CS601 SHORT NOTES

THEME 124 TO 220

BY VUONLINEHELP.BLOGSPOT.COM

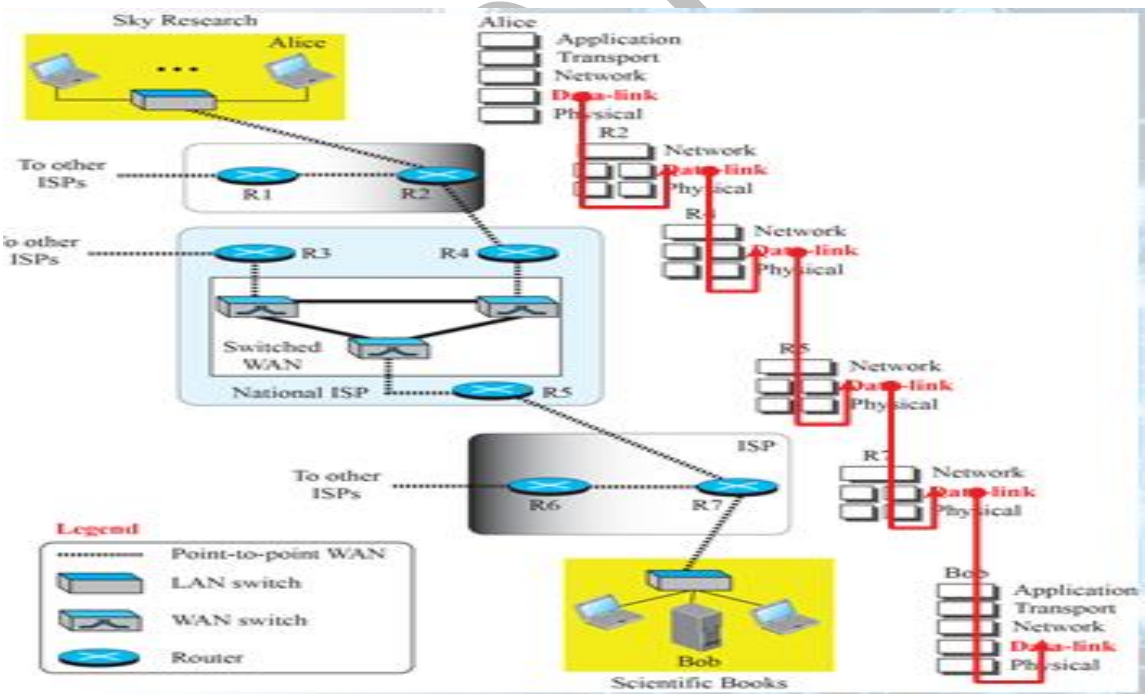
Chap 9

Data-Link Layer

The data link layer, or layer 2, is the second layer of the seven-layer OSI model of computer networking. This layer is the protocol layer that transfers data between nodes on a network segment across the physical layer. The data link layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the physical layer. Data link layer control Node-to-Node communication.

- The Internet is a combination of networks glued together by connecting devices (routers or switches).
- If a packet is to travel from a host to another host, it needs to pass through these networks.
- Data Link layer controls node-to-node communication.

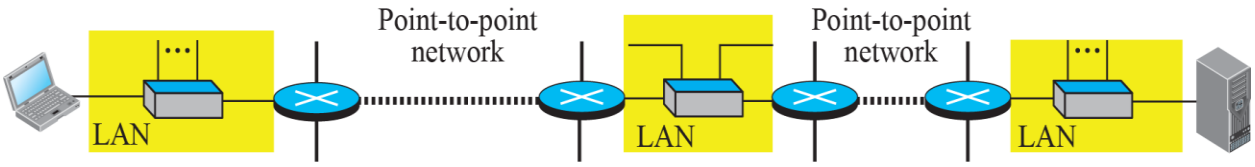
Communication at the Data-Link Layer



Nodes and Links

- Communication at the data-link layer is node-to-node

- A data unit from one point in the Internet needs to pass through many networks (LANs and WANs) to reach another point
- We refer to the two end hosts and the routers as nodes and the networks in between as links



a. A small part of the Internet

b. Nodes and links

Services provided by Data-Link Layer

- Located between the physical and the network layers
- Provides services to Network Layer and receives services from Physical layer
- Framing
- Flow Control
- Error Control
- Congestion Control

Two Categories of Links

- Two nodes are physically connected by a transmission medium such as cable or air
- Data-link layer controls how the medium is used
  - Data-link layer can use whole capacity

- Data-link layer can use only part of the capacity

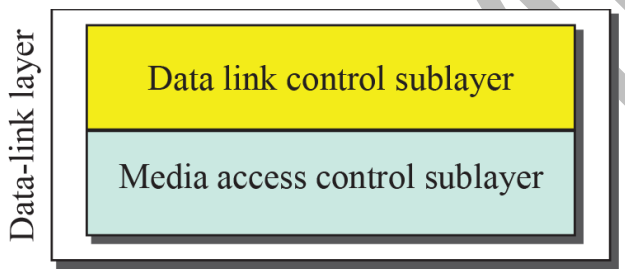
➢ We can have the following two types of links:

- Point-to-point link or a
- Broadcast link

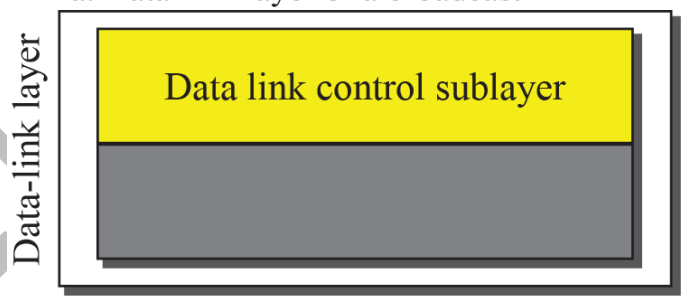
Two Sublayers of Data-Link Layer

- We can divide the data-link layer into two sublayers:
  - Data Link Control (DLC)
  - Media Access Control (MAC)

Dividing the data-link layer into two sublayers



a. Data-link layer of a broadcast link

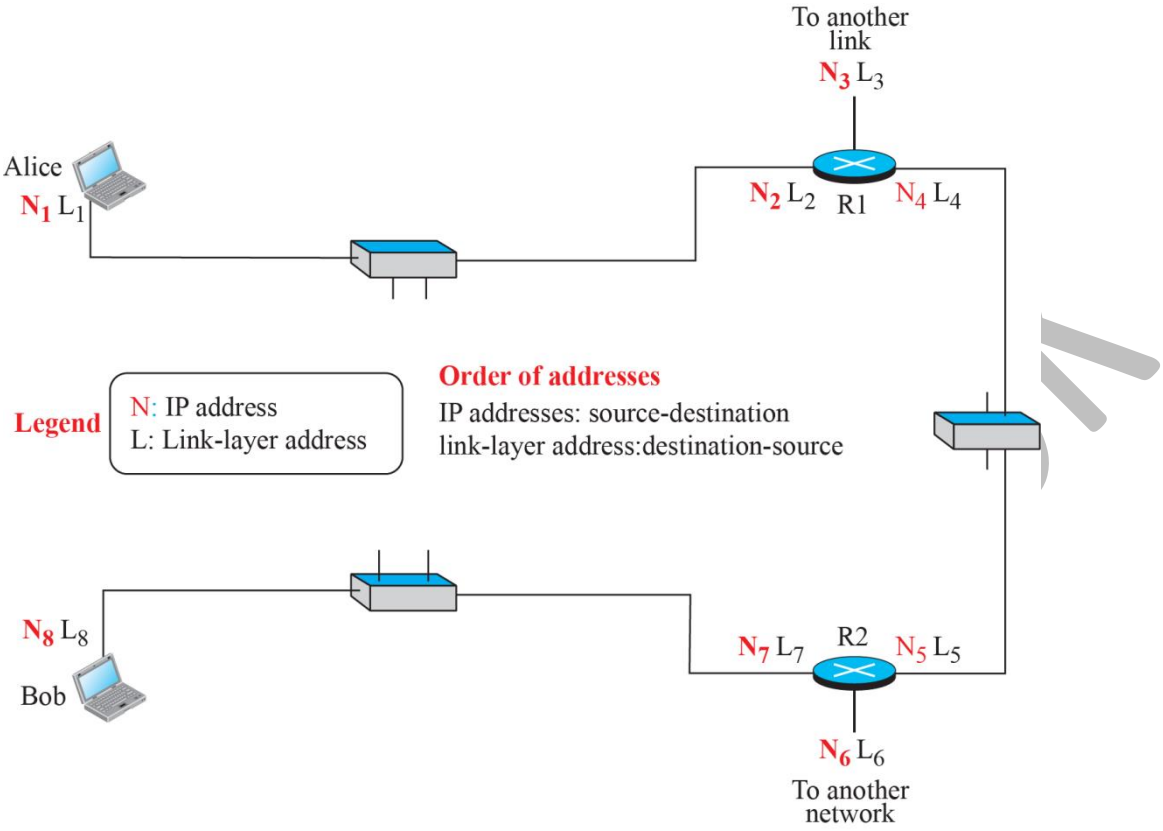


b. Data-link layer of a point-to-point link

Why LINK-LAYER ADDRESSING?

- IP addresses are the identifiers at the network layer
- In Internet we cannot make a packet reach its destination using only IP addresses

- Source and destination IP addresses define the two ends but cannot define which links the packet will take



Three Types of addresses

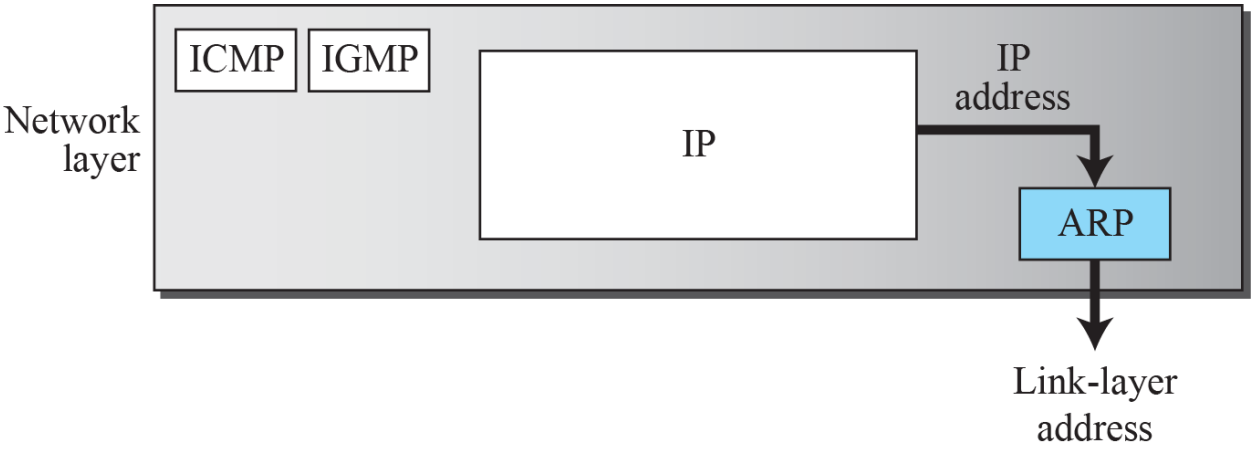
Some link-layer protocols define three types of addresses:

- Unicast
- Multicast
- Broadcast

Address Resolution Protocol (ARP)

- Anytime a node has an IP packet to send to another node in a link, it has the IP address of the receiving node
- IP address of the next node is not helpful in moving a frame through a link; we need the link-layer address of the next node

- We need Address Resolution Protocol (ARP)



ARP Packet

Hardware: LAN or WAN protocol

Protocol: Network-layer protocol

0	8	16	31
Hardware Type		Protocol Type	
Hardware length	Protocol length	Operation **Request:1, Reply:2**	
Source hardware address			
Source protocol address			
Destination hardware address (Empty in request)			
Destination protocol address			

Chap 10

Types of Errors

Data transmission suffers unpredictable changes because of interference .The interference can change the shape of the signal

- Single-bit error means that only 1 bit of a given data unit (such as a byte, character, or packet) is changed from 1 to 0 or from 0 to 1
- Burst Error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1

Redundancy

- Central concept in detecting or correcting errors is Redundancy
- To be able to detect or correct errors, we send some extra bits with our data
- The presence of these redundant bits allows the receiver to detect or correct corrupted bits

Detection versus Correction

- Correction is more difficult than the detection.
- In error detection, we are only looking to see if any error has occurred (Yes or No).
- We are not interested in the number of corrupted bits in Detection.
- Single-bit error is same as a Burst error.
- In Error Correction, we need to know:
    - The exact number of bits that are corrupted and,
    - Their location in the message

Coding LONG

- Redundancy is achieved through various coding schemes.
- Sender adds redundant bits through a process that creates a relationship between redundant bits and the actual data bits.
- The receiver checks the relationships between the two sets of bits to detect errors.
- The ratio of redundant bits to data bits and the robustness of the process are important factors in any coding scheme.

Types of Coding Schemes

Coding schemes can be divided into 2 broad categories:

- Block Coding
- Convolution Coding

Block Coding

- We divide our message into blocks, each of 'k' bits, called datawords
- We add 'r' redundant bits to each block to make the length 'n = k + r'
- The resulting 'n-bit' blocks are called codewords

BLOCK CODING in Error Detection

If the following two conditions are met, the receiver can detect a change in the original codeword:

- The receiver has (or can find) a list of valid codewords.
- The original codeword has changed to an invalid one

Hamming Distance

- Hamming Distance between two words of the same size is the number of differences between the corresponding bits

- Hamming Distance between two words x and y is $d(x,y)$
- Hamming distance between received codeword and sent codeword is number of bits corrupted

Minimum Hamming Distance

- Minimum Hamming Distance is smallest hamming distance between all possible pairs of codewords
- dmin= s+1

where,

s →no. of detectable errors

dmin→ minimum hamming distance

Linear Block Codes

Subset of Block Codes in which the exclusive OR of two valid codewords creates another valid codeword

Parity-Check Code

- Most common error-detecting code
- Linear block code (n=k+1)
- The extra parity bit is selected to make total number of 1s in codeword even

CYCLIC CODES

- Special linear block codes with one extra property
- If a codeword is cyclically shifted (rotated), the result is another codeword
- If 1011000 is a codeword and we cyclically left-shift, then 0110001 is also a codeword

Cyclic Redundancy Check (CRC)

- Subset of Cyclic Codes

- Cyclic redundancy check (CRC) is used in networks such as LANs and WANs

A CRC code with C(7, 4)

Dataword	*Codeword*	*Dataword*	*Codeword*
0000	0000000	1000	1000101
0001	0001011	1001	1001110
0010	0010110	1010	1010011
0011	0011101	1011	1011000
0100	0100111	1100	1100010
0101	0101100	1101	1101001
0110	0110001	1110	1110100
0111	0111010	1111	1111111

Cyclic Redundancy Check (CRC)

- Subset of Cyclic Codes
- Cyclic redundancy check (CRC) is used in networks such as LANs and WANs

Advantages of Cyclic Codes

- Good performance in detection:
  - Single-bit errors
  - Double errors
  - Odd number of errors
  - Burst errors
- Easy Implementation
- Fast Implementation

CHECKSUM

- Error-detection technique that can be applied to a message of any length
- Checksum mostly used at the network and transport layer rather than the data-link layer

Concept behind Checksum

- The idea of the traditional checksum is simple. We show this using a simple example

Suppose the message is a list of five 4-bit numbers that we want to send to a destination. In addition to sending these numbers, we send the sum of the numbers. Set of numbers is (7, 11, 12, 0, 6)

Forward Error Correction

- Retransmission of corrupted and lost packets is not useful for real-time multimedia transmission
- We need to correct the error or reproduce the packet immediately
- Several techniques developed and are commonly called Forward Error Correction techniques

Using Hamming Distance

- For error detection, we definitely need more distance
- It can be shown that to correct 't' errors, we need to have:

$$d_{min} = 2t + 1$$

- If we want to correct 10 bits in a packet, we need to make the minimum hamming distance 21 bits
- A lot of redundant bits need to be sent with the data

Using Hamming Distance

If we want to correct 10 bits in a packet, we need to make the minimum hamming distance 21 bits

Using XOR

Another recommendation is to use the property of the exclusive OR operation as shown below.

$R = P_1 + P_2 + \ldots + P_i + \ldots + P_N$

This means:

$P_i = P_1 + P_2 + \ldots + R + \ldots + P_N$

Chunk Interleaving

- Another way to achieve FEC in multimedia is to allow some small chunks to be missing at the receiver
- We cannot afford to let all the chunks belonging to the same packet be missing; however, we can afford to let one chunk be missing in each packet

Combining Hamming Distance & Interleaving

- Hamming distance and interleaving can be combined.
- We can first create n-bit packets that can correct t-bit errors.
- Then we interleave m rows and send the bits column by column.
- Possible to correct burst errors up to m × t bits of errors.

Compounding High & Low Resolution Packets

Creation of a duplicate of each packet with a low-resolution redundancy and combine the redundant version with the next packet

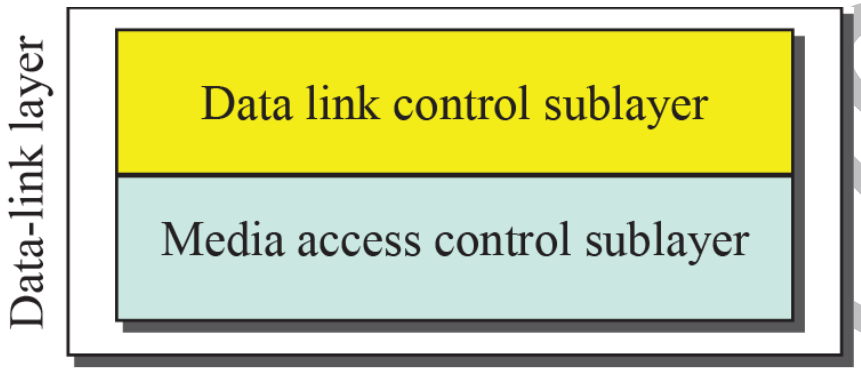
For example, we can create four low-resolution packets out of five high-resolution packets and send them

Chap 11

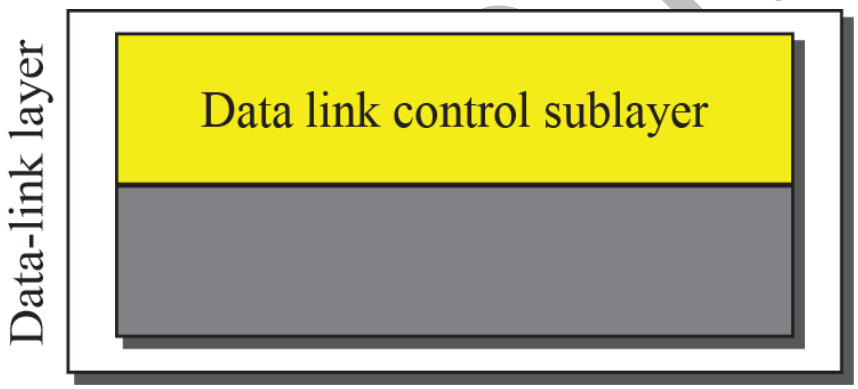
Data Link Control (DLC) Services

The data link control (DLC) deals with procedures for communication between two adjacent nodes no matter whether the link is dedicated or broadcast. Data link control functions include framing, flow control and error control.

DLC Services



a. Data-link layer of a broadcast link



b. Data-link layer of a point-to-point link

Framing

Data-Link layer needs to pack bits into frames, so that each frame is distinguishable from another. Our postal system practices a type of framing. Framing separates a message by adding a sender address and a destination address. The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

Frame Size

Why not one BIG Frame?

Frames can be of:

- Fixed Size
  - Size acts as a boundary/delimiter
- Variable Size
  - How to define Beginning and End of a Frame?

Variable Framing Techniques

Framing in the data link layer separates a message from one source to a destination, or from other messages to other destinations, by adding a sender address and a destination address.

Connection Oriented Framing

- Data to be carried are 8-bit characters

Byte Stuffing in Connection-Oriented Framing

Connection-oriented Framing used text characters as flags. Nowadays any character used for flag can also be a part of the data. In order to avoid confusing the receiver, we use Byte Stuffing.

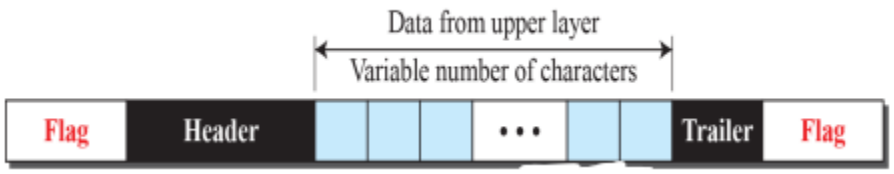
Several Issues:

- One or more escape characters followed by a byte with same pattern as a flag?
- Unicode (16/32 bit) vs. 8-bit characters.

- Data is stuffed with a pre-defined Escape Character (byte) when there is a character with same pattern as a flag.

Bit-Oriented Framing

Data section of frame is a sequence of bits. We need a delimiter to separate one frame from the other. A special 8-bit pattern (01111110) to define beginning and end of a frame. Same issue as Connection-oriented Framing.



Flow and Error Control

One of the responsibilities of the data-link control sublayer is flow and error control at the data-link layer.

Flow Control

Balance between production and consumption rates. If frames are produced faster than they are consumed at the receiving data link layer, the frames will be discarded. Use of buffers; one at sending end and other at receiving end.

Error Control

Error Control at Data Link layer uses CRC in one of the two ways:

- If a frame is corrupted, it is silently discarded and if it is good, it is delivered to network layer.
- If frame is corrupted, it is silently discarded and if it is good, an acknowledgement is sent to sender.

Connectionless and Connection-Oriented

A DLC protocol can be either connectionless or connection-oriented. Connectionless: No relationship between the frames. Connection-Oriented: Frames are numbered and sent in order.

DATA-LINK LAYER PROTOCOLS

Traditionally four protocols have been defined for the data-link layer to deal with flow and error control:

- ✓ Simple Protocol
- ✓ Stop-and-Wait Protocol
- ✓ Go-Back-N Protocol
- ✓ Selective-Repeat Protocol
- ✓ Last two protocols have almost disappeared completely

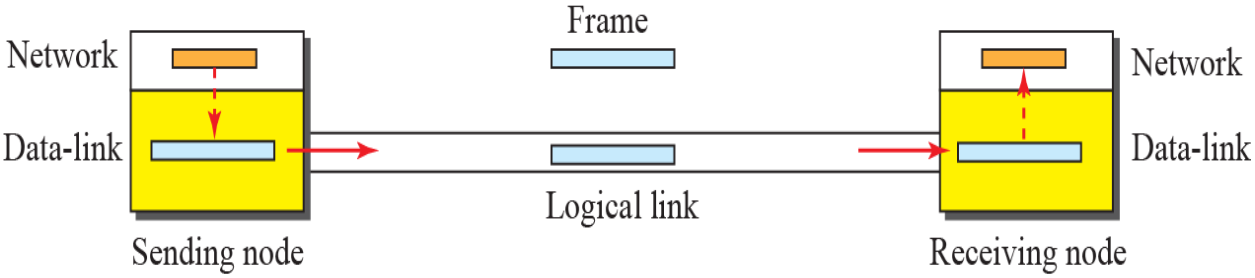
Finite State Machine (FSM)

A machine with a finite number of states. Machines stays in one of the states until an event occurs. Each event is associated with 2 reactions:

- ➢ List of actions to be performed
- ➢ Determining the next state

Simple Protocol

Simple protocol has neither flow nor error control. Assumption: The receiver can immediately handle any frame it receives. The receiver can never be overwhelmed with incoming frames.



Stop-and-Wait Protocol

Stop-and-Wait protocol uses both flow and error control. The sender sends one frame at a time and waits for an acknowledgment before sending the next one. To detect corrupted frames, we add a CRC code.

Piggybacking

Both Simple and Stop-and-wait protocols are designed for unidirectional communication. Data flows in one direction and ACK travels in the other. To make

the system efficient, the data in one direction is piggybacked with the acknowledgment in the other direction.

High-level Data Link Control (HDLC)

Bit -oriented protocol for communication over point-to-point and multipoint links. It implements Stop-and-Wait protocol. Most of the concepts defined in this protocol is the basis for other protocols such as PPP, Ethernet, or wireless LANs

Configurations & Transfer Modes in HDLC

HDLC provides two common transfer modes that can be used in different configurations:

- Normal Response Mode (NRM) &
- Asynchronous Balanced Mode (ABM)

Framing

HDLC defines three types of frames:

- information frames (I-frames)
- Supervisory frames (S-frames)
- Unnumbered frames (U-frames)

Point-to-Point Protocol (PPP)

Most common protocol for point-to-point access. Millions of Internet users who need to connect their home computers to the server of an Internet service provider use PPP. To control and manage the transfer of data, there is a need for a PPP at the data-link layer.

Services provided by PPP

The designers of PPP have included several services to make it suitable for a point-to-point protocol, but have ignored some traditional services to make it simple

Services Included	Services Not Included
Framing	Flow Control
Link Establishment and Data Exchange	Error Correction (PPP has CRC detection only)
Authentication	No Sequence Numbering
Multilink PPP Address configuration	Absence of sophisticated Addressing Mechanism
Network Address configuration	

Point-to-Point Protocol (PPP)

Most common protocol for point-to-point access. Millions of Internet users who need to connect their home computers to the server of an Internet service provider use PPP. To control and manage the transfer of data, there is a need for a PPP at the data-link layer

Multiplexing in PPP

Although PPP is a link-layer protocol, it uses another set of protocols to establish the link, authenticate and carry the network-layer data.

Three sets of protocols are:

- Link Control Protocol (LCP)
- Two Authentication Protocols (APs)
- Several Network Control Protocols (NCPs)

Link Control Protocol (LCP): This is responsible for establishing, maintaining, configuring and terminating our PPP links.

Two Authentication Protocols (APs): AP has two types: PAP stands for Password Authentication Protocol. CHAP stands for Challenge handshake Authentication protocol.

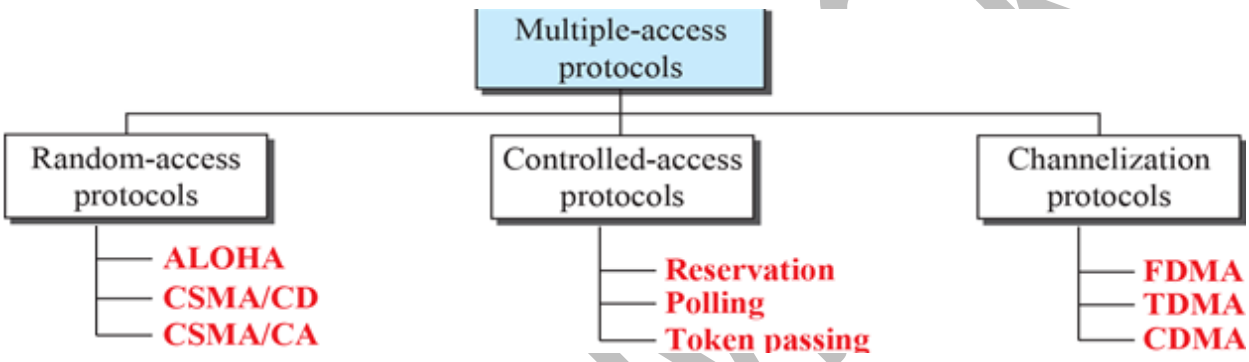
Several Network Control Protocols (NCPs): It has OSI, CP and IPCP.s

Chap 12

Media Access Control (MAC) Sub-Layer

When nodes use a multipoint or broadcast link, we need a multiple-access protocol to coordinate access to the link. Many protocols have been devised to handle access to a shared link. All of these protocols belong to Media Access Control (MAC) sub-layer.

Taxonomy of Multiple-Access Protocols



Random Access

In random-access or contention no station is superior to the other and none is assigned control over the other. Station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send. This decision depends on the state of the medium (idle or busy)

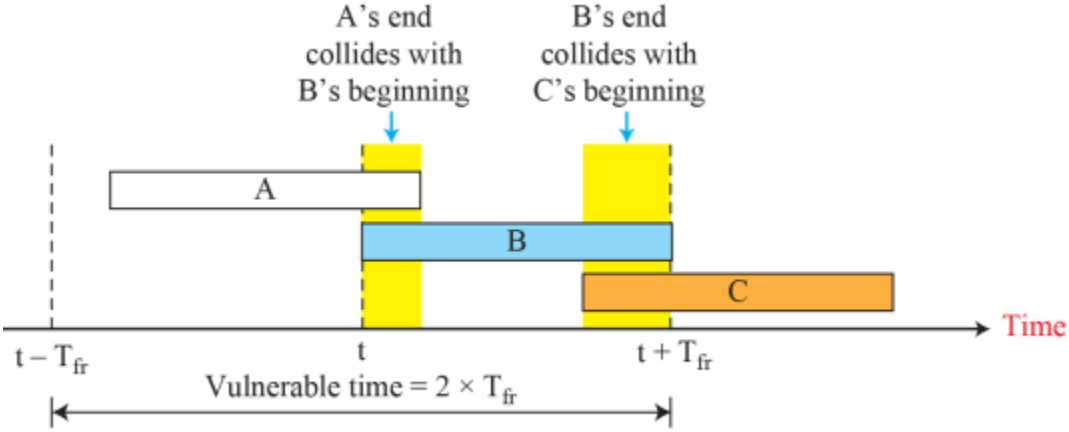
ALOHA

ALOHA, the earliest random access method, was developed in early 1970s.Designed for a radio (wireless) LAN, but it can be used on any shared medium. Potential collisions in this arrangement as the medium is shared between the stations. When a station sends data, another station may attempt to do so at the same time. The data from the two stations collide and become garbled.

Frames in a pure ALOHA Network: In pure

ALOHA, the time of transmission is continuous. Whenever a station hasn't available frame, it sends the frame. If there is collision and the frame is destroyed, the sender waits for a random amount of time before retransmitting it.

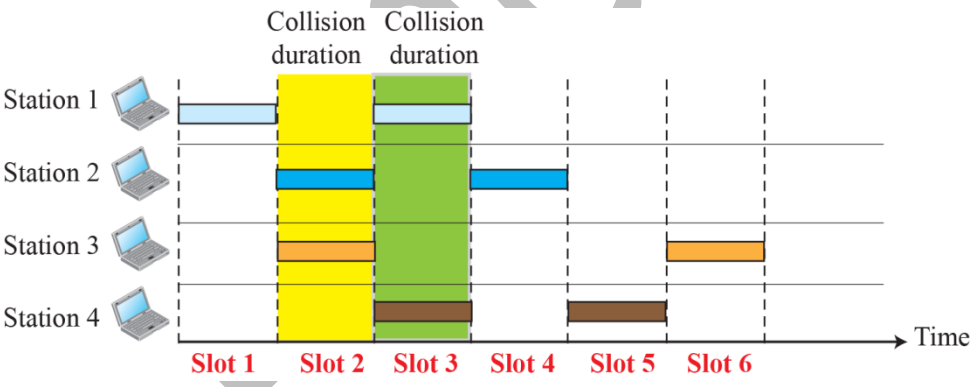
Vulnerable Time for pure ALOHA protocol:20



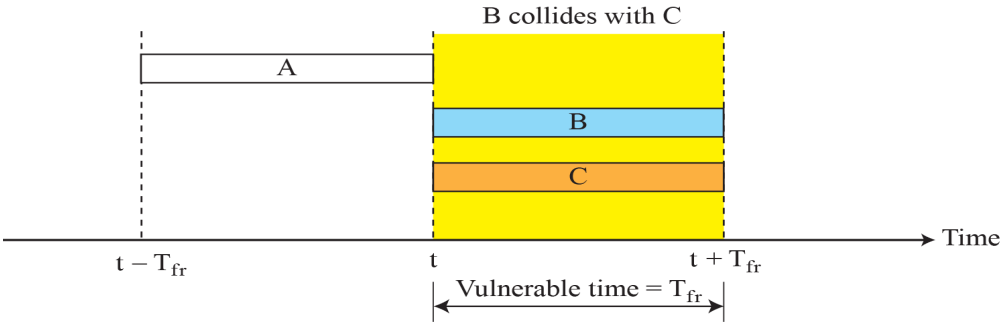
Slotted ALOHA:

We divide time into slots of Tfr sec and force the station to send only at the beginning of the slot. Invented to improve the efficiency of pure ALOHA. If a station misses the time slot, it must wait until beginning of next time slot reducing vulnerable time to Tfr (vs. 2 x Tfr for pure ALOHA).

Frames in a Slotted ALOHA Network



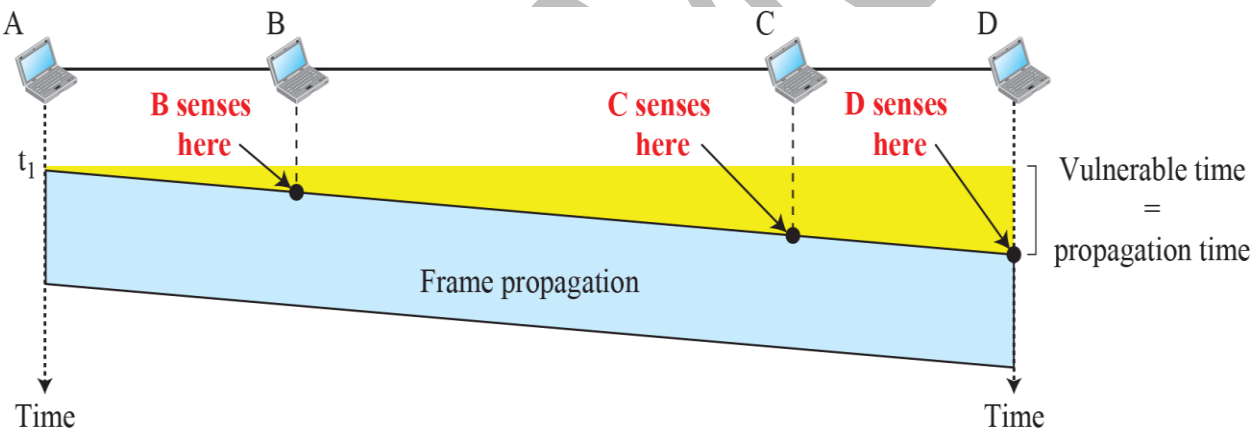
Vulnerable Time for Slotted ALOHA



Carrier Sense Multiple Access (CSMA)

To minimize the chance of collision and, therefore, increase the performance, CSMA was developed. The chance of collision is reduced as the station is required to sense/listen to the medium before sending data. 'Sense before transmit' or 'listen before talk'.

Vulnerable Time in CSMA



Carrier Sense Multiple Access/Collision Detection

CSMA method does not specify the procedure following a collision. CSMA/CD augments the algorithm to handle the collision. The station monitors the medium after it sends a frame to see if the transmission was successful. If there is a collision, the frame is sent again.

I-persistence:

This is a simplest method. In this method after the station find link ideal it sends immediately without waiting. This method has got highest chance of collision.

Non-persistence:

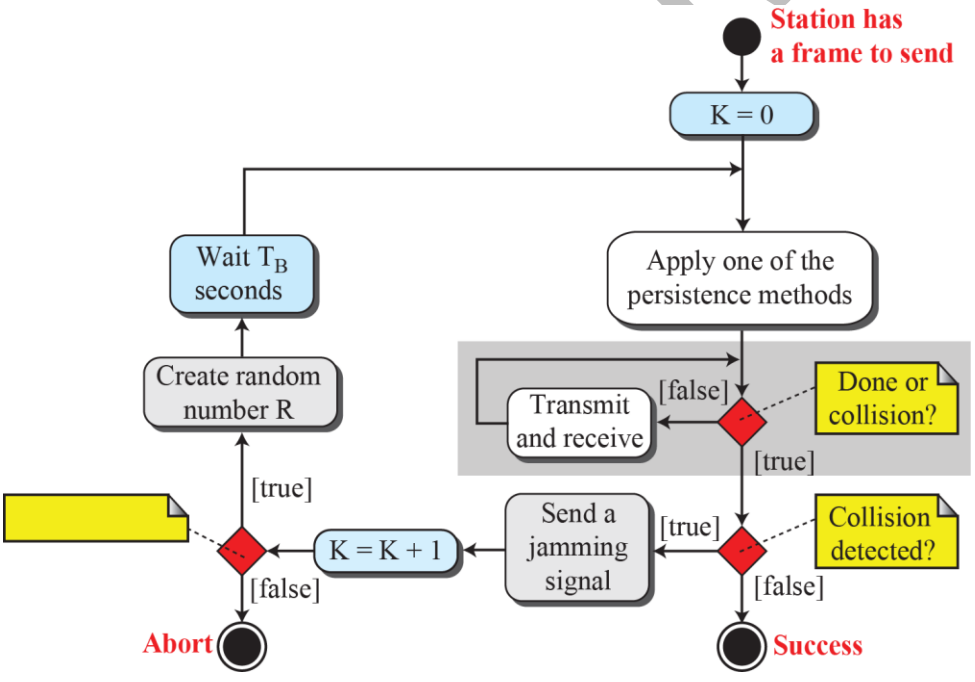
In this method the channel has time slots. A station that has frame to send, it sense the link. If the link is Idle it send frame immediately. If links are not idle, it waits for a random amount of time and the sense that link again. So Collision rate in this case goes down as compared to I-persistence but the efficiency goes also down.

P-persistence:

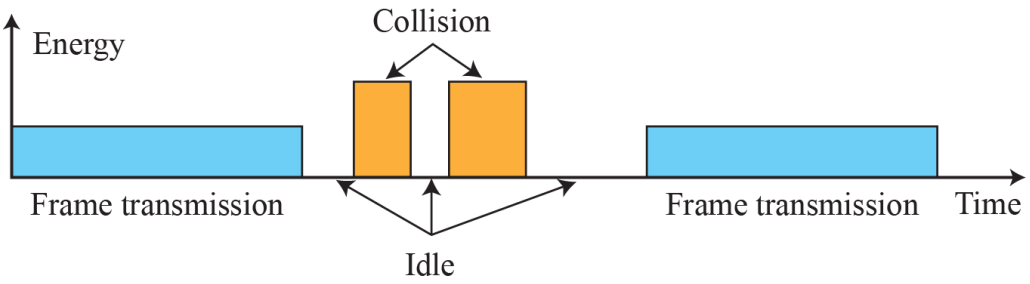
In this case we have got a slot duration which is equal to or greater than the maximum propagation time. This approach combined the advantages of both I-persistence and Non-persistence.

Legend

T_{fr}: Frame average transmission time
K : Number of attempts
R : (random number): 0 to $2^K - 1$
T_B: (Back-off time) = R × T_{fr}



Energy Level During Transmission, Idleness and Collision:22



Carrier Sense Multiple Access/Collision Avoidance

CSMA/CA was invented for Wireless Networks. Collisions are avoided through the use of three strategies:

The Interfame Space

The Contention Window

Acknowledgements

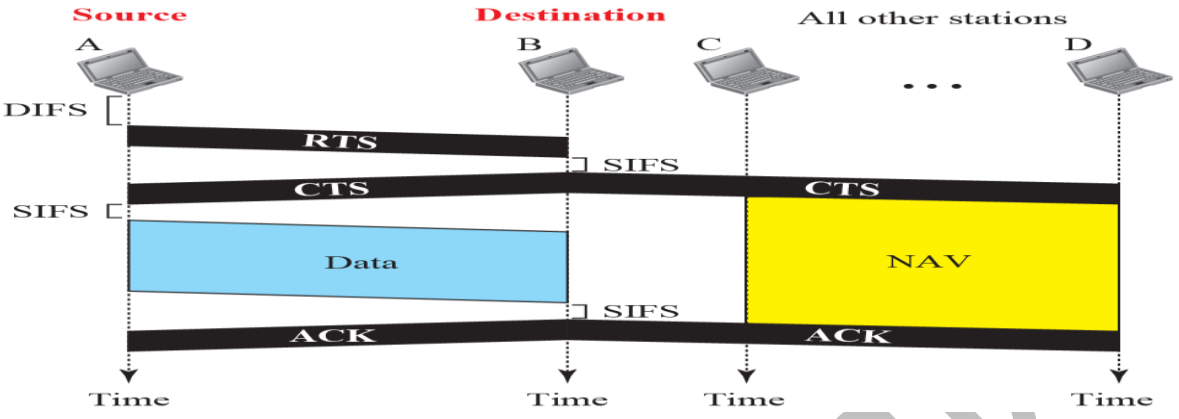
CSMA/CA

Interframe Space (IFS): Collisions are avoided by deferring transmission even if the channel is idle.

Contention Window: Amount of time divided into slots. Station chooses a random number of slots as its wait time (one slot first time and double each time system cannot detect an idle channel).

Acknowledgement: Positive acknowledgement and time-out timer can help guarantee that the receiver has received the frame.

CSMA/CA and Network Allocation Vector (NAV)



CONTROLLED ACCESS

The stations consult one another to find which station has the right to send. A station cannot send unless authorized by other stations. We discuss three controlled-access methods:

Reservation

Polling

Token Passing

Reservation

In the reservation method, a station needs to make a reservation before sending data. Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval.

Polling

Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations. All data exchanges must be made through primary device even when the ultimate destination is a secondary device. The primary device controls the link; the secondary devices follow its instructions.

Token Passing

In the token-passing method, the stations in a network are organized in a logical ring. For each station, there is a predecessor and a successor. The predecessor is the station which is logically before the station in the ring; the successor is the station which is after the station in the ring.

Special packet called TOKEN circulates through the ring. Possession of TOKEN gives the station the right to send the data. TOKEN Management is required to manage possession time, Token monitoring, priority assignment etc.

CHANNELIZATION (Channel Partition)

The available bandwidth of a link is shared in time, frequency, or through code, among different stations we discuss three protocols:

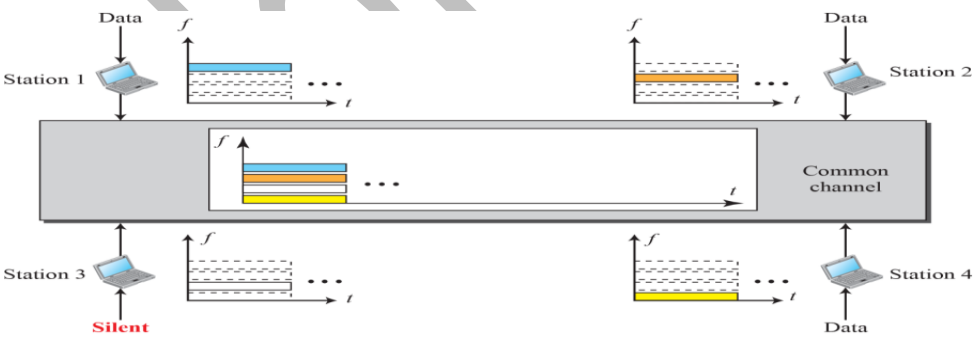
Frequency Division Multiple Access (FDMA)

Time Division multiple Access (TDMA)

Code Division Multiple Access (CDMA)

Frequency-Division Multiple Access (FDMA)

In FDMA, the available bandwidth is divided into frequency bands. Each station is allocated a band to send its data i.e. each band is reserved for a specific station, and it belongs to the station all the time. Each station also uses a bandpass filter to confine the transmitter frequencies.



CHANNELIZATION (Channel Partition)

Three protocols:

Frequency Division Multiple Access (FDMA)

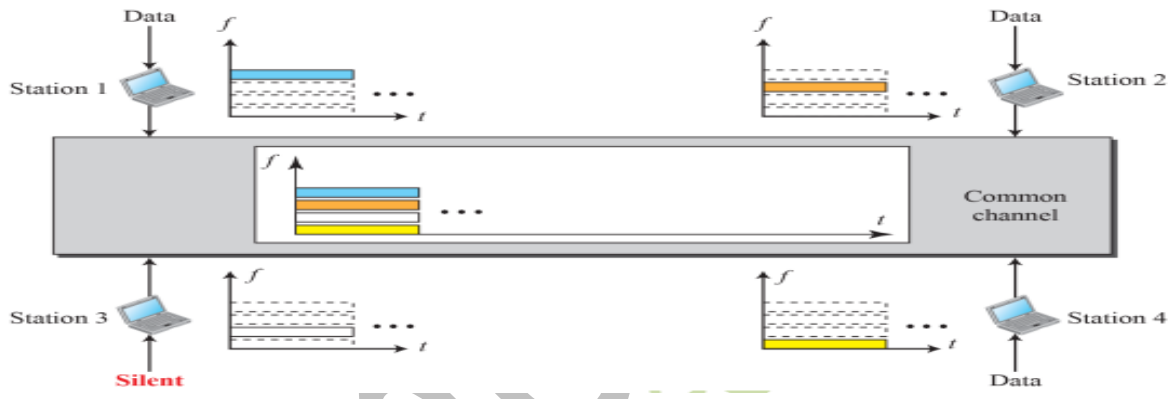
Time Division Multiple Access (TDMA)

Code Division Multiple Access (CDMA)

Frequency-Division Multiple Access (FDMA)

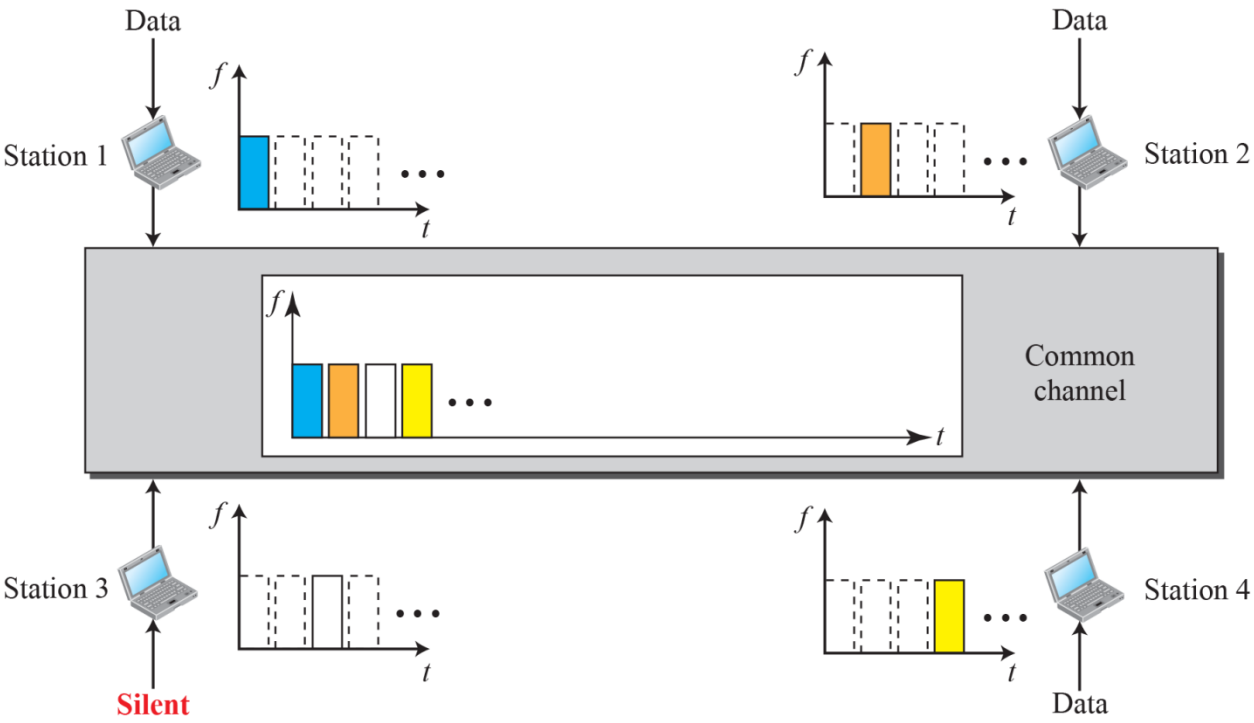
In FDMA, the available bandwidth is divided into frequency bands. Each station is allocated a band to send its data i.e. each band is reserved for a specific station, and it belongs to the station all the time. Each station also uses a band pass filter to confine the transmitter frequencies.

Frequency-Division Multiple Access (FDMA)26



TDMA

Stations share the bandwidth of the channel in time. Each station is allocated a time slot during which it can send data. Each station transmits its data in its assigned time slot.

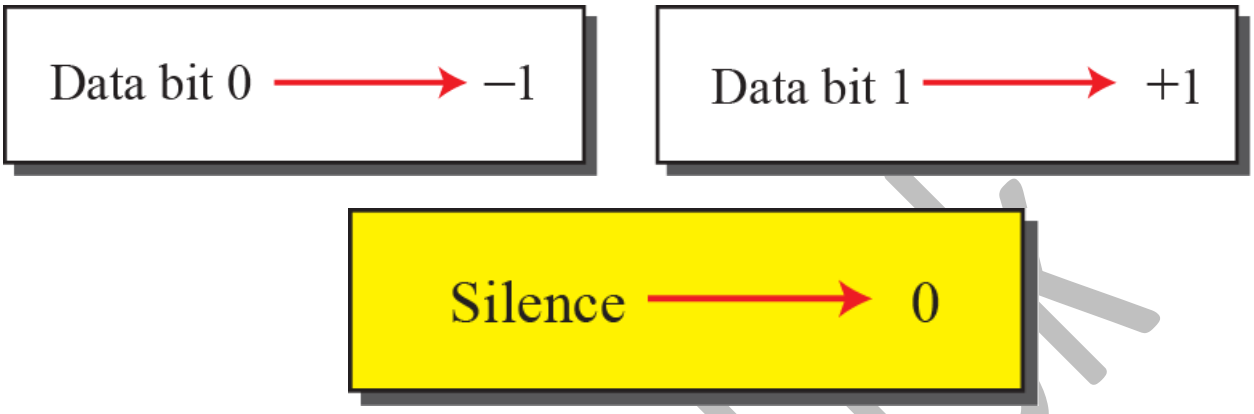


Code Division Multiple Access (CDMA

CDMA differs from FDMA in that only one channel occupies the entire bandwidth of the link. CDMA differs from TDMA in that all stations can send data simultaneously; there is no timesharing.

Data Rep-resentation in CDMA

Optical CDMA protects data confidentiality by using a code pattern to represent "0" and "1" bits Multiple users with different (orthogonal) codes can share the same channel to transmit data simultaneously.



Chap 13

Chap 13

Ethernet Protocol

Data-link layer and the physical layer are the territory of the local and wide area networks. We can have wired or wireless networks.

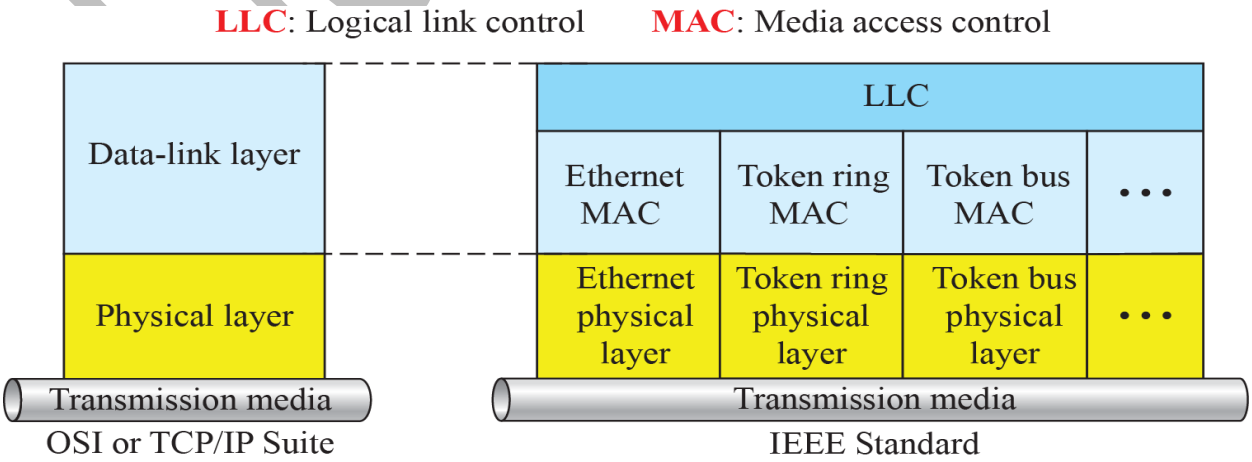
Ethernet Short and long

Ethernet is a family of wired computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN). It was commercially introduced in 1980 and first standardized in 1983 as IEEE 802.3. Ethernet has since been refined to support higher bit rates, a greater number of nodes, and longer link distances, but retains much backward compatibility. Over time, Ethernet has largely replaced competing wired LAN technologies such as Token Ring, FDDI and ARCNET.

IEEE Project 802

In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable inter-communication among equipment from a variety of manufacturers. Project 802 did not seek to replace any part of the OSI model or TCP/IP protocol suite. A way of specifying functions of the physical layer and the data-link layer of major LAN protocols.

IEEE Standard for LANs



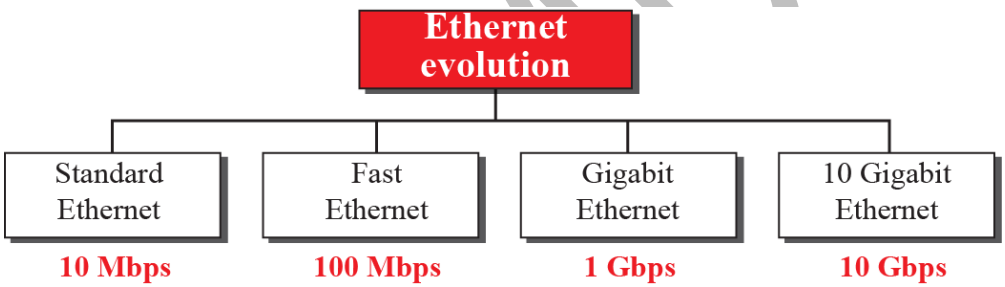
Ethernet Evolution/Standard Ethernet/ Connectionless & Unreliable Service

Long

Ethernet Evolution

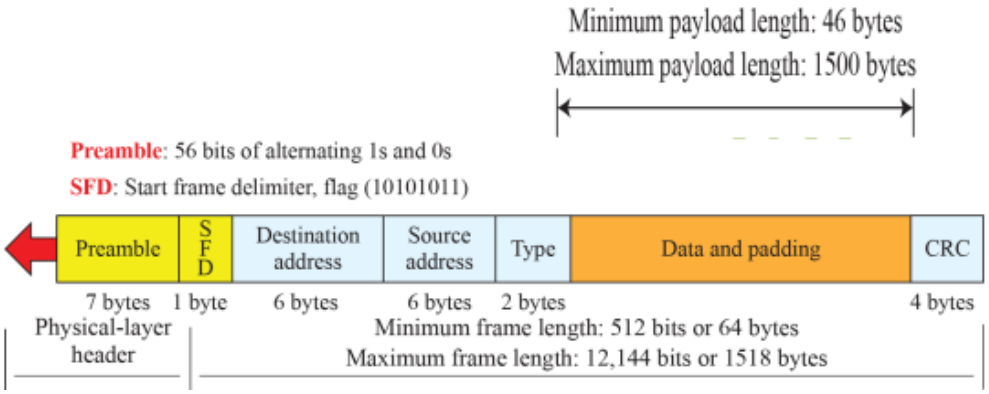
The Ethernet LAN was developed in the 1970s. Since then, it has gone through four generations:

- Standard Ethernet (10 Mbps)
- Fast Ethernet (100 Mbps)
- Gigabit Ethernet (1 Gbps)
- 10 Gigabit Ethernet (10 Gbps)



Standard Ethernet

The original Ethernet technology with the data rate of 10 Mbps is called Standard Ethernet. Most implementations have moved to later evolutions. Still some features of the Standard Ethernet that have not changed during the evolution.



Connectionless & Unreliable Service

Each frame is independent of other. No connection establishment or tear down process. The sender may overwhelm receiver with frames and frames are dropped. If frame drops, sender will not know about it unless we are using TCP (Transport).Ethernet is unreliable like IP and UDP. If a frame is corrupted, receiver silently drops it. Left to high level protocols to find out about it.

Addressing in Standard Ethernet

Each station on Ethernet has its own network interface card (NIC). The NIC fits inside the station and provides the station with a link-layer/physical address. The Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.

For example, the following shows an Ethernet MAC address:

4A:30:10:21:10:1A

Transmission of Address Bits

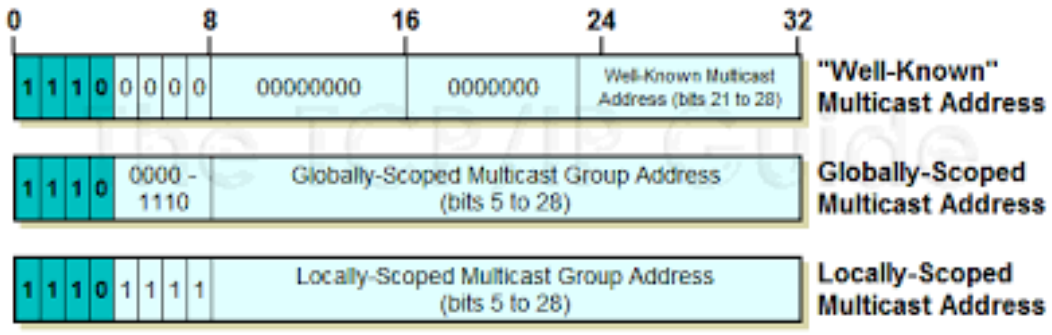
How the address 47:20:1B:2E:08: EE is sent out online.

The address is sent left to right, byte by byte; for each byte, it is sent right to left, bit by bit, as shown below:

Hexadecimal	47	20	1B	2E	08	EE
Binarys	01000111	00100000	00011011	00101110	00001000	11101110
Transmitted ←	11100010	00000100	11011000	01110100	00010000	01110111

Unicast and Multicast Addresses

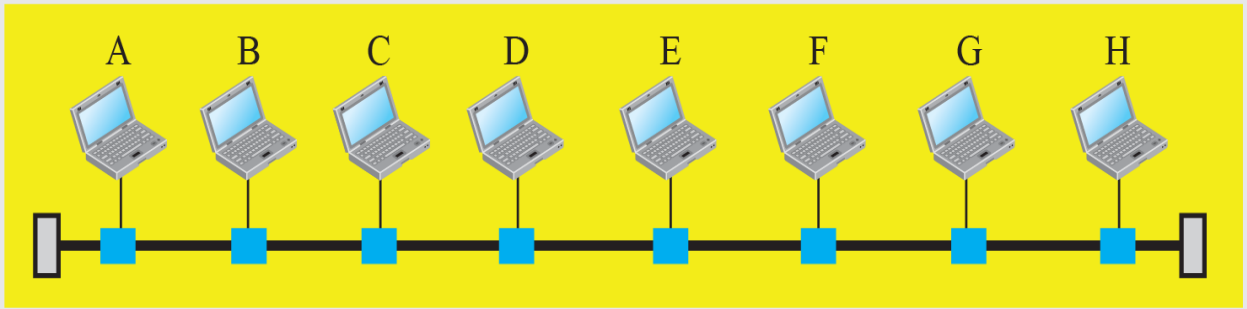
A unicast address represents a single device in the network. A multicast address represents a group of devices in the network. A broadcast address represents all devices in the network. If a device wants to share the information only with a single device, it uses the unicast address of that device.



Access Method in Standard Ethernet/ Efficiency of Standard Ethernet LONG

Access Method in Standard Ethernet

As we know all the frames in Ethernet by nature is broadcast. If the all frame are broadcast then how we know which of the unicast or multicast. The answer is we know that by specifying the way these frame are actually treated when they reach at destination.



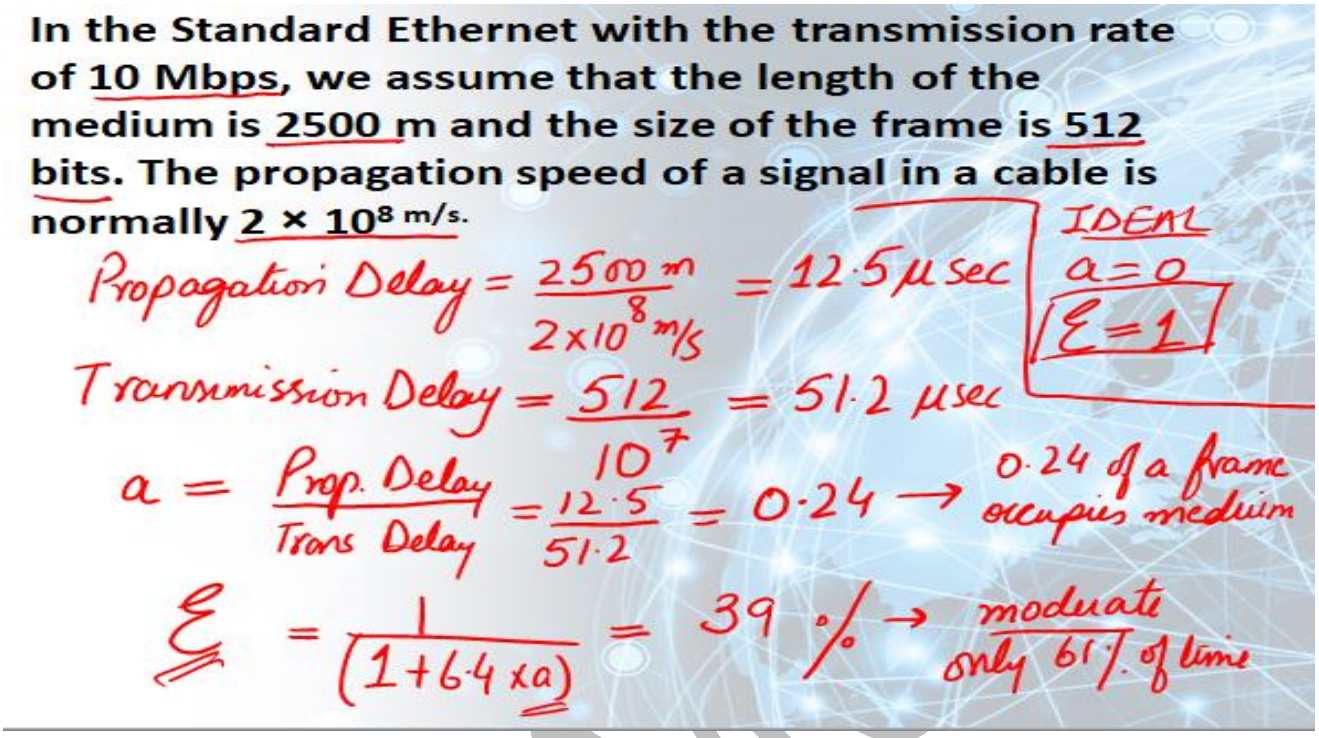
a. A LAN with a bus topology using a coaxial cable

Efficiency of Standard Ethernet

The ratio of the time used by a station to send data to the time the medium is occupied by this station. The practical efficiency of standard Ethernet has been measured to be:

Efficiency = 1/(1+ 6.4 x a)

Where a = number of frames that can fit on a medium



Implementation of Standard Ethernet

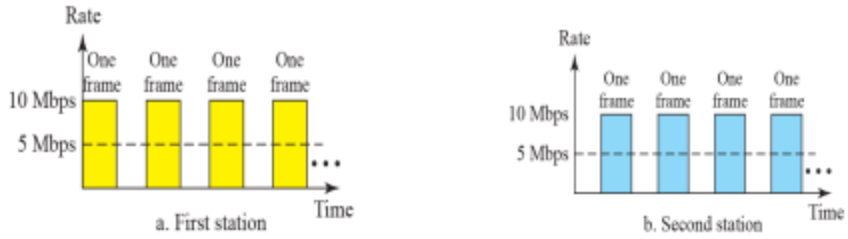
The Standard Ethernet defined several implementations, but only four of them became popular during the 1980s.

Implementation	*Medium*	*Medium Length*	*Encoding*
10Base5	Thick coax	500 m	Manchester
10Base2	Thin coax	185 m	Manchester
10Base-T	2 UTP	100 m	Manchester
10Base-F	2 Fiber	2000	Manchester

Changes in the Standard LONG

The changes that occurred to the 10-Mbps Standard Ethernet opened the road to the evolution of the Ethernet to become compatible with other high-data-rate LANs

- Bridged Ethernet
- Switched Ethernet
- Full-Duplex Ethernet



Bridged Ethernet

An Ethernet network bridge is a device which connects two different local area networks together. Both networks must connect using the same Ethernet protocol. Bridges can also be used to add remote computers to a LAN. Many bridges can connect multiple computers or other compatible devices with or without wires.

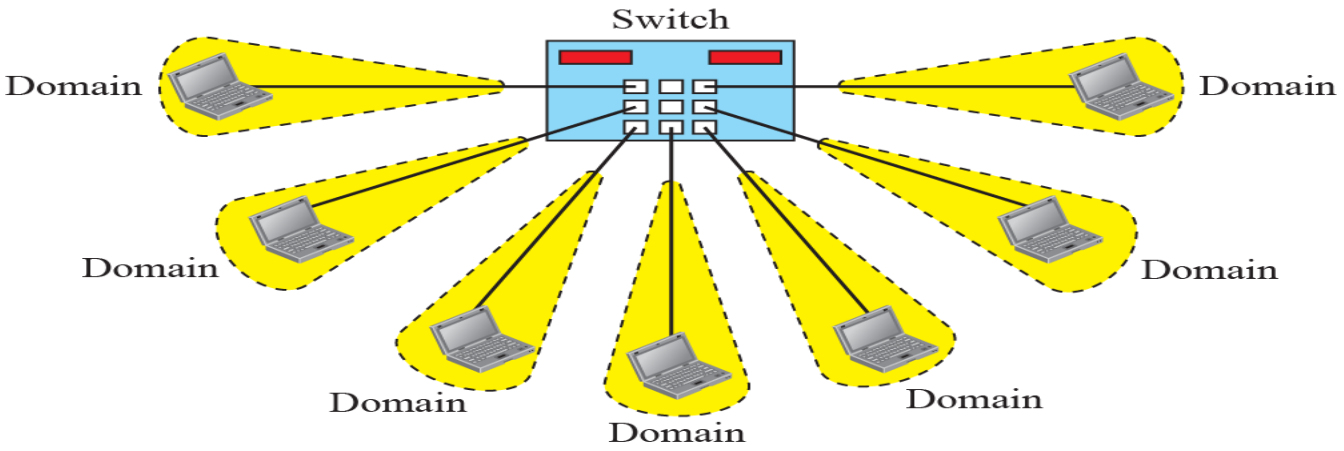
A Network with and without Bridging:

Advantages:

- The basic advantage of bridging is that we can now divide 10Mbps capacity.
- We also separate the collision domains as well.

Switched Ethernet

Switched Ethernet A network switch (also called switching hub, bridging hub, and, by the IEEE, MAC bridge) is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device.

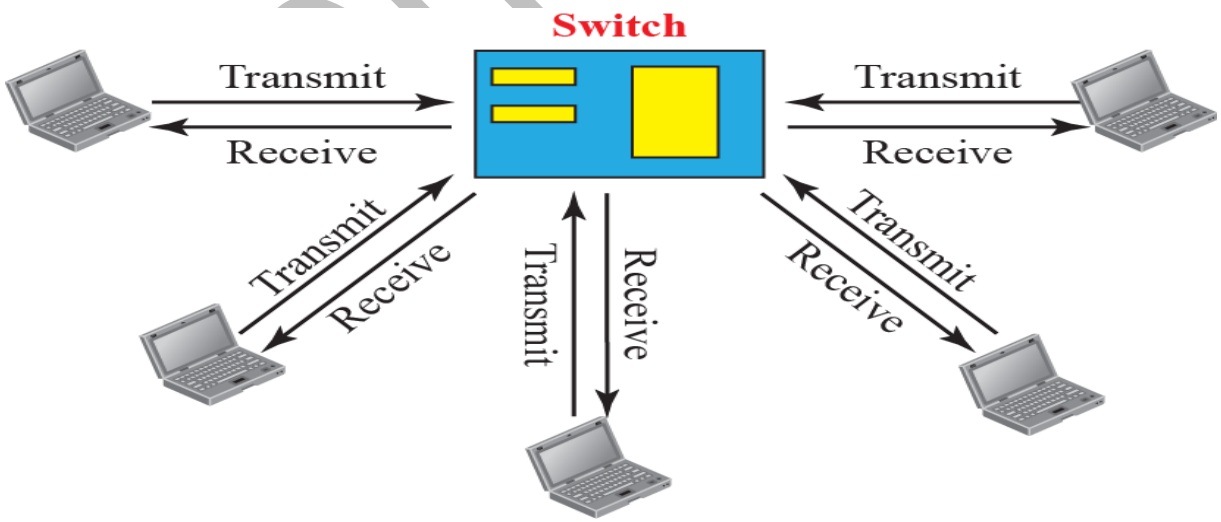


Advantages:

- Reduce network downtime.
- Improve network performance.
- Increase available bandwidth on your network.
- Reduce strain on individual host computers suffer with lower workloads.

Full – Duplex Switched Ethernet

The Ethernet switch or Ethernet FDSE (Full Duplex Switched Ethernet), was born in the early 1990s before the advent of switched Ethernet, shared Ethernet networks were cut into shared subnets autonomous, interconnected by bridges. Therefore, the traffic was multiplied by the number of subnets.



Advantages of FDSE

- This increases the direct capacity from 10MBS to 20MBS.
- Instead of using one link between stations, we use two links.
- CSMA / CD are not required.

Fast Ethernet

In the 1990s, Ethernet made a big jump by increasing the transmission rate to 100 Mbps, and the new generation was called the Fast Ethernet. To make it compatible with the Standard Ethernet, the MAC sub layer was left unchanged. But the features of the Standard Ethernet that depend on the transmission rate, had to be changed

Goals of Fast Ethernet:

- Upgrade data rate to 100Mbps
- Make it compatible with Standard Ethernet
- Keep same 48-bit address
- Keep same frame format

Physical Layer

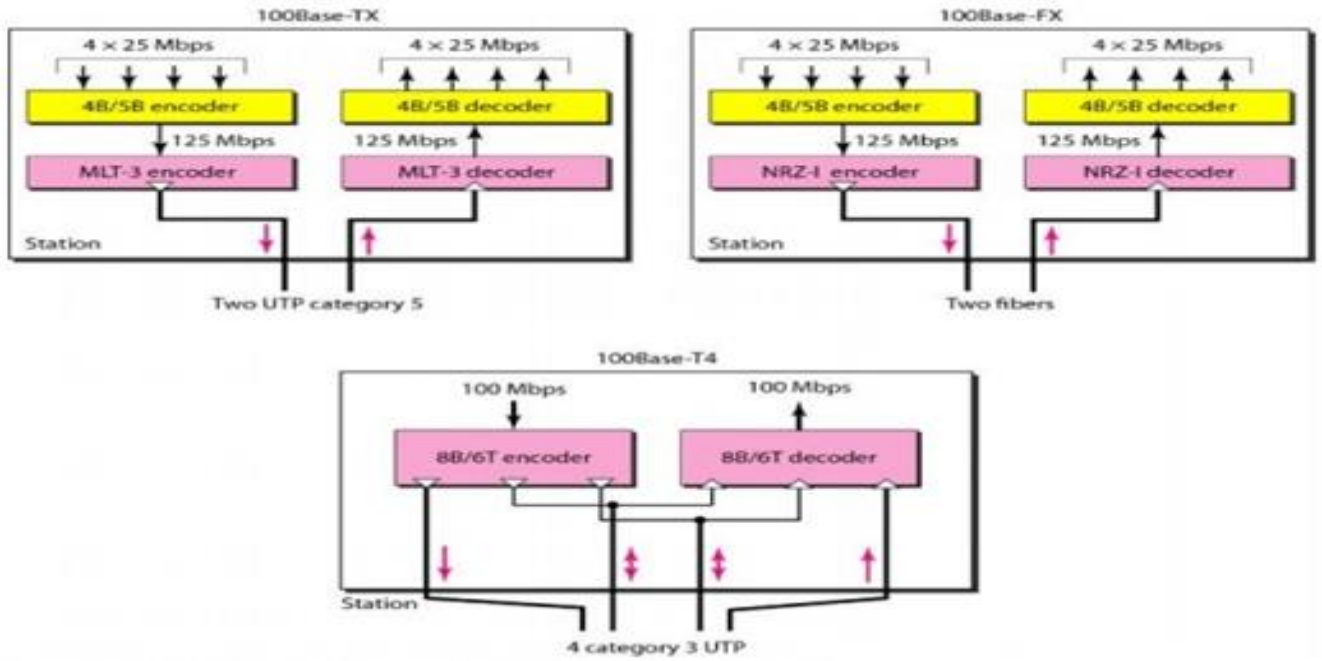
To be able to handle a 100 Mbps data rate, several changes need to be made at the physical layer.

Advantages:

- Physical Layer maintains the data rate (how many bits a sender can send per second).
- It performs Synchronization of bits.
- It helps in Transmission Medium decision (direction of data transfer).

Implementation of Fast Ethernet implementations

Implementation	*Medium*	*Medium Length*	*Wires*	*Encoding*
100Base-TX	STP	100 m	2	4B5B + MLT-3
100Base-FX	Fiber	185 m	2	4B5B + NRZ-I
100Base-T4	UTP	100 m	4	Two 8B/6T



Gigabit Ethernet

Need for an even higher data rate resulted in the design of IEEE Standard 802.3z Gigabit Ethernet Protocol (1000 Mbps).
The goals of the Gigabit Ethernet were:

- Upgrade the data rate to 1 Gbps
- Make it compatible with standard or Fast Ethernet
- Use same 48 bit address
- Use the same frame format
- Keep same minimum and maximum frame lengths

MAC Sub-layer

A main consideration in the evolution of Ethernet was to keep the MAC sublayer untouched. To achieve a data rate of 1 Gbps, this was no longer possible.

Gigabit Ethernet has two distinctive approaches for medium access:

- Half-duplex
- Full-duplex

10-gigabit Ehternet

The idea is to extend the technology, the data rate, and the coverage distance so that the Ethernet can be used in LANs and MANs (metropolitan area network). The IEEE committee created 10 Gigabit Ethernet and called it Standard 802.3ae.

Implementation

10 Gigabit Ethernet operates only in full-duplex mode, which means there is no need for contention; CSMA/CD is not used in 10 Gigabit Ethernet

Four implementations are most common:

Implementation	*Medium*	*Medium Length*	*Number of wires*	*Encoding*
10GBase-SR	Fiber 850 nm	300 m	2	64B66B
10GBase-LR	Fiber 1310 nm	10 Km	2	64B66B
10GBase-EW	Fiber 1350 nm	40 Km	2	SONET
10GBase-X4	Fiber 1310 nm	300 m to 10 Km	2	8B10B

Chap 14

Other Wired Networks LONG / Short

Access Networks

Networks that connect a small LAN to an ISP

Wide Area Networks

Wired networks used to transfer data over long distances

Telephone Network

The telephone network had its beginnings in the late 1800s. Plain Old Telephone System (POTS) was originally an analog system using analog signals to transmit voice. With the advent of the computer era, the network, in the 1980s, began to carry data in addition to voice. During the last decade, the telephone network has undergone many technical changes and the network is now digital as well as analog.

Major Components

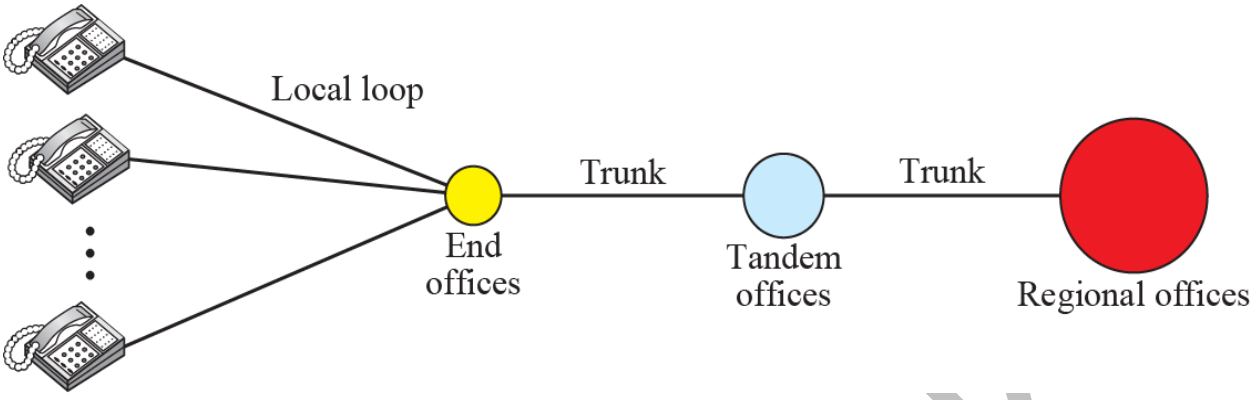
The telephone network is made of three major components:

- **Local Loops**
- **Trunks**
- **Switching offices**

The telephone network has several levels of switching offices:

- End offices
- Tandem offices
- Regional offices

A Telephone System



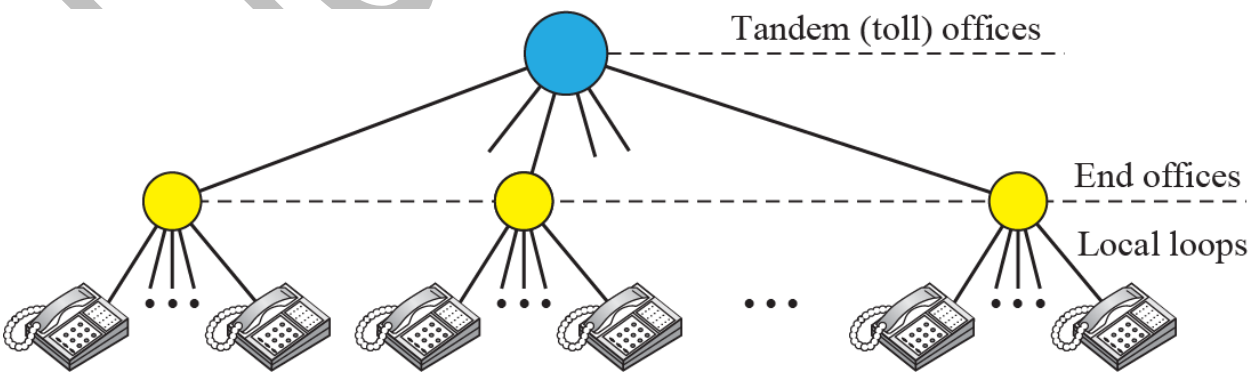
Local-Access Transport Areas (LATAs)

A LATA can be a small or large metropolitan area. A small state may have a single LATA; a large state may have several LATAs .A LATA boundary may overlap with state boundary; part of a LATA can be in one state, part in another state.

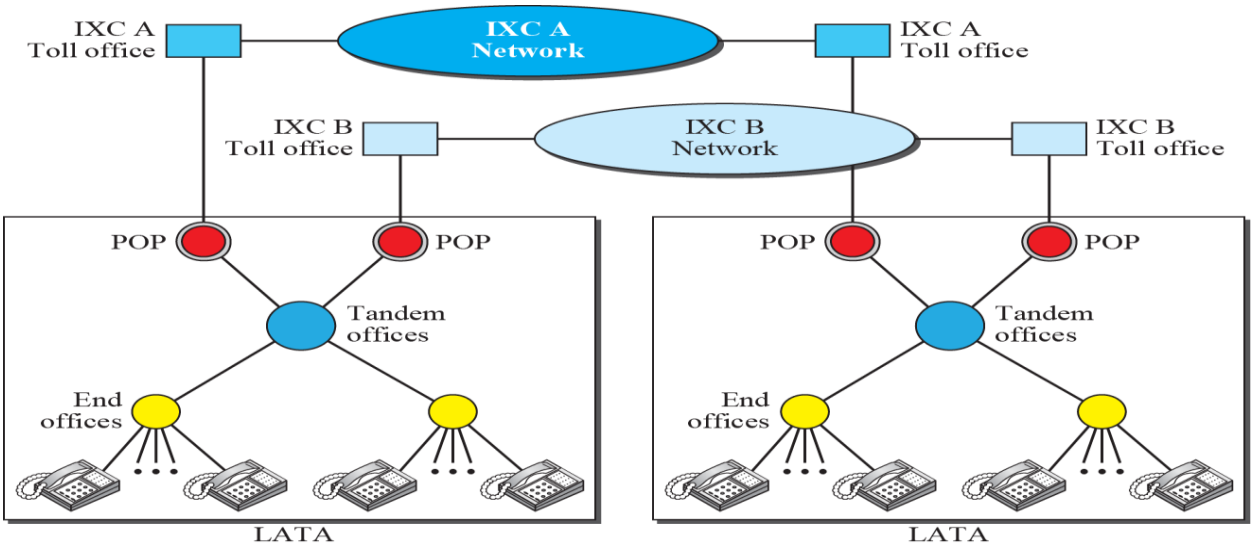
Intra-LATA and Inter-LATA Services

- **Services offered by Telephone companies inside a LATA are called Intra-LATA services and between LATAs are called Inter-LATA services**
- **Carrier that handles Intra-LATA are called a Local Exchange Carrier (LEC) and the ones that handle Inter-LATA are called Interexchange Carriers (IXCs)**

Switching Offices in a LATA



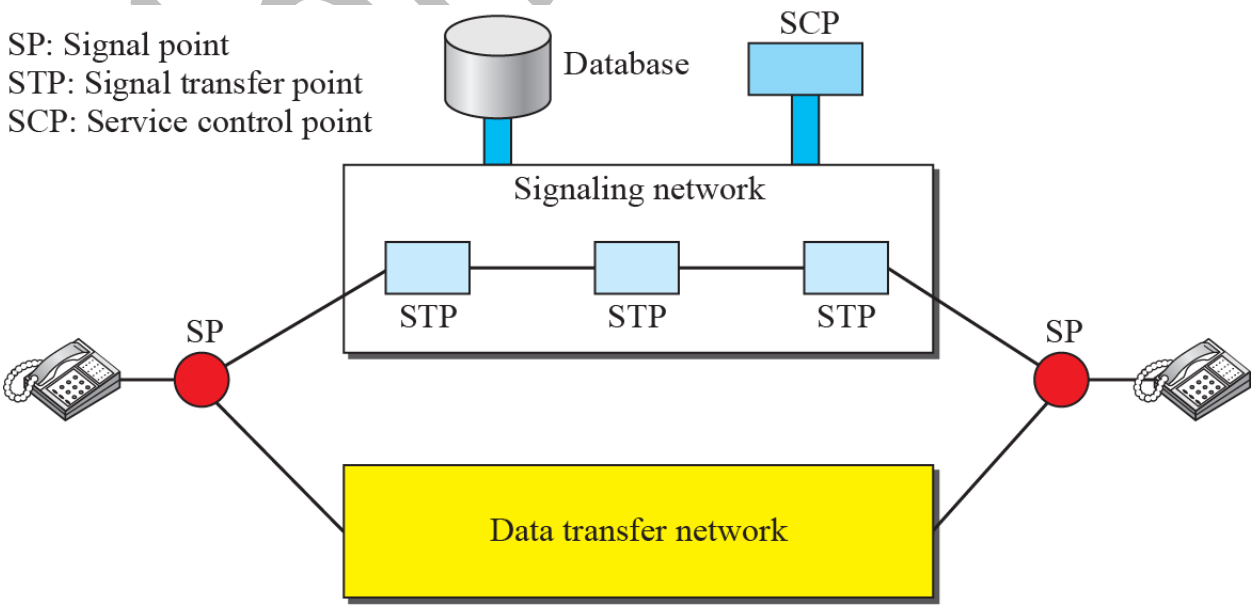
Points of Presence (POPs)



Signaling

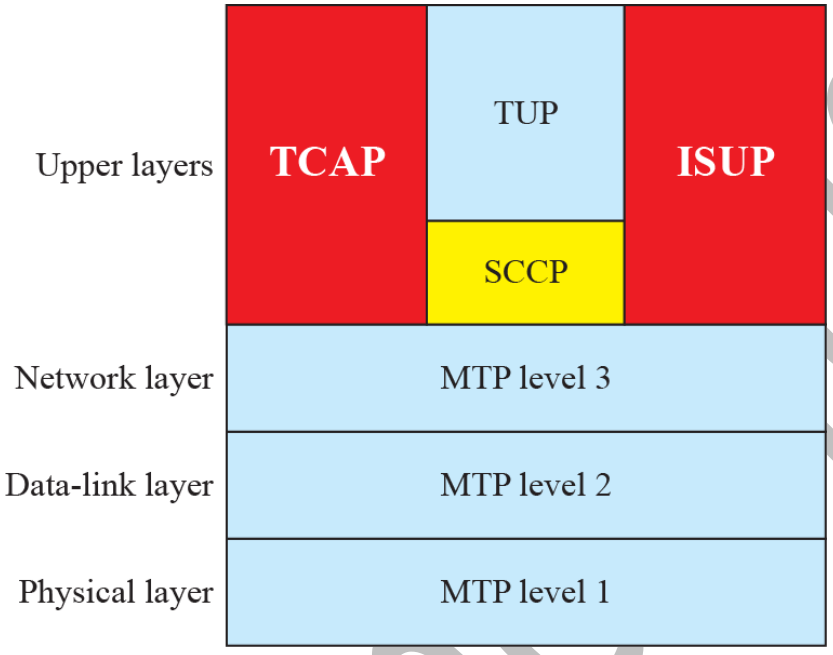
The telephone network in the beginning used a circuit-switched network with dedicated links to transfer voice communication. The operator connected the two parties by using a wire with two plugs inserted into the corresponding two jacks. Later, the signaling system became automatic. Rotary telephones were invented that sent a digital signal defining each digit in a multi-digit telephone number. As telephone networks evolved into a complex network, the functionality of the signaling system increased.

Data Transfer and Signaling Network



Layers in SS7

MTP: Message transfer part
SCCP: Signaling connection control point
TCAP: Transaction capabilities application port
TUP: Telephone user port
ISUP: ISDN user port



Services

Telephone companies provide two types of services:

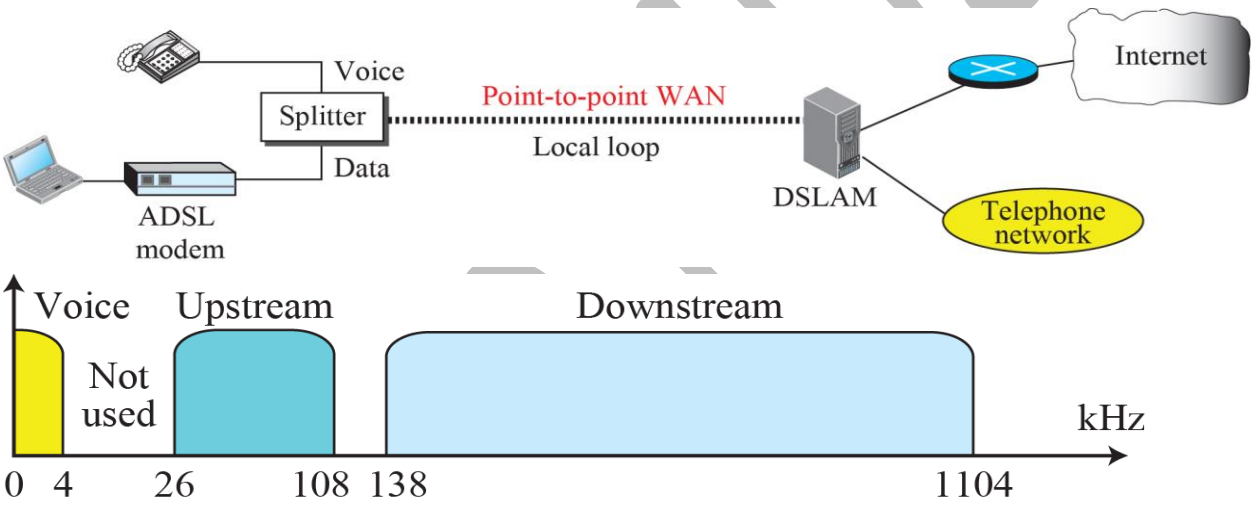
- **Analog Services**
  - **Analog Switched Services**
  - **Analog Leased Services**
- **Digital Services**
  - **Switched /56 Service**
  - **Digital Data Service**

Digital Subscriber Line (DSL)

After traditional dial-up modems reached their peak data rate, telephone companies developed another technology, DSL, to provide higher-speed access to the Internet. DSL supports high-speed digital communication over the existing telephone. DSL technology is a set of technologies, each differing in the first letter (ADSL, VDSL, HDSL, and SDSL).

ADSL Point-to-Point Network

A Point to Point Network is a private data connection securely connecting two or more locations for private data services. A point to point network is a closed network data transport service which does not traverse the public Internet and is inherently secure with no data encryption needed.

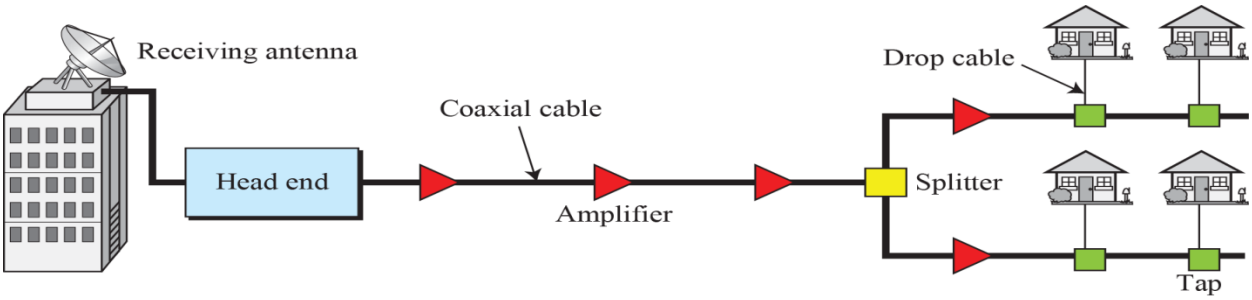


Cable Network

The Cable TV networks were initially created to provide remote subscribers access to TV programs. Cable networks enabled access to remote broadcasting stations via microwave connections. Cable TV also found a good ISP market by using some of the channels originally designed for video.

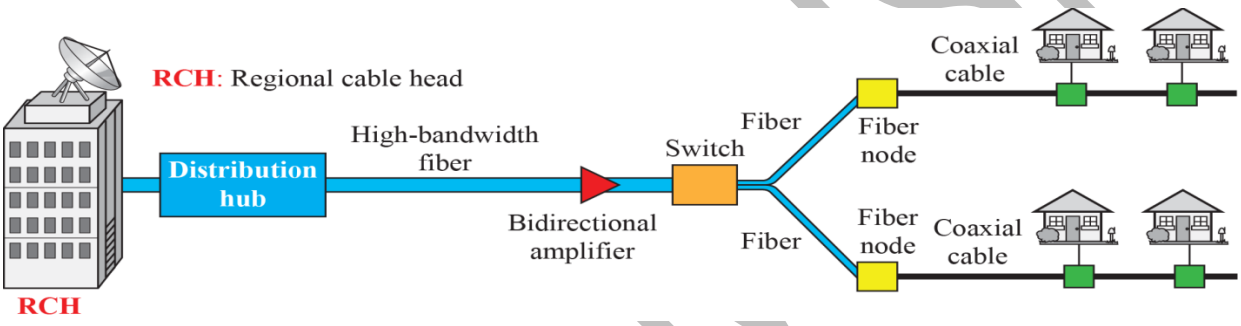
Traditional Cable Networks

Cable TV started to distribute broadcast video signals to locations with poor or no reception in the late 1940s it was called community antenna television (CATV) because an antenna at the top of a tall hill or building received the signals from the TV stations.



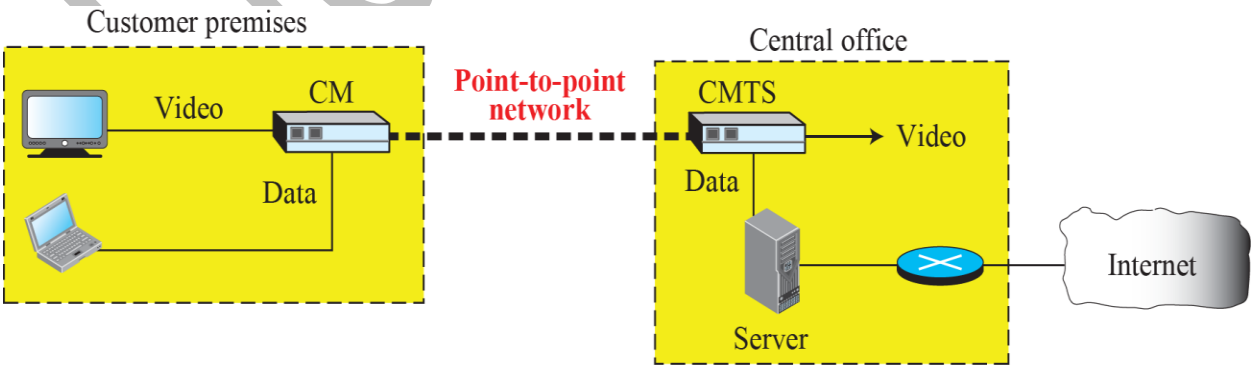
Hybrid Fiber Coaxial (HFC) Network

Second generation of cable network is called a Hybrid Fiber-Coaxial (HFC) network. The network uses a combination of fiber-optic and coaxial cable.



Cable TV for Data Transfer

Cable companies are now competing with telephone companies for the residential customer who wants high-speed data transfer. DSL technology provides high-data-rate connections for residential subscribers over the local loop BUT UTP is susceptible to Inference. This imposes an upper limit on the data rate. A solution is the use of the cable TV network.



Synchronous Optical Network (SONET)

A wide area network (WAN) that is used as a transport network to carry loads from other WANs. ITU–T standard called Synchronous Digital Hierarchy (SDH) .Architecture of a SONET system consists of signals, devices, and connections.

SONET Architecture

- Signals
  - Synchronous Transport Signals (STS)
  - Optical Carriers (OCs)
  - Synchronous Transport Module (STM)
- SONET Devcies
  - STS Mux/Demux
  - Regenerators
  - Add-Drop Multiplexer and Terminals
- Connections
  - Section
  - Line
  - Path

STS	*OC*	*Rate (Mbps)*	*STM*
STS-1	OC-1	51.840	
STS-3	OC-3	155.520	STM-1
STS-9	OC-9	466.560	STM-3
STS-12	OC-12	622.080	STM-4
STS-18	OC-18	933.120	STM-6
STS-24	OC-24	1244.160	STM-8
STS-36	OC-36	1866.230	STM-12
STS-48	OC-48	2488.320	STM-16
STS-96	OC-96	4976.640	STM-32
STS-192	OC-192	9953.280	STM-64

SONET Connections

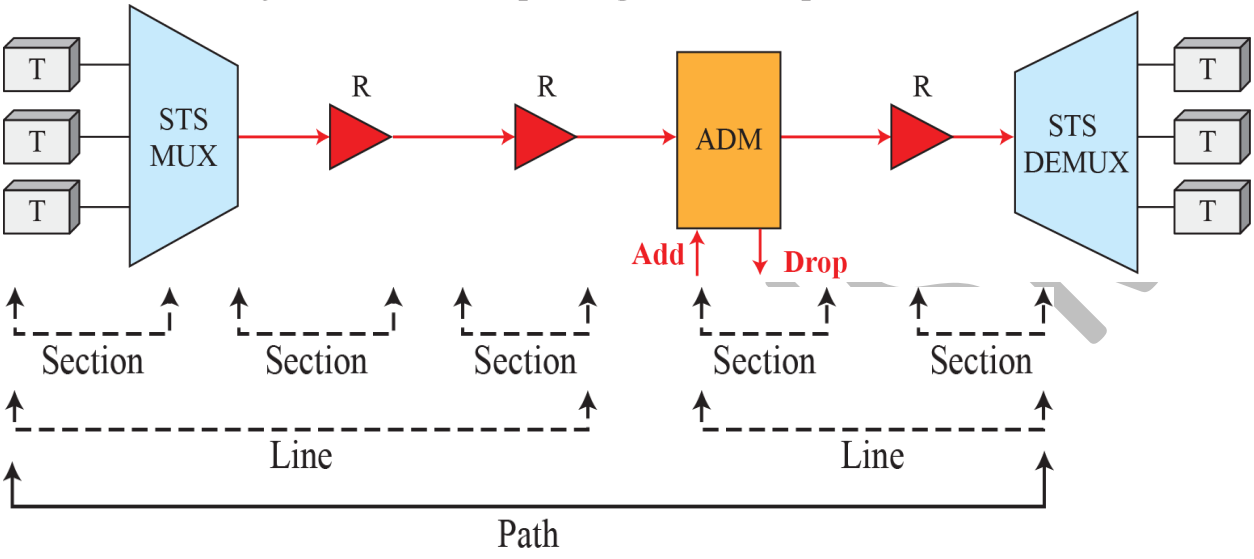
ADM: Add/drop multiplexer

R: Regenerator

STS MUX: Synchronous transport signal multiplexer

T: Terminal

STS DEMUX: Synchronous transport signal demultiplexer



SONET Layers

The SONET standard includes four functional layers:

- The Path Layer
- The Line Layer
- The Section Layer
- The Photonic Layer

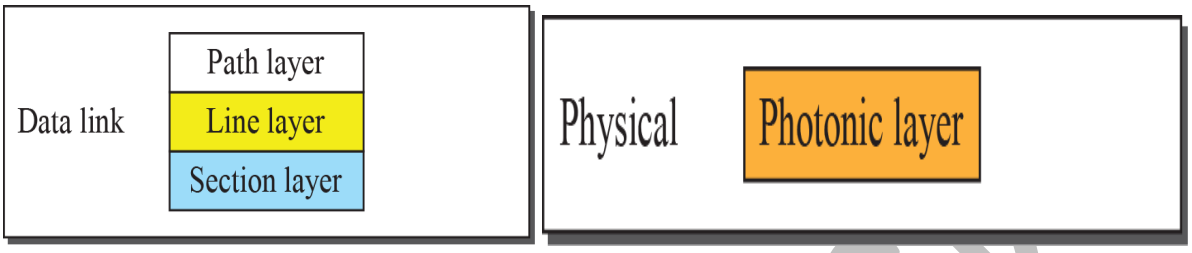
The layers correspond to both the physical and the data-link layers

Path Layer is responsible for the movement of a signal from source to the destination.

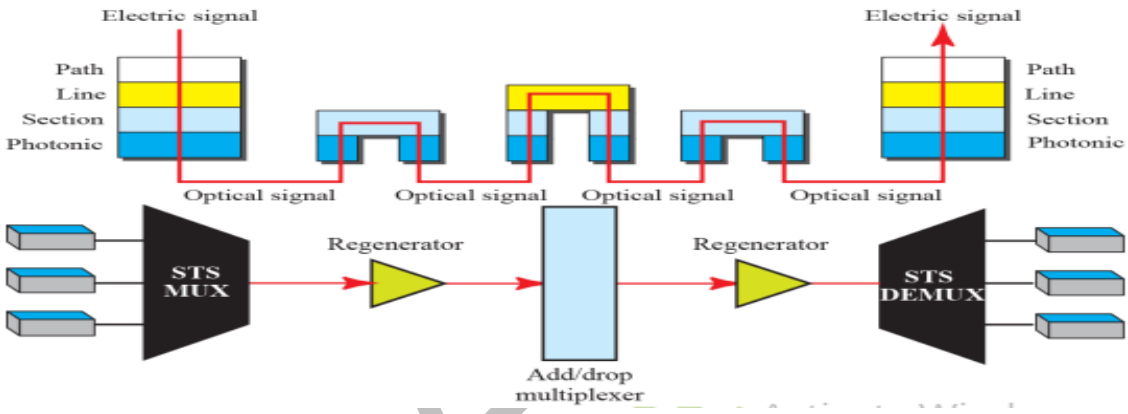
Link layer is a particular type of connection it is responsible for the movement of the signal across a physical line.

Section layer is responsible for the movement of the same signal across the physical section.

Photonic layer is equivalent to physical layer of OSI model. In this case use and encoding in an encoding her presence of light is represent 1 in binary and absence of light is a represent 0.



Device-Layer Relationship in SONET47



SONET Frames

Each synchronous transport signal STS-n is composed of 8000 frames. Each frame is a two-dimensional matrix of bytes with 9 rows by 90×n columns. STS-1 frame is 9 rows by 90 columns (810 bytes), and an STS-3 is 9 rows by 270 columns (2430 bytes).

STS Multiplexing

In SONET, frames of lower rate can be synchronously time-division multiplexed into a higher-rate frame

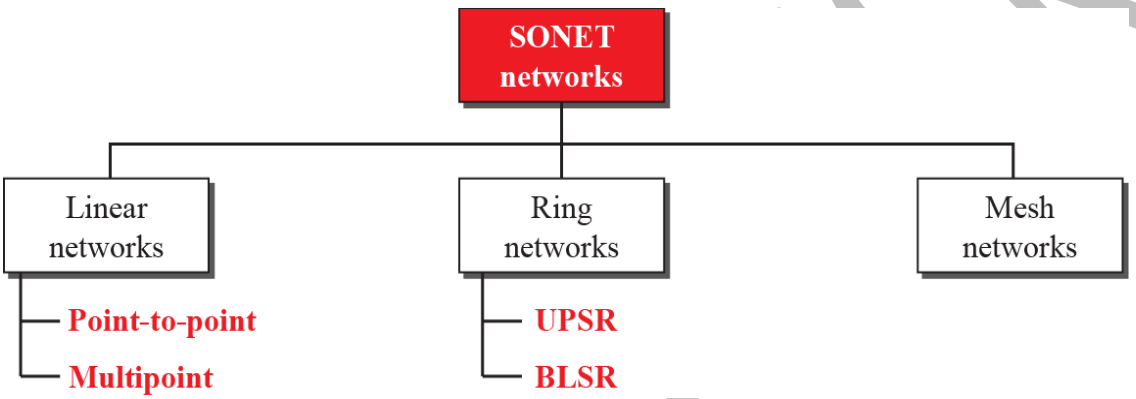
For example, three STS-1 signals (channels) can be combined into one STS-3 signal (channel), four STS-3s can be multiplexed into one STS-12, and so on

SONET Networks

SONET network can be used as a high-speed backbone carrying loads from other networks such as ATM or IP. We can roughly divide SONET networks into three categories:

- ✓ Linear Networks
- ✓ Ring Networks
- ✓ Mesh networks

Taxonomy of SONET Networks



ATM Short

Asynchronous Transfer Mode (ATM) is a switched wide area network based on the cell relay protocol designed by the ATM forum. The combination of ATM and SONET will allow high-speed interconnection of networks.

Problems

Some of the problems associated with existing systems are:

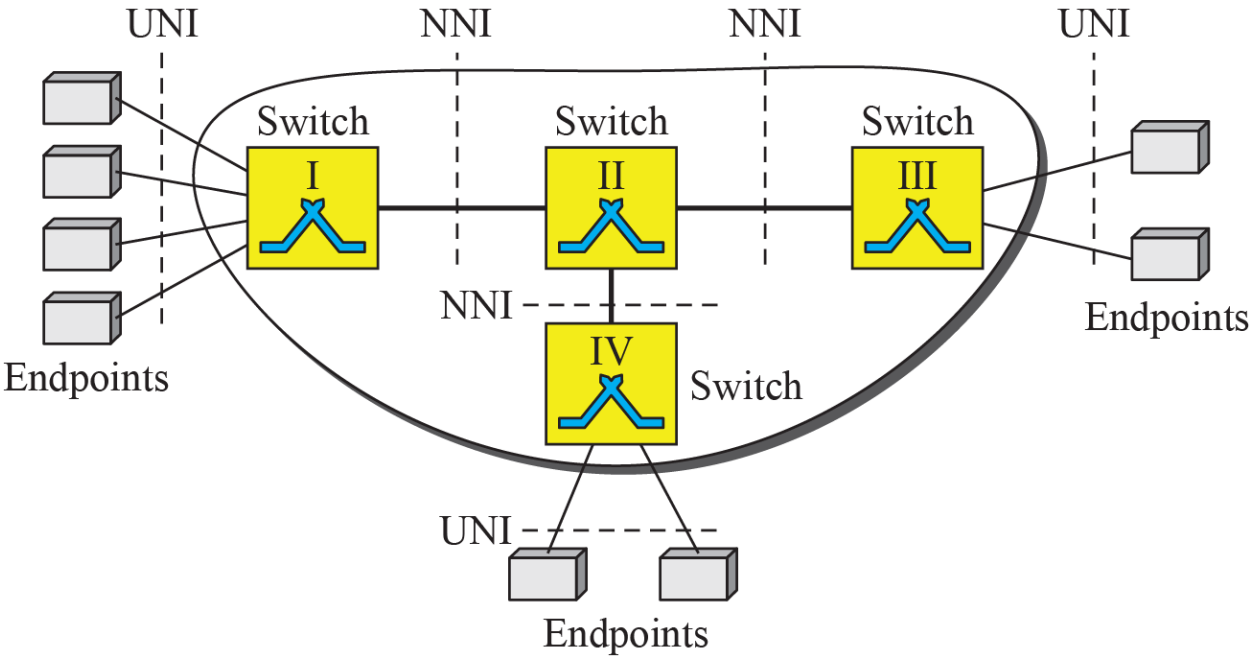
- Frame Networks
- Mixed Network Traffic

Solution

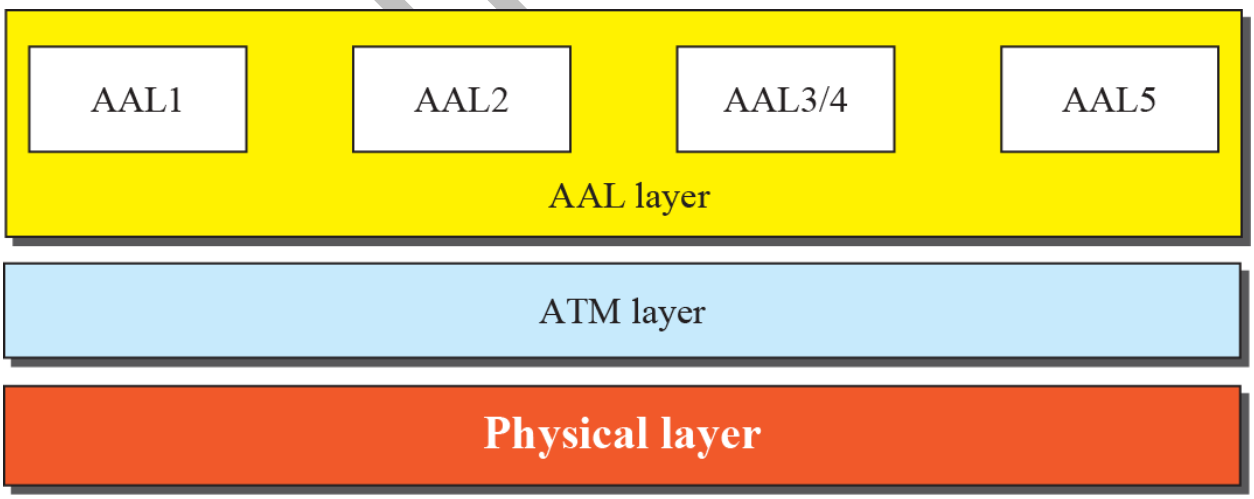
- Cell Networks
- Asynchronous TDM

Architecture

ATM is a cell-switched network. The user access devices, called the endpoints, are connected through a user-to-network interface (UNI) to the switches inside the network. The switches are connected through network-to-network interfaces (NNIs).



ATM Layers



Chap 15

Wireless communication LONG

Wireless communication is one of the fastest-growing technologies. The demand for connecting devices without the use of cables is increasing everywhere. Wireless LANs can be found on college campuses, in office buildings, and in many public areas.

Architectural Comparison

Architecture comparison of wired and wireless LANs

- Medium
- Hosts
- Isolated LANs
- Connection to other Networks
- Moving between Environments

Characteristics of a Wireless LAN

Several characteristics of wireless LANs either do not apply to wired LANs or the existence of these is negligible and can be ignored

- Attenuation
- Interference
- Multipath Propagation
- Error

Access Control

Most important issue in a wireless LAN is how a wireless host can get access to the shared medium (air). CSMA/CD does not work in wireless LANs for three reasons:

1. Wireless hosts don't have power to send and receive at the same time

2. The hidden station problem prevents collision detection
3. The distance between stations can be large

IEEE 802.11 PROJECT

IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data-link layers. It is sometimes called Wireless Ethernet. The term WiFi (short for wireless fidelity) as a synonym for wireless LAN (certified by WiFi alliance).

Architecture

The standard defines two kinds of services:

- The basic service set (BSS
- The Extended service set (ESS)

The basic service set (BSS)
Basic Service Set (BSS), as the name suggests, is basically a network topology that allows all wireless devices to communicate with each other through a common medium i.e. AP (Access point). It also manages these wireless devices or clients.

The Extended service set (ESS)

An extended service set (ESS) is one or more interconnected basic service sets (BSSs) and their associated LANs. Each BSS consists of a single access point (AP) together with all wireless client devices (stations, also called STAs) creating a local or enterprise 802.11 wireless LAN (WLAN).

Types of Stations

There are three Types of Stations.

- No-Transition Mobility
- BSS-Transition Mobility
- ESS-Transition Mobility

MAC Sub-layer

IEEE 802.11 defines two MAC sub-layers:

- The Distributed Coordination Function (DCF)
- The Point Coordination Function (PCF)

MAC Sub-layer

IEEE 802.11 defines two MAC sub-layers:

- The Distributed Coordination Function (DCF) ; and
- The Point Coordination Function (PCF)

Subfields in FC field

Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 6.2)
To DS	Defined later
From DS	Defined later
More flag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

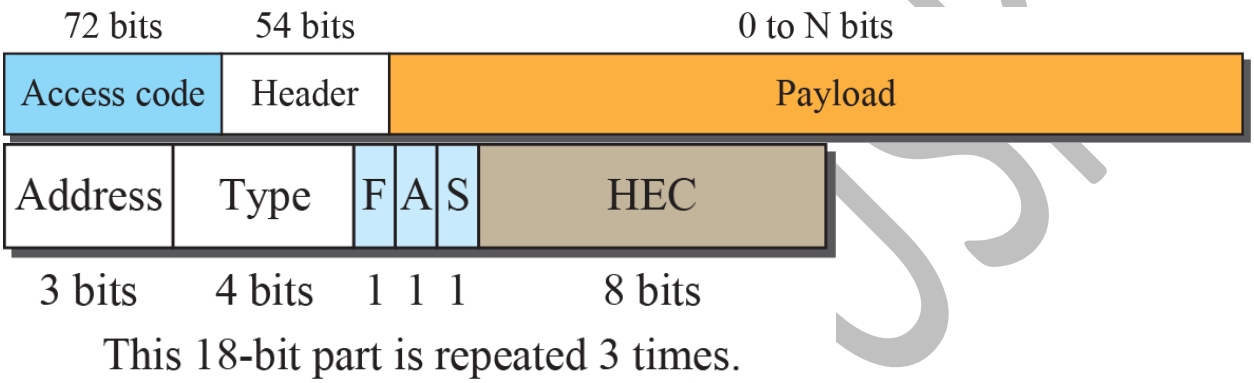
Frame Types

- Management Frames
- Control Frames
- Data Frames

Values of Subfields in Control Frames

Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

Frame Format Types



Physical Layer

All physical implementations, except the infrared, operate in the industrial, scientific, and medical (ISM) band, which defines 3 unlicensed bands in 3 ranges:

- 902–928 MHz
- 2.400–4.835 GHz
- 5.725–5.850 GHz

Specifications

IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.400–4.835 GHz	FSK	1 and 2
	DSSS	2.400–4.835 GHz	PSK	1 and 2
	None	Infrared	PPM	1 and 2
802.11a	OFDM	5.725–5.850 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.400–4.835 GHz	PSK	5.5 and 11
802.11g	OFDM	2.400–4.835 GHz	Different	22 and 54
802.11n	OFDM	5.725–5.850 GHz	Different	600

BLUETOOTH LONG/Short

Bluetooth is a wireless LAN technology designed to connect devices of different functions when they are at a short distance from each other. A Bluetooth LAN is an ad hoc network. The devices, sometimes called gadgets, find each other and make a network called a Pico net.

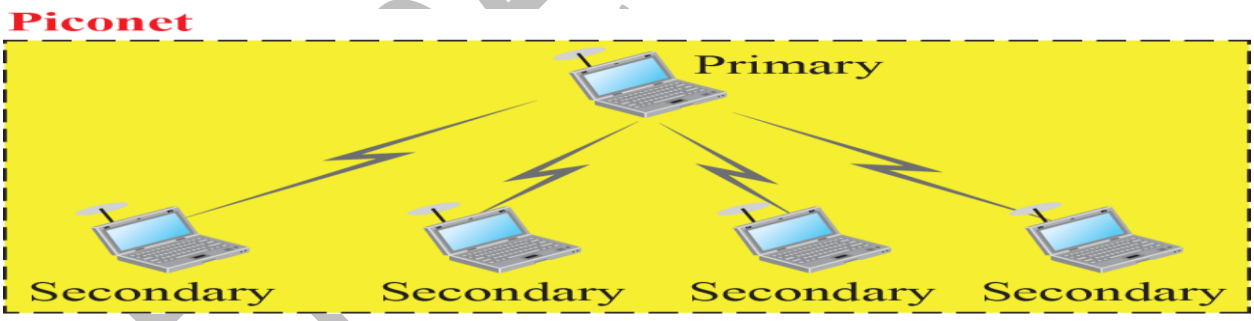
Architecture

Bluetooth defines two types of networks:

- Piconet
- Scatternet

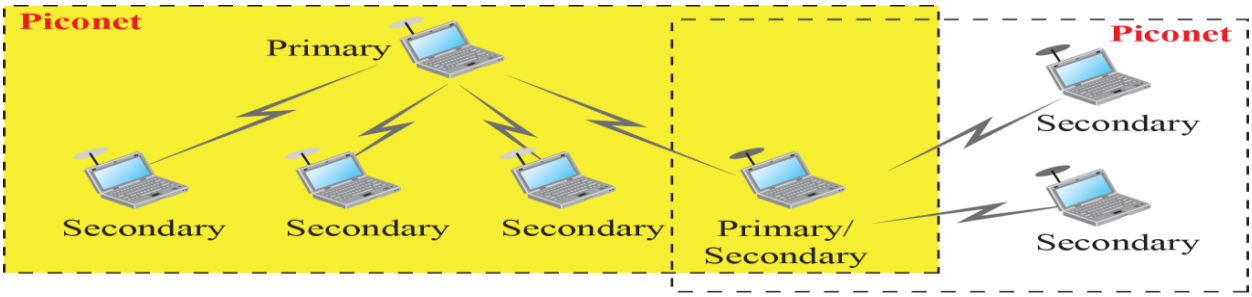
Piconet

Piconets have a 7 member address space (3 bits, with zero reserved for broadcast), which limits the maximum size of a piconet to 8 devices, 1 master and 7 slaves. A piconet is a network of devices connected using Bluetooth technology. The network ranges from two to eight connected devices. When a network is established, one device takes the role of the master while all the other devices act as slaves. Piconet gets its name from the word "pico", which means very small.



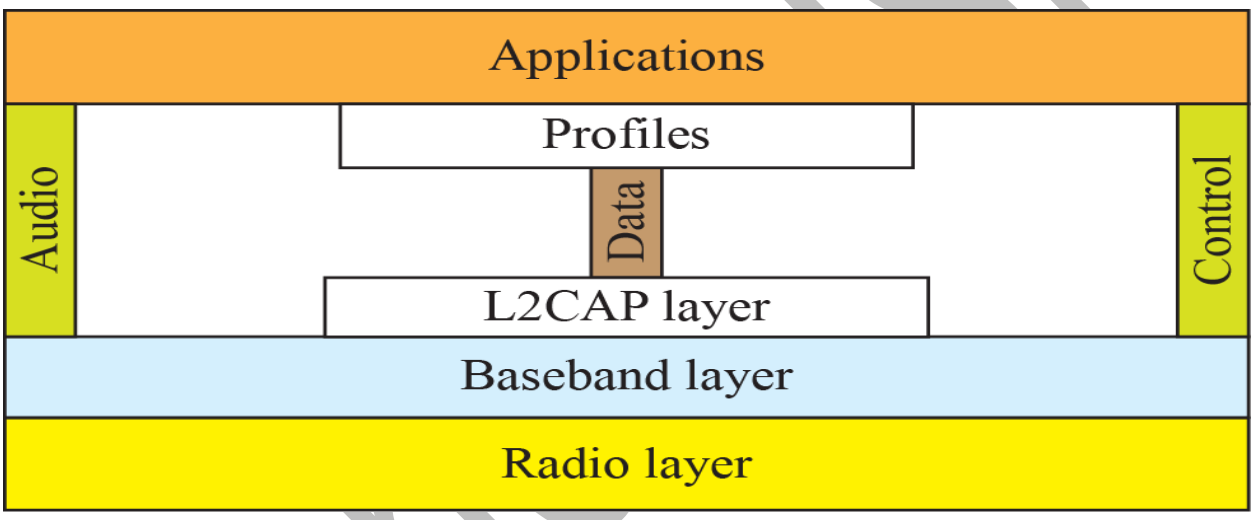
Scatternet

A scatternet is a number of interconnected piconets that supports communication between more than 8 devices. Scatternets are formed when a device in a piconet, whether a master or a slave, decides to participate as a slave to the master of another piconet. This device then becomes the bridge between the two piconets, connecting both networks



Bluetooth Layers

Bluetooth uses several layers that do not exactly match those of the Internet model we have defined in this book.



Chap 16

Connecting Devices LONG

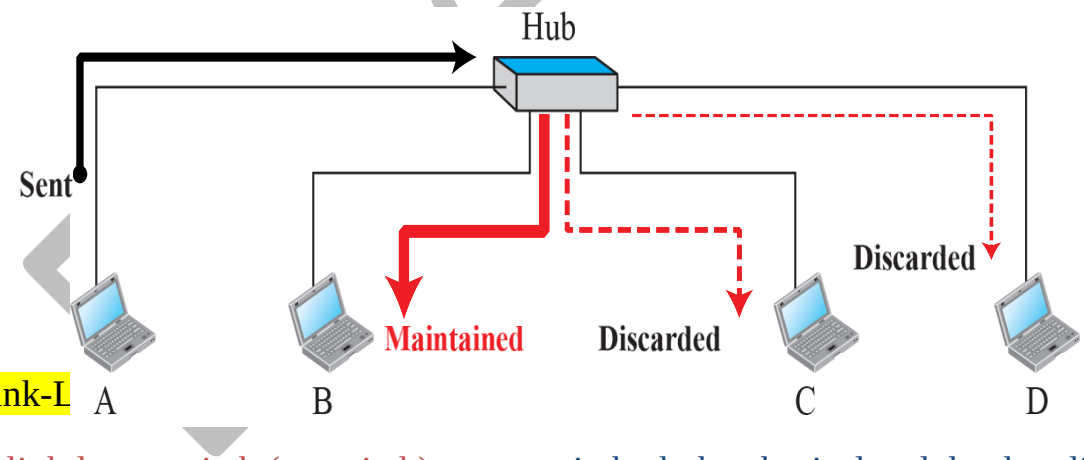
Hosts and networks do not normally operate in isolation. Connecting devices connect hosts together to make a network or connect networks together to make an internet. Connecting devices can operate in different layers of the Internet model.

Three kinds of connecting devices: Three Categories of Connecting Devices

- Hubs
- Link-layer switches
- Routers

Hubs

Hub is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation impacts the data. A hub (repeater) receives a signal and, before it becomes too weak or corrupted, regenerates it. Hub is a device that operates only in the physical layer.



Link-L

A link-layer switch (or switch) operates in both the physical and the data-link layers. As a physical-layer device, it regenerates the signal it receives. As a link-layer device, the link-layer switch can check the MAC addresses (source and destination) contained in the frame.

Switch versus Hub

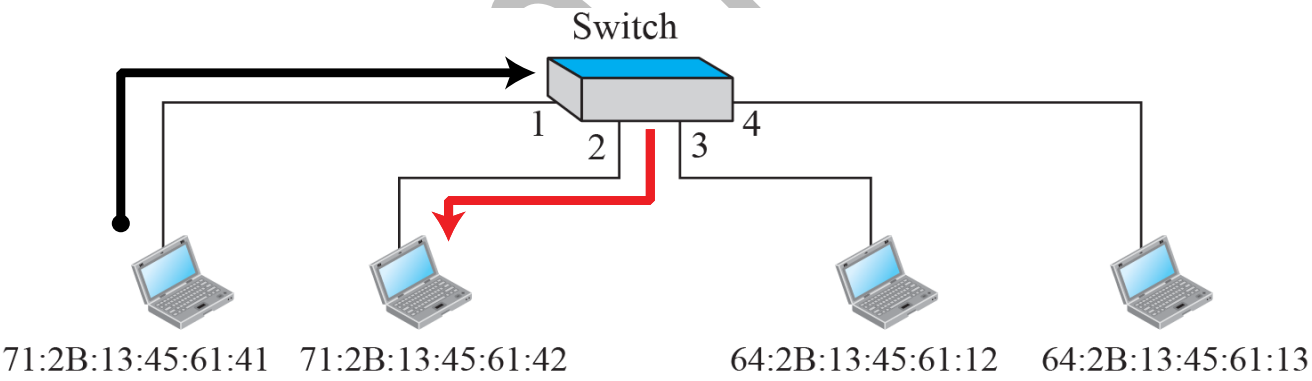
Switch has the 'Filtering' capability. Unlike hub, a switch can check the destination address of a frame and decide on outgoing port. Switch eliminates collisions and does not require carrier sensing. Switches connect heterogeneous devices.

Link-Layer Switch

A link-layer switch (or switch) operates in both the physical and the data-link layers. A network switch is a device that operates at the Data Link layer of the OSI model Layer 2. It takes in packets being sent by devices that are connected to its physical ports and sends them out again, but only through the ports that lead to the devices the packets are intended to reach.

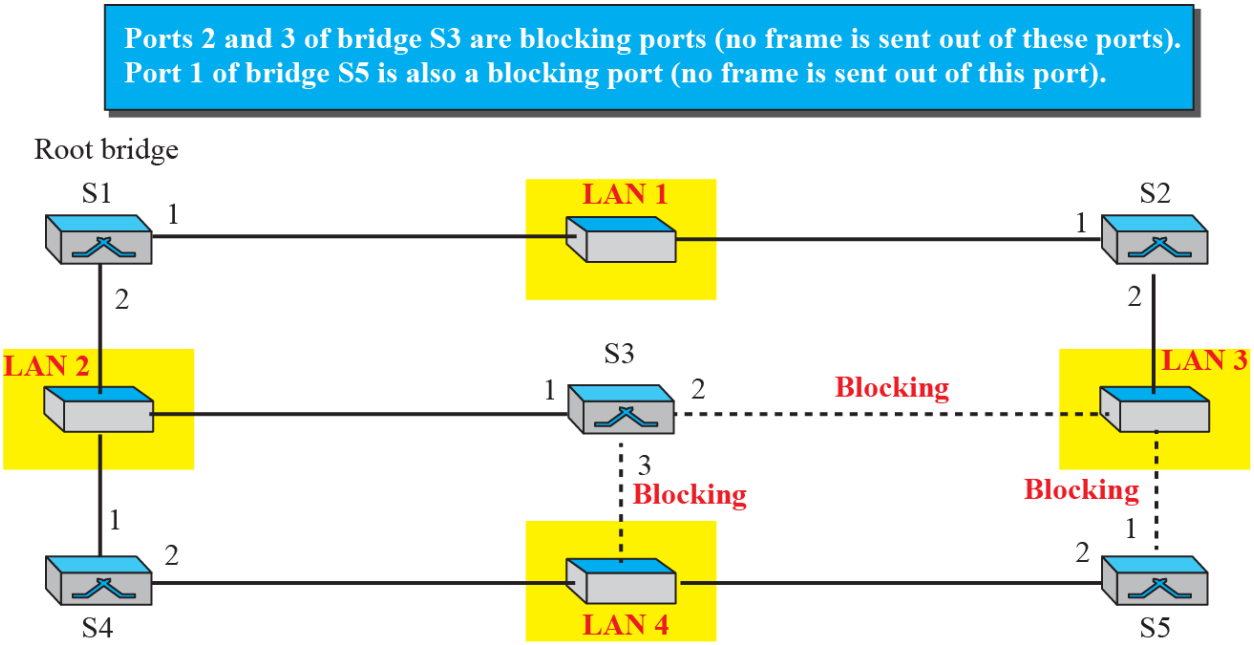
Switching table

Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3
64:2B:13:45:61:13	4



Spanning Tree Algorithm

- In graph theory, Spanning Tree is a graph in which there is no loop
- In a switched LAN, this means creating a topology in which each LAN can be reached from any other LAN through one path only (no loop)
- To find the spanning tree, we assign a cost (metric) to each LAN link



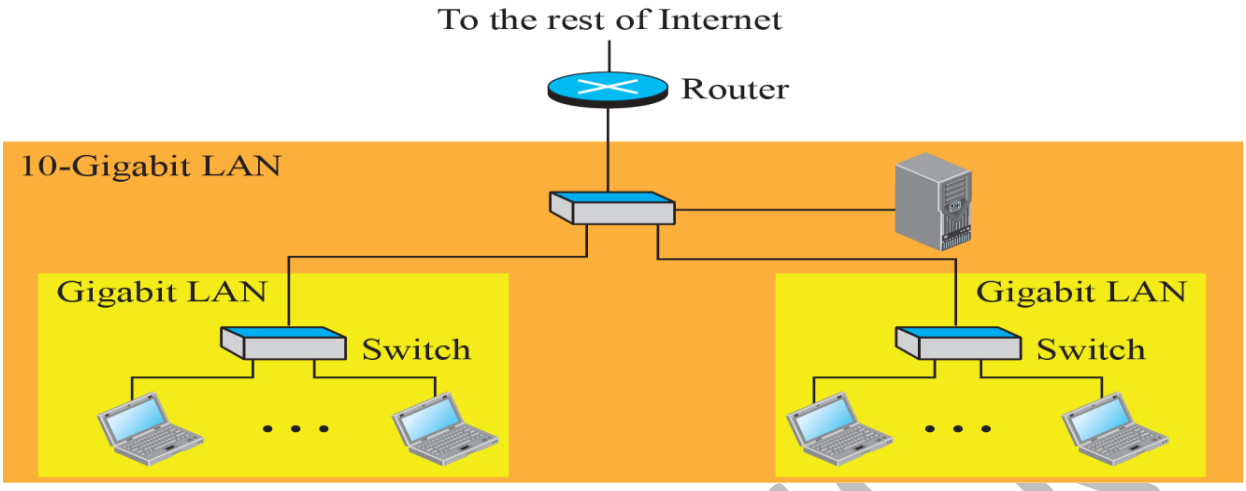
Routers

We compare routers to two-layer switch and a hub. A router is a three-layer device; it operates in the physical, data-link, and network layers.

Router vs. Switch Short

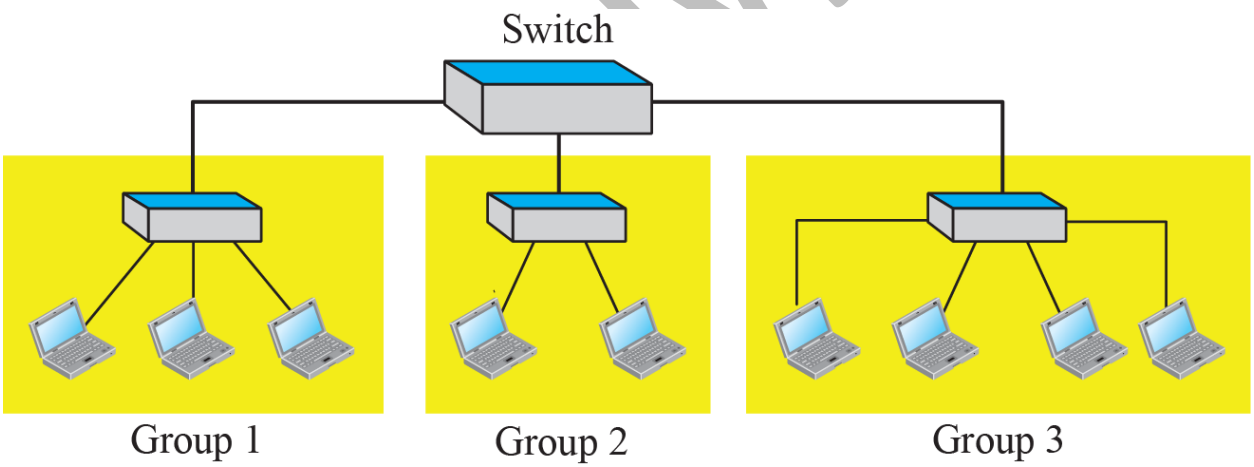
Three differences between a router and a repeater or a switch:

1. A router has a physical and logical (IP) address for each of its interfaces.
2. A router acts only on those packets in which the link-layer destination address matches the address of the interface at which the packet arrives.
3. A router changes the link-layer address of the packet (both source and destination) when it forwards the packet.



VIRTUAL LANS (VLAN) LONG

A VLAN is a LAN configured by software, not by physical wiring. A station is considered part of a LAN if it physically belongs to that LAN i.e. The criterion of membership is geographic. Provides a virtual connection between two stations belonging to two different physical LANs.



Membership of a VLAN

What characteristic can be used to group stations in a VLAN?

Vendors use different characteristics such as interface numbers, port numbers, MAC addresses, IP addresses, IP multicast addresses, or a combination of two or more of these.

Configuration of a VLAN

How are the stations grouped into different VLANs?

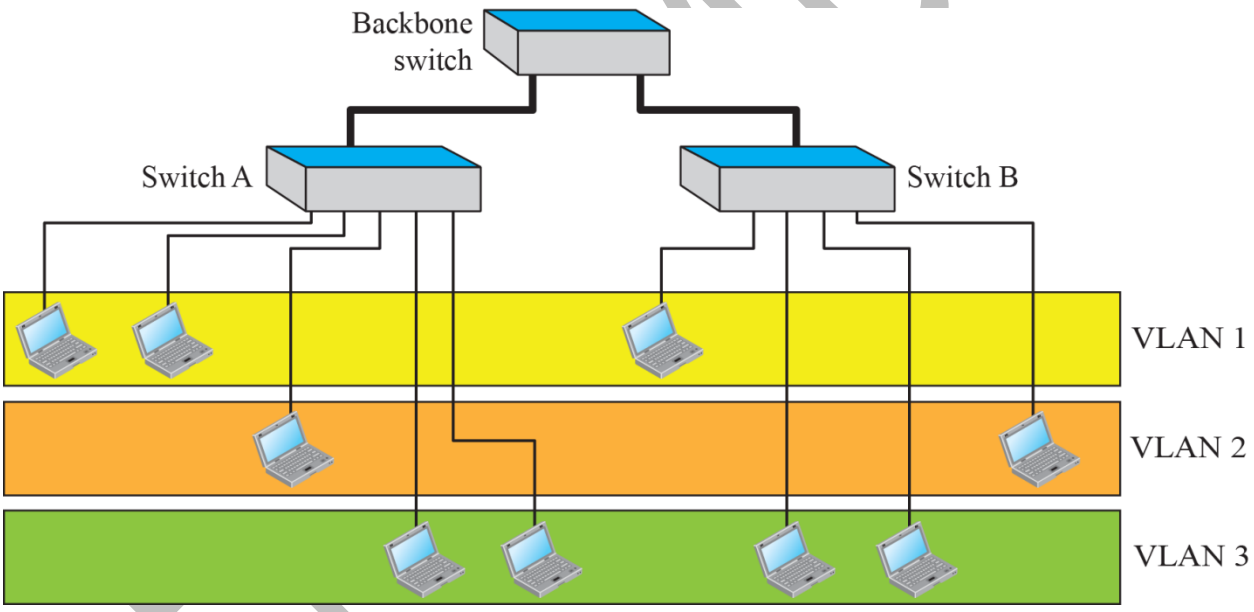
Stations are configured in one of three ways:

- Manually
- Semi-Automatically
- Automatically

Communication between Switches

In a multi-switched backbone, each switch must know:

- Which station belongs to which VLAN; and
- The membership of stations connected to other switches



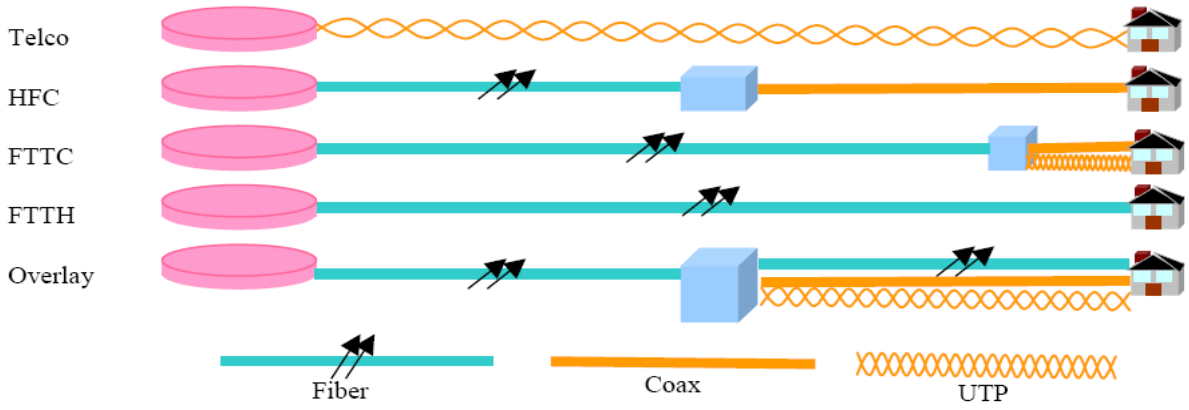
Switch A must know the membership status of stations connected to switch B, and switch B must know the same about switch A. Three methods have been devised for this purpose: table maintenance, frame tagging, and time-division multiplexing.

Advantages of using VLANs

- Cost and Time Reduction
- Creating virtual Workgroups
- Security

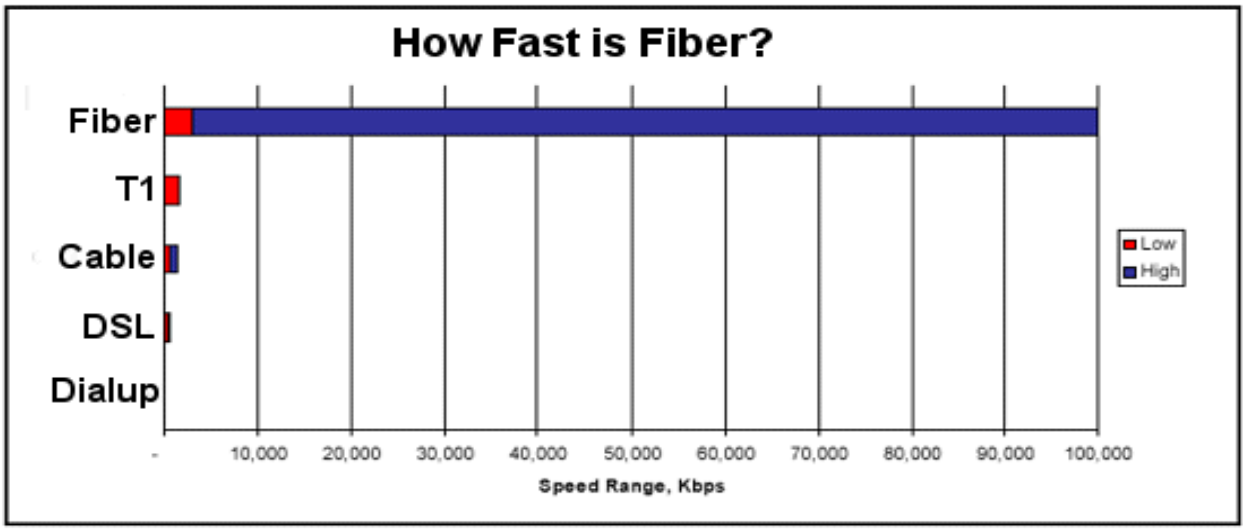
Comparison of Modern Access Technologies

- Telco
- HFC
- FTTx



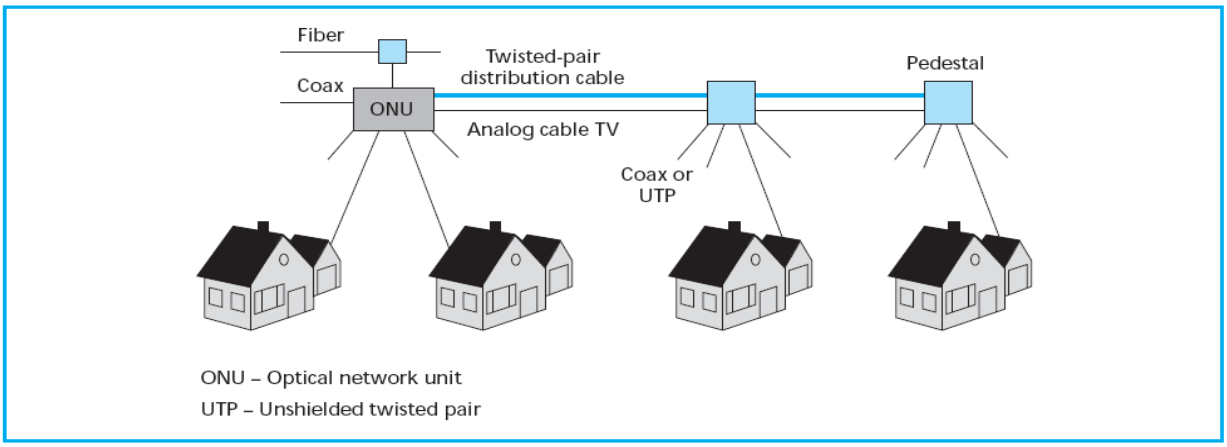
Fiber – The Medium of the Future!

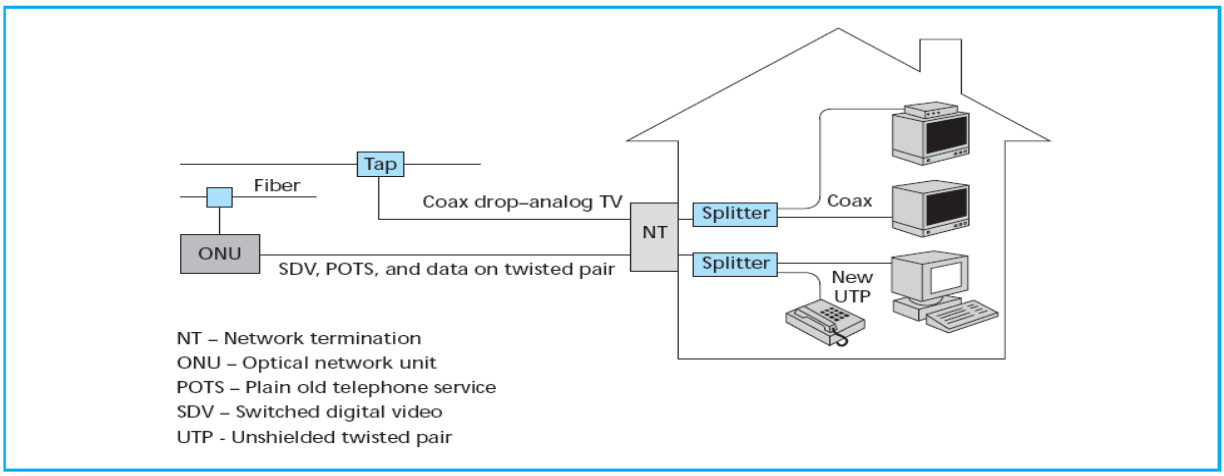
LONG AND SHORT



Fiber To The Curb (FTTC)

An access network in which fiber is used for part, but not the entire link from the provider to the end-use an optical to electrical (O/E) conversion takes place somewhere near the end-user. The terminal network segment of a FTTC network is usually twisted pair or coaxial cable. The final optical receiver in a FTTC network typically serves several customers





Fiber To The Home (FTTH)

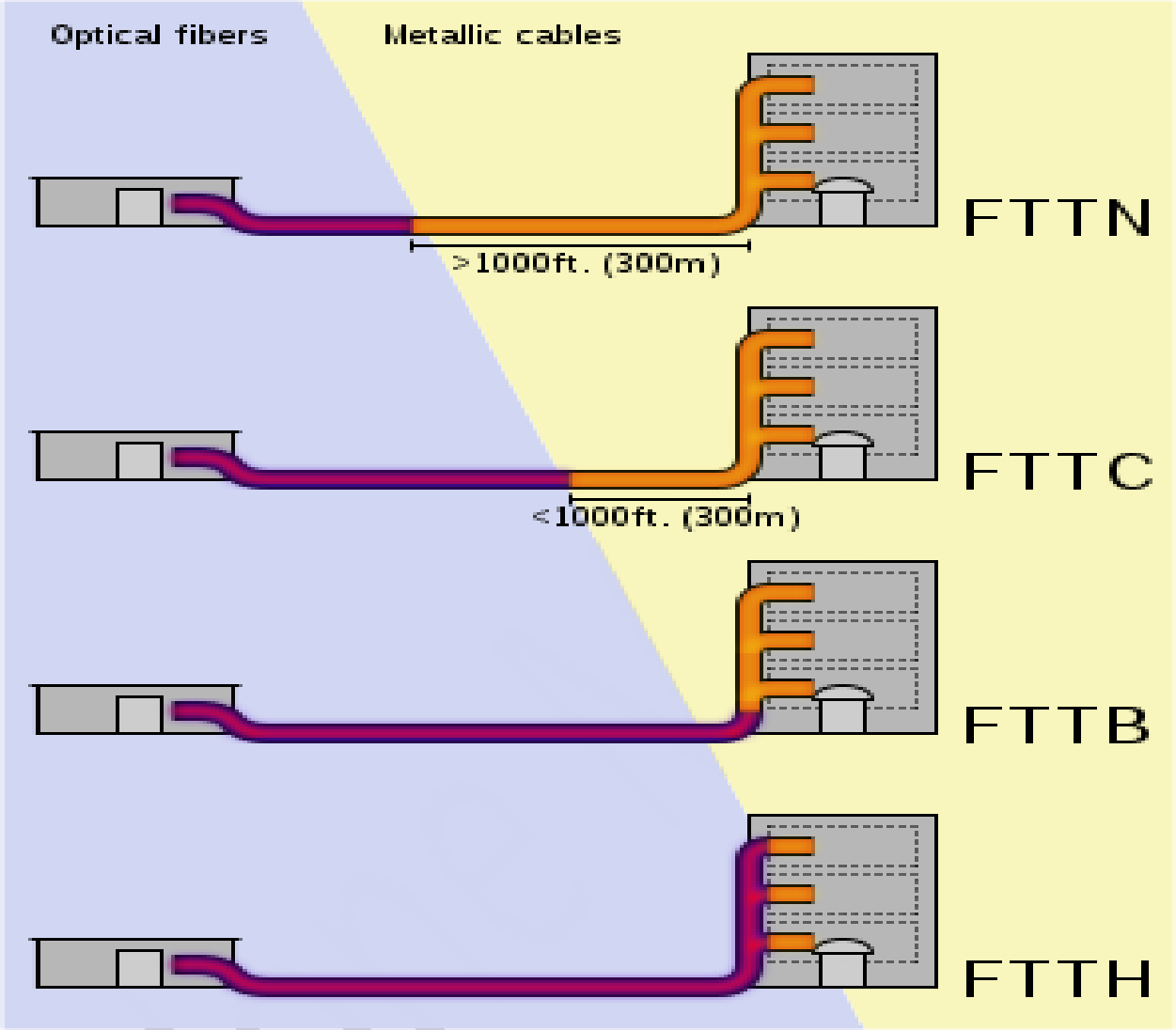
Need: High-speed data, reliable voice and high-quality video

Problems:

- ✓ How to get high speed lines out to each customer?
- ✓ How to future-proof the architecture?

Solution: FTTH

Fiber-to-the-home (FTTH) is the installation of optical fiber from a telephone switch directly into the subscriber's home. It is one of the latest access technologies. FTTH is also referred to as Fiber-to-the-Building (FTTB)


Optical fibers
Metallic cables
>1000ft. (300m)
<1000ft. (300m)
FTTN
FTTC
FTTB
FTTH

FOR SHORT NOTES

https://vuonlinehelp.blogspot.com/p/notes.html

OVER YOUTUBE CANNEL

https://www.youtube.com/results?search_query=orange+monkey+team

CS601 YOUTUBE FINAL TERM SHORT VIDEO

https://www.youtube.com/watch?v=jgkoimzkpw4 TIME 46:07

MORE