, only after a sufficient number of failed attempts. Only authentication protocol, LCP, and link quality determination packets can be sent and received during this phase. All other packets received must be discarded and logged.

There are two types of authentication protocols that can be implemented.

4.4.3.1 Password Authentication Protocol (PAP)

The PAP provides an easy implementation of peer authentication. It is only performed after the link establishment phase. The peer repeatedly requests an ID/Password pair until authentication is acknowledged. If invalid authentication is received after repeated multiple requests, the link is terminated.

This protocol is not the most secure implementation since passwords are sent without any encryption over the links. There is no protection from repeated trial attacks to hack the password.

4.4.3.1.1 Configuration option

Figure 4.3 shows the format for the authentication protocol configuration option to request PAP validation by the peer [2]. In this format,

Type = 3
Length = 4
Authentication-Protocol = 0xC023 for PAP

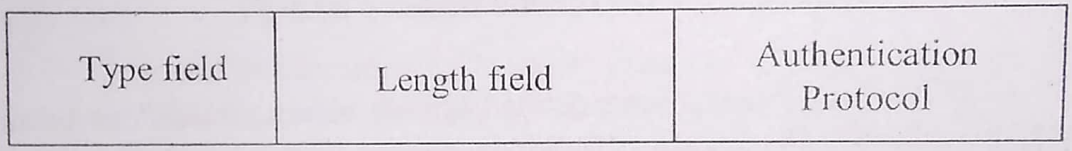


Figure 4.3: Configuration format for PAP

4.4.3.1.2 Packet format

The generic PAP packet is shown in Figure 4.4 [2]. Each PPP frame houses only one PAP packet in its information field. The protocol field is set to 0xC023, reserved for the PAP.

The **code** field is 1-byte wide and is either 1,2 or 3 depending on whether an **Authentication-Request**, **Authentication-Ack**, or **Authentication-Nak** is being sent or received.

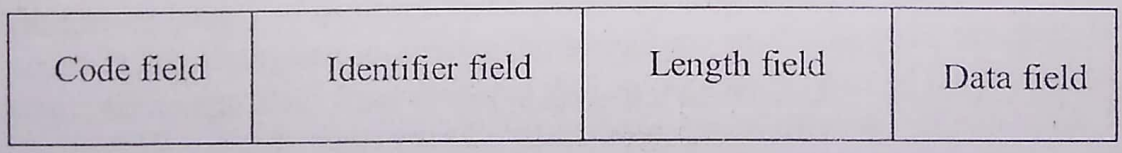


Figure 4.4: Configuration format for PAP,LCP

The **identifier** field (1-byte wide) is used to match requests and replies.

The **length** field (2-bytes wide) holds the length of the PAP packet, which includes all the fields transmitted (**Code**, **length**, **identifier**, and **data** fields).

The **data** field is zero or more bytes wide and its content depends on the **code** field contents (Request, Acknowledge or Not-Acknowledge).

For more details on the different command structures for **Authentication-Request**, **Authentication-Ack**, or **Authentication-Nak**, please refer to [2].

4.4.3.2 Challenge-Handshake Authentication Protocol (CHAP)

Unlike the PAP, where authentication is requested only at the initial time of link establishment, the CHAP necessitates periodic peer validation. This is done at initial link establishment, and could also be requested after link establishment. The authenticator sends a challenge signal to the peer who responds with a value computed from a complex algorithm. This returned value is compared at the authenticator's end with its expected value. If the values match, the peer is validated or else the link is terminated after a specified number of failed attempts. This ensures greater security in the implementation. If this protocol is implemented, the **protocol** field value in the PPP frames has a value of 0xC223. More information on this protocol can be found in reference [2].

4.4.4 Network Layer Protocol phase

Once the PPP has successfully passed through the authentication phase, the NLP phases must be configured (similar to the LCP phases). Some examples of NLPs are Internet Protocol (IP), AppleTalk (AT) etc. The configuration of these NLPs is achieved by implementing the appropriate NCPs. The corresponding NCPs are Internet Protocol Control Protocol (IPCP) for IP, AppleTalk Control Protocol (ATCP) for AT etc.

Each NCP can be opened and closed independently at any time. The RFC rules strongly recommend the avoidance of fixed timeouts while waiting for NCPs to configure. This is due to the significant latency involved in piercing through the link establishment phase (including quality determination and possible authentication). Any **supported** NLP packets received when the corresponding NCP is closed are discarded after logging. Similarly, any **unsupported** NLP packet must, in the LCP open state, be returned with a **Protocol-Reject** packet.

4.4.5 Link Termination phase

The link can be terminated at any point of time. This can happen due to any of the following factors -- carrier can not be detected, authentication failure, idle-period time-out, human intervention or bad link quality.

The link is shut down after sending and receiving **Terminate** packets. Before shutting down, PPP informs the upper NLPs so that appropriate action (termination) is taken at all layers.

After **Terminate** packets are exchanged, the implementation closes the physical-link thus terminating the link. Upon sending a **Terminate-Request**, the requester waits for a **Terminate-Ack** or waits for a timer to expire before actual termination. Likewise, the receiver of a **Terminate-Request** packet waits for the peer to disconnect or waits for at least one time-out period after issuing a **Terminate-Ack** packet before disconnecting.

Any non-LCP packets received after the link is terminated are logged and discarded. Link closure at the LCP level is sufficient for termination. It is not

Serial Line Internet Protocol (SLIP)

SLIP is different from most TCP/IP protocols in that it has never been defined as a formalized standard. It was created informally in the early 1980s and its use spread as a de facto standard before it was ever described in an RFC document. Even when it was eventually published, in 1988, the decision was specifically made that SLIP would ***not*** be designated an official Internet standard. The authors of the paper that describes it, RFC 1055, made sure nobody would miss this point, by naming it *A Nonstandard For Transmission Of IP Datagrams Over Serial Lines: SLIP*.

SLIP is a TCP/IP protocol used for communication between two machines that are previously configured for communication with each other. For example, your Internet server provider may provide you with a SLIP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. Your dial-up connection to the server is typically on a slower serial line rather than on the parallel or multiplex lines such as a line of the network you are hooking up to.

Short for *Serial Line Internet Protocol*, a protocol for connection to the Internet via a dial-up connection. Developed in the 80s whenmodem communications typically were limited to 2400 bps, it was designed for simple communication over serial lines. SLIP can be used on RS-232 serial ports and supports asynchronous links.

A more common protocol is PPP (Point-to-Point Protocol) because it is faster and more reliable and supports functions that SLIP does not, such as error detection, dynamic assignment of IP addresses and data compression.

SLIP has been largely replaced by the Point-to-Point Protocol (PPP), which is better engineered, has more features and does not require its IP address configuration to be set before it is established.

On microcontrollers, however, SLIP is still the preferred way of encapsulating IP packets due to its very small overhead.

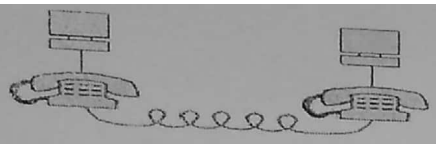
PPP and SLIP protocols

The majority of people. not having lines (cable or Ethernet) linked directly to the Internet, must use telephone lines (the most widely used network) to connect to the Internet. The connection is made using a modem, a device capable of converting digital data from the computer into analogue signals (that can circulate on telephone lines by amplitude or frequency modulation, in the same way as voice when you use the telephone).

Considering that only two computers are communicating and the speed of a telephone line is slow in comparison to that of a local network, it is necessary to use a protocol enabling standard communication between the different machines using a modem, and not overload the telephone line. These protocols are called *modem protocols*.

The notion of a point to point link

Via a standard telephone line, a maximum of two computers can communicate using a modem, in the same way that it is impossible to call two people simultaneously using the same telephone line. This is thus called a **point to point link**, i.e. a link between two machines reduced to its most simple expression: there is no need to share the line between several machines, each one speaks and responds in turn.



So, many modem protocols have been developed. The first of them allowed a single transmission of data between two machines, then some of them were equipped with error control and with the growth of the Internet, were equipped with the ability to address machines. In this way, there are now two main modem protocols:

- SLIP: an old protocol, low in controls
- PPP: the most widely used protocol for accessing the Internet via a modem, it authorizes addressing machines

The SLIP protocol

SLIP means *Serial Line Internet Protocol*. SLIP is the result of the integration of modem protocols prior to the suite of TCP/IP protocols.

It is a simple Internet link protocol conducting neither address or error control, this is the reason that it is quickly becoming obsolete in comparison to PPP.

Data transmission with SLIP is very simple: this protocol sends a frame composed only of data to be sent followed by an end of transmission character (the *END* character, the ASCII code of which is 192). A SLIP frame looks like this:

Data to be transmitted	END

The PPP protocol

PPP means *Point to Point Protocol*. It is a much more developed protocol than SLIP (which is why it is replacing it), insofar as it transfers additional data, better suited to data transmission over the Internet (the addition of data in a frame is mainly due to the increase in bandwidth).

In reality, PPP is a collection of three protocols:

- a datagram encapsulation protocol
- an **LCP**, Link Control Protocol, enabling testing and communication configuration
- a collection of **NCPs**, Network Control Protocols allowing integration control of PPP within the protocols of the upper layers

Data encapsulated in a PPP frame is called a *packet*. These packets are generally datagrams, but can also be different (hence the specific designation of *packet* instead of datagram). So, one field of the frame is reserved for the type of protocol to which the packet belongs. A PPP frame looks like this:

Protocol (1-2 bytes)	Data to be transmitted	Padding data

The padding data is used to adapt the length of the frame for certain protocols.

A PPP session (from opening to closure) takes place as follows:

- Upon connection, an LCP packet is sent

- In the event of an authentication request from the server, a packet relating to an authentication protocol may be sent (PAP, *Password Authentication Protocol*, or CHAP, *Challenge Handshake Authentication Protocol* or Kerberos)
- Once communication is established, PPP sends configuration information using the NCP protocol
- Datagrams to be sent are transmitted as packets
- Upon disconnection, an LCP packet is sent to end the session

Routing is the process of selecting best paths in a network. In the past, the term routing was also used to mean forwarding network traffic among networks. However this latter function is much better described as simply forwarding. Routing is performed for many kinds of networks, including the telephone network (circuit switching), electronic data networks (such as the Internet), and transportation networks. This article is concerned primarily with routing in electronic data networks using packet switching technology.

In packet switching networks, routing directs packet forwarding (the transit of logically addressed network packets from their source toward their ultimate destination) through intermediate nodes. Intermediate nodes are typically network hardware devices such as routers, bridges, gateways, firewalls, or switches. General-purpose computers can also forward packets and perform routing, though they are not specialized hardware and may suffer from limited performance. The routing process usually directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router's memory, is very important for efficient routing. Most routing algorithms use only one network path at a time. Multipath routing techniques enable the use of multiple alternative paths.

In case of overlapping/equal routes, the following elements are considered in order to decide which routes get installed into the routing table (sorted by priority):

1. *Prefix-Length*: where longer subnet masks are preferred (independent of whether it is within a routing protocol or over different routing protocol)
2. *Metric*: where a lower metric/cost is preferred (only valid within one and the same routing protocol)
3. *Administrative distance*: where a route learned from a more reliable routing protocol is preferred (only valid between different routing protocols)

Routing, in a more narrow sense of the term, is often contrasted with bridging in its assumption that network addresses are structured and that similar addresses imply proximity within the network. Structured addresses allow a single routing table entry to represent the route to a group of devices. In large networks, structured addressing (routing, in the narrow sense) outperforms unstructured addressing (bridging). Routing has become the dominant form of addressing on the Internet. Bridging is still widely used within localized environments.

Routing schemes differ in their delivery semantics:

- unicast delivers a message to a single specific node
- broadcast delivers a message to all nodes in the network
- multicast delivers a message to a group of nodes that have expressed interest in receiving the message
- anycast delivers a message to anyone out of a group of nodes, typically the one nearest to the source
- geocast delivers a message to a geographic area

Unicast is the dominant form of message delivery on the Internet. This article focuses on unicast routing algorithms.

Routing Table

A routing table uses the same idea that one does when using a map in package delivery. Whenever a node needs to send data to another node on a network, it must first know *where* to send it. If the node cannot directly connect to the destination node, it has to send it via other nodes along a proper route to the destination node. Most nodes do not try to figure out which route(s) might work; instead, a node will send an IP packet to a gateway in the LAN, which then decides how to route the "package" of data to the correct destination. Each gateway will need to keep track of which way to deliver various packages of data, and for this it uses a Routing Table. A routing table is a database which keeps track of paths, like a map, and allows the gateway to provide this information to the node requesting the information.

In computer networking a **routing table**, or **routing information base** (RIB), is a data table stored in a router or a networked computer that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes. The routing table contains information about the topology of the network immediately around it. The construction of routing tables is the primary goal of routing protocols.

Modulation

A signal can be anything like a sound wave which comes out when you shout. This shout can be heard only up to a certain distance. But for the same wave to travel over a long distance, you'll need a technique which adds strength to this signal, without disturbing the parameters of the original signal.

What is Signal Modulation?

A message carrying signal has to get transmitted over a distance and for it to establish a reliable communication, it needs to take the help of a high frequency signal which should not affect the original characteristics of the message signal.

The characteristics of the message signal, if changed, the message contained in it also alters. Hence it is a must to take care of the message signal. A high frequency signal can travel up to a longer distance, without getting affected by external disturbances. We take the help of such high frequency signal which is called as a **carrier signal** to transmit our message signal. Such a process is simply called as Modulation.

Modulation is the process of changing the parameters of the carrier signal, in accordance with the instantaneous values of the modulating signal.

Need for Modulation

The baseband signals are incompatible for direct transmission. For such a signal, to travel longer distances, its strength has to be increased by modulating with a high frequency carrier wave, which doesn't affect the parameters of the modulating signal.

Advantages of Modulation

The antenna used for transmission, had to be very large, if modulation was not introduced. The range of communication gets limited as the wave cannot travel to a distance without getting distorted.

Following are some of the advantages for implementing modulation in the communication systems.

- Antenna size gets reduced.
- No signal mixing occurs.
- Communication range increases.
- Multiplexing of signals occur.
- Adjustments in the bandwidth is allowed.
- Reception quality improves.

Signals in the Modulation Process

Following are the three types of signals in the modulation process.

Message or Modulating Signal

The signal which contains a message to be transmitted, is called as a **message signal**. It is a baseband signal, which has to undergo the process of modulation, to get transmitted. Hence, it is also called as the **modulating signal**.

Carrier Signal

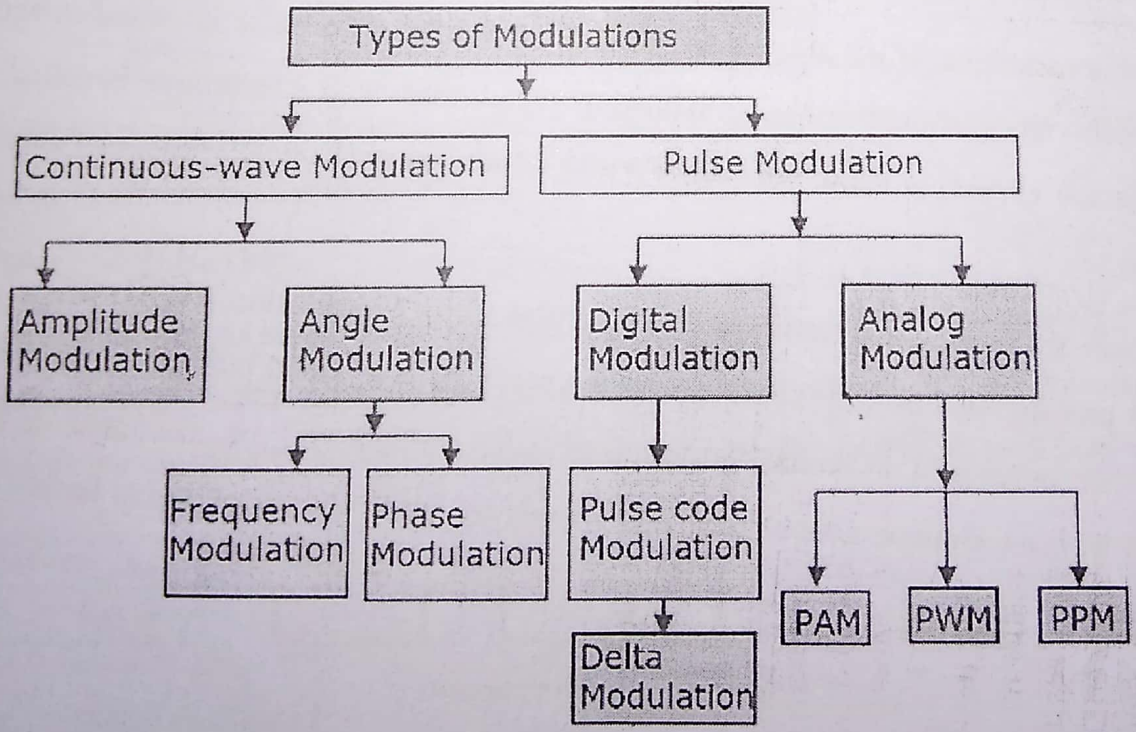
The high frequency signal which has a certain phase, frequency, and amplitude but contains no information, is called a **carrier signal**. It is an empty signal. It is just used to carry the signal to the receiver after modulation.

Modulated Signal

The resultant signal after the process of modulation, is called as the **modulated signal**. This signal is a combination of the modulating signal and the carrier signal.

Types of Modulation

There are many types of modulations. Depending upon the modulation techniques used, they are classified as shown in the following figure.



The types of modulations are broadly classified into continuous-wave modulation and pulse modulation.

Continuous-wave Modulation

In the continuous-wave modulation, a high frequency sine wave is used as a carrier wave. This is further divided into amplitude and angle modulation.

- If the amplitude of the high frequency carrier wave is varied in accordance with the instantaneous amplitude of the modulating signal, then such a technique is called as **Amplitude Modulation**.
- If the angle of the carrier wave is varied, in accordance with the instantaneous value of the modulating signal, then such a technique is called as **Angle Modulation**.

  The angle modulation is further divided into frequency and phase modulation.

  - If the frequency of the carrier wave is varied, in accordance with the instantaneous value of the modulating signal, then such a technique is called as **Frequency Modulation**.
  - If the phase of the high frequency carrier wave is varied in accordance with the instantaneous value of the modulating signal, then such a technique is called as **Phase Modulation**.

Pulse Modulation

In Pulse modulation, a periodic sequence of rectangular pulses, is used as a carrier wave. This is further divided into analog and digital modulation.

In **analog modulation** technique, if the amplitude, duration or position of a pulse is varied in accordance with the instantaneous values of the baseband modulating signal, then such a technique is called as **Pulse Amplitude Modulation (PAM)** or **Pulse Duration/Width Modulation (PDM/PWM)**, or **Pulse Position Modulation (PPM)**.

In **digital modulation**, the modulation technique used is **Pulse Code Modulation (PCM)** where the analog signal is converted into digital form of 1s and 0s. As the resultant is a coded pulse train, this is called as PCM. This is further developed as **Delta Modulation (DM)**, which will be discussed in subsequent chapters. Hence, PCM is a technique where the analog signals are converted into a digital form.

Digital Modulation Techniques

Digital Modulation provides more information capacity, high data security, quicker system availability with great quality communication. Hence, digital modulation techniques have a greater demand, for their capacity to convey larger amounts of data than analog ones.

There are many types of digital modulation techniques and we can even use a combination of these techniques as well. The most prominent digital modulation techniques are:

Amplitude Shift Keying

The amplitude of the resultant output depends upon the input data whether it should be a zero level or a variation of positive and negative, depending upon the carrier frequency. Amplitude Shift Keying (ASK) is a type of Amplitude Modulation which represents the binary data in the form of variations in the amplitude of a signal.

Following is the diagram for ASK modulated waveform along with its input.

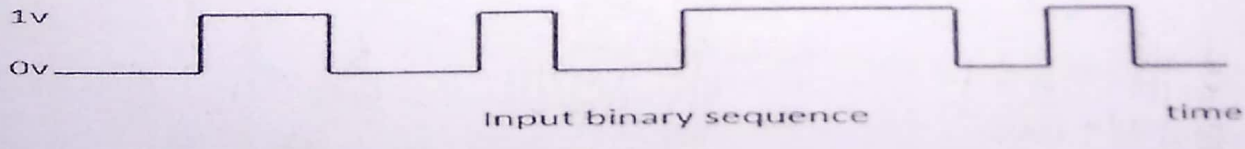
Input binary sequence

ASK Modulated output wave

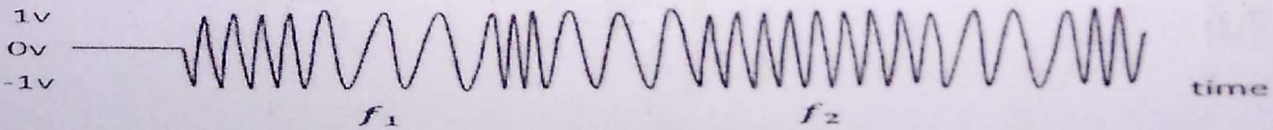
Any modulated signal has a high frequency carrier. The binary signal when ASK is modulated, gives a zero value for LOW input and gives the carrier output for HIGH input.

Frequency Shift Keying

The frequency of the output signal will be either high or low, depending upon the input data applied. Frequency Shift Keying (FSK) is the digital modulation technique in which the frequency of the carrier signal varies according to the discrete digital changes. FSK is a scheme of frequency modulation. Following is the diagram for FSK modulated waveform along with its input.



Input binary sequence time



FSK Modulated output wave

The output of a FSK modulated wave is high in frequency for a binary HIGH input and is low in frequency for a binary LOW input. The binary 1s and 0s are called Mark and Space frequencies.

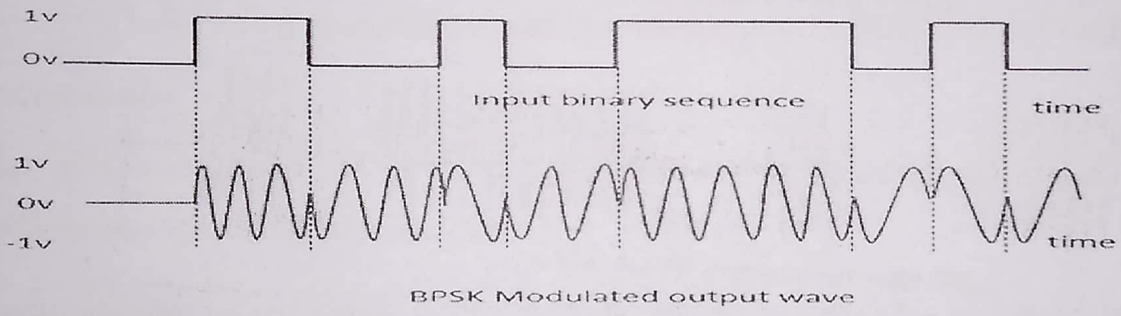
Phase Shift Keying

The phase of the output signal gets shifted depending upon the input. These are mainly of two types, namely BPSK and QPSK, according to the number of phase shifts. The other one is DPSK which changes the phase according to the previous value.

Phase Shift Keying (PSK) is the digital modulation technique in which the phase of the carrier signal is changed by varying the sine and cosine inputs at a particular time. PSK technique is widely used for wireless LANs, bio-metric, contactless operations, along with RFID and Bluetooth communications. PSK is of two types, depending upon the phases the signal gets shifted. They are –

Binary Phase Shift Keying (BPSK)

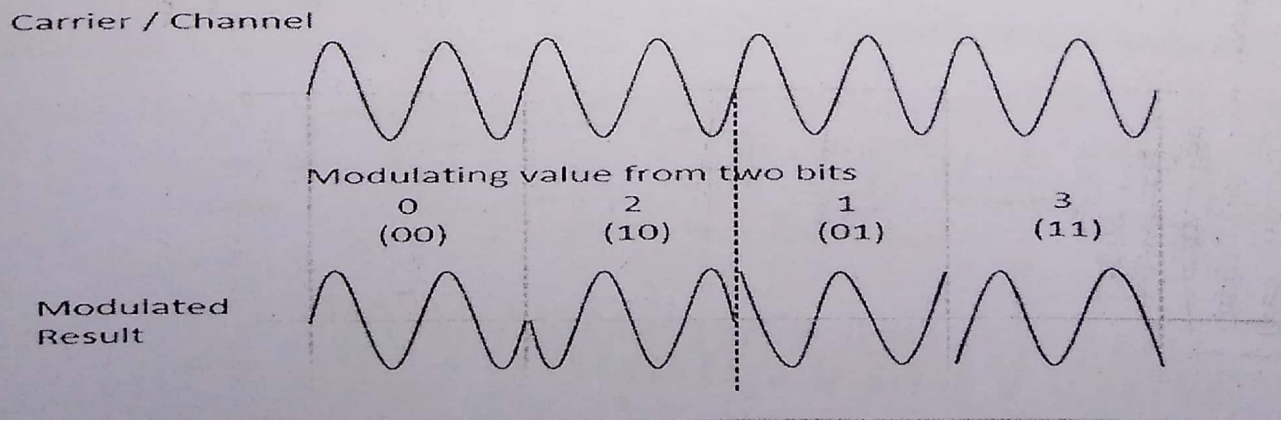
This is also called as 2-phase PSK (or) Phase Reversal Keying. In this technique, the sine wave carrier takes two phase reversals such as 0° and 180°. BPSK is basically a DSB-SC (Double Sideband Suppressed Carrier) modulation scheme, for message being the digital information. Following is the image of BPSK Modulated output wave along with its input.



BPSK Modulated output wave

Quadrature Phase Shift Keying (QPSK)

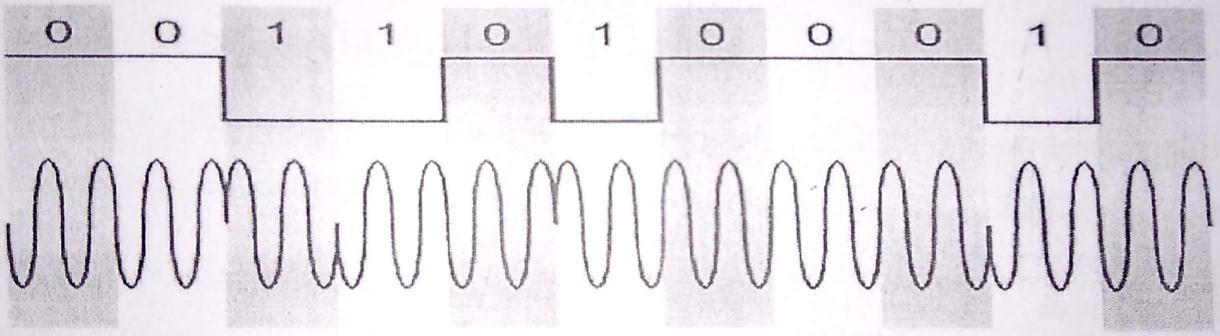
This is the phase shift keying technique, in which the sine wave carrier takes four phase reversals such as 0°, 90°, 180°, and 270°. If this kind of techniques are further extended, PSK can be done by eight or sixteen values also, depending upon the requirement. The following figure represents the QPSK waveform for two bits input, which shows the modulated result for different instances of binary inputs.



QPSK is a variation of BPSK, and it is also a DSB-SC (Double Sideband Suppressed Carrier) modulation scheme, which send two bits of digital information at a time, called as bigits. Instead of the conversion of digital bits into a series of digital stream, it converts them into bit-pairs. This decreases the data bit rate to half, which allows space for the other users.

Differential Phase Shift Keying (DPSK)

In DPSK (Differential Phase Shift Keying) the phase of the modulated signal is shifted relative to the previous signal element. No reference signal is considered here. The signal phase follows the high or low state of the previous element. This DPSK technique doesn't need a reference oscillator. The following figure represents the model waveform of DPSK.



It is seen from the above figure that, if the data bit is LOW i.e., 0, then the phase of the signal is not reversed, but is continued as it was. If the data is HIGH i.e., 1, then the phase of the signal is reversed, as with NRZI, invert on 1 (a form of differential encoding). If we observe the above waveform, we can say that the HIGH state represents an M in the modulating signal and the LOW state represents a W in the modulating signal.

Multiplexing

Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link. Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams.

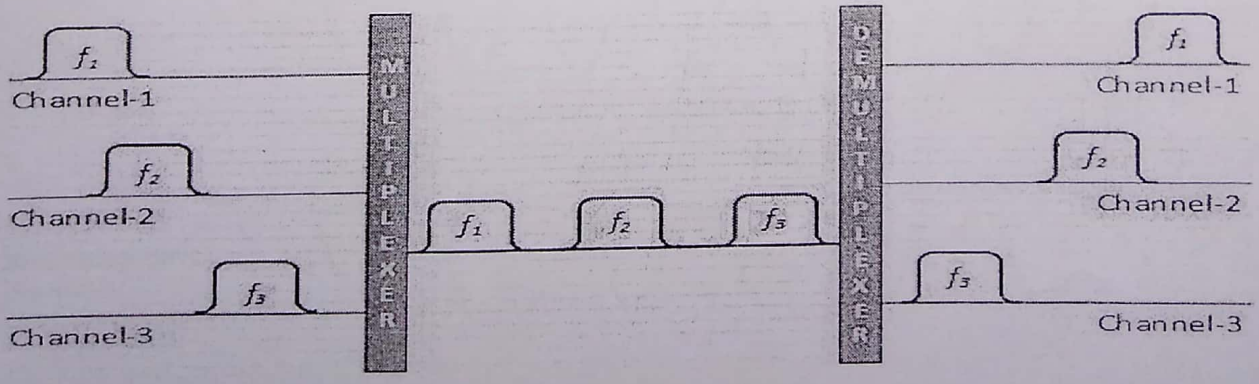
Communication is possible over the air (radio frequency), using a physical media (cable), and light (optical fiber). All mediums are capable of multiplexing.

When multiple senders try to send over a single medium, a device called Multiplexer divides the physical channel and allocates one to each. On the other end of communication, a De-multiplexer receives data from a single medium, identifies each, and sends to different receivers.

Networks use multiplexing to make it possible for any network device to talk to any other network device without having to dedicate a connection for each pair. This requires shared media.

Frequency Division Multiplexing

When the carrier is frequency, FDM is used. FDM is an analog technology. FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel. Each user can use the channel frequency independently and has exclusive access of it. All channels are divided in such a way that they do not overlap with each other. Channels are separated by guard bands. Guard band is a frequency which is not used by either channel.



In analog radio transmission, signals are commonly multiplexed using frequency-division multiplexing (FDM), in which the bandwidth on a communications link is

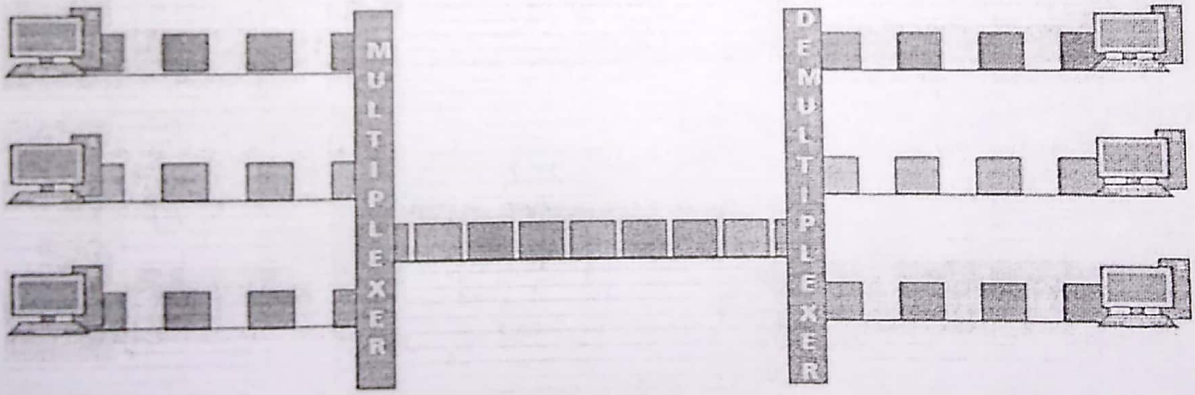
divided into subchannels of different frequency widths, each carrying a signal at the same time in parallel. Analog cable TV works the same way, sending multiple channels of material down the same strands of coaxial cable.

Time Division Multiplexing

TDM is applied primarily on digital signals but can be applied on analog signals as well. In TDM the shared channel is divided among its user by means of time slot. Each user can transmit data within the provided time slot only. Digital signals are divided in frames, equivalent to time slot i.e. frame of an optimal size which can be transmitted in given time slot.

TDM works in synchronized mode. Both ends, i.e. Multiplexer and De-multiplexer are timely synchronized and both switch to next channel simultaneously.

When channel A transmits its frame at one end, the De-multiplexer provides media to channel A on the other end. As soon as the channel A's time slot expires, this side switches to channel B. On the other end, the De-multiplexer works in a synchronized manner and provides media to channel B. Signals from different channels travel the path in interleaved manner.

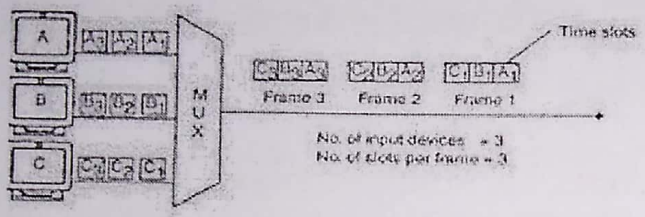


Types of TDM: Time division multiplexing is classifieds into four types:

1. Synchronous time-division multiplexing
2. Asynchronous time-division multiplexing
3. Interleaving time-division multiplexing
4. Statistical time-division multiplexing

Synchronous Time Division Multiplexing

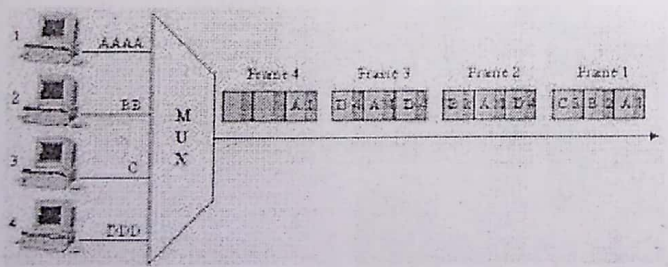
Synchronous time division multiplexing can be used for both analog and digital signals. In synchronous TDM, the connection of input is connected to a frame. If there are 'n' connections, then a frame is divided into 'n' time slots – and, for each unit, one slot is allocated – one for each input line. In this synchronous TDM sampling, the rate is same for all the signals, and this sampling requires a common clock signal at both the sender and receiver end. In synchronous TDM, the multiplexer allocates the same slot to each device at all times.



Synchronous Time Division Multiplexing

Asynchronous Time-Division Multiplexing

In asynchronous time-division multiplexing, the sampling rate is different for different signals, and it doesn't require a common clock. If the devices have nothing to transmit, then their time slot is allocated to another device. Designing of a commutator or de-commutator is difficult and the bandwidth is less for time-division multiplexing. This type of time-division multiplexing is used in asynchronous transfer mode networks.

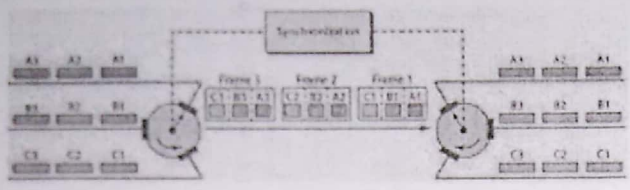


Asynchronous Time-Division Multiplexing

Interleaving

Time-division multiplexing can be visualized as two fast rotating switches on the multiplexing and demultiplexing side. At the same speed these switches rotate and synchronize, but in opposite directions. When the switch opens at the multiplexer

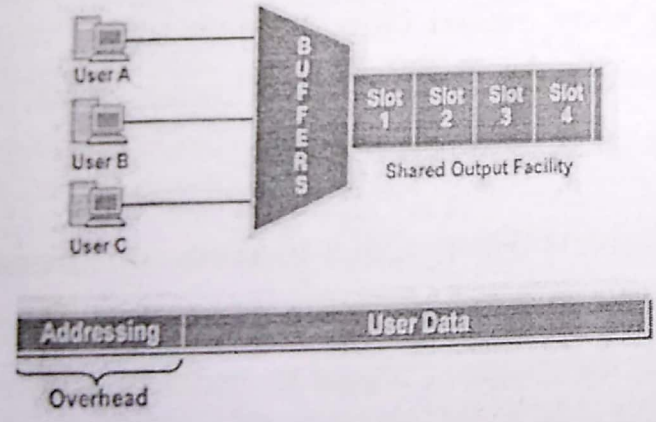
side in front of a connection, it has the opportunity to send a unit into the path. In the same way, when the switch opens on the demultiplexer side in front of a connection that has the opportunity to receive a unit from the path. This process is called interleaving.



Interleaving

Statistical Time-Division Multiplexing

Statistical time-division multiplexing is used to transmit several types of data concurrently across a single transmission cable. This is often used for managing data being transmitted via LAN or WAN. The data is simultaneously transmitted from the input devices that are connected to the network including printers, fax machines, and computers. This type of multiplexing is also used in telephone switch board settings to manage the calls. Statistical TDM is similar to dynamic bandwidth allocation, and in this type of time-division multiplexing, a communication channel is divided into an arbitrary number of data streams.



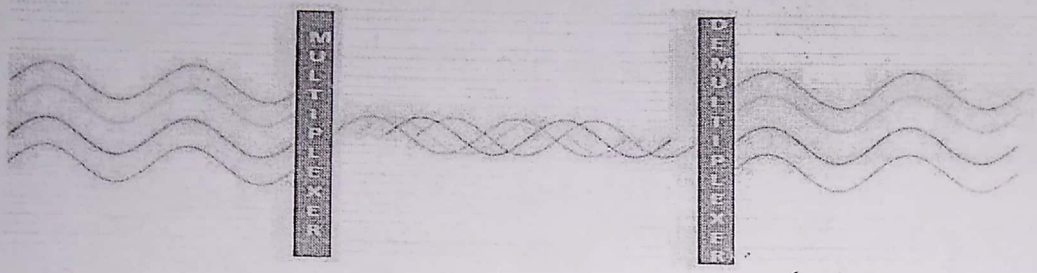
Statistical Time-Division Multiplexing

Wavelength Division Multiplexing

Light has different wavelength (colors). In fiber optic mode, multiple optical carrier signals are multiplexed into an optical fiber by using different wavelengths. This is an

analog multiplexing technique and is done conceptually in the same manner as FDM but uses light as signals.

Further, on each wavelength time division multiplexing can be incorporated to accommodate more data signals.



Similarly, in some optical networks, data for different communications channels are sent on lightwaves of different wavelengths, a variety of multiplexing called wavelength division multiplexing (WDM).

Code Division Multiplexing

Multiple data signals can be transmitted over a single frequency by using Code Division Multiplexing. FDM divides the frequency in smaller channels but CDM allows its users to full bandwidth and transmit signals all the time using a unique code. CDM uses orthogonal codes to spread signals.

Each station is assigned with a unique code, called chip. Signals travel with these codes independently, inside the whole bandwidth. The receiver knows in advance the chip code signal it has to receive.

Code Division Multiplexing (CDM) uses identifying codes to distinguish one signal from another on a shared medium. Each signal is assigned a sequence of bits called the spreading code that is combined with the original signal to produce a new stream of encoded data; a receiver that knows the code can retrieve the original signal by subtracting out the spreading code (a process called dispreading). CDM is widely used in digital television and radio broadcasting and in 3G mobile cellular networks. Where CDM allows multiple signals from multiple sources, it is called Code-Division Multiple Access (CDMA).

Channel Allocation Problem

II

In the OSI protocol stack, channel allocation is addressed in the Medium access control (MAC) sublayer. This is a sublayer of the Data Link Layer - considered to be below the Logical Link Control (LLC) sub-layer. Many LAN technologies, such as Ethernet are based on this type of architecture. The MAC layer provides an unreliable connectionless service; if required, the LLC layer can convert this into a reliable service by using an ARQ protocol.

Basic problem: How to allocate a multi-access channel among competing users.

In other words, we need a set of rules (i.e. a protocol) to allow each user to communicate and avoid interference. There are a variety of solutions to this problem that are used in practice. These solutions can be classified as either static or dynamic. With a static approach, the channel's capacity is essentially divided into fixed portions; each user is then allocated a portion for all time. If the user has no traffic to use in its portion, then it goes unused. With a dynamic approach the allocation of the channel changes based on the traffic generated by the users. Generally, a static allocation performs better when the traffic is predictable. A dynamic channel allocation tries to get better utilization and lower delay on a channel when the traffic is unpredictable.

Static Channel Allocation Techniques

Two common static channel allocation techniques are TDMA and FDMA.

Time Division Multiple Access (TDMA) – With TDMA the time axis is divided into time slots of a fixed length. Each user is allocated a fixed set of time slots at which it can transmit. TDMA requires that users be synchronized to a common clock. Typically extra overhead bits are required for synchronization.

Frequency Division Multiple Access (FDMA) – With FDMA the available frequency bandwidth is divided into disjoint frequency bands. A fixed band is allocated to each user. FDMA requires a guard band between user frequency bands to avoid cross-talk.

Another static allocation technique is **Code Division Multiple Access (CDMA)**, this technique is used in many wireless networks.

The performance of static channel allocation depends on:

The variation in the number of users over time

The nature of the traffic sent by the user

If the traffic on a shared medium is from a fixed number of sources each transmitting at a fixed rate, static channel allocation can be very efficient.

Voice and Video (in their fixed rate forms) have this property and commonly are placed in a shared channel using a static channel allocation.

The variation in the number of users over time impacts the performance of a static allocation because some method is needed to allocate the slot to users as they come and go.

When the traffic sent by a user is very heavy, then, under a static allocation, a user's portion of the channel may be empty when another user could use it. This leads one to think that a dynamic allocation will perform better in such cases

nication Channels

Channel Allocation Problem

- In an organization, information flows forward, backwards and sideways. This information flow is referred to as communication. Communication channels refer to the way this information flows within the organization and with other organizations.
- In this web known as communication, a manager becomes a link. Decisions and directions flow upward or downwards or sideways depending on the position of the manager in the communication web.
- For example, reports from lower level manager will flow upwards. A good manager has to inspire, steer and organize his employees efficiently, and for all this, the tools in his possession are spoken and written words.
- For the flow of information and for a manager to handle his employees, it is important for an effectual communication channel to be in place.

he Working of a Communication Channel

- Through a modem of communication, be it face-to-face conversations or an inter-department memo, information is transmitted from a manager to a subordinate or vice versa.
- An important element of the communication process is the feedback mechanism between the management and employees.
- In this mechanism, employees inform managers that they have understood the task at hand while managers provide employees with comments and directions on employee's work.

mportance of a Communication Channel

- A breakdown in the communication channel leads to an inefficient flow of information. Employees are unaware of what the company expects of them. They are uninformed of what is going on in the company.
- This will cause them to become suspicious of motives and any changes in the company. Also without effective communication, employees become department minded rather than company minded, and this affects their decision making and productivity in the workplace.
- Eventually, this harms the overall organizational objectives as well. Hence, in order for an organization to be run effectively, a good manager should be able to communicate to his/her employees what is expected of them, make sure they are fully aware of company policies and any upcoming changes.
- Therefore, an effective communication channel should be implemented by managers to optimize worker productivity to ensure the smooth running of the organization.

Types of Communication Channels

- The number of communication channels available to a manager has increased over the last 20 odd years. Video conferencing, mobile technology, electronic bulletin boards and fax machines are some of the new possibilities.
- As organizations grow in size, managers cannot rely on face-to-face communication alone to get their message across.
- A challenge the managers face today is to determine what type of communication channel should they opt for in order to carryout effective communication.
- In order to make a manager's task easier, the types of communication channels are grouped into three main groups: formal, informal and unofficial.