BACHELOR OF COMPUTER APPLICATIONS

SEMESTER 3

DCA2201

COMPUTER NETWORKING

Unit 2

Data Link Layer and Local Area Networks

Table of Contents

1. INTRODUCTION

In the previous unit, we discussed the basics of networking and network reference models. This unit introduces the concept of Data link layer and local area networks. In discussing the data link layer, we will see there are two different link layer channels in the OSI reference model protocol layer. The first one is broadcast channels, which connect multiple hosts using wireless medium, satellite networks and hybrid fiber-coaxial cable (HFC) access networks. The second type of link-layer channel is the point-to-point communication link.

We will start this unit with an explanation about modulation and multiplexing. In this unit, we are going to discuss Ethernet and Wireless LANs. In the next session we will discuss Link virtualization. In the last sections of this unit, we will discuss different multiple access protocols.

1.1 Objectives:

After studying this unit, you should be able to:

- *Describe modulation and multiplexing*
- *Explain ethernet*
- *Describe wireless LANs*
- *Describe link virtualization*
- *Explain multiple access protocols*

2. MODULATION AND MULTIPLEXING

Modulation is the process of varying one or more properties of a signal (carrier signal) with a modulating signal which contains the information to be transmitted. In digital modulation, an analog carrier signal is modulated by a discrete signal. Digital modulation is digital to analog conversion, and demodulation is analog to digital conversion.

The scheme that directly converts bits into a signal, resulting in *baseband transmission*. In baseband transmission, the signal occupies frequencies from zero up to a maximum that depends on the signaling rate. *Passband* transmission is the scheme that regulates the amplitude, phase, or frequency of a carrier signal to convey bits. Channels are often shared by multiple signals. After all, it is much more convenient to use a single wire to carry several signals than to install a wire for every signal. This kind of sharing is called *multiplexing*. Multiplexing is sending multiple signals on a carrier in the form of a single, complex signal and then recovering separate signals at the receiving end.

Baseband Transmission

The direct method of digital modulation is to use a positive voltage to represent a binary logic 1 and a negative voltage to represent a binary logic 0. In the case of optical fiber, the presence of light might represent a binary logic 1 and the absence of light might represent a binary logic 0. This scheme of representing the signal with logic 1's and 0's is called *NRZ (Non-Return-to-Zero)*. The NRZ signals propagate down the wire, and at the other end, the receiver converts it into bits by sampling the signal at regular intervals of time. An example is shown in Figure 2.1.

This signal will not look exactly like the signal that was sent. It will be attenuated and distorted by the channel and noise at the receiver. To decode the bits, the receiver maps the signal samples to the most likely closest symbols. For NRZ, a positive voltage will be taken to indicate that a 1 was sent and a negative voltage will be taken to indicate that a 0 was sent.

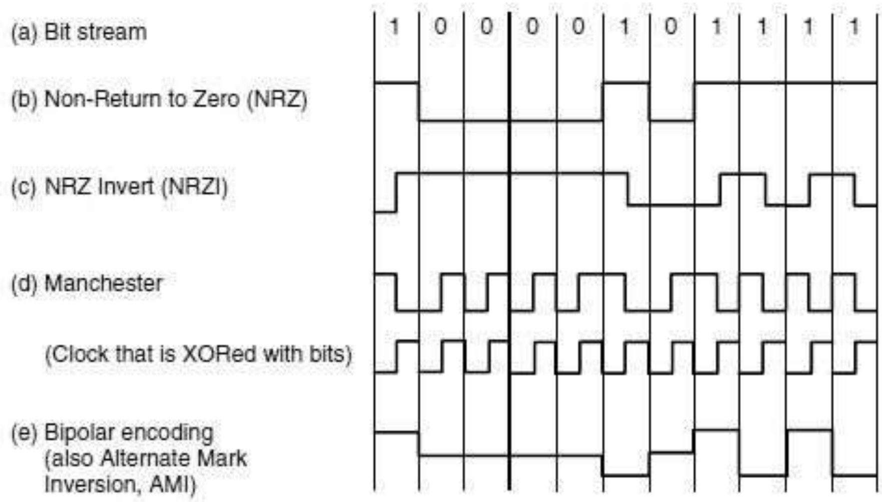

Figure 2.1: Line codes: (a) Bits, (b) NRZ, (c) NRZI, (d) Manchester, (e) Bipolar or AMI.

Passband Transmission

As we discussed, *Passband transmission* is the scheme that regulates the amplitude, phase, or frequency of a carrier signal to convey bits. Passband transmission can be used if we want to use a range of frequencies that does not start at zero to send information across a channel.

For wireless channels, it is not practical to send very low frequency signals because the size of the antenna needs to be a fraction of the signal wavelength, which becomes large. In Passband transmission, an arbitrary band of frequencies is used to pass the signal.

Digital modulation is possible in passband transmission. A carrier signal can be modulated by the message signal so that it can pass through the passband channel. Since modulation of amplitude, frequency, or phase of the carrier signal is possible, we can have digital modulation technique based on amplitude, frequency and phase of carrier signal. *ASK (Amplitude Shift Keying) is the digital modulation technique* where two different amplitudes are used to represent 0 and 1. *FSK (Frequency Shift Keying),* is *the digital modulation technique* where two or more different tones of frequencies are used to represent 0 and 1. *PSK (Phase Shift Keying)* is the digital modulation technique where phases are altered to represent 0's and 1's. In the simplest form of PSK (Phase Shift Keying), known as *BPSK (Binary Phase Shift Keying)*, the carrier wave is systematically shifted between 0 or 180 degrees at each symbol period. Because there are two phases, it is called BPSK (Binary Phase Shift Keying). An example is shown in figure 2.2.

Another better scheme that uses the channel bandwidth more efficiently is to use four shifts of different phases of the carrier signal, e.g., 45, 135, 225, or 315 degrees, to transmit 2 bits of information per symbol. This version is called QPSK (Quadrature Phase Shift Keying).

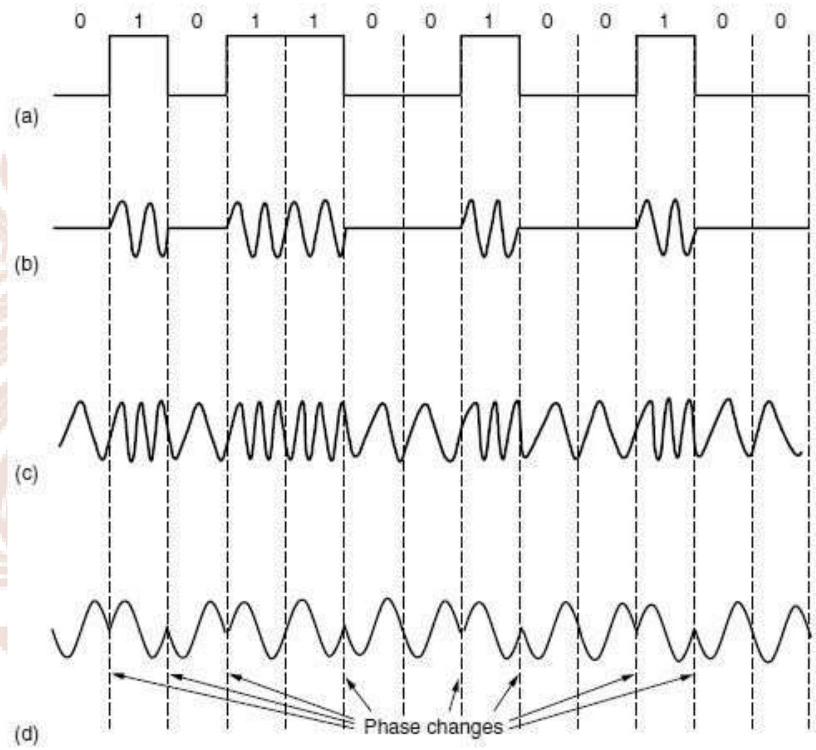

Figure 2.2: (a) A binary signal. (b) Amplitude shift keying.

(c) Frequency Shift keying. (d) Phase shift keying.

Only one frequency or phase can be modulated at a time because they are related, with frequency being the rate of change of phase over time. Usually, amplitude and phase are modulated in combination. Figure 2.3 is a representation of QPSK. This kind of diagram is called a *constellation diagram*. In figure 2.3 (a), we can see equidistant dots at 45, 135, 225, and 315 degrees. The phase of a dot is indicated by the angle a line from it to the origin makes with the positive x-axis. The amplitude of a dot is the distance from the origin. In Fig. 2.3(b) we see a modulation scheme with a denser constellation. Sixteen combinations of amplitudes and phase are used, so the modulation scheme can be used to transmit 4 bits per symbol.It is called **QAM-16,** where QAM stands for *Quadrature Amplitude Modulation*.

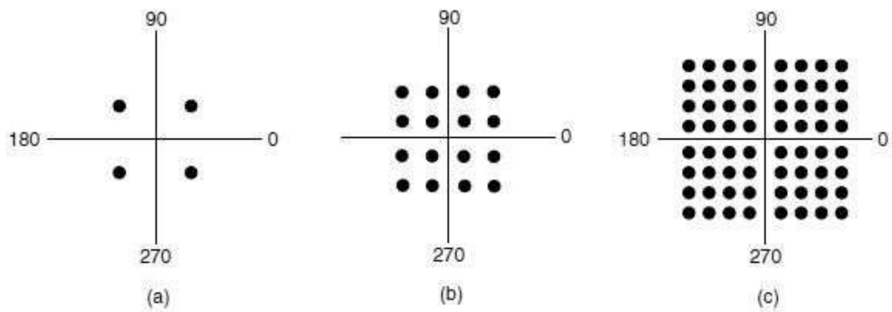

Figure 2.3: (a) QPSK. (b) QAM-16. (c) QAM-64.

Figure 2.3(c) is a still denser modulation scheme with 64 different combinations, so 6 bits can be transmitted per symbol. It is called QAM-64.

Frequency Division Multiplexing

FDM (Frequency Division Multiplexing) is a technique to divide the spectrum of communication channel into frequency bands, with each user having exclusive possession of some band in which to send their signal. The radio broadcasting mechanism illustrates FDM. Different frequencies are allocated to different logical channels (stations), each operating in a portion of the spectrum, with the inter-channel separation to prevent interference. Figure 2.4 shows three voice-grade telephone channels multiplexed using FDM.

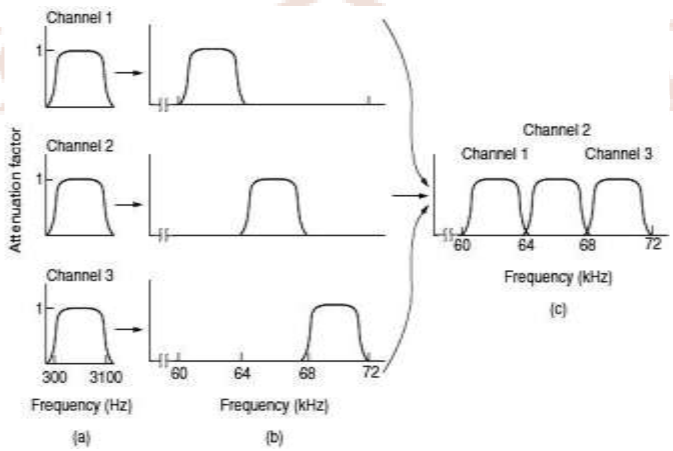

Figure 2.4: Frequency division multiplexing. (a) The original bandwidths.

(b) The bandwidths raised in frequency. (c) The multiplexed channel.

The excess band of the communication channel is called a guard band. It keeps the channels well separated.

We can also divide the spectrum without using guard bands. In *OFDM (Orthogonal Frequency Division Multiplexing)*, the channel bandwidth is divided into many subcarriers that independently send data. Figure 2.5 shows an example of OFDM.

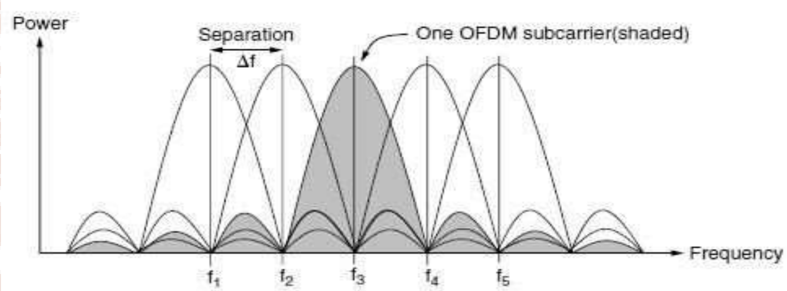

Figure 2.5: Orthogonal frequency division multiplexing (OFDM).

In OFDM, the subcarriers are packed tightly together in the frequency domain and thus, signals from each subcarrier extend into adjacent ones. The frequency response of each subcarrier is designed so that it is zero at the center of the adjacent subcarriers. The subcarriers can therefore be sampled at their center frequencies without interference from their Neighbours. OFDM is used in IEEE 802.11 standards, cable networks and power line networking, and is planned for fourth-generation cellular systems.

Time Division Multiplexing

TDM (Time Division Multiplexing), users take turns (in a round-robin fashion), each one periodically getting the entire

Bandwidth for a little burst of time to transmit its signal and receive the signal. Multiplexing of three streams is shown in figure 2.6.

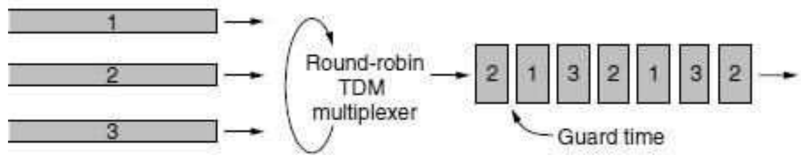

Figure 2.6: Time Division Multiplexing (TDM).

Time Division Multiplexing is widely used as part of the telephone and cellular networks. In the example above, Bits from each input stream are taken in a fixed time slot and output to the combine stream. This stream runs at the sum rate of the individual streams. For this, the streams must be synchronized in time. Small intervals of guard *time* analogous to a frequency guard band may be added to accommodate small timing variations.

Code Division Multiplexing

Code Division Multiplexing (CDM) is the multiplexing scheme where, input of analog signal is first converted into binary elements and then the frequency of the transmitted signal is made to vary based on a defined pattern (code). This signal is converted back by a receiver whose frequency response is programmed with the same code. It allows multiple signals from different users to share the same frequency band, so it is commonly called *CDMA (Code Division Multiple Access).*

Self-Assessment Questions - 1

1. The process of converting between bits and signals that represent them is called __________.
2. The scheme that directly converts bits into a signal, results in ____________transmission.
3. *FDM (Frequency Division Multiplexing)* takes advantage of ______________ transmission to share a channel.

3. ETHERNET (IEEE 802.3)

IEEE 802.3, popularly called *Ethernet*, and is the most common type of wired LAN (Local Area Network). Ethernet was created in 1976, at Xerox's Palo Alto Research Center (PARC). Since then, it has gone through four generations, they are Standard Ethernet (l0 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (l Gbps), and Ten-Gigabit Ethernet (l0 Gbps). Following figure 2.7 shows different types of Ethernet.

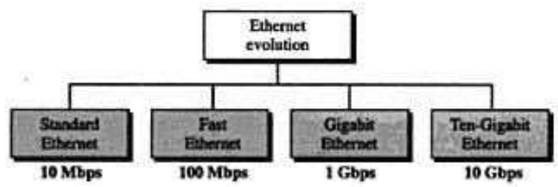

Figure 2.7: Ethernet evolution through four generations

In standard Ethernet, the MAC (Medium Access Control) Sublayer governs the operation of the access method. It also frames data received from the upper layer and passes them to the physical layer. Ethernet frame contains several fields, they are Preamble, Start Frame Delimiter (SFD), Destination Address (DA), Source Address (SA), length or type of protocol data unit (PDU), upper-layer data, and the Cyclic Redundancy Check (CRC). The format of MAC frame is shown in figure 2.8.

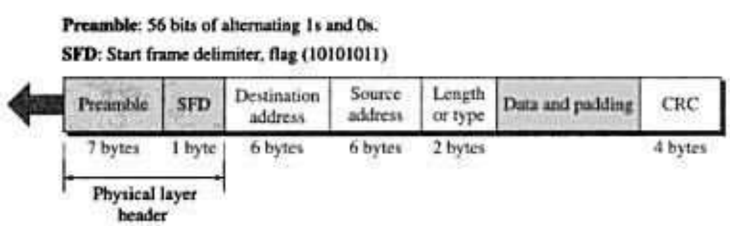

Figure 2.8: IEEE802.3 MAC frame

In this frame, preamble is added by the physical layer. This is the first part of the frame which contains 7 bytes of alternate 0s and 1s that alert the receiver about the coming frame and enables it to synchronize its input timing. SFD field signals the beginning of the frame. In this, the last 2 bits is 11 and alerts the receiver that the next field is the destination address. DA and SA are 6 bytes each which gives the destination and source address respectively. Length field specifies the number of bytes in the data field. Data field carries data, which is a minimum of 46 and maximum of 1500 bytes. The last field CRC contains error detection information.

Categories of Standard Ethernet:

The Standard Ethernet defines several physical layer implementations; four of the most common, are shown in Figure 2.9.

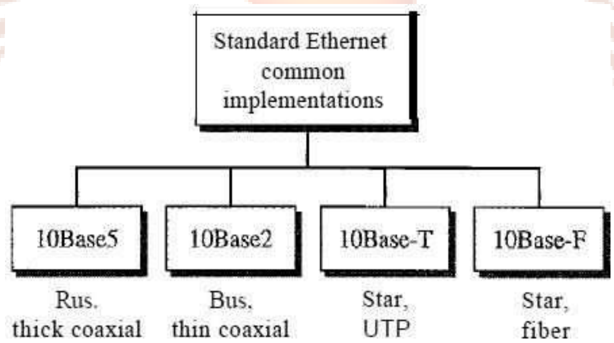

Figure 2.9: Standard Ethernet Common Implementation

10 Base 5: Thick Ethernet

The first implementation is called *10Base5 thick Ethernet*, or *Thicknet*. 10 base 5 was the first Ethernet specification to use a bus topology with an external transceiver (transmitter/receiver) connected via a tap to a thick coaxial cable. Following figure 2.10 shows 10 Base 5 implementation.

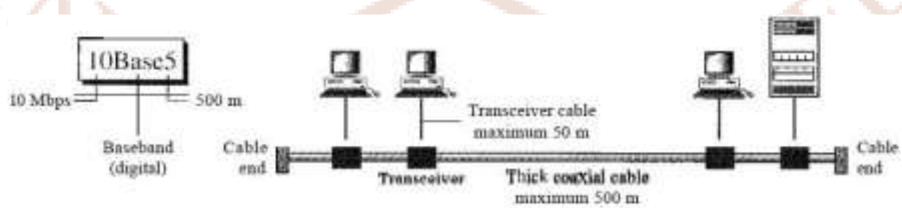

Figure 2.10: 10 Base 5 Implementation

The transceiver is responsible for transmitting, receiving, and detecting collisions. The transceiver is connected to the station via a transceiver cable that provides separate paths for sending and receiving. This means that collision can only happen in the coaxial cable. The maximum length of the coaxial cable must not exceed 500 m, otherwise, there is excessive degradation of the signal.

10 Base 2: Thin Ethernet

The second implementation is called 10Base2, thin ethernet, or Cheapernet. 10Base2 also uses a bus topology, but the cable is much thinner and more flexible. In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station. Figure 2.11 shows 10 Base2 implementations.

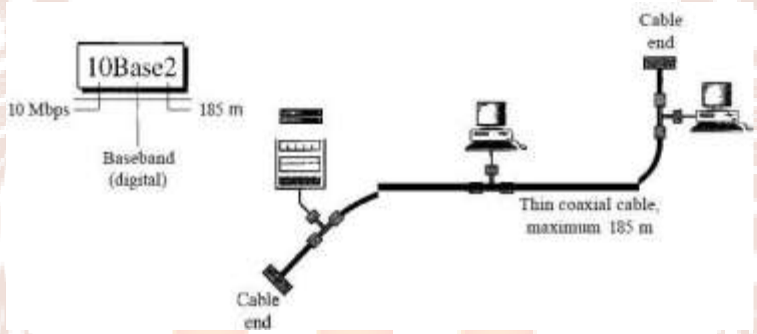

Figure 2.11: 10Base2 Implementation

This implementation is more cost effective than 10Base5 because thin coaxial cable is less expensive than thick coaxial. However, the length of each segment cannot exceed *185 m* (close to 200 m) due to the high level of attenuation in thin coaxial cable.

10 Base T: Twisted-Pair Ethernet

The third implementation is called 10 Base-T or twisted-pair Ethernet. 10Base-T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable. The maximum length of the twisted cable here is defined as 100 m, to minimize the effect of attenuation in the twisted cable. Figure 2.12 shows 10BaseT implementation.

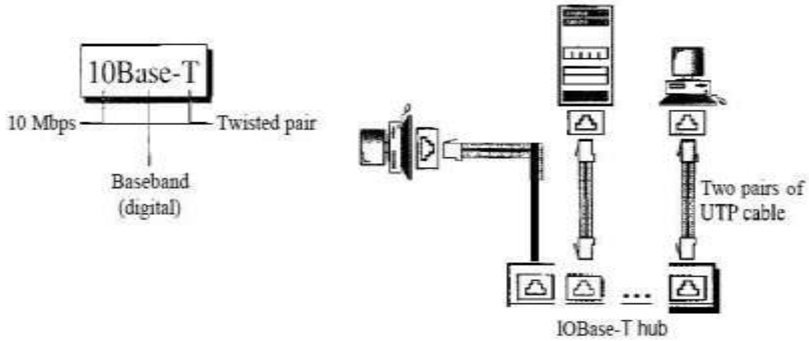

Figure 2.12: 10BaseT Implementation

10Base F: Fiber Ethernet

Although there are several types of optical fiber 10-Mbps Ethernet, the most common is called 10BaseF. 10BaseF uses a star topology to connect stations to a hub. The stations are connected to the hub using two fiber-optic cables, as shown in Figure 2.13

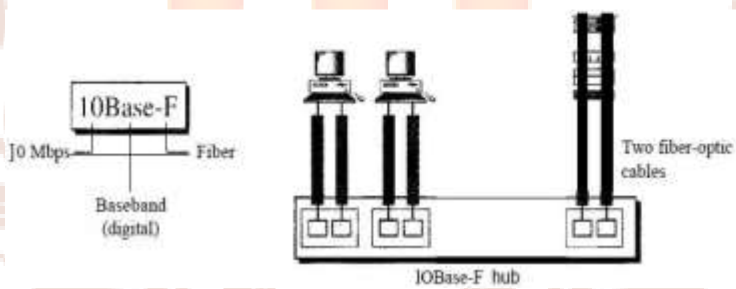

Figure 2.13: 10BaseF Implementation

Self-Assessment Questions - 2

4. IEEE 802.3 is also known as _______ .
5. Which implementation is called thin ethernet, or Cheapernet?
6. _________uses a physical star topology.

4. WIRELESS LANS

A local area network which does not need cables to connect the different devices is known as wireless LAN. Communication occurred using radio waves.

Wireless LANs can be classified into different categories by the data rates they provide and based on the distance between nodes. In this section, we will discuss three main wireless technologies: Wi-Fi (more formally known as 802.11), Bluetooth, and the third-generation or “3G” family of cellular wireless standards.

4.1 Wi-Fi (802.11)

A wireless network based on IEEE802.11 standards, often referred to as Wi-Fi is technically a trademark owned by a trade group called the Wi-Fi Alliance, which certifies product compliance with 802.11. Like ethernet, Wi-Fi can also be used in a limited geographical area.

Physical Properties:

The original 802.11 standard defined two radio-based physical layers standards, one using frequency hopping and the other using direct sequence spread spectrum. Both provided data rates in the 2 Mbps range. The physical layer standard 802.11b was added subsequently. Using a variant of direct sequence, 802.11b provides up to 11 Mbps. Then came 802.11a, which delivers up to 54 Mbps using a variant of FDM called *orthogonal frequency division multiplexing (OFDM)*. After that 802.11g was added. 802.11g also uses OFDM and it delivers up to 54 Mbps.

Most recently 802.11n has appeared on the scene, with a standard that was approved in 2009. 802.11n achieves considerable advances in maximum possible data rate using multiple antennas and allowing greater wireless channel bandwidths. The use of multiple antennas is often called *MIMO* for multiple input, multiple-output. All the 802.11 standards define a *maximum* bit rate that can be supported, they mostly support lower bit rates as well. Different modulation schemes are used to achieve the various bit rates.

IEEE 802.11 family specifications (IEEE 802.11x)

802.11x is the generic term for 802.11 family specifications. 802.11a, b, g etc. are the revised versions of 802.11 standard.

- 802.11a specification uses orthogonal frequency division multiplexing, and it provides an enhanced data speed up to 54Mbps.
- 802.11b is another enhancement to 802.11 that added higher data rate modes to direct sequence spread spectrum. It provides a boosted speed to 11 Mbps. Also, 22 MHz bandwidth gives 3 non-overlapping channels in the frequency range of 2.400 GHz to 2.4835 GHz.
- 802.11d is an enhancement to 802.11a and 802.11b that allows global roaming.
- 802.11e is an enhancement to 802.11 that includes quality of service features. It provides prioritization of data, voice and video transmissions.
- 802.11g extends the maximum data rate of WLAN devices that operate in 2.4 GHz band, in a manner that allows interoperation with 802.11b devices. It uses orthogonal frequency division modulation. It operates at 54Mbps speed.
- 802.11h is an enhancement to 802.11a that resolves interference issue. Dynamic frequency selection and transmission power control are the other properties of this standard.
- 802.11i is an enhancement to 802.11 that offers additional security for wireless LAN applications. It defines more robust encryption, authentication and key exchange. It also provides options for key caching and pre-authentication.
- 802.11j is the Japanese regulatory extensions to 802.11a specification. It provides a frequency range 4.9 GHz to 5.0 GHz.
- 802.11k provides radio resource measurement for networks using
- 802.11 family specifications.
- 802.11m provides maintenance of 802.11 family specifications. It provides corrections and modifications to existing documentation.
- 802.11n is a higher-speed standard. Top speed of 108, 240 and 350+ MHz is provided.

4.2 Bluetooth (802.15.1)

Bluetooth is used for short range communication between devices like mobile phones, PDAs, notebook computers, and other personal or peripheral devices. Bluetooth is sometimes categorized as a Personal Area Network (PAN) because bluetooth links have typical bandwidths of around 1 to 3 Mbps and a range of about 10 m. Bluetooth is specified by an industry consortium called the *Bluetooth Special Interest Group*. It specifies an entire suite of protocols, going beyond the link layer to define application protocols, which it *calls profiles*, for a range of applications. The basic Bluetooth network configuration, called a piconet, consists of a master device and up to seven slave devices, as shown in figure 2.17. Any communication is between the master and a slave; the slaves do not communicate directly with each other. Because slaves have a simpler role, their Bluetooth hardware and software can be simpler and cheaper. A slave device can be parked; that is, it is set to an inactive, low-power state. A parked device cannot communicate on the piconet; it can only be reactivated by the master. A piconet can have up to 255 parked devices in addition to its active slave devices.

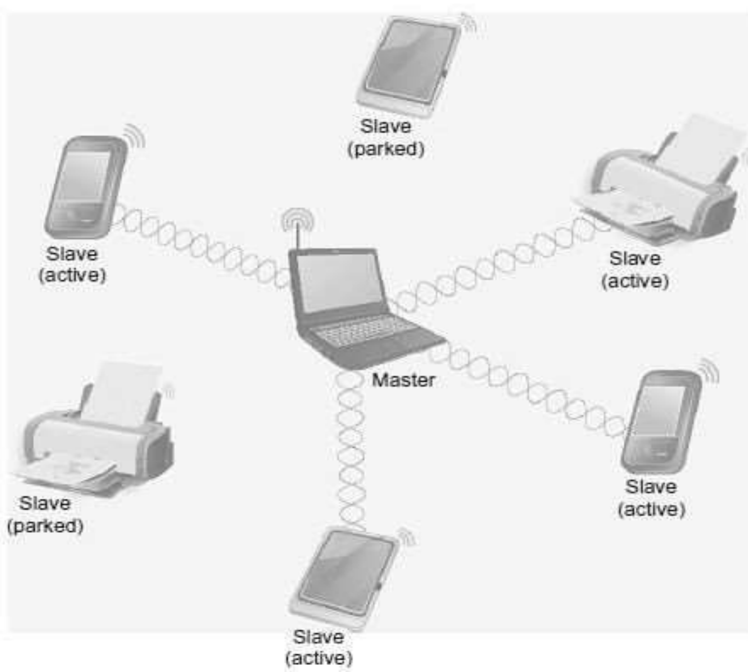

Figure 2.17: A Bluetooth piconet

In the realm of very low-power, short-range communication there are a few other technologies besides Bluetooth. ZigBee is one among them, devised by the ZigBee alliance and standardized as IEEE 802.15.4. It is designed for situations where the bandwidth requirements are low and power consumption must be very low to give very long battery life. It is also intended to be simpler and cheaper than Bluetooth, making it financially feasible to incorporate in cheaper devices such as *sensors*.

4.3 Cellphone Technologies

Like Wi-Fi, cellular technology relies on the use of base stations that are part of a wired network. The geographic area served by a base station's antenna is called a *cell*. A base station could serve a single cell or use multiple directional antennas to serve multiple cells. Cells don't have crisp boundaries, and they overlap. Where they overlap, a mobile phone could potentially communicate with multiple base stations.

At any time, however, the phone is in communication with, and under the control of, just one base station. As the phone begins to leave a cell, it moves into an area of overlap with one or more other cells. The current base station senses the weakening signal from the phone and gives control of the phone to whichever base station is receiving the strongest signal from it. If the phone is involved in a call at the time, the call must be transferred to the new base station in what is called a *handoff*.

There is not one unique standard for cellular, but rather a collection of competing technologies that support data traffic in different ways and deliver different speeds. These technologies are loosely categorized by *generation*. The first generation (1G) was analog, and thus of limited interest from a data communications perspective. Second-generation standards moved to digital and introduced wireless data services, while third generation (3G) allowed greater bandwidths and simultaneous voice and data transmission. Most of the 3G standards are based on variants of CDMA (Code Division Multiple Access). CDMA uses a form of spread spectrum to multiplex the traffic from multiple devices into a common wireless channel.

Self-Assessment Questions - 3

7. A local area network which does not need cables to connect the different devices is known as _________ .
8. A wireless network based on IEEE802.11 standards is also known as________ .
9. ___________is used for short range communication between devices like mobile phones, PDAs etc.

5. LINK VIRTUALIZATION

The Internet virtualizes the telephone network, viewing the telephone network as a link-layer technology providing link-layer connectivity between two Internet hosts. A link can be viewed as a physical layer connecting two communicating hosts. In this section, we will discuss Asynchronous Transfer Mode (ATM) networks and Multiprotocol Label Switching (MPLS) networks. Both of these networks are packet switched, virtual circuit networks. They have their own packet formats and forwarding behaviors.

5.1 Asynchronous Transfer Mode (ATM)

Asynchronous Transfer Mode (ATM) is often used as a link-layer technology in the backbone of the Internet. The standards of ATM were first developed in the mid-1980s. ATM provides complete networking solutions for distributed applications.

Characteristics of ATM:

The ATM standards define a complete set of communication protocols from transport layer to the physical layer. ATM uses packet switching with fixed length packets of 53 bytes which is known as cells. Each cell has 5 bytes header and 48 bytes of payload/data. These fixed length cells and simple header facilitate high-speed switching. ATM uses virtual circuits which are also known as virtual channels. ATM header includes a field for virtual channel numbers, which is called virtual channel identifier (VCI). Packet switches use this VCI to route cells towards their destinations. In ATM, no data retransmission required because if a switch detects an error in an ATM cell, it attempts to correct the error using error correcting codes. If it cannot correct the error, it drops the cell and does not ask the preceding switch to retransmit the cell. ATM also provides congestion control on an end-to-end basis. The transmission of ATM cells is not directly regulated by the switches in times of congestion. However, the network switches themselves do provide feedback to a sending end system to help it regulate its transmission rate when the network becomes congested. ATM can run over any physical layer.

Overview of ATM Layers:

ATM has a layered architecture. ATM protocol stack consists of three layers. They are ATM adaptation layer (AAL), ATM Layer and ATM physical layer. Figure 2.18 (a) illustrates different layers of ATM and Figure 2.18 (b) shows the protocol stack for the regions of the internet that use ATM.

ATM Physical layer deals with voltages, bit timings and framing on the physical medium. The ATM layer is the core of the ATM standard, which defines the structure of the ATM cell. ATM adaptation layer is analogous to the transport layer in the Internet protocol stack. A special AAL type, AAL5, has been developed to allow TCP/IP to interface with ATM. At the IP-to-ATM interface, AAl5 prepares IP datagrams for ATM transport. At the ATM-to-IP interface, AAL5 reassembles ATM cells into IP datagrams.

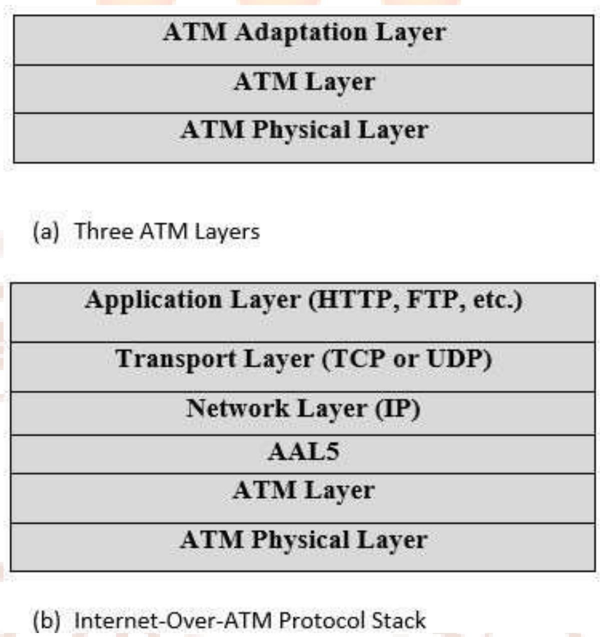

Figure 2.18: a) Three ATM Layers (b) Internet-over-ATM Protocol Stack

InInternet-over-ATM protocol stack, the three ATM layers have been combined into the lower two layers of the Internet protocol stack.

5.2 Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) was developed in the late 1990s to improve the forwarding speed of IP routers by adopting a key concept 'fixed-length label' from virtual circuit networks. The goal was to enlarge it by selectively labelling datagrams and allowing routers to forward datagrams based on fixed-length labels (rather than destination IP addresses) when possible.

Figure 2.19 shows that a link-layer frame transmitted between MPLS-capable devices has a small MPLS header added between the layer-2 (e.g., Ethernet) header and layer-3 (i.e., IP) header.

Figure 2.19: MPLS Header: Located between link and network layer headers

Fields in the MPLS header are the label, 3 bits reserved for experimental use, a single S bit, which is used to indicate the end of a series of stacked MPLS headers, and a time-to-live field. An MPLS-enhanced frame can only be sent between routers that are both MPLS capable. An MPLS-capable router is often referred to as a **label-switched router**, since it forwards an MPLS frame by looking up the MPLS label in its forwarding table and then immediately passing the datagram to the appropriate output interface. Thus, the MPLS-capable router need not extract the destination IP address and perform a lookup of the longest prefix match in the forwarding table.

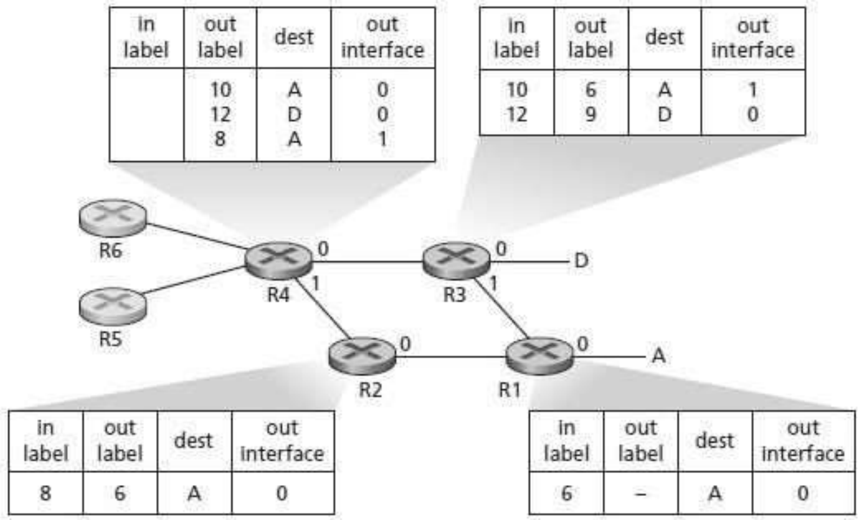

Figure 2.20: MPLS-Enhanced Forwarding

Let's see the example in figure 2.20. Here, routers R1 through R4 are MPLS capable. R5 and R6 are standard IP routers. R1 has advertised to R2 and R3 that it (R1) can route to destination A, and that a received frame with MPLS label 6 will be forwarded to destination A. Router R3 has advertised to router R4 that it can route to destinations A and D, and that incoming frames with MPLS labels 10 and 12, respectively, will be switched toward those destinations. Router R2 has also advertised to router R4 that it (R2) can reach destination A, and that a received frame with MPLS label 8 will be switched toward A. Note that router R4 is having two MPLS paths to reach A: via interface 0 with outbound MPLS label 10, and via interface 1 with an MPLS label of 8. Figure 2.20 shows that IP devices R5, R6, A, and D are connected together via an MPLS infrastructure (MPLS-capable routers R1, R2, R3, and R4) in much the same way that a switched LAN or an ATM network can connect together IP devices. And like a switched LAN or ATM network, the MPLS-capable routers R1 through R4 do so *without ever touching the IP header of a packet*.

Self-Assessment Questions - 4

10. ________________ is often used as a link-layer technology in the backbone of the Internet.
11. Multiprotocol Label Switching (MPLS) improves the forwarding speed of IP routers by adopting ____________ key concept from virtual circuit networks.

6. MULTIPLE ACCESS PROTOCOLS

There are two types of network links:They are point-to-point links and broadcast links. A point-to-point link consists of a single sender at one end of the link and a single receiver at the other end of the link. Broadcast link can have multiple sending and receiving nodes. Multiple access problem is how to coordinate the access of multiple sending and receiving nodes to a shared broadcast channel. Multiple access protocols are rules by which nodes regulate their transmission into the shared broadcast channel. Multiple access protocol can be classified into three categories. They are **channel partitioning protocols, random access protocols,** and **take-turns protocols.** Multiple access protocol for a broadcast channel of rate R bits per second should have the following desirable characteristics.

- When only one node has data to send, that node has a throughput of R bps.
- When M nodes have data to send, each of these nodes has a throughput of R/M bps (average transmission rate).
- The Protocol is decentralized; that means, there is no master node that represents a single point of failure for the network.
- The protocol is simple, so it is inexpensive to implement.

6.1 Channel Partitioning Protocols

Time-division multiplexing (TDM) and frequency-division multiplexing (FDM) are two techniques used for channel partitioning. TDM divides time into time frames and further divides each time frame into N time slots. Each time slot is then assigned to one of the N *nodes*. Whenever a node has a packet to send, it transmits the packet's bits during its assigned time slot in the revolving TDM frame. TDM eliminates collisions and each node gets a dedicated transmission rate of R/N bps during each frame time. However, it has two major drawbacks. First, a node is limited to an average rate of R/N bps even when it is the only node with packets to send. A second drawback is that a node must always wait for its turn in the transmission sequence.

While TDM shares the broadcast channel in time, FDM divides the R bps channel into different frequencies (each with a bandwidth of R/N) and assigns each frequency to one of the *N* nodes. FDM thus creates N smaller channels of *R/N* bps out of the single, larger *R* bps channel. FDM shares both the advantages and drawbacks of TDM. It avoids collisions and divides the bandwidth fairly among the *N* nodes. However, FDM also shares a principal disadvantage with TDM – a node is limited to a bandwidth of *R/N*, even when it is the only node with packets to send.

Another channel partitioning protocol is code division multiple access (CDMA). While TDM and FDM assign time slots and frequencies, respectively, to the nodes, CDMA assigns a different *code* to each node. Each node then uses its unique code to encode the data bits it sends. In CDMA network, different nodes can transmit *simultaneously* and yet have their respective receivers correctly receive a sender's encoded data bits.

6.2 Random Access Protocols

The second broad class of multiple access protocols are random access protocols. In a random-access protocol, a transmitting node always transmits at the full rate of the channel, namely, R bps. When there is a collision, each node involved in the collision repeatedly retransmits its frame (that is, packet) until its frame gets through without a collision. But when a node experiences a collision, it doesn't necessarily retransmit the frame right away. *Instead, it waits for a random delay before retransmitting the frame.* The two most commonly used random access protocols are ALOHA protocols and Carrier Sense Multiple Access (CSMA) protocols.

Slotted ALOHA

In Slotted ALOHA, when the node has a fresh frame to send, it waits until the beginning of the next slot and transmits the entire frame in the slot. If there isn't a collision, the node has successfully transmitted its frame and thus need not consider retransmitting the frame. If there is a collision, the node detects the collision before the end of the slot. The node retransmits its frame in each subsequent slot with probability *p* until the frame is transmitted without a collision. Unlike channel partitioning, slotted ALOHA allows a node to transmit continuously at the full rate*, R,* when that node is the only active node.

ALOHA

The slotted ALOHA protocol required that all nodes synchronize their transmissions to start at the beginning of a slot. The first ALOHA protocol [Abramson 1970] was actually an unslotted, fully decentralized protocol. In pure ALOHA, when a frame first arrives (that is, a network-layer datagram is passed down from the network layer at the sending node), the node immediately transmits the frame in its entirety into the broadcast channel. If a transmitted frame experiences a collision with one or more other transmissions, the node will then immediately (after completely transmitting its collided frame) retransmit the frame with probability *p*. Otherwise, the node waits for a frame transmission time.

Carrier Sense Multiple Access (CSMA)

In both slotted and pure ALOHA, a node's decision to transmit is made independently of the activity of the other nodes attached to the broadcast channel. In particular, a node neither pays attention to whether another node happens to be transmitting when it begins to transmit, nor stops transmitting if another node begins to interfere with its transmission. In CSMA, each node listens to the channel before transmitting. If a frame from another node is currently being transmitted into the channel, a node then waits until it detects no transmissions for a short amount of time and then begins transmission. This technique is known as carrier sensing. A transmitting node listens to the channel while it is transmitting. If it detects that another node is transmitting an interfering frame, it stops transmitting and waits a random amount of time before repeating the sense-and-transmit-when-idle cycle. This is known as collision detection.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

Adding collision detection to a multiple access protocol will help protocol performance by not transmitting a useless, damaged frame in its entirety. When a node performs collision detection, it ceases transmission as soon as it detects a collision. Figure 2.21 shows collision detection scenario. In that the two nodes each abort their transmission a short time after detecting a collision.

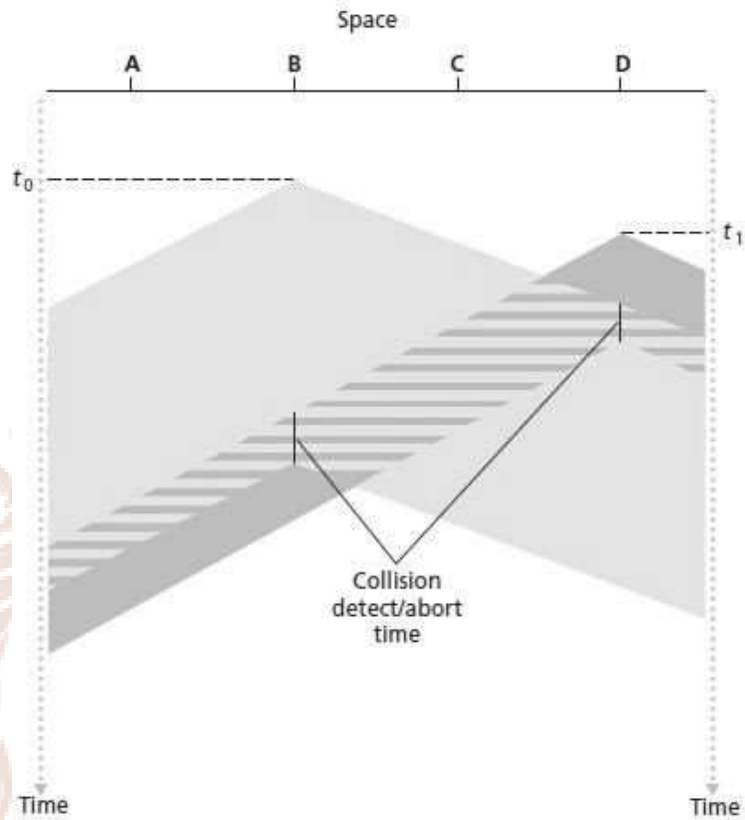

Figure 2.21: CSMA with collision detection

In CSMA/CD, if the adapter sense that the channel is idle, it starts to transmit the frame. If the adapter senses that the channel is busy, it waits until it senses no signal energy and then starts to transmit the frame. While transmitting, the adapter monitors for the presence of signal energy coming from other adapters using the broadcast channel. If the adapter transmits the entire frame without detecting signal energy from other adapters, the adapter is finished with the frame. If, on the other hand, the adapter detects signal energy from other adapters while transmitting, it aborts the transmission. After aborting, the adapter waits a random amount of time and then repeats the process.

6.3 Taking-Turns Protocols

Two desirable properties of a multiple access protocol are: when only one node is active; the active node has a throughput of *R* bps, and when M nodes are active; then each active node has a throughput of nearly *R/M* bps. The ALOHA and CSMA protocols have this first property but not the second. This has motivated researchers to create another class of protocols known as *taking-turns protocols*. There are many taking-turns protocols. Two of the most important protocols are *polling protocol* and *token-passing protocol*.

The polling protocol requires one of the nodes to be designated as a master node. The master node polls each of the nodes in a round-robin fashion. In particular, the master node first sends a message to node 1, saying that it (node 1) can transmit up to a maximum number of frames. After node 1 transmits some frames, the master node tells node 2 can transmit up to the maximum number of frames. The procedure continues in this manner, with the master node polling each of the nodes in a cyclic manner. The master node can determine when a node has finished sending its frames by observing the lack of a signal on the channel. The advantages of this protocol are that it eliminates collisions and empty slots. It also has a few drawbacks. First is, the protocol introduces a polling delay (the amount of time required to notify a node that it can transmit). The second drawback is that if the master node fails, the entire channel becomes inoperative.

The second taking-turns protocol is the *token-passing protocol*. In this protocol there is no master node. A small, special-purpose frame known as a token is exchanged among the nodes in some fixed order. For example, node 1 might always send the token to node 2, node 2 might always send the token to node 3, and node *N* might always send the token to node 1. When a node receives a token, it holds onto the token only if it has some frames to transmit; otherwise, it immediately forwards the token to the next node. If a node does have frames to transmit when it receives the token, it sends up to a maximum number of frames and then forwards the token to the next node. Token passing is decentralized and highly efficient. But it has its problems as well. For example, the failure of one node can crash the entire channel. Few examples of token-passing protocols are fiber distributed data interface (FDDI) protocol and the IEEE 802.5 token ring protocol.

Self-Assessment Questions - 5

12. There are two types of network links: they are __________ and ____________.
13. Two most commonly used random access protocols are___________ and ______________.
14. The ___________ protocol required that all nodes synchronize their transmissions to start at the beginning of a slot.
15. Two of the most important taking-turns protocols are __________ and _______.

7. SUMMARY

Let us recapitulate the important concepts discussed in this unit:

- The process of converting between bits and signals that represent them is called digital modulation.
- The scheme that directly converts bits into a signal, resulting in *baseband transmission. Passband transmission* is the scheme that regulates the amplitude, phase, or frequency of a carrier signal to convey bits.
- IEEE 802.3, popularly called *Ethernet*, is the most common type of wired LAN.
- Asynchronous Transfer Mode (ATM) is often used as a link-layer technology in the backbone of the Internet.
- Multiprotocol Label Switching (MPLS) was developed in the late 1990s to improve the forwarding speed of IP routers by adopting a key concept 'fixed-length label' from virtual circuit networks.

8. TERMINAL QUESTIONS

1. Differentiate between baseband transmission and Passband Transmission.
2. Write short notes on FDM, TDM and CDM.
3. Describe different implementations of ethernet.
4. List and explain different wireless LANs.
5. Describe Multiprotocol Label Switching (MPLS).

9. ANSWERS

Self-Assessment Questions

1. Digital Modulation
2. Baseband
3. Passband
4. Ethernet
5. 10 Base 2
6. 10 base-T
7. Wireless LAN
8. Wi-Fi
9. Bluetooth
10. Asynchronous Transfer Mode (ATM)
11. Fixed length label
12. Point-to-point links, broadcast links
13. ALOHA protocol, CSMA Protocol
14. Slotted ALOHA
15. Polling protocol, token-passing protocol

Terminal Questions

1. The scheme that directly converts bits into a signal, resulting in *baseband transmission*. In baseband transmission, the signal occupies frequencies from zero up to a maximum that depends on the signalling rate. *Passband transmission* is the scheme that regulates the amplitude, phase, or frequency of a carrier signal to convey bits. (Refer section 2 for more details).
2. *FDM (Frequency Division Multiplexing)* takes advantage of passband transmission to share a channel. It divides the spectrum into frequency bands, with each user having exclusive possession of some band in which to send their signal. TDM (Time Division Multiplexing) is an alternative to FDM. In TDM, users take turns (in a round-robin fashion), each one periodically getting the entire Bandwidth for a little burst of time.). In CDM, analog input is first converted into binary elements and then the frequency of

the transmitted signal is made to vary based on a defined pattern (code). (Refer section 2 for more details)

3. IEEE 802.3, popularly called *Ethernet*, is the most common type of wired LAN. Ethernet was created in 1976, at Xerox's Palo Alto Research Center (PARC). (Refer section 3 for more details).
4. A local area network which does not need cables to connect the different devices is known as wireless LAN. Three main wireless technologies are Wi-Fi (more formally known as 802.11), Bluetooth, and the third-generation or "3G" family of cellular wireless standards. (Refer section 4 for more details).
5. Multiprotocol Label Switching (MPLS) was developed in the late 1990s to improve the forwarding speed of IP routers by adopting a key concept 'fixed-length label' from virtual circuit networks. (Refer section 5.2 for more details).

References:

- Andrew S Tanenbaum, David J. Wetherall, *"Computer Networks,"* Fifth edition.
- Larry L. Peterson, Bruce S. Davie, *"Computer Networks- a Systems Approach," Fifth edition.*
- James F. Kurose, Keith W. Ross, *"Computer Networking-A top-down approach*," Sixth edition.
- Behrouz A. Forouzan, Sophia Chung Fegan, *"Data Communication and Networking*," Fourth edition.
- William Stallings, *"Computer Networking with Internet Protocols and Technology,"* Third edition.