UNIT - I

Learning Objectives

- Overview of Computer Network
- Discuss OSI Model - Seven- Layer architecture
- TCP/IP suite of protocol
- Mac protocol
- FDDI, DQDB, HIPPI
- Gigabit Ethernet, Wireless Ethernet
- Fast access technologies
- ADSL, Cable Modem
- Wi Fi
- Wimax.

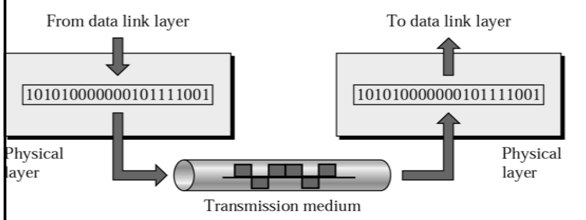
OSI Model

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data link
1	Physical

Physical Layer

The physical layer is responsible for transmitting individual bits from one node to the next.



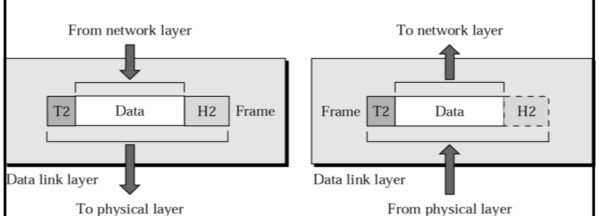
Physical Layer

Responsibilities of Physical Layer :-

- Physical Characteristics of interfaces and medium
- Representation of bits
- Data rate
- Synchronization of bits
- Line configuration
- Physical topology
- Transmission mode

Data Link Layer

The data link layer is responsible for transmitting frames from one node to the next.



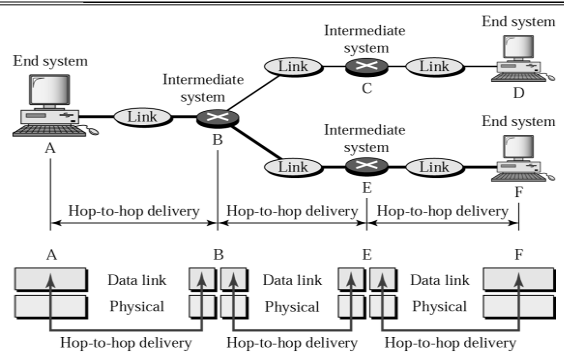
Data Link Layer

Responsibilities of Data Link Layer :-

- Framing
- Physical Addressing
- Flow Control
- Error Control
- Access Control

 U1.7

Node to Node Delivery



 U1.8

Node to Node Delivery

Example

In Figure, a node with physical address 10 sends a frame to a node with physical address 87.

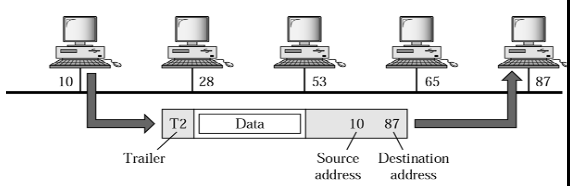
The two nodes are connected by a link. At the data link level this frame contains physical addresses in the header. These are the only addresses needed.

The rest of the header contains other information needed at this level. The trailer usually contains extra bits needed for error detection

 U1.9

Node to Node Delivery

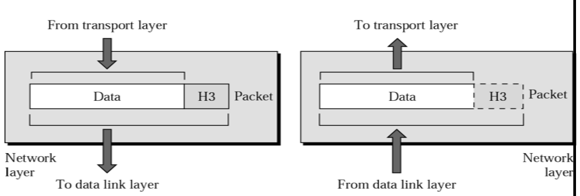
Example



© Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi-63 by Vishal Jain U1.10

Network Layer

The network layer is responsible for the delivery of packets from the original source to the final destination.



© Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi-63 by Vishal Jain U1.11

Network Layer

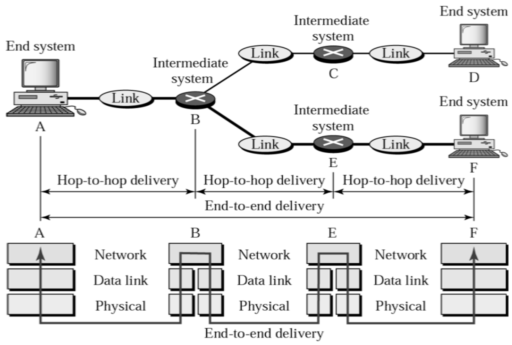
Responsibilities of Network Layer :-

•Logical Addressing

•Routing

© Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi-63 by Vishal Jain U1.12

Source to Destination



Source to Destination

Example

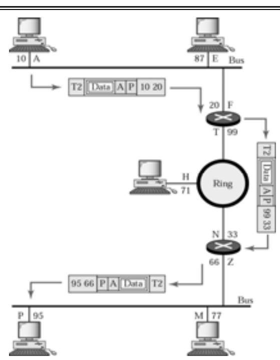
In Figure, we want to send data from a node with network address A and physical address 10, located on one LAN, to a node with a network address P and physical address 95, located on another LAN.

Because the two devices are located on different networks, we cannot use physical addresses only; the physical addresses only have local jurisdiction.

What we need here are universal addresses that can pass through the LAN boundaries. The network (logical) addresses have this characteristic.

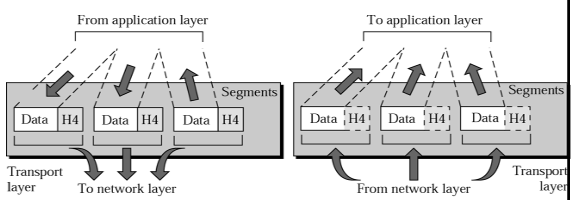
Source to Destination

Example



Transport Layer

The transport layer is responsible for delivery of a message from one process to another.



 U1.16

Transport Layer

Responsibilities of Transport Layer :-

•Service-point addressing

•Segmentation and reassembly

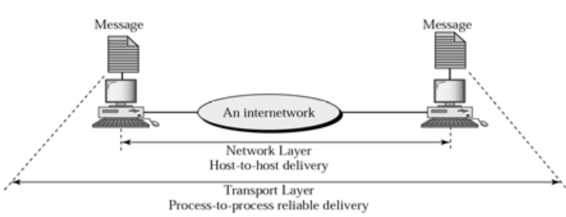
•Connection control

•Flow control

•Error Control

 U1.17

Process to Process



 U1.18

Process to Process

Example

Figure, shows an example of transport layer communication.

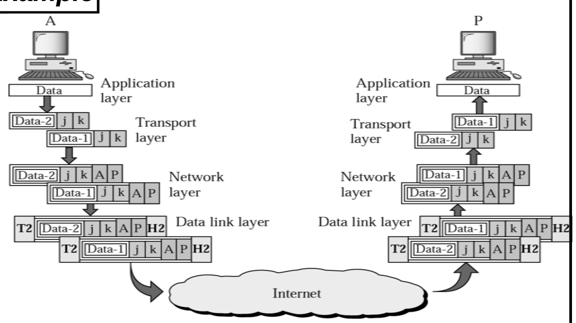
Data coming from the upper layers have port addresses j and k (j is the address of the sending process, and k is the address of the receiving process).

Since the data size is larger than the network layer can handle, the data are split into two packets, each packet retaining the port addresses (j and k). Then in the network layer, network addresses (A and P) are added to each packet.

 U1.19

Process to Process

Example



 U1.20

Session Layer

The session layer is responsible for dialog control and synchronization.

 U1.21

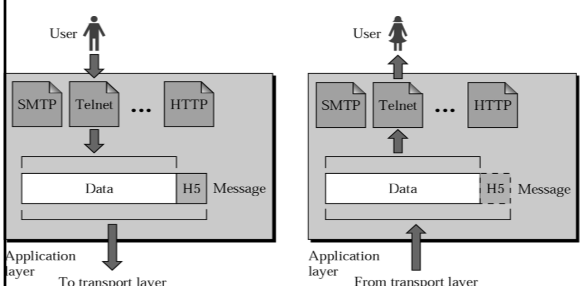
Presentation Layer

The presentation layer is responsible for translation, compression, and encryption.

 U1.22

Application Layer

The application layer is responsible for providing services to the user.



 U1.23

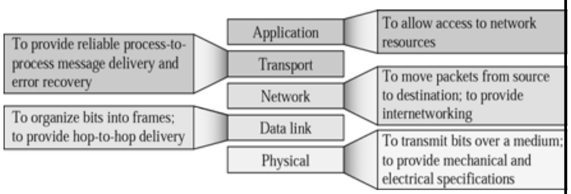
Application Layer

Services provided by the Application Layer :-

- •Network virtual terminal
- •File transfer, access and management
- •Mail services
- •Directory services

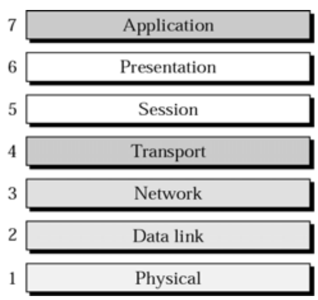
 U1.24

Summary of Layers



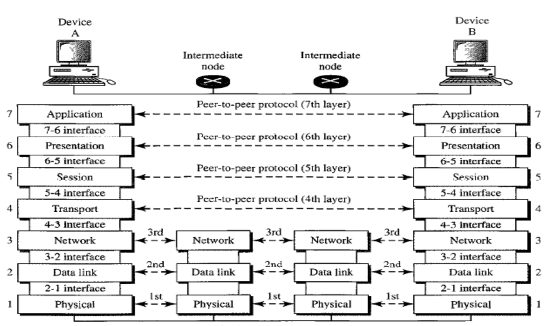
 U1.25

OSI Model



 U1.26

OSI Model



 U1.27

OSI Model

Physical layer	Deals with the mechanical and electrical specification of the interface and transmission media.
Data Link Layer	Transforms the physical layer, to a reliable link and is responsible for node-to-node delivery.
Network Layer	Responsible for the source-to-destination delivery of a packet across multiple links.

 U1.28

OSI Model

Transport Layer	Responsible for the source-to-destination (end-to-end) delivery of the entire message.
Session Layer	It establishes, maintains and synchronizes the interaction between communicating systems.
Presentation Layer	It concerns with the syntax and semantics of the information between two systems.

 U1.29

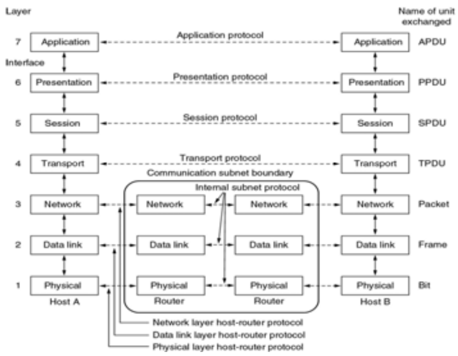
OSI Model

Application Layer	It provides user interfaces and support for services such as E-Mail, Remote Login and other types of Distributed Information Services.

 U1.30

Reference Models

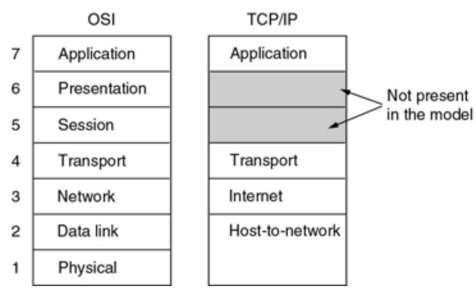
The OSI reference model.



 U1.31

Reference Models (2)

The TCP/IP reference model.



 U1.32

Medium Access Control

- A network of computers based on multi-access medium requires a protocol for effective sharing of the media.
- As only one node can send or transmit signal at a time using the broadcast mode, the main problem here is how different nodes get control of the medium to send data, that is "who goes next?".
- The protocols used for this purpose are known as Medium Access Control (MAC) techniques. The key issues involved here are - Where and How the control is exercised.

 U1.33

Medium Access Control

- 'Where' refers to whether the control is exercised in a centralized or distributed manner.
- In a centralized system a master node grants access of the medium to other nodes.
- A centralized scheme has a number of advantages as mentioned below:
  - Greater control to provide features like priority, overrides, and guaranteed bandwidth.
  - Simpler logic at each node.
  - Easy coordination

 U1.34

Medium Access Control

- Although this approach is easier to implement, it is vulnerable to the failure of the master node and reduces efficiency.
- On the other hand, in a distributed approach all the nodes collectively perform a medium access control function and dynamically decide which node to be granted access.
- This approach is more reliable than the former one.

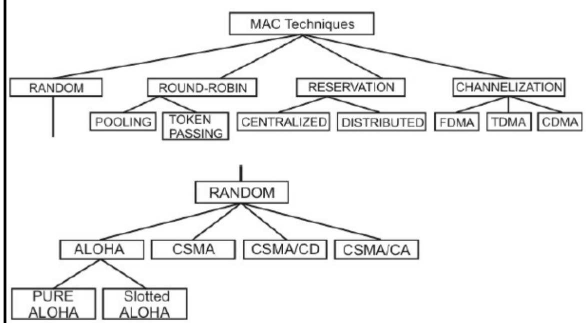
 U1.35

Medium Access Control

- 'How' refers to in what manner the control is exercised. It is constrained by the topology and trade off between cost-performance and complexity.
- Various approaches for medium access control are :

 U1.36

Medium Access Control



© Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi-63 by Vishal Jain U1.37

Medium Access Control

- The MAC techniques can be broadly divided into four categories;
- Contention-based,
- Round-Robin,
- Reservation-based and.
- Channelization-based.

- Under these four broad categories there are specific techniques, as shown in.

- We shall concentrate of the MACs of the first two categories, which have been used in the legacy LANs of the IEEE standard.

© Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi-63 by Vishal Jain U1.38

Medium Access Control

- The CSMA/CA, a collision-free protocol used in wireless LAN
- Channelization-based MACs, which are used in cellular telephone networks
- the reservation-based MACs, which are used in satellite networks .

© Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi-63 by Vishal Jain U1.39

Medium Access Control

- Medium Access Control techniques are designed with the following goals in mind :-
- **Initialization:** The technique enables network stations, upon power-up, to enter the state required for operation.
- **Fairness:** The technique should treat each station fairly in terms of the time it is made to wait until it gains entry to the network, access time and the time it is allowed to spend for transmission.
- **Priority:** In managing access and communications time, the technique should be able to give priority to some stations over other stations to facilitate different type of services needed.

Medium Access Control

- **Limitations to one station:** The techniques should allow transmission by one station at a time.
- **Receipt**: The technique should ensure that message packets are actually received (no lost packets) and delivered only once (no duplicate packets), and are received in the proper order.
- **Error Limitation:** The method should be capable of encompassing an appropriate error detection scheme.
- **Recovery**: If two packets collide (are present on the network at the same time), or if notice of a collision appears, the method should be able to recover, i.e. be able to halt all the transmissions and select one station to retransmit.

Medium Access Control

Round Robin Techniques

- In Round Robin techniques, each and every node is given the chance to send or transmit by rotation.
- When a node gets its turn to send, it may either decline to send, if it has no data or may send if it has got data to send.
- After getting the opportunity to send, it must relinquish its turn after some maximum period of time.
- The right to send then passes to the next node based on a predetermined logical sequence.
- The right to send may be controlled in a centralised or distributed manner.
- Polling is an example of centralised control and token passing is an example of distributed control as discussed below.

Medium Access Control

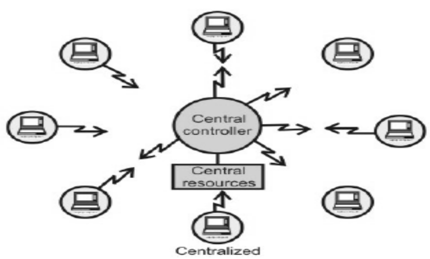
Polling

- The mechanism of polling is similar to the roll-call performed in a classroom.
- Just like the teacher, a controller sends a message to each node in turn.
- The message contains the address of the node being selected for granting access.
- Although all nodes receive the message, only the addressed node responds and then it sends data, if any. If there is no data, usually a “poll reject” message is sent back. In this way, each node is interrogated in a round-robin fashion, one after the other, for granting access to the medium.
- The first node is again polled when the controller finishes with the remaining codes.

 U1.43

Medium Access Control

- The polling scheme has the flexibility of either giving equal access to all the nodes, or some nodes may be given higher priority than others. In other words, priority of access can be easily implemented.



 U1.44

Medium Access Control

Token Passing

- In token passing scheme, all stations are logically connected in the form of a ring and control of the access to the medium is performed using a token.
- A token is a special bit pattern or a small packet, usually several bits in length, which circulate from node to node. Token passing can be used with both broadcast (token bus) and sequentially connected (token ring) type of networks with some variation

 U1.45

Medium Access Control

- In case of token ring, token is passed from a node to the physically adjacent node.
- On the other hand, in the token bus, token is passed with the help of the address of the nodes, which form a logical ring. In either case a node currently holding the token has the 'right to transmit'.
- When it has got data to send, it removes the token and transmits the data and then forwards the token to the next logical or physical node in the ring.
- If a node currently holding the token has no data to send, it simply forwards the token to the next node.

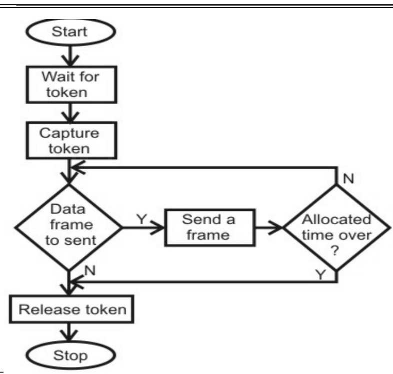
 U1.46

Medium Access Control

- The token passing scheme is efficient compared to the polling technique, but it relies on the correct and reliable operation of all the nodes.
- There exists a number of potential problems, such as lost token, duplicate token, and insertion of a node, removal of a node, which must be tackled for correct and reliable operation of this scheme.

 U1.47

Medium Access Control



 U1.48

Medium Access Control

Contention-based Approaches

- Round-Robin techniques work efficiently when majority of the stations have data to send most of the time.
- But, in situations where only a few nodes have data to send for brief periods of time, Round-Robin techniques are unsuitable.
- Contention techniques are suitable for bursty nature of traffic. In contention techniques, there is no centralized control and when a node has data to send, it contends for gaining control of the medium.
- The principle advantage of contention techniques is their simplicity. They can be easily implemented in each node. The techniques work efficiently under light to moderate load, but performance rapidly falls under heavy load.

Medium Access Control

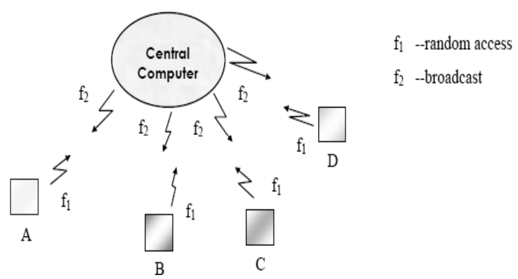
ALOHA

- The ALOHA scheme was invented by Abramson in 1970 for a packet radio network connecting remote stations to a central computer and various data terminals at the campus of the university of Hawaii.
- A simplified situation is shown in Fig.
- Users are allowed random access of the central computer through a common radio frequency band f1 and the computer centre broadcasts all received signals on a different frequency band f2.

Medium Access Control

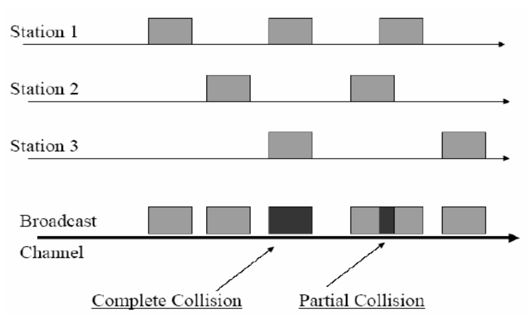
- This enables the users to monitor packet collisions, if any. The protocol followed by the users is simplest; whenever a node has a packet to sent, it simply does so.
- The scheme, known as Pure ALOHA, is truly a free-for-all scheme. Of course, frames will suffer collision and colliding frames will be destroyed.
- By monitoring the signal sent by the central computer, after the maximum round-trip propagation time, an user comes to know whether the packet sent by him has suffered a collision or not.

Medium Access Control



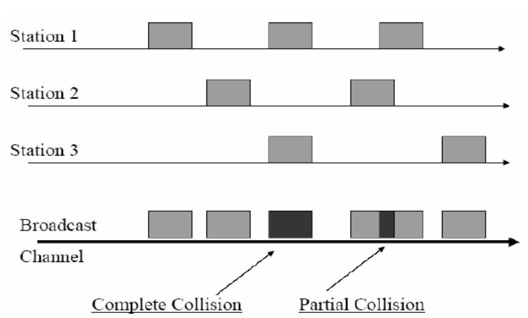
 U1.52

Medium Access Control



 U1.53

Medium Access Control

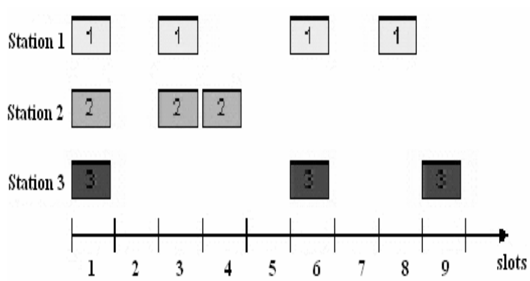


 U1.54

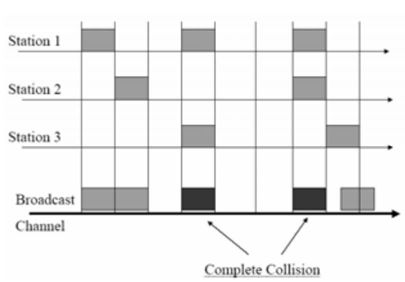
Medium Access Control

- **Slotted Aloha**
- Subsequently, in a new scheme, known as Slotted ALOHA, was suggested to improve upon the efficiency of pure ALOHA.
- In this scheme, the channel is divided into slots equal to τ and packet transmission can start only at the beginning of a slot as shown in Fig.
- This reduces the vulnerable period from 2τ to τ and improves efficiency by reducing the probability of collision.. This gives a maximum throughput of 37% at 100 percent of offered load

Medium Access Control



Medium Access Control



Medium Access Control

CSMA

- The poor efficiency of the ALOHA scheme can be attributed to the fact that a node start transmission without paying any attention to what others are doing.
- In situations where propagation delay of the signal between two nodes is small compared to the transmission time of a packet, all other nodes will know very quickly when a node starts transmission.
- This observation is the basis of the carrier-sense multiple-access (CSMA) protocol. In this scheme, a node having data to transmit first listens to the medium to check whether another transmission is in progress or not.

Medium Access Control

- The node starts sending only when the channel is free, that is there is no carrier.
- That is why the scheme is also known as listen-before-talk.
- There are three variations of this basic scheme as outlined below.

(i) 1-persistent CSMA:

- In this case, a node having data to send, start sending, if the channel is sensed free.
- If the medium is busy, the node continues to monitor until the channel is idle.
- Then it starts sending data.

Medium Access Control

(ii) **Non-persistent CSMA**:

- If the channel is sensed free, the node starts sending the packet.
- Otherwise, the node waits for a random amount of time and then monitors the channel.

(iii) **p-persistent CSMA:**

- If the channel is free, a node starts sending the packet.
- Otherwise the node continues to monitor until the channel is free and then it sends with probability p.

Medium Access Control

CSMA/CD

- CSMA/CD protocol can be considered as a refinement over the CSMA scheme.
- It has evolved to overcome one glaring inefficiency of CSMA. In CSMA scheme, when two packets collide the channel remains unutilized for the entire duration of transmission time of both the packets.
- If the propagation time is small (which is usually the case) compared to the packet transmission time, wasted channel capacity can be considerable.

 U1.61

Medium Access Control

- This wastage of channel capacity can be reduced if the nodes continue to monitor the channel while transmitting a packet and immediately cease transmission when collision is detected.
- This refined scheme is known as *Carrier Sensed Multiple Access with Collision Detection (CSMA/CD) or Listen-While-Talk.*

 U1.62

Medium Access Control

- On top of the CSMA, the following rules are added to convert it into CSMA/CD:

(i) If a collision is detected during transmission of a packet, the node immediately ceases transmission and it transmits jamming signal for a brief duration to ensure that all stations know that collision has occurred.

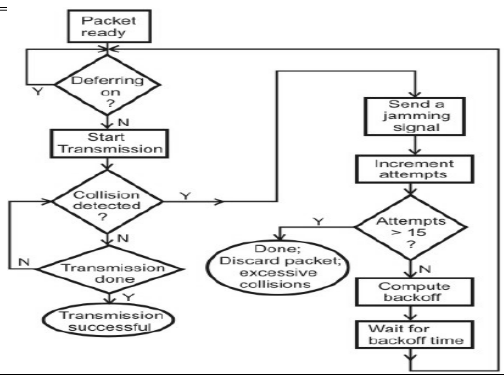
(ii) After transmitting the jamming signal, the node waits for a random amount of time and then transmission is resumed.

 U1.63

Medium Access Control

- The random delay ensures that the nodes, which were involved in the collision are not likely to have a collision at the time of retransmissions.
- To achieve stability in the back off scheme, a technique known as binary exponential back off is used.
- A node will attempt to transmit repeatedly in the face of repeated collisions, but after each collision, the mean value of the random delay is doubled.
- After 15 retries (excluding the original try), the unlucky packet is discarded and the node reports an error.

Medium Access Control



Medium Access Control

Performance Comparison between CSMA/CD and Token ring:

- It has been observed that smaller the mean packet length, the higher the maximum mean throughput rate for token passing compared to that of CSMA/CD.
- The token ring is also least sensitive to workload and propagation effects compared to CSMS/CD protocol.

Medium Access Control

- The CSMA/CD has the shortest delay under light load conditions, but is most sensitive to variations to load, particularly when the load is heavy.
- In CSMA/CD, the delay is not deterministic and a packet may be dropped after fifteen collisions based on binary exponential back off algorithm.
- As a consequence, CSMA/CD is not suitable for real-time traffic.

 U1.67

Medium Access Control

CSMA Vs CSMA/CD

- In CSMA scheme, a station monitors the channel before sending a packet.
- Whenever a collision is detected, it does not stop transmission leading to some wastage of time.
- On the other hand, in CSMA/CD scheme, whenever a station detects a collision, it sends a jamming signal by which other station comes to know that a collision occurs.
- As a result, wastage of time is reduced leading to improvement in performance.

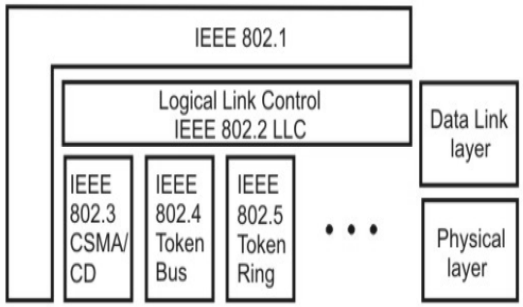
 U1.68

IEEE Ring LANs

- Explain the operation of IEEE 802 LANs
- 802.4 – Token bus-based
- 802.5 – Token ring-based

 U1.69

IEEE Ring LANs



IEEE Ring LANs

Token Ring

- Originally, IBM developed Token Ring network in the 1970s. It is still IBM's primary local-area network (LAN) technology.
- The related IEEE 802.5 specification is almost identical to and completely compatible with IBM's Token Ring network. In fact, the IEEE 802.5 specification was modeled after IBM Token Ring, and on the same lines.
- The term Token Ring is generally used to refer to both IBM's Token Ring network and IEEE 802.5 networks.

IEEE Ring LANs

- Before going into the details of the Token Ring protocol, let's first discuss the motivation behind it.
- As already discussed, the medium access mechanism used by Ethernet (CSMA/CD) may results in collision.
- Nodes attempt to a number of times before they can actually transmit, and even when they start transmitting there are chances to encounter collisions and entire transmission need to be repeated.
- And all this become worse one the traffic is heavy i.e. all nodes have some data to transmit.

IEEE Ring LANs

- Apart from this there is no way to predict either the occurrence of collision or delays produced by multiple stations attempting to capture the link at the same time.
- So all these problems with the Ethernet gives way to an alternate LAN technology, Token Ring.

IEEE Ring LANs

- Token Ring and IEEE802.5 are based on token passing MAC protocol with ring topology.
- They resolve the uncertainty by giving each station a turn on by one. Each node takes turns sending the data; each station may transmit data during its turn.
- The technique that coordinates this turn mechanism is called Token passing; as a Token is passed in the network and the station that gets the token can only transmit.
- As one node transmits at a time, there is no chance of collision.

IEEE Ring LANs

- Stations are connected by point-to-point links using repeaters.
- Mainly these links are of shielded twisted-pair cables. The repeaters function in two basic modes: Listen mode, Transmit mode.
- A disadvantage of this topology is that it is vulnerable to link or station failure.
- But a few measures can be taken to take care of it.

IEEE Ring LANs

Differences between Token Ring and IEEE 802.5

- Both of these networks are basically compatible, although the specifications differ in some ways.
- IEEE 802.5 does not specify a topology, although virtually all IEEE 802.5 implementations are based on the star topology. While IBM's Token Ring network explicitly specifies a star, with all end stations attached to a device called a Multi-Station Access Unit (MSAU).
- IEEE 802.5 does not specify a media type, although IBM Token Ring networks use twisted-pair wire.
- There are few differences in routing information field size of the two.

 U1.76

IEEE Ring LANs

Token Ring Operation

- Token-passing networks move a small frame, called a token, around the network.
- Possession of the token grants the right to transmit.
- If a node receiving the token has no information to send, it passes the token to the next end station.
- Each station can hold the token for a maximum period of time.

 U1.77

IEEE Ring LANs

- If a station possessing the token does have information to transmit, it seizes the token, alters 1 bit of the token (which turns the token into a start-of-frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring.
- While the information frame is circling the ring, no token is on the network (unless the ring supports early token release), which means that other stations wanting to transmit must wait.
- Therefore, collisions cannot occur in Token Ring networks.
- If early token release is supported, a new token can be released immediately after a frame transmission is complete.

 U1.78

IEEE Ring LANs

- The information frame circulates around the ring until it reaches the intended destination station, which copies the information for further processing.
- The information frame makes a round trip and is finally removed when it reaches the sending station.
- The sending station can check the returning frame to see whether the frame was seen and subsequently copied by the destination station in error-free form.
- Then the sending station inserts a new free token on the ring, if it has finished transmission of its packets.

 U1.79

IEEE Ring LANs

- Unlike CSMA/CD networks (such as Ethernet), token-passing networks are deterministic, which means that it is possible to calculate the maximum time that will pass before any end station will be capable of transmitting.
- Token Ring networks are ideal for applications in which delay must be predictable and robust network operation is important.

 U1.80

IEEE Ring LANs

Priority System

- Token Ring networks use a sophisticated priority system that permits certain user-designated, high-priority stations to use the network more frequently. Token Ring frames have two fields that control priority: *the priority field and the reservation field.*

 U1.81

IEEE Ring LANs

- Only stations with a priority equal to or higher than the priority value contained in a token can seize that token.
- After the token is seized and changed to an information frame, only stations with a priority value higher than that of the transmitting station can reserve the token for the next pass around the network.
- When the next token is generated, it includes the higher priority of the reserving station.
- Stations that raise a token's priority level must reinstate the previous priority after their transmission is complete.

 U1.82

IEEE Ring LANs

Ring Maintenance

- There are two error conditions that could cause the token ring to break down.
- One is the lost token in which case there is no token the ring, the other is the busy token that circulates endlessly.
- To overcome these problems, the IEEE 802 standard specifies that one of the stations be designated as 'active monitor'.

 U1.83

IEEE Ring LANs

- The monitor detects the lost condition using a timer by time-out mechanism and recovers by using a new free token.
- To detect a circulating busy token, the monitor sets a 'monitor bit' to one on any passing busy token.
- If it detects a busy token with the monitor bit already set, it implies that the sending station has failed to remove its packet and recovers by changing the busy token to a free token.

 U1.84

IEEE Ring LANs

- Other stations on the ring have the role of passive monitor.
- The Primary job of these stations is to detect failure of the active monitor and assume the role of active monitor.
- A contention-resolution is used to determine which station to take over.

 U1.85

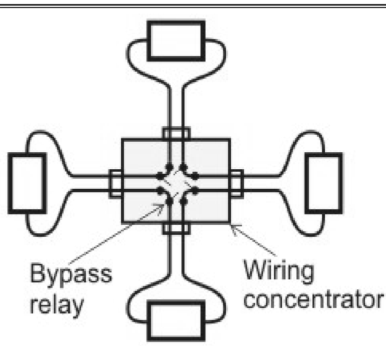
IEEE Ring LANs

Physical Layer

- The Token Ring uses shielded twisted pair of wire to establish point-point links between the adjacent stations. The baseband signaling uses differential Manchester encoding.
- To overcome the problem of cable break or network failure, which brings the entire network down, one suggested technique, is to use *wiring concentrator as shown in Fig.*

 U1.86

IEEE Ring LANs



 U1.87

IEEE Ring LANs

- It imposes the reliability in an elegant manner.
- Although logically the network remains as a ring, physically each station is connected to the wire center with two twisted pairs for 2-way communication.
- Inside the wire center, bypass relays are used to isolate a broken wire or a faulty station.
- This Topology is known as Star-Connected Ring**.**

IEEE Ring LANs

Frame Format

- Token Ring and IEEE 802.5 support two basic frame types: tokens and data/command frames.
- Tokens are 3 bytes in length and consist of a start delimiter, an access control byte, and an end delimiter. Data/command frames vary in size, depending on the size of the Information field. Data frames carry information for upper-layer protocols, while command frames contain control information and have no data for upper-layer protocols.

Start Delimiter	Access Control	Ending delimiter

Token Frame contains three fields, each of which is 1 byte in length:

IEEE Ring LANs

Start delimiter (1 byte):

- Alerts each station of the arrival of a token (or data/command frame).
- This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.

Access-control (1 byte):

- Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).

IEEE Ring LANs

End delimiter (1 byte):

- Signals the end of the token or data/command frame.
- This field also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.

 U1.91

IEEE Ring LANs

Data/Command Frame Fields

Start Delimiter	Access Control	Frame Control	Destination address	Source address	Data	Frame check sequence	End Delimiter	Frame Status

Data/command frames have the same three fields as Token Frames, plus several others. The Data/command frame fields are described below:

Frame-control byte (1 byte)—Indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.

Destination and source addresses (2-6 bytes)—Consists of two 6-byte address fields that identify the destination and source station addresses.

 U1.92

IEEE Ring LANs

- **Data (up to 4500 bytes)—**Indicates that the length of field is limited by the ring token holding time, which defines the maximum time a station can hold the token.
- **Frame-check sequence (FCS- 4 byte)—**Is filed by the source station with a calculated value dependent on the frame contents. The destination station recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.
- **Frame Status (1 byte)—**This is the terminating field of a command/data frame. The Frame Status field includes the address-recognized indicator and frame-copied indicator.

 U1.93

IEEE Ring LANs

Token BUS

- Although Ethernet was widely used in the offices, but people interested in factory automation did not like it because of the probabilistic MAC layer protocol.
- They wanted a protocol which can support priorities and has predictable delay.
- These people liked the conceptual idea of Token Ring network but did not like its physical implementation as a break in the ring cable could bring the whole network down and ring is a poor fit to their linear assembly lines.
- Thus a new standard, known as Token bus, was developed, having the robustness of the Bus topology, but the known worst-case behavior of a ring.

 U1.94

IEEE Ring LANs

- stations are logically connected as a ring but physically on a Bus and follows the collision-free token passing medium access control protocol. So the motivation behind token bus protocol can be summarized as:
- The probabilistic nature of CSMA/ CD leads to uncertainty about the delivery time; which created the need for a different protocol
- The token ring, on the hand, is very vulnerable to failure.
- Token bus provides deterministic delivery time, which is necessary for real time traffic.
- Token bus is also less vulnerable compared to token ring.

 U1.95

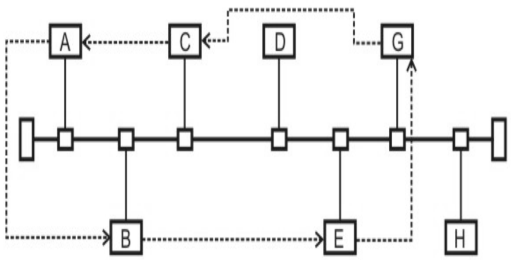
IEEE Ring LANs

Functions of a Token Bus

- It is the technique in which the station on bus or tree forms a logical ring, that is the stations are assigned positions in an ordered sequence, with the last number of the sequence followed by the first one as shown in Fig.
- Each station knows the identity of the station following it and preceding it.

 U1.96

IEEE Ring LANs



IEEE Ring LANs

- A control packet known as a Token regulates the right to access.
- When a station receives the token, it is granted control to the media for a specified time, during which it may transmit one or more packets and may poll stations and receive responses when the station is done, or if its time has expired then it passes token to next station in logical sequence.
- Hence, steady phase consists of alternate phases of token passing and data transfer.

IEEE Ring LANs

- The MAC sublayer consists of four major functions: the interface machine (IFM), the access control machine (ACM), the receiver machine (RxM) and the transmit machine (TxM).
- IFM interfaces with the LLC sublayer. The LLC sublayer frames are passed on to the ACM by the IFM and if the received frame is also an LLC type, it is passed from RxM component to the LLC sublayer.
- IFM also provides quality of service.

IEEE Ring LANs

- The ACM is the heart of the system. It determines when to place a frame on the bus, and responsible for the maintenance of the logical ring including the error detection and fault recovery.
- It also cooperates with other stations ACM's to control the access to theshared bus, controls the admission of new stations and attempts recovery from faults and failures.

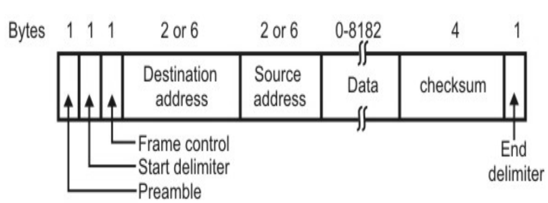
IEEE Ring LANs

- The responsibility of a TxM is to transmit frame to physical layer. It accepts the frame from the ACM and builds a MAC protocol data unit (PDU) as per the format.
- The RxM accepts data from the physical layer and identifies a full frame by detecting the SD and ED (start and end delimiter).
- It also checks the FCS field to validate an error-free transmission.

IEEE Ring LANs

Frame Form

- The frame format of the Token Bus is shown in Fig. Most of the fields are same as Token Ring. So, we shall just look at the Frame Control Field in Table



IEEE Ring LANs

Frame Control	Name	Use
0000 0000	Claim-Token	Ring Initialization
0000 0001	Solicit-successor -1	Addition to the Ring
0000 0010	Solicit-successor -2	Addition to the Ring
0000 0011	Who-follows	Recovery from lost token
0000 0100	Resolve Contention	Multiple station to join the Ring
0000 1000	Token	Pass the Token
0000 1100	Set-Successor	Deletion from the ring

 U1.103

IEEE Ring LANs

Logical ring maintenance

- The MAC performs the following functions as part of its maintenance role of the ring.
- **Addition to the Ring:** Non-participating stations must periodically be granted the opportunity to insert themselves into the ring.
- Each node in the ring periodically grants an opportunity for new nodes to enter the ring while holding the token.

 U1.104

IEEE Ring LANs

- The node issues a solicit–successor–1 packet, inviting nodes with an address between itself and the next node in logical sequence to request entrance.
- The transmitting node then waits for a period of time equal to one response window or slot time (twice the end-to-end propagation delay of the medium).
- If there is no request, the token holder sets its successor node to be the requesting node and transmits the token to it; the requester sets the linkages accordingly and proceeds.
- If more than one node requests, to enter the ring, the token holder will detect a garbled transmission.

 U1.105

IEEE Ring LANs

- The conflict is resolved by addressed based contention scheme; the token holder transmits a resolved contention packet and waits for four response windows.
- Each requester can transmit in one of these windows, based on the first two bits of its address. If requester hears anything before its windows comes up, it refrains from requesting entrance.
- If a token holder receives a valid response, then it can proceed, otherwise it tries again and only those nodes that request the first time are allowed to request this time, based on the second pair of bits in their address.

 U1.106

IEEE Ring LANs

- This process continues until a valid request is received or no request is received, or a maximum retry count is reached. In latter cases, the token holder passes the token to logical successor in the ring.
- **Deletion from Ring**: A station can voluntarily remove itself from the ring by splicing together its predecessor and successor. The node which wants to be deleted from the ring waits until token comes to it, then it sends a set successor packet to its predecessor, instructing it to splice to its successor.

 U1.107

IEEE Ring LANs

Relative comparison of the three standards

Function	CSMA/CD	Token bus	Token ring
Access determination	Contention	Token	Token
Packet length restriction	64 bytes (Greater than 2.Tprop)	None	None
Priority	Not supported	Supported	Supported
Sensitivity to work load	Most sensitive	Sensitive	Least sensitive
Principle advantage	Simplicity, wide installed base	Regulated/fair access	Regulated/fair access
Principle disadvantage	Nondeterministic delay	Complexity	Complexity

 U1.108

High Speed LANs – Token Ring Based

- The IEEE 802.3 and 802.5 LANs, discussed in the previous sections, having data transfer rate in the range of 10 Mb/s to 16 Mb/s have served the purpose very well for many years.
- But with the availability of powerful computers at a low cost and emergence of new applications, particularly based on multimedia, there is a growing demand for higher network bandwidth.
- The combined effect of the growth in the number of users and increasing bandwidth requirement per user has led to the development of High Speed LANs with data transfer rate of 100 Mb/s or more.

 U1.109

High Speed LANs – Token Ring Based

- The high speed LANs that have emerged can be broadly categorized into three types based on token passing, successors of Ethernet and based on switching technology.
- In the first category we have FDDI and its variations, and high-speed token ring. In the second category we have the fast Ethernet and Gigabit Ethernet.
- In the third category we have ATM, fiber channel and the Ether switches.

 U1.110

High Speed LANs – Token Ring Based

FDDI

- Fiber Distributed Data Interface (FDDI), developed by American National Standards Institute (ANSI) is a token passing ring network that operates at 100 Mb/s on optical fiber-medium.
- Its medium access control approach has close similarity with the IEEE 802.5 standard, but certain features have been added to it for higher reliability and better performance.
- Key features of FDDI are outlined in this section.

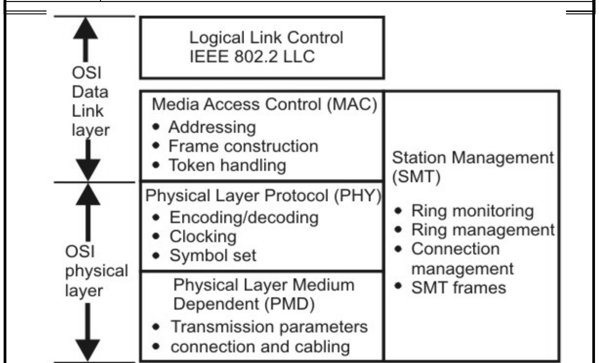
 U1.111

High Speed LANs – Token Ring Based

- The FDDI standard divides transmission functions into 4 protocols: physical medium dependent (PMD), Physical (PHY), media access control(MAC) and Logical link control(LLC) as shown in Fig.
- These protocols correspond to the physical and data link layer of OSI reference model.
- Apart from these four protocols, one more protocol which span across both data link and physical layer (if considered of OSI), used for the station management.

 U1.112

High Speed LANs – Token Ring Based



 U1.113

High Speed LANs – Token Ring Based

Medium

- The standard physical medium is multi-mode 62.5/125 micron optical fiber cable using light emitting diode (LED) transmitting at 1300 nanometers, as the light source.
- FDDI can support up to 500 stations with a maximum distance of 2 Km between stations and maximum ring circumference of 200 Km. Single-mode 8-10/125 micron optical fiber cable has also been included in the standard for connecting a pair of stations separated by a distance in excess of 20 km.

 U1.114

High Speed LANs – Token Ring Based

- The standard has also been extended to include copper media - Shielded Twisted Pair (STP) and some categories of Unshielded Twisted Pair (UTP) with a maximum distance of 100 m between stations. FDDI over copper is referred to as Copper-Distributed Data Interface (CDDI).
- In particular, security, reliability, and performance are all enhanced with optical fiber media because fiber does not emit electrical signals.
- A physical medium that does emit electrical signals (copper) can be tapped and therefore vulnerable to unauthorized access to the data that is transmitted through the medium.

 U1.115

High Speed LANs – Token Ring Based

FDDI Physical layer specification

Trans. Medium	Optical Fiber 62.5/125 um	Twisted pair CAT5-UTP
Data Rate	100 Mbps	100Mbps
Signaling Technique	4B/5B/NRZ-I 125 Mbaud	MTL-3
Max. No. Repeaters	100	100
Max. distance	2Km	100m

 U1.116

High Speed LANs – Token Ring Based

Topology

- The basic topology for FDDI is *dual counter rotating rings: one* transmitting clockwise and the other transmitting counter clockwise as illustrated in the Fig.
- One is known as primary ring and the other secondary ring. Although theoretically both the rings can be used to achieve a data transfer rate of 200 Mb/s, the standard recommends the use of the primary ring for data transmission and secondary ring as a backup.

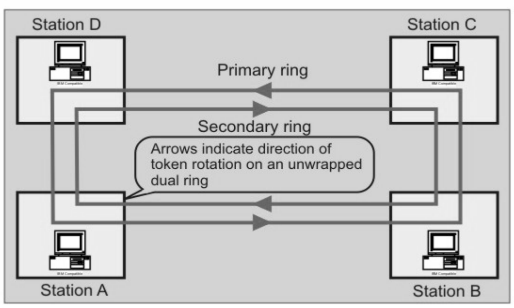
 U1.117

High Speed LANs – Token Ring Based

- In case of failure of a node or a fiber link, the ring is restored by wrapping the primary ring to the secondary ring as shown in Fig.
- The redundancy in the ring design provides a degree of fault tolerance, not found in other network standards.
- Further improvement in reliability and availability can be achieved by using *dual ring of trees and dual homing mechanism.*

 U1.118

High Speed LANs – Token Ring Based



 U1.119

High Speed LANs – Token Ring Based

Fault Tolerance

- FDDI provides a number of fault-tolerant features. In particular, FDDI's dual-ring environment, the implementation of the optical bypass switch, and dual-homing support make FDDI a resilient media technology.

Dual Ring

- FDDI's primary fault-tolerant feature is the dual ring. If a station on the dual ring fails or is powered down, or if the cable is damaged, the dual ring is automatically wrapped (doubled back onto itself) into a single ring.

 U1.120

High Speed LANs – Token Ring Based

Frame Format

- Each Frame is preceded by a preamble (16 idle symbols-1111), for a total of 64 bits, to initialize clock synchronization with the receiver. There are 8 fields in the FDDI frame as shown in Fig.

Data/Command Frame

PA	SD	FC	DA	SA	DATA	FCS	ED	FS

Token

PA	SD	FC	ED

PA :	Preamble
SD :	Starting Delimiter
FC :	Frame Control
DA :	Destination Address
SA :	Source Address
FCS:	Frame Check Sequence
ED :	Ending Delimiter
FS :	Frame Status

High Speed LANs – Token Ring Based

- **SD:** The first byte, after the preamble, of the field is the frame's starting flag. As in Token ring these bits are replaced in physical layer by the control codes.
- **FC**: it identifies the frame type i.e. token or a data frame.
- **Address**: the next 2 fields are destination and source addresses. Each address consists of 2-6 bytes.
- **Data**: Each data frame carries up to 4500 bytes.
- **FCS**: FDDI uses the standard IEEE four-byte cyclic redundancy check.
- **ED:** this field consists of half a byte in data frame or a full byte in token frame. This represents end of the Token.
- **FS:** FDDI FS field is similar to that of Token Ring. It is included only in data/Command frame and consists of one and a half bytes**.**

High Speed LANs – Token Ring Based

Media Access Control

- The FDDI media access control protocol is responsible for the following services.

(i) Fair and equal access to the ring by using a *timed token protocol.*

- To transmit on the ring, a station must first acquire the token.
- A station holds the token until it has transmitted all of its frames or until the transmission time for the appropriate service is over.
- Synchronous traffic is given a guaranteed bandwidth by ensuring that token rotation time does not exceed a preset value.

High Speed LANs – Token Ring Based

- FDDI implements these using three timers, Token holding Timer (THT), which determines how long a station may continue once it has captured a token.
- **Token Rotation Timer (TRT)** is reset every time a token is seen. When timer expires, it indicates that the token is lost and recovery is started.
- **The Valid Transmission Timer (VTT)** is used to time out and recover from some transmit ring errors.

(ii) Construction of frames and tokens are done as per the format shown in Figure. The frame status (FS) byte is set by the destination and checked by the source station, which removes its frame from the ring and generates another token.

High Speed LANs – Token Ring Based

(iii) Transmitting, receiving, repeating and stripping frames and tokens from the ring, unlike IEEE 802.5, is possible for several frames on the ring simultaneously.

- Thus a station will transmit a token immediately after completion of its frame transmission. A station further down the ring is allowed to insert its own frame.
- This improves the potential throughput of the system. When the frame returns to the sending station, that station removes the frame from the ring by a process called stripping.

(iv) It also does ring initialization, fault isolation and error detection as we have discussed for IEEE 802.5.

High Speed LANs – Token Ring Based

(iii) Transmitting, receiving, repeating and stripping frames and tokens from the ring, unlike IEEE 802.5, is possible for several frames on the ring simultaneously.

- Thus a station will transmit a token immediately after completion of its frame transmission. A station further down the ring is allowed to insert its own frame.
- This improves the potential throughput of the system. When the frame returns to the sending station, that station removes the frame from the ring by a process called stripping.

(iv) It also does ring initialization, fault isolation and error detection as we have discussed for IEEE 802.5.

High Speed LANs – Token Ring Based

FDDI and the OSI model

- The relationship between the OSI model and the FDDI layered architecture is shown in Fig.
- The physical layer is divided into two sub layers: PMD and PHY.
- The lower sub layer is defined by Physical Layer Medium Dependent (PMD) standards, which specify requirements such as media and connection types.
- The upper sub layer is defined in the physical layer protocol (PHY) standard, which is medium-independent.
- It defines symbols, line status, encoding/decoding techniques, clocking requirements and data framing requirements.

High Speed LANs – Token Ring Based

- The Data Link Layer is divided into two sub layers, MAC and LLC. The lower sub layer, the FDDI Media Access Control (MAC) standard defines addressing conventions, frame formats and the timed token protocol.
- The upper sub layer is defined in the IEEE 802.2 LLC standard, which provides a means for exchanging data between LLC users.
- The Station Management (SMT) standard provides services that monitor and control a FDDI station. SMT include facilities for connection management, node configuration, recovery from error condition, and encoding of SMT frames.
- The FDDI has been successfully used as a backbone LAN in an enterprise network or in a campus network.

High Speed LANs – Token Ring Based

COMPARISON AMONG STANDARDS

Parameters	FDDI	IEEE 802.3	IEEE 802.5
• BANDWIDTH	100Mb/s	10Mb/s	4 or 16Mb/s
• NUMBER OF STATIONS	500	1024	250
• MAX. DISTANCE BETWEEN STATIONS	2Km (MMF) 20Km (SMF)	2.8Km	300m (4Mb/s) 100m (RECO.)
• MAX. NETWORK EXTENT	100Km	2.8Km	VARIED WITH CONFIGURATION
• LOGICAL TOPOLOGY	DUAL RING, DUAL RING OF TREES	BUS	SINGLE RING
• PHYSICAL TOPOLOGY	RING, STAR HIERARCHICAL STAR	BUS, STAR	RING BUS HIERARCHICAL STAR

High Speed LANs – Token Ring Based

• MEDIA	OPTICAL FIBER	OPTICAL FIBRE, TWISTED-WIRE, COAXIAL CABLE	TWISTED-WIRE OPTICAL FIBER
• ACCESS METHOD	TIMED-TOKEN PASSING	CSMA/CD	TOKEN PASSING
• TOKEN ACQUISITION	CAPTURES THE TOKEN	-	BY SETTING A STATUS BIT
• TOKEN RELEASE	AFTER TRANSMIT	-	AFTER STRIPPING OR AFTER TRANSMIT (16)
• FRAMES ON LAN	MULTIPLE	SINGLE	SINGLE
• FRAMES TRANSMITTED PER ACCESS	MULTIPLE	SINGLE	SINGLE
• MAX. FRAME SIZE	4500 BYTES	1518 BYTES	4500 BYTES (4) 17,800 BYTES (16)

High Speed LANs – Token Ring Based

How FDDI offers higher reliability than token ring protocol?

- Token ring protocol is applicable in a single ring. Disadvantage of this protocol is that, if one segment of wires fails or a node fails, the protocol cannot work.
- To increase reliability, dual counter ring topology used in FDDI protocol, where there are two rings, called primary ring and secondary ring. In case of failure of a node or a fiber link, the ring is restored the by wrapping up the primary ring to the secondary ring.
- Further improvement in reliability can achieve by using dual ring of trees and dual homing mechanism. It will provide multiple paths and if one path fails, another path will be available for passing token or data.

High Speed LANs – Token Ring Based

In what way the MAC protocol of FDDI differs from that of token ring?

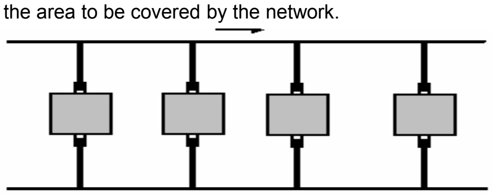
- In the frame format of FDDI protocol, preamble is eight bytes instead of one byte in token ring. Also token has one additional byte.
- FDDI can have multiple frames simultaneously, which cannot be present in token ring. Here, the access method is timed token passing. Multiple frames can be transmitted after capturing a token.
- First, the entire token is captured and then the data frames are introduced, whereas token ring follows token passing protocol and beginning of token is converted to the header of a frame.

High Speed LANs – Token Ring Based

- In case of token ring token is released after receiving the acknowledgement (as the data frame returns after circulating the ring).
- On the other hand, in case of FDDI, token is released immediately after sending data frame, which is known as early token release.

High Speed LANs – DQDB

- IEEE defined a MAN standard for covering an entire city. This was called **Distributed Queue Data Interface (DQDB) and put up as IEEE standard 802.6.**
- The basic geometry of DQDB is as shown in the figure below. Two parallel unidirectional buses are laid down in the area to be covered by the network.



High Speed LANs – DQDB

- The stations are attached to both the buses in parallel.
- Each bus has a head-end, which generates a steady stream of 53byte cells.
- Each cell travels downstream from the head end. When it reaches the end, it falls off the bus.
- Each cell carries a 44 byte payload field, making it compatible with some AAL modes.
- Each cell also holds two protocol bits, Busy, set to indicate that a cell is occupied, and Request, which can be set when a station wants to make a request.

High Speed LANs – DQDB

- To transmit a cell, a station has to know whether the destination is to the left of it or to its right.
- If the destination is to the right, the sender uses bus A. Otherwise it uses bus B.
- Data are inserted onto either bus using a wired-OR-circuit, so failure of a station does not take down the network.

High Speed LANs – DQDB

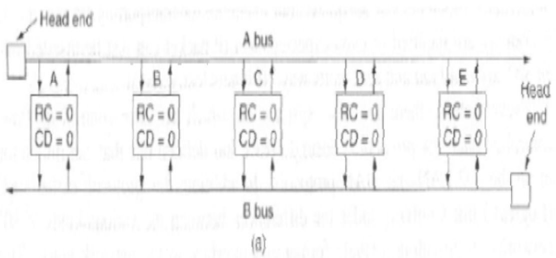
- The 802.6 protocol does not have greedy stations.
- In all others, if a station gets a chance to send, it sends. Here the queue up and become ready to transmit in FIFO order, all this without having a central queue.
- To simulate the FIFO queue, each station maintains two counters, *RC and CD.*
- RC (Request Counter) counts the number of downstream request pending until the station itself has a frame to send.
- At that point, RC is copied to CD, RC is reset to 0 and now counts the number of requests made after the station became ready.

High Speed LANs – DQDB

- For example, if CD = 3 and RC = 2 for station k, the next three empty cells that pass by station k are reserved for downstream stations, then station k may send, then two more cells are reserved for downstream stations.
- For simplicity, we assume a station can have only one cell ready for transmission at a time.
- To send a cell, a station must first make a reservation by setting the Request bit in some cell on the reverse bus (i.e., on bus B for a transmission that will later take place on bus A).
- As this cell propagates down the reverse bus, every station along the *way notes it and increments it's RC.*

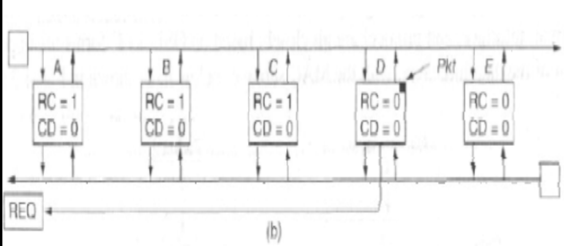
High Speed LANs – DQDB

- To illustrate this concept, we will use an example.
- Initially, all the *RC counters are 0, and no cells are queued up, as shown in Fig.*



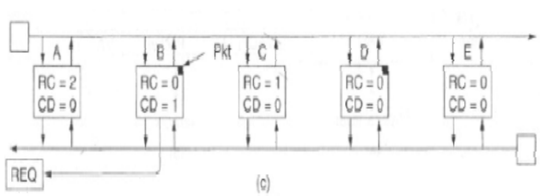
High Speed LANs – DQDB

- Then station D makes a request, which causes stations, C, *B, and A, to increment their RC counters, as shown in Fig.*



High Speed LANs – DQDB

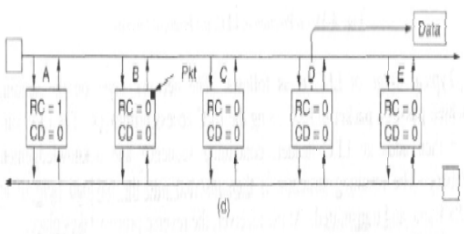
- After that, *B makes* a request, copying its current *RC value into CD, leading to the situation of Fig.*



High Speed LANs – DQDB

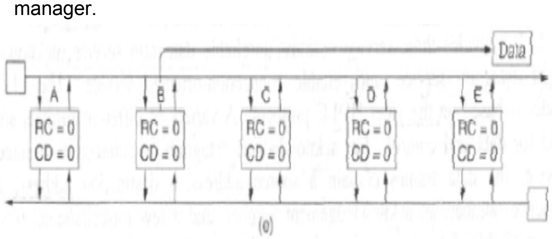
- At this point, the head-end on bus A generates an empty cell.
- As it passes by B, that station sees that its CD > 0, so it may not use the empty cell.
- (When a station has a cell queued, CD represents its position in the queue, with 0 being the front of the queue). Instead it decrements CD.
- When the still-empty cell gets to D, that station sees that CD = 0, meaning that no one is ahead of it on the queue, so it ORs its data into the cell and sets the Busy bit. After the transmissions are done, we have the situation of Fig.

High Speed LANs – DQDB



High Speed LANs – DQDB

- When the next empty cell is generated, station B sees that it is now at the head of the queue, and seizes the cell (by setting I bit), as illustrated in Fig. In this way, stations queue up to take turns, without a centralized queue manager.



High Speed LANs – HIPPI

- The High-Performance Peripheral Interface (HIPPI) protocol was designed to facilitate high-speed communications between very high-performance computers (such as supercomputers), and thereby to attempt to meet their I/O requirements.

High Speed LANs – HIPPI

Overview of HIPPI

- HIPPI is a very high-speed data transfer protocol, with the following properties, features, and limitations:
- Data rates of 800 or 1600 Mb/s.
- Uses a 50- or 100-pair connection. (50-pair for 800 Mb/s data-rate, 100-pair for 1600 Mb/s datarate.) The 100-pair connection is actually a set of two identical 50-pair cables.
- Useful for distances up to 25 meters. (Serial-HIPPI extensions are being proposed for operation up to 10km.)
- Transfers 32 bits (for 800 Mb/s data-rate) or 64 bits (for 1600 Mb/s data-rate) in parallel. Packet format allows byte alignment.
- Connection-oriented protocol.

High Speed LANs – HIPPI

- Point-to-point connection.
- Simplex (i.e., one-way data transfer) operation.
- First standard in its class (data-transfer for high-performance computing environments).
- Designed for ease of implementation: available options are very limited.

High Speed LANs – HIPPI

- The HIPPI protocol is defined, at several layers, by a collection of standards :

1. HIPPI-PH (Physical Layer)
2. HIPPI-FP (Framing Protocol)
3. HIPPI-SC (Switch Control)
4. HIPPI-LE(Link Encapsulation)
5. HIPPI-FC(Fibre Channel)
6. HIPPI-IPI(Disk & Tape Commands)
7. Serial HIPPI

 U1.148

High Speed LANs – HIPPI

- **HIPPI-PH (Physical Layer)**
- The HIPPI-PH standard defines the mechanical, electrical, and signaling of the HIPPI physical layer.
- Note that since HIPPI is a simplex protocol, a full-duplex link would be achieved by another HIPPI connection in the opposite direction.
- HIPPI's physical layer consists of a set of 50-twisted-pair copper cables (maximum length of 25 meters).
- Two options exist, based the desired data-rate: 800 or 1600 Mb/s.

 U1.149

High Speed LANs – HIPPI

Conceptual Transmission Elements

- To understand signaling, one must first understand how HIPPI transmits data. The conceptual elements of data transmission are the *connection, the packet, the burst, and the word.*
- One connection consists of any number of packets.
- One packet consists of any number of bursts.
- One burst consists of 1 to 256 words of data. (Maximum of 1 K-byte of data per burst.)
- Each data word is 32 bits long.

 U1.150

High Speed LANs – HIPPI

Signal Lines

- The HIPPI signals and timing are described below. Each line is dedicated to its own function. (Since HIPPI is simplex, this includes the data bus and parity bus.)
-
- The item in parentheses is the line direction: source is denoted by *S , and destination by D .*
- *Note that the source initiates the data connection. One* may think of a common example of a computer talking to an external disk drive where the computer is the data source and the disk is the destination.

 U1.151

High Speed LANs – HIPPI

- *REQUEST(S-->D) -- The source raises this line to initiate a connection.*
- *CONNECT(D-->S) -- The destination raises this line if accepts the source's initiation. Once this* line is raised, a connection is in progress.

 U1.152

High Speed LANs – HIPPI

- *READY(D-->S) -- Once the connection has been established, the destination sends one ready pulse* for each burst that it can receive (up to a maximum of 63). (These pulses are called "credits“) Two things are accomplished by this means:

1. The destination performs flow control by not sending ready pulses until it knows it can handle the resulting burst.
2. These ready pulses can be sent at a much faster rate than the bursts themselves, and in parallel with bursts.

- This allows the source to have advanced notice of the amount of data it can send, and not interrupt the source's sending with these notifications.

 U1.153

High Speed LANs – HIPPI

- *PACKET(S-->D) -- The source raises this line at the beginning of a packet transmission. It* remains high as long as the packet is in progress.

- *BURST(S-->D) -- The source raises this line at the beginning of a burst transmission. It remains* high as long as data is being transmitted, then is dropped to transmit the *LLRC* .

High Speed LANs – HIPPI

- *DATA BUS(S-->D) -- These 32 lines carry the data during the transmission burst. All data-bits are* transmitted in parallel, with line (bit) 0 being the *LSB* .

The DATA BUS also carries two other important items:

- When the REQUEST line is raised, the *I-Field (specified in the HIPPI-SC layer) is put onto* the DATA BUS. This I-Field is used by physical layer switches as a destination address.
- When the BURST line is dropped, the *LLRC is put on the DATA BUS. This is a* longitudinal, even check-sum of the entire burst data.

High Speed LANs – HIPPI

- *PARITY BUS(S-->D) -- These 4 lines carry the parity bits (one for each word) along with data* word.

- *CLOCK(S-->D) -- Provided by the source, this is a continuous 25 MHz clock. (Timing issues are* described below.)

- *INTERCONNECT(S<-->D) -- This is a set of two* lines, one in each direction, which inform each end that the other is powered up and connected.

High Speed LANs – HIPPI

- **Timing**
- Though the HIPPI connection is considered synchronous (probably because connections can be requested asynchronously), it uses a 25 MHz (+/- 5%) clock, provided by the source, to transfer data synchronously within each burst.
- The clock signal is symmetrical (i.e., high and low pulses split the clock cycle evenly).
- During data transmission, one word is transmitted each clock cycle.

High Speed LANs – HIPPI

- The CONNECT and READY signals are raised and dropped for a minimum of four clock cycles.
- Maximum signal times for most signals are not specified, to give both source and destination as much time as each needs during the times when the other is waiting on it.
- The BURST and PACKET signals should be dropped for a minimum of two clock cycles, but the standard specifies that the destination should operate properly if BURST or PACKET are dropped for only one clock.
- This gives intermediate switches one clock cycle to synchronize.

High Speed LANs – HIPPI

- **HIPPI-FP (Framing Protocol)**
- This standard describes the format and content (including header) of each packet of user information.
- Note that other layers may be implemented above this one. Note also that this is the layer which splits higher layer packets to the 1 or 2 K-byte packets required by the physical layer.

High Speed LANs – HIPPI

Header Area (64 bits)

- D2_Offset (word 0, bits 0 - 2)) -- The offset into the D2_Area buffer of the first byte of user information. This allows byte alignment of user data.
- D1_Area_Size (word 0, bits 3 - 10) -- Defines the size of the D1_Area.
- Reserved (word 0, bits 11 - 21).
- B (word 0, bit 22) -- This bit gives a hint to the destination: it is set to 1 if the D2_Area will arrive in a subsequent burst (not the current one). This gives higher layer protocols a bit of advanced notice, if necessary, of the arrival of user data.

High Speed LANs – HIPPI

- P (word 0, bit 23) -- Set to 1 if the D1_Area is present. (Otherwise, the D1_Area is zero bytes.)
- ULP-id (word 0, bits 24-31) -- Designates the upper layer protocol to which the packet data is to be delivered. Options currently include IEEE 802.2, various IPI-3 options, or HIPPIFC. Space is reserved for locally assigned ULP-id's.
- D2_Size (word 1) -- Contains the number of bytes to be found in D2_Area .
- D1_Area (0 - 1016 bytes) -- This area contains protocol data. (In other words, the data transmitted here is based on the particular higher layer protocol.)

High Speed LANs – HIPPI

- D2_Area (0 - (2^32 - 2)) -- This area contains user data.
- Padding (0 - 7 bytes) -- Up to the first 7 bytes may be unused, to allow byte alignment of the D2_Data_Set on the source and/or destination.
- D2_Data_Set (0 - (2^32 - 2) bytes) -- Contains user data.
- Padding (0 - 2047 bytes) -- May be unused.

High Speed LANs – HIPPI

HIPPI-SC (Switch Control)

- The most glaring limitation of HIPPI-PH is that it supports only a single point-to-point connection.
- Though this is necessary for practical purposes (to achieve the required data-rates), it goes against the dominant paradigm of networking: to allow many computers to share data. HIPPI-SC was developed as one workable solution to this quandary.
- It allows for a switching mechanism to be built which could allow multiple simultaneous point-to-point connections to occur

 U1.163

High Speed LANs – HIPPI

Mapping HIPPI to Other Protocols

- **HIPPI-LE(Link Encapsulation)** provides mapping of IEEE 802.2 LLC headers to the D1_Area and the beginning of the D2_Area
- **HIPPI-FC(Fibre Channel)** maps Fibre Channel products to the HIPPI-FP standard. This standard seems to be rather unimportant
- **HIPPI-IPI(Disk & Tape Commands)** maps IPI-x standard command-sets into HIPPI-FP headers.This standard may also disappear: it may be incorporated into the IPI standards instead of retaining a set of separate HIPPI-IPI standards.

 U1.164

High Speed LANs – HIPPI

HIPPI Connection Management

Three such policies are considered:

1. Centralized–

- One centralized, distinct management system, closely integrated with the switches, maintains all connection management information for the entire network. When a connection is established or broken,
- this system performs the next assignments which need to be made.

 U1.165

High Speed LANs – HIPPI

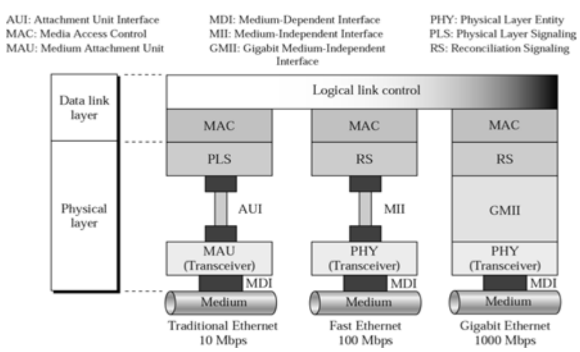
2. ***Broadcast–***

- *A separate bus-type communications system allows nodes to broadcast information* regarding the HIPPI links, and therefore manage connections by policies built upon this shared knowledge..

3. ***Distributed–***

- *HIPPI node works with no explicit knowledge of any others. Management* policies are then built upon random waiting and retrying methods.

Three generations of Ethernet



Traditional Ethernet

MAC Sublayer

Physical Layer

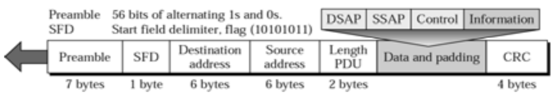
Physical Layer Implementation

Bridged Ethernet

Switched Ethernet

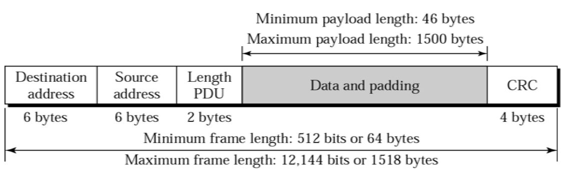
Full-Duplex Ethernet

MAC frame



 U1.169

Minimum and Maximum Length



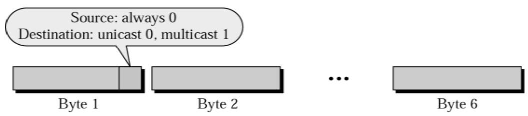
 U1.170

Ethernet Addresses

06-01-02-01-2C-4B

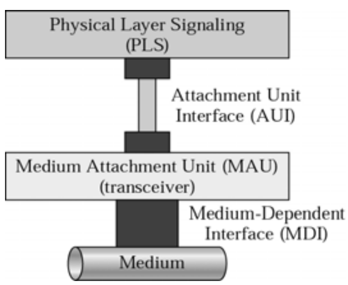
 U1.171

Unicast and Multicast Addresses



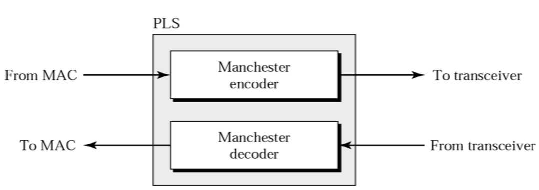
 U1.172

Physical layer



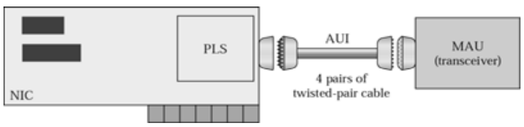
 U1.173

PLS

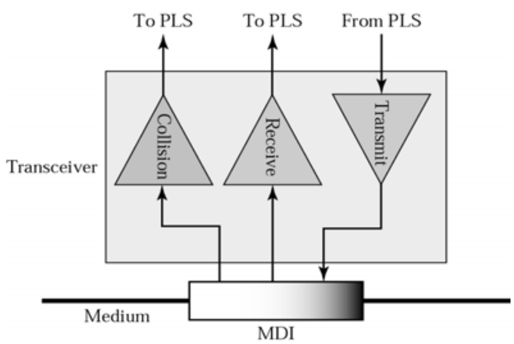


 U1.174

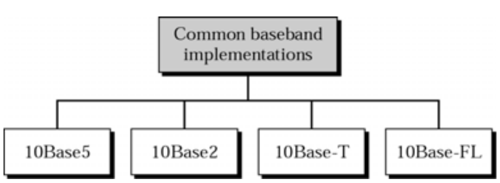
AUI



MAU (Transceiver)



Categories of Traditional Ethernet



Categories of Traditional Ethernet

Name	Segment Length (Max.)	Cable
10Base5	500m / 1640ft.	RG-8 or RG-11 coaxial
10Base2	185m / 606ft.	RG 58 A/U or RG 58 C/U coaxial
10Base-T	100m / 328ft.	Category 3 or better unshielded twisted pair

 U1.178

Categories of Traditional Ethernet

•**Ethernet cables** likewise are manufactured to any of several standard specifications.

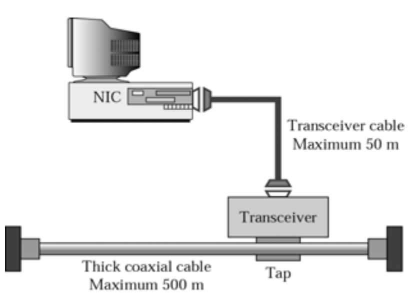
•The most popular Ethernet cable in current use, Category 5 or CAT5, supports both traditional and Fast Ethernet.

•The Category 5e (CAT5e) cable supports Gigabit Ethernet.

•To connect Ethernet cables to a computer, a person normally uses a network adapter, also known as a network interface card (NIC).

 U1.179

Connection of a Station



 U1.180

Connection of a Station

Fast Ethernet

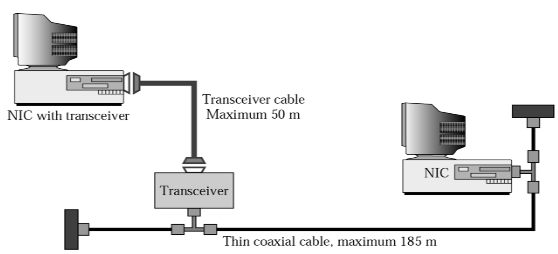
•In the mid-1990s, Fast Ethernet technology matured and met its design goals of a) increasing the performance of traditional Ethernet while b) avoiding the need to completely re-cable existing Ethernet networks.

•Fast Ethernet comes in two major varieties:

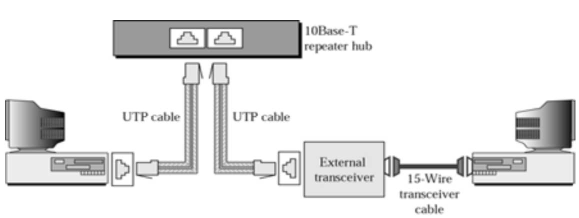
•100Base-T (using unshielded twisted pair cable)

•100Base-FX (using fiber optic cable)

Connection of Stations



Connection of Stations

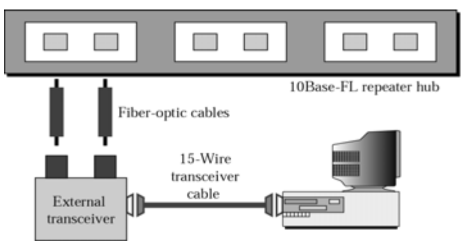


Connection of Stations

- Whereas Fast Ethernet improved traditional Ethernet from 10 Megabit to 100 Megabit speed,
- Gigabit Ethernet boasts the same order-of-magnitude improvement over Fast Ethernet by offering speeds of 1000 Megabits (1 Gigabit).
- Gigabit Ethernet was first made to travel over optical and copper cabling, but the 1000Base-T standard successfully supports it as well.
- 1000Base-T uses Category 5 cabling similar to 100 Mbps Ethernet, although achieving gigabit speed requires the use of additional wire pairs.

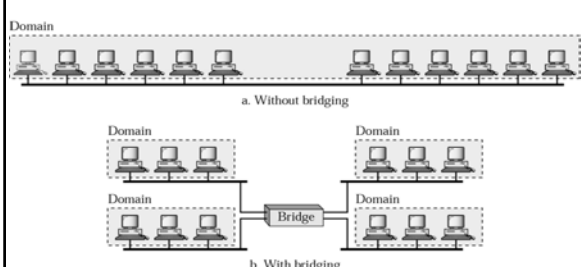
 U1.184

Connection of Stations



 U1.185

Collision Domains



 U1.186

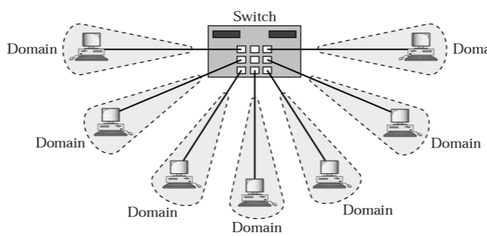
Switched Ethernet

Switched Ethernet

- An Ethernet switch is a bridge which can connect more than two segments together.
- The idea behind a switch is that it removes all unneeded traffic from each segment by only forwarding the traffic needed on that segment, which provides better performance on the network.

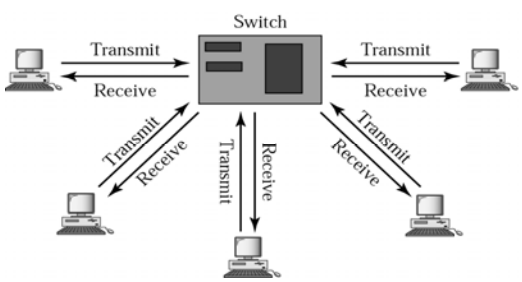
© Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi-63 by Vishal Jain U1.187

Switched Ethernet



© Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi-63 by Vishal Jain U1.188

Full-Duplex Switched Ethernet



© Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi-63 by Vishal Jain U1.189

Fast Ethernet

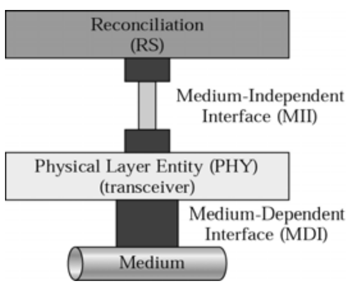
MAC Sublayer

Physical Layer

Physical Layer Implementation

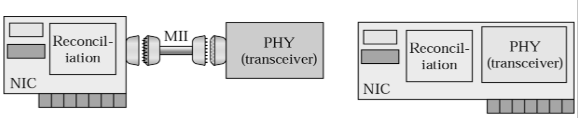
 U1.190

Fast Ethernet Physical Layer



 U1.191

MII

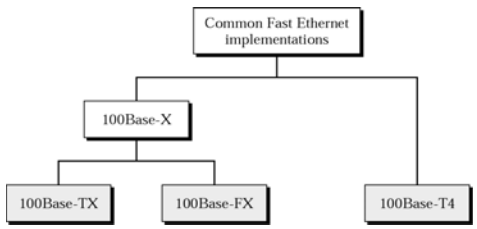


a. MII is needed for external transceiver

b. MII is not needed for internal transceiver

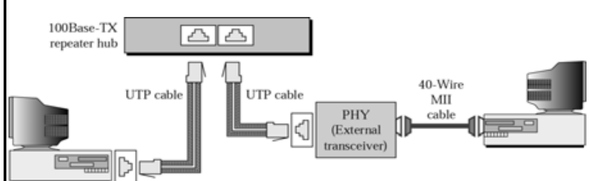
 U1.192

Fast Ethernet Implementations



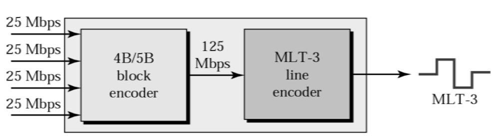
 U1.193

100Base-TX Implementation



 U1.194

Encoding and Decoding



 U1.195

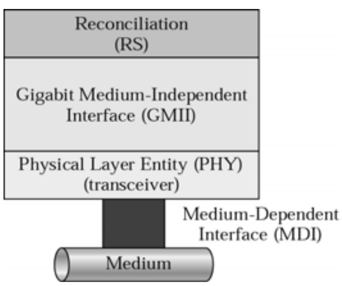
Gigabit Ethernet

MAC Sublayer

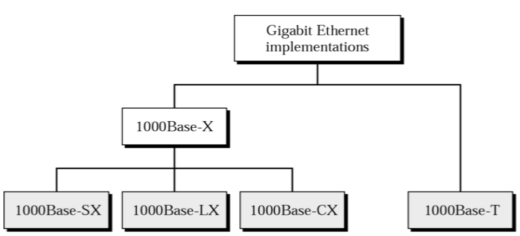
Physical Layer

Physical Layer Implementation

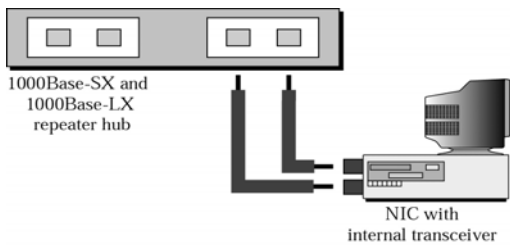
Physical layer in Gigabit Ethernet



Gigabit Ethernet Implementations

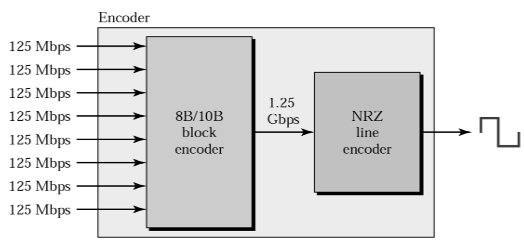


1000Base-X Implementation



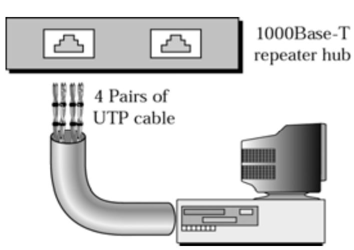
 U1.199

Encoding in 1000Base-X



 U1.200

1000Base-T Implementation



 U1.201

Wireless Ethernet

Architecture

Physical Layer

MAC Layer

Addressing Mechanism

 U1.202

Wireless LANs

Some of the advantages are mentioned below :

Availability of low-cost portable equipments:

- Due to the technology enhancements, the equipment cost that are required for WLAN set-up have reduced a lot.

Mobility:

- An increasing number of LAN users are becoming mobile. These mobile users require that they are connected to the network regardless of where they are because they want simultaneous access to the network.

 U1.203

Wireless LANs

Installation speed and simplicity:

- Wireless LANs are very easy to install. There is no requirement for wiring every workstation and every room.

Installation flexibility:

- If a company moves to a new location, the wireless system is much easier to move than ripping up all of the cables that a wired system would have snaked throughout the building.
- This also provides portability. Wireless technology allows network to go anywhere wire cannot reach.

 U1.204

Wireless LANs

Reduced cost of ownership:

- While the initial cost of wireless LAN can be higher than the cost of wired LAN hardware, it is envisaged that the overall installation expenses and life cycle costs can be significantly lower.

Scalability:

- Wireless LAN can be configured in a variety of topologies to meet the users need and can be easily scaled to cover a large area with thousands of users roaming within it.

IEEE 802.11 Architecture

IEEE has defined the specifications for a Wireless LAN, called IEEE 802.11, which covers the physical and data link layers.

The standard defines two kinds of services :

- BSS (Basic Service Set)
- ESS (Extended Service Set)

IEEE 802.11 Architecture

BSS

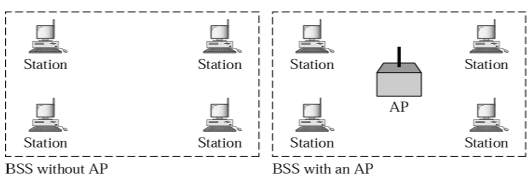
- IEEE 802.11defines the BSS as the building block of a wireless LAN.
- A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).
- BSS without an AP is stand alone network and can not send data to other BSSs.
- It is called an **ad-hoc network** architecture.

IEEE 802.11 Architecture

- In this architecture, stations can form a network without the need of an AP.
- They can locate one another and agree to be part of a BSS.
- A BSS with an AP is sometimes referred to as an **infrastructure network.**

 U1.208

BSSs



 U1.209

IEEE 802.11 Architecture

ESS

- An ESS is made up of two or more BSSs with APs.
- In this case, the BSSs are connected through a distribution system, which is usually a wired LAN.
- The distribution system connects the APs in the BSSs.
- IEEE 802.11 des not restrict the distribution system; it can be any IEEE LAN such as Ethernet.

 U1.210

IEEE 802.11 Architecture

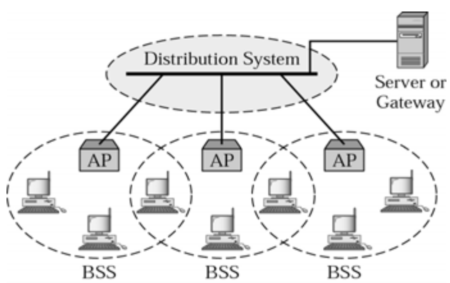
The extended service set uses two types of stations :

Mobile :- Mobile stations are normal stations inside a BSS.

Stationary :- Stationary stations are AP stations that are part of a wired LAN.

 U1.211

ESS



 U1.212

ESS

- When BSSs are connected, the stations within reach of one another can communicate without the use of an AP.
- However, communication between two stations in two different BSSs usually occurs via two APs.
- The idea is similar to communication in a cellular network if we consider each BSS to be cell.
- Each AP to be a base station.
- Note that a mobile station can belong to more than one BSS at the same time.

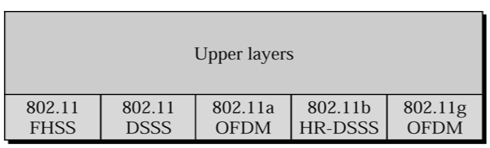
 U1.213

Station Types

IEEE 802.11, defines three types of stations based on their mobility in a wireless LAN

- **No-transition** – A station with no-transition mobility is either stationary or moving only inside a BSS
- **BSS-transition** – A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS.
- **ESS-transition** – A station with ESS-transition mobility can move from one ESS to another.

Physical Layer Specifications



Physical layer

FHSS

- The idea behind spread spectrum is to *spread the signal over a wider frequency band*, so as to make jamming and interception more difficult and to minimize the effect of interference from other devices
- In FH it is done by transmitting the signal over a random sequence of frequencies; that is, first transmitting at one frequency, then second, then a third and so on.
- The random sequence of frequencies is generated with the help of a pseudorandom number generator.

FHSS

- As both the receiver and sender use the same algorithm to generate random sequence, both the devices hop frequencies in a synchronous manner and frames transmitted by the sender are received correctly by the receiver.
- This is somewhat similar to sending different parts of one song over several FM channels.
- Eavesdroppers hear only unintelligible blips and any attempt to jam the signal results in damaging a few bits only.

DSSS

- With direct sequence spread spectrum the transmission signal is spread over an allowed band (for example 25MHz).
- A random binary string is used to modulate the transmitted signal. This random string is called the ***spreading code***.
- The data bits are mapped to into a pattern of "chips" and mapped back into a bit at the destination.
- The number of chips that represent a bit is the ***spreading ratio***.

DSSS

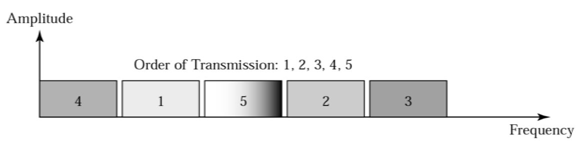
- The higher the spreading ratio, the more the signal is resistant to interference.
- The lower the spreading ratio, the more bandwidth is available to the user.
- The FCC dictates that the spreading ratio must be more than ten.
- Most products have a spreading ratio of less than 20 and the new IEEE 802.11 standard requires a spreading ratio of eleven.
- The transmitter and the receiver must be synchronized with the same spreading code.

DSSS

- If orthogonal spreading codes are used then more than one LAN can share the same band.
- However, because DSSS systems use wide sub channels, the number of co-located LANs is limited by the size of those sub channels.
- Recovery is faster in DSSS systems because of the ability to spread the signal over a wider band.

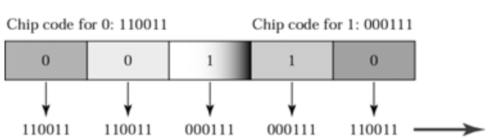
 U1.220

FHSS



 U1.221

DSSS



 U1.222

MAC layers in IEEE 802.11 standard

Medium Access Control

- Most wired LANs products use Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as the MAC protocol.
- Carrier Sense means that the station will listen before it transmits.
- If there is already someone transmitting, then the station waits and tries again later.
- If no one is transmitting then the station goes ahead and sends what it has. But when more than one station tries to transmit, the transmissions will collide and the information will be lost.
- This is where Collision Detection comes into play.

MAC layers in IEEE 802.11 standard

- The station will listen to ensure that its transmission made it to the destination without collisions.
- If a collision occurred then the stations wait and try again later.
- The time the station waits is determined by the back off algorithm.
- This technique works great for wired LANs but wireless topologies can create a problem for CSMA/CD.

MAC layers in IEEE 802.11 standard

However, the wireless medium presents some unique challenges not present in wired LANs that must be dealt with by the MAC used for IEEE 802.11. Some of the challenges are:

- The wireless LAN is prone to more interference and is less reliable.
- The wireless LAN is susceptible to unwanted interception leading to security problems.
- There are so called *hidden station and exposed station problems.*

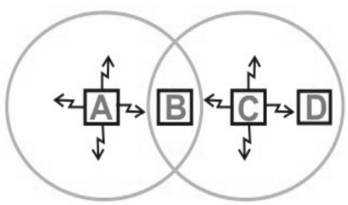
MAC layers in IEEE 802.11 standard

The Hidden Station Problem

- Consider a situation when A is transmitting to B, as depicted in the Fig.
- If C senses the media, it will not hear anything because it is out of range, and thus will falsely conclude that no transmission is going on and will start transmit to B.
- The transmission will interfere at B, wiping out the frame from A.
- The problem of a station not been able to detect a potential competitor for the medium because the competitor is too far away is referred as *Hidden Station Problem*. ***As in the described scenario C act as a hidden station to A, which is also competing for the medium.***

 U1.226

MAC layers in IEEE 802.11 standard



 U1.227

MAC layers in IEEE 802.11 standard

Exposed Station problem

- Now consider a different situation where B is transmitting to A, and C sense the medium and detects the ongoing transmission between B and A.
- C falsely conclude that it can not transmit to D, when the fact is that such transmission would cause on problem.
- A transmission could cause a problem only when the destination is in zone between B and C.
- This problem is referred as ***Exposed station Problem.***

 U1.228

MAC layers in IEEE 802.11 standard

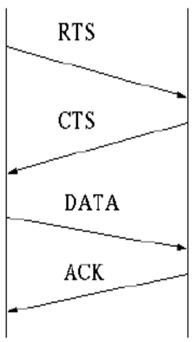
- In this scenario as B is exposed to C, that's why C assumes it cannot transmit to D.
- So this problem is known as Exposed station problem (i.e. problem caused due to exposing of a station).
- The problem here is that before transmission, a station really wants to know that whether or not there is any activity around the receiver.
- CSMA merely tells whether or not there is any activity around the station sensing the carrier.
- The solution to these problems is Carrier Sense Multiple Access with Collision Avoidance or CSMA/CA.

 U1.229

MAC layers in IEEE 802.11 standard

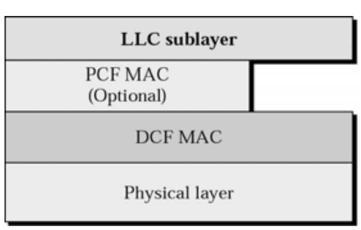
Main steps can be summarized as:

- Sender sends a short frame called *Request to send RTS (20bytes) to the destination. RTS also contains the length of the data frame.*
- Destination station responds with a short (14 bytes) *clear to send (CTS) frame.*
- After receiving the CTS, the sender starts sending the data frame.
- If collision occurs, CTS frame is not received within a certain period of time.



 U1.230

MAC layers in IEEE 802.11 standard



 U1.231

MAC layers in IEEE 802.11 standard

IEEE 802.11 defines two MAC sublayers

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

MAC layers in IEEE 802.11 standard

DCF (Distributed Coordination Function)

DCF uses CSMA/CA as the access method. Wireless LANs can not implement CSMA/CD due to following reasons :

- Costly stations and increased bandwidth requirements.
- Hidden station problem
- Signal fading – if distance is great

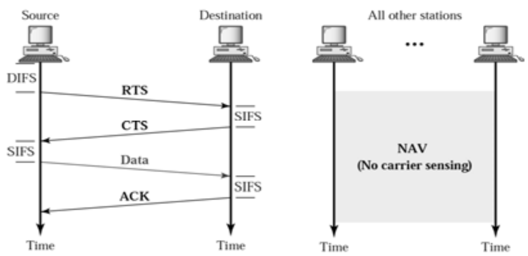
CSMA/CA flowchart

CSMA/CA Process

- **DIFS** – Distributed Inter frame Space – After the station is found to be idle, the station waits for a period of time.
- **RTS** – Request to Send – after receive DIFS , then the station sends a control frame, RTS
- After receiving the RTS and waiting a period of time called the SIFS (short inter frame space)
- Then the destination station sends a control frame, called the clear to send (CTS).

 U1.235

CSMA/CA and NAV



 U1.236

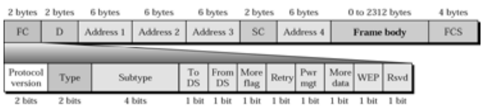
PCF

Point Coordination Function

- It is an optional access method that can be implemented in an infrastructure network (not in an ad-hoc network).
- It is implemented on top of the DCF and is used mostly for time-sensitive transmission.
- PCF has centralized, contention free polling access method.
- The AP performs polling for stations that are being polled.
- The stations are polled one after another, sending any data they have to the AP.

 U1.237

Frame format



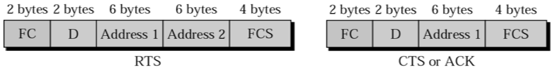
 U1.238

Subfields in FC field

Field	Explanation
Version	The current version is 0.
Type	Type of information: management (00), control (01), or data (10).
Subtype	Defines the subtype of each type (see).
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.

 U1.239

Control frames



 U1.240

Control frames

Values of Subfields in Control Frames

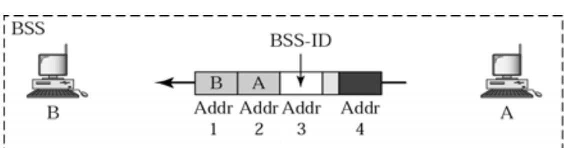
Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

Control frames

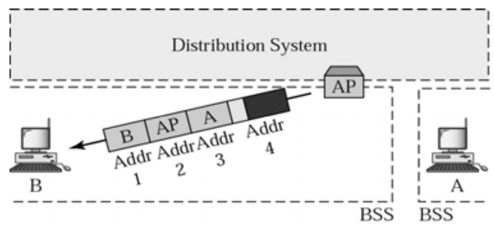
Subfields in FC Field

To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination station	Source station	BSS ID	N/A
0	1	Destination station	Sending AP	Source station	N/A
1	0	Receiving AP	Source station	Destination station	N/A
1	1	Receiving AP	Sending AP	Destination station	Source station

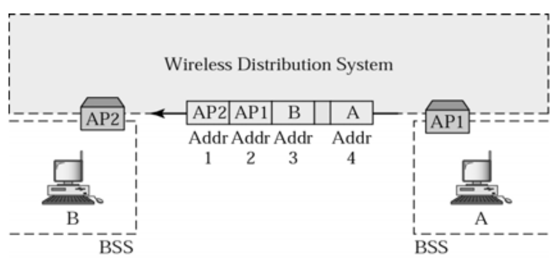
Addressing Mechanism: Case 1



Addressing Mechanism: Case 2



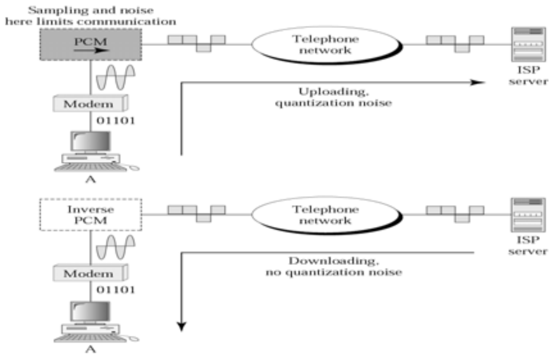
Addressing Mechanism: Case 3



Fast Access Technologies

- A second type of network we encounter in the Internet is the point-to-point wide area network.
- A point-to-point WAN connects two remote devices using a line available from a public network such as a telephone network.

56K Modem



 U1.247

56K Modem

56K Modem —

- A traditional modem is used to connect end users of the Internet from home or small businesses to an ISP
- A development in the modem is 56K modem (DTR is 56 Kbps) which uses the existing telephone line.

 U1.248

56K Modem

Digital Subscriber Line (DSL) —

- A technology that uses the existing telecommunication networks to achieve high-speed delivery of different forms of communication is called as Digital Subscriber Line (DSL).
- The communication network can be a local loop telephone line which is a connection between the telephone company and the subscriber resident.
- The different forms of communication are data, voice, video and multimedia. DSL is basically a family of technologies.

 U1.249

56K Modem

Asymmetric Digital Subscriber Line (**ADSL**) —

- It provides higher bit rates in the downstream direction than the upstream direction.
- Thus, it is called as asymmetrical. The subscribers usually want to receive high volume files quickly from the Internet.
- They usually have small files to send such as an e-mail message.

 U1.250

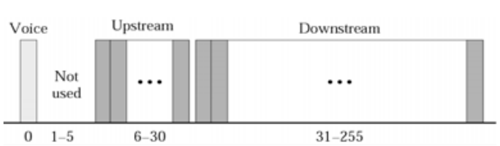
56K Modem

ADSL is an asymmetric communication technology designed for residential users; it is not suitable for businesses.

 U1.251

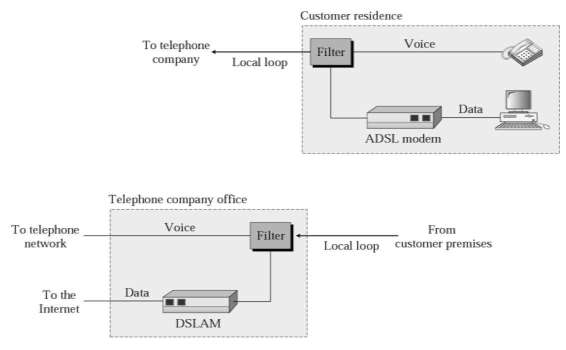
56K Modem

Bandwidth Division



 U1.252

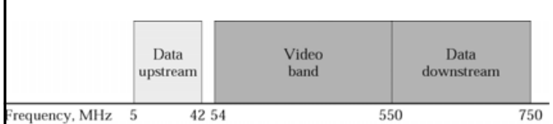
ADSL



 U1.253

ADSL

Cable Bandwidth



 U1.254

ADSL

High Bit Rate Digital Subscriber Line (HDSL) —

- It was designed as an alternative to the T-1 line (1.544 Mbps).
- It has a restriction of 1 km length. However, HDSL can operate at lengths up to 3.6 km.

Symmetric Digital Subscriber Line (SDSL) —

- It is also called as single-line digital subscriber line.
- To achieve the same data rate as HDSL, it uses one single twisted pair cable which is available to most of the residential subscribers.
- To create a full-duplex transmission, it employs a technique called as echo cancellation.

 U1.255

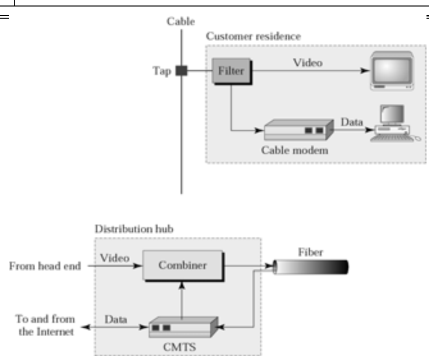
ADSL

Very High Bit Rate Digital Subscriber Line (VDSL) —

For short distances (300 to 1800 meters), it uses coaxial, fiber-optic or twisted pair cable. With VDSL, a bit rate of 50 to 55 Mbps downstream and 1.5 to 2.5 Mbps upstream can be achieved.

 U1.256

Cable Modem



 U1.257

Cable Modem

- A modem designed to operate over cable TV lines.
- Because the coaxial cable used by cable TV provides much greater bandwidth than telephone lines, a cable modem can be used to achieve extremely fast access to the World Wide Web.
- This, combined with the fact that millions of homes are already wired for cable TV, has made the cable modem something of a holy grail for Internet and cable TV companies.

 U1.258

WiFi

- Wireless Fidelity, better known as Wi-Fi, is a term used to describe the underlying technology of wireless local area networks (WLAN) based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards.
- Initially intended to connect mobile computing devices in local area networks (LAN), Wi-Fi applications have grown to include various data, voice, and video services such as Internet access and Voice over Internet Protocol (VoIP).
- With the growing popularity of small portable devices, a wireless network connection proves more beneficial by minimizing expensive.

 U1.259

WiFi

- In addition, various IEEE 802.11 standards now in development are aimed to increase the performance of Wi-Fi networks and to provide users with greater flexibility in wireless communications.
- Wi-Fi technology platform is based on single-carrier direct-sequence spread spectrum (DSSS) and multi-carrier Orthogonal Frequency Division Multiplexing (OFDM) radio technologies to transmit and receive signals.
- The original version of the standard, now referred to as “802.11legacy,” was released in 1997 and had specified a maximum data rate of 2 Megabits per second (Mbps).

 U1.260

WiFi

- The IEEE 802.11 standards family consists of many amendments and service enhancements to the original standard, with the most popular being the “a,” “b,” and “g” standards.
- Although the 802.11a standard was the first standard created in the 802.11 family, the 802.11b standard became the first widely accepted wireless networking standard, later followed by 802.11a and 802.11g.

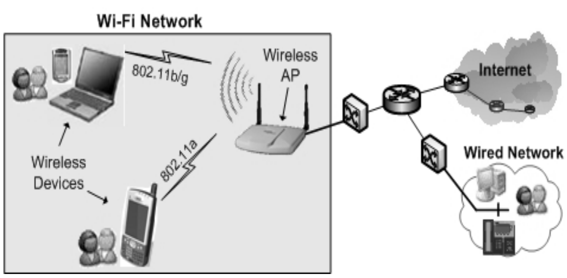
 U1.261

WiFi

- Wi-Fi is more commonly used in point-to-multipoint (PMP) environments to allow extended network connectivity (e.g., private/backbone network, Internet) of multiple portable devices such as laptops, telephones, or PDAs.
- Wi-Fi also allows connectivity in point-to-point (P2P) mode, which enables devices to directly connect and communicate to each other. .

 U1.262

WiFi



 U1.263

WiFi

Technology	**Wi-Fi**
Features	• WLANs (e.g., indoor, office, campus environment) • PMP mode, with each client connected to an AP; P2P mode, with each mobile user connected directly to each other • Can operate in line-of-sight and non line-of-sight situations • Supports fixed, portable and mobile communications

 U1.264

WiFi

Access

- Wi-Fi networks typically consist of one or more APs and one or more clients.
- An AP will broadcast its Network Name, also referred to as the "Service Set Identifier" (SSID), through data packets, called beacons, every 100 milliseconds (ms).
- Beacons are transmitted at a rate of 1 Mbps to ensure that the connected user receiving the beacon is actually provided an expected data rate of at least 1 Mbps .

.

WiFi

- The Wi-Fi standard enables users to decide whether to connect to an AP.
- The firmware installed in the Wi-Fi client adapter card also has an influence during the connection process.
- If two APs of the same SSID are in range of the client, the firmware may automatically decide which of the two APs it will connect to based on signal strength.

WiFi

Media Access Control and Physical Layers

- The 802.11a, 802.11b, and 802.11g Wi-Fi amendments all use the same Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) signaling method in the media access control (MAC) layer as defined in the original 802.11 standard.
- The difference between the three standards lies in the physical (PHY) layer and with the modulation technique used to transmit a signal.

WiFi

- The 802.11b amendment employs complementary code keying (CCK), which is a direct extension of the DSSS modulation technique .
- Conversely, 802.11a uses OFDM technology, which results in an increase in channel availability and data rate performance.
- 802.11g utilizes both techniques depending on the application need for a particular situation.

WiFi

Technical Feature	Primary Wi-Fi Technology		
	802.11a	802.11b	802.11g
Security	WEP, WPA	WEP, WPA	WEP, WPA
Frequency Band/ Channel Modulation	5 GHz/ OFDM	2.4 GHz / 11 Channels, DSSS with CCK	2.4 GHz/ OFDM above 20Mbps, DSSS with CCK below 20Mbps
Range and Coverage (commonly advertised)	shorter range than 802.11b (~225 feet)	300 feet (indoors) 1000 feet (outdoors)	300 feet (indoors) 1000 feet (outdoors)
Data Rate	Up to 54Mbps	Up to 11Mbps	Up to 54Mbps
Quality of Service (QoS)	Supports 802.11e	Supports 802.11e	Supports 802.11e
Scalable	Yes	Yes	Yes

WiFi

WEP - Wired Equivalent Privacy

WPA - Wi-Fi Protected Access

DSSS - Direct-Sequence Spread Spectrum

CCK – Complementary Code Keying

OFDM - Orthogonal Frequency Division Multiplexing

WiFi

Frequencies and Channels
Two major frequencies are used in Wi-Fi networks:

- 2.4-Gigahertz (GHz) Industrial, Scientific, Medical (ISM) band
- 5-GHz Unlicensed National Information Infrastructure (UNII) band.

WiFi

- The 2.4-GHz band is used by 802.11, 802.11b, and 802.11g wireless devices.
- Operating in the unlicensed 2.4 GHz band can allow 802.11b/g signals to become susceptible to interference from other devices operating on the same frequency, such as microwaves, cordless telephones, and Bluetooth.

WiFi

- The 5-GHz band, which is used for 802.11a wireless devices, is further divided into three bands: lower, middle, and upper.
- These bands use 100 MHz of spectrum, with each band providing four non-overlapping channels and subject to less interference than 802.11b and 802.11g devices.
- Where 2.4 GHz operating devices use FHSS or DSSS signal coding techniques, wireless devices operating in the 5 GHz range use OFDM signal coding.
- Using a higher carrier frequency results in 802.11a signals being absorbed more readily by its surroundings.

WiFi

Advantages of Wi-Fi

- Network connections based on the Wi-Fi platform present many benefits to clients, especially in the areas of ease of deployment, cost, and flexibility.
- Wi-Fi technology does not require the use of wires to set up a LAN. Thus, Wi-Fi networks are easier and quicker to install compared with traditional wired LANs.
- This feature can be useful in emergency situations where communications must be established in a short period of time.
- Wi-Fi also offers users situated in locations not accessible by wires with an alternative method for easily connecting to a nearby network.

 U1.274

WiFi

Disadvantages of Wi-Fi

- Although Wi-Fi technology is growing in popularity, a few challenges need to be considered.
- Wi-Fi networks are limited in range, and thus are commonly used in localized regions. As mentioned earlier, commonly vendor-advertised 802.11b/g AP routers can cover roughly 300 feet indoors and 1,000 feet outdoors.
- Range also varies according to the frequency band used, where the 2.4 GHz band (802.11b/g) has a greater range than the 5 GHz band (802.11a).

.

 U1.275

WiFi

- Users interested in certain voice and video services (e.g., VoIP) should consider expanding the coverage area by either mounting more APs or connecting multiple hotspots using other wireless technologies (e.g., WiMAX, Wireless Mesh) because mobile coverage, especially in rural areas, could span miles or tens of miles.
- Another setback with Wi-Fi regards the overloading of APs. Wi-Fi can handle tens of communicating clients simultaneously per AP.

 U1.276

WiFi

Media Access Control

- Whereas traditional wired Ethernet protocols use the Carrier Sense Multiple Access/Collision Detection (CSMA/CD) signaling method, the 802.11a protocol uses the same CSMA/CA media access method as defined in the original 802.11 standard.
- CSMA/CA is a method used to avoid two signals colliding and canceling out each other.
- The process starts with the sending station sensing the air for activity. If the channel is busy, the transmission is scheduled for later, at which point the channel is sensed again

WiFi

- If no activity is detected, the station waits an additional random period of time and then transmits information if the medium is still free.
- The receiving station sends a packet acknowledgement (ACK) frame back to the sending station after it obtains the data packet intact.
- The process is complete when the sending station receives the ACK frame.
- If the ACK frame is not detected by the sending station.

WiFi

- An optional request to send/clear to send (RTS/CTS) protocol is also available at the 802.11a media access control (MAC) layer.
- In general, the MAC layer manages and maintains communications between 802.11 stations (e.g., radio network cards and access points) by coordinating access to a shared radio channel and utilizing protocols that enhance communications over a wireless medium.

WiFi

- The RTS/CTS feature significantly reduces the chances for collision and is used for larger size packets, where retransmission would be expensive from a bandwidth standpoint.
- A sending station requests authorization to transmit for a specific amount of time by broadcasting an RTS frame before sending any information.
- If approved, the receiving device broadcasts a CTS frame, at which point the sending machine can transmit its information without any chance of collision

 U1.280

Wimax

- WiMAX describes the technology based on the Institute of Electrical and Electronic Engineers (IEEE) 802.16 family of standards for metropolitan area networks (MAN).
- Originally known as WirelessMAN, the 802.16 standards were labeled WiMAX by the WiMAX Forum, an industry group composed of leading service providers and communications component and equipment companies.
- The original 802.16 standard, published in April 2002, specified fixed point-to-multipoint (PMP) broadband wireless systems operating in the 10–66 gigahertz (GHz) licensed spectrum.

 U1.281

Wimax

- This amendment was updated in July 2004, with the release of 802.16-2004 (also known as 802.16d), to align the standard with aspects of the European Telecommunications Standards Institute (ETSI) HIPERMAN standard as well as lay down conformance and test specifications
- WiMAX is a rather new technology and is intended to provide line-of-sight (LOS) service coverage of 30 miles from a base station to a subscriber station.

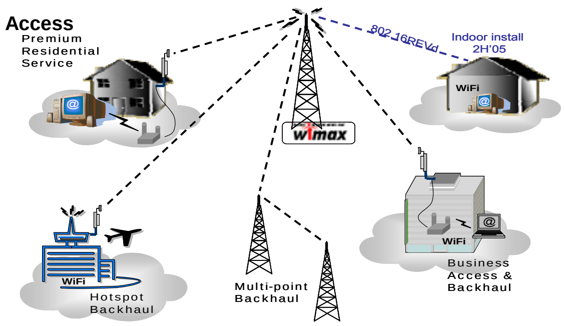
 U1.282

Wimax

- WiMAX can also be implemented in a wireless mesh network, which is a decentralized, reliable, resilient, and relatively inexpensive type of Internet infrastructure, to provide connectivity to external servers.
- Mesh networks consist of several nodes that act as repeaters to transmit data from nearby nodes to users located far away, resulting in networks that span large distances.

 U1.283

Wimax



 U1.284

Wimax

- WiMAX operates similarly to Wi-Fi technology but at higher speeds, over larger distances, and accommodates more wireless users.
- As illustrated in Figure , a typical WiMAX system consists of a WiMAX-enabled base station or tower, and a subscriber station or receiver.
- WiMAX towers are implemented by service providers and can provide a wireless service footprint as large as 2,500 square miles, similar in concept to cellular communications towers

 U1.285

Wimax

- This capability provides broadband wireless access for users in remote rural areas, which can be difficult to reach with wires used by traditional telephone and cable companies.
- Initially, WiMAX receivers and antennas will consist of a small box or Personal Computer Memory Card International Association (PCMCIA) card, and eventually will be developed into portable devices that will be comparable to Wi-Fi-enabled products (e.g., laptops, telephones, PDA) on the market today

 U1.286

Wimax

- Depending on the scenario, WiMAX towers can be deployed in either P2P or PMP architectures, resulting in variations in throughput based on the number of subscribers.
- The WiMAX base station can connect to the network backbone using a high-bandwidth, wired line (e.g., T3 line), or it can connect to another tower using a LOS microwave link, often referred to as backhaul
- Using an external antenna, base stations can send and receive high-speed data and voice to/from subscriber equipment, thereby eliminating extensive and expensive wireline infrastructures.

 U1.287

Wimax

- By using different frequencies,
- WiMAX can offer two primary forms of wireless services, LOS and NLOS.
- In LOS mode, a fixed dish antenna is pointed directly at the WiMAX base station from a rooftop or window.
- The transmissions are stronger and more stable because higher frequencies in the 10–66 GHz range can used, in which case, there is less interference and more bandwidth.

 U1.288

Wimax

- On the other hand, NLOS service uses the 2–11 GHz range (similar to Wi-Fi) to transmit data because lower-wavelength transmissions are subject to fewer disruptions from physical obstructions.
- This is an improvement from earlier wireless technologies (e.g., local multipoint distribution system [LMDS] and multichannel multipoint distribution system [MMDS]), which were unable to provide NLOS service.

Wimax

Media Access Control

- The 802.16 media access control (MAC) layer, which is designed for PMP broadband wireless access, employs a grant-request mechanism to allow users into the network.
- A subscriber station initially makes a request to the base station for an uplink slot.
- Based on the service-level agreement, the base station decides whether or not to allocate a time slot, which is intended solely for the subscriber station that made the request

Wimax

- The 802.16 media access control (MAC) layer, which is primarily responsible for efficiently managing the resources of the airlink between a base station and subscriber station, is designed for point to multipoint (PMP) broadband wireless access.
- The MAC layer provides algorithms for allocating required bandwidth, associating traffic parameters, and transporting and routing data to the appropriate sublayer.
- In addition to bandwidth allocation and data transport, the MAC layer has a privacy sublayer that offers access and connection establishment authentication to avoid service theft and supports encryption and key exchange to ensure data privacy and confidentiality .

Wimax

Major difference between WiMAX and Wi-Fi

- In Wi-Fi, the MAC layer uses contention access with mechanisms such as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) or Carrier Sense Multiple Access with Collision Detection (CSMA/CD).
- All users in wireless local area networks (WLAN) employing these mechanisms essentially compete for a wireless access point's (AP) attention on a random interrupt basis.

Wimax

- In cases where there are fewer than 10 users per AP, occasional packet collisions may occur requiring retransmissions, but the resulting overhead does not waste a significant amount of bandwidth.
- However, when the number of users rises into the hundreds, the increased number of collisions and retransmissions can result in noticeable delays, which negatively affect streaming-media services such as voice and video applications

Wimax

- In contrast, WiMAX avoids such issues by using a grant-request mechanism, in which the user only competes once for initial entry into the network.
- The base station evaluates the subscriber station's request in the context of the subscriber's service-level agreement and allocates an uplink slot in which the user can transmit data.
- This time slot can enlarge and contract, but remains assigned to the subscriber station, prohibiting other clients from using it.
- In addition, the base station controls quality of service (QoS) parameters by balancing the time-slot assignments among the application needs of the subscriber stations .

Wimax

- WiMAX supports multiple modulation schemes, including binary phase-shift keying (BPSK), quadrature phase-shift keying (QPSK), 16-QAM, and 64-QAM.
- Each modulation scheme chosen is directly related to distance and is used according to the signal-to-noise (SNR) ratio within the radio link.
- If an acceptable SNR is attained, the system can use the highest throughput modulation (64-QAM), and appropriately switch to lower modulation schemes as the SNR decrease

Wimax

- WiMAX technology can be used to support various applications that include voice communications, video communications, and data services.

Summary

- In Wi-Fi, the MAC layer uses contention access with mechanisms such as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) or Carrier Sense Multiple Access with Collision Detection (CSMA/CD).
- The high speed LANs that have emerged can be broadly categorized into three types based on token passing, successors of Ethernet and based on switching technology.
- In token passing scheme, all stations are logically connected in the form of a ring and control of the access to the medium is performed using a token.

.

Short Questions

1. Describe the token format of FDDI.
2. Explain the basic geometry of DQDB
3. Explain Cable Modem and ADSL.
4. How FHSS works?
5. Differentiate between OSI and TCP/IP.
6. What is the basic difference between CSMA/CD and CSMA/CA?
7. How MAC layer of Wi-Max layer works?
8. Explain seven- layer architecture,
9. What do you mean by Mac protocol Fast access
10. Write a short note on ADSL .

Long Questions

1. Explain the frame format of FDDI. How FDDI media access control works?
2. Differentiate between the working of Token Ring and Token Bus. Explain its frame formats.
3. Compare IEEE 802.11a, 802.11b and 802.11g standards of Wi-Fi.
4. Comparison between FDDI, IEEE802.3 and IEEE802.5
5. What are the different layers of HIPPI? Explain.
6. What do you mean by Hidden Station and Exposed System problem? How we can solve this?
7. Compare CSMA/CD and CSMA/CA.
8. Distinguish between TCP/IP and OSI Model.
9. Explain BSS and ESS in Wireless Networks.
10. Explain the different layers of HIPPI.

References

1. W. ER. Stevens, “TCP/IP illustrated, Volume 1: The protocols”, Addison Wesley,
2. 1994.
3. G. R. Wright, “TCP/IP illustrated volume 2. The Implementation”, Addison Wesley,1995.
4. Frouzan, “TCP/IP Protocol Suite”, Tata Mc Grew Hill, 4th Ed., 2009.
5. William Stalling, “Cryptography and Network Security”, Pearson Publication.
6. James Martin, Joseph Lebin, Kavanagh Chapman “Asynchronous Transfer Mode: ATM Architecture and Implementation”, Prentice Hall PTR, Facsimile Ed.