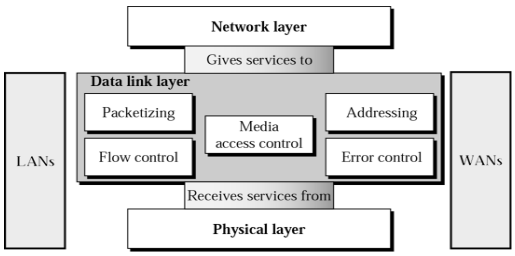
Data Link Layer

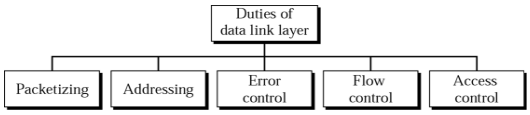
Learning Objectives

- To introduce the design issues of data link layer.
- To discuss different error control methods and flow control protocols
- To discuss protocols of medium access control sublayer
- To discuss Ethernet and Wireless Lan's s
- To discuss Bluetooth

Position of the data-link layer

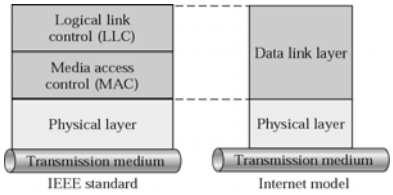


Data Link Layer Duties



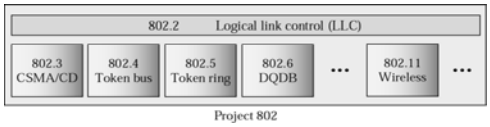
 U2.4

LLC and MAC Sublayers



 U2.5

IEEE standards for LANs



 U2.6

Topics

Error Detection and Correction

Data Link Control and Protocols

Multiple Access

Local Area Networks

Wireless LANs

Switching

 U2.7

Error Detection and Correction

 U2.8

Learning Objectives

- To introduce the types of errors.
- To discuss different error detection methods.
- To discuss parity check, CRC and checksum.
- To discuss different error detection methods.

 U2.9

Cont ….

Note:

Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected.

 U2.10

Types of Error

Single-Bit Error

Burst Error

 U2.11

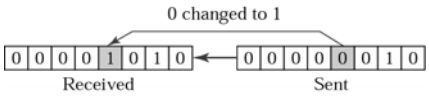
Cont ….

Note:

In a single-bit error, only one bit in the data unit has changed.

 U2.12

Single-Bit Error

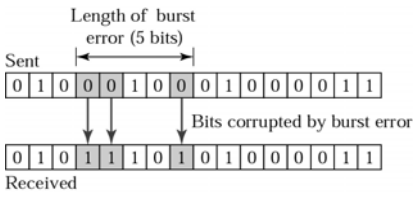


Cont ....

Note:

A burst error means that 2 or more bits in the data unit have changed.

Burst Error of Length 5



Detection

Redundancy

Parity Check

Cyclic Redundancy Check (CRC)

Checksum

 U2.16

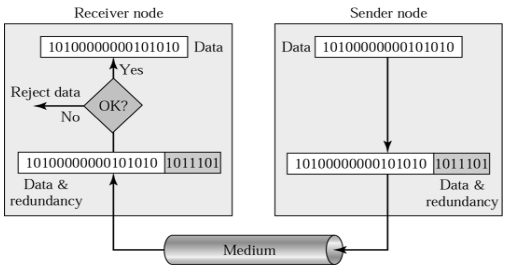
Cont ....

Note:

Error detection uses the concept of redundancy, which means adding extra bits for detecting errors at the destination.

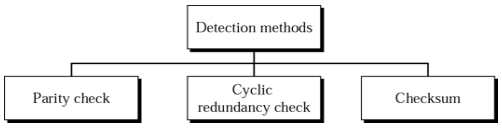
 U2.17

Redundancy



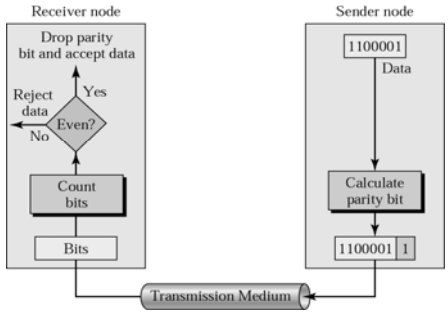
 U2.18

Detection Methods



 U2.19

Even-Parity Concept



 U2.20

Cont ….

Note:

In parity check, a parity bit is added to every data unit so that the total number of 1s is even (or odd for odd-parity).

 U2.21

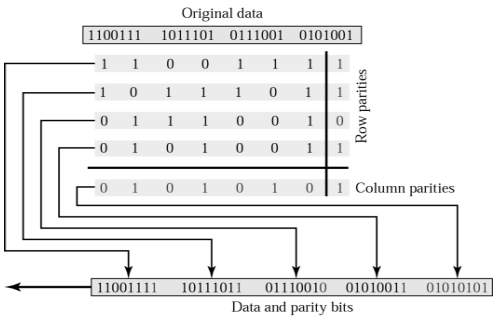
Cont ….

Note:

Simple parity check can detect all single-bit errors. It can detect burst errors only if the total number of errors in each data unit is odd.

 U2.22

Two-Dimensional Parity



 U2.23

Cont ….

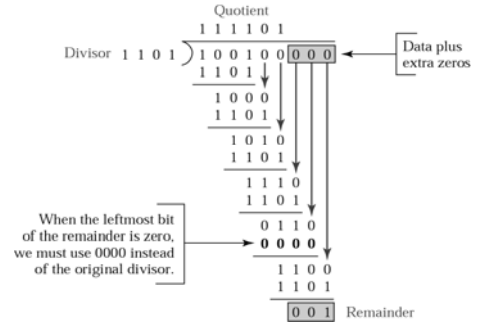
Note:

In two-dimensional parity check, a block of bits is divided into rows and a redundant row of bits is added to the whole block.

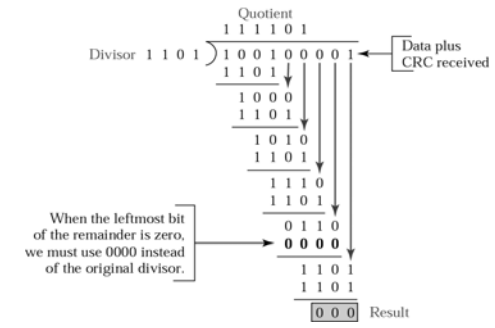
 U2.24

CRC Generator and Checker

Binary Division in a CRC



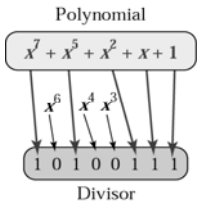
Binary division in CRC checker



A polynomial

$$x^7 + x^5 + x^2 + x + 1$$

A Polynomial Representing a Divisor

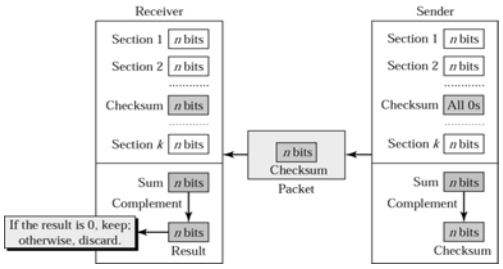


Cont ….

Table Standard polynomials

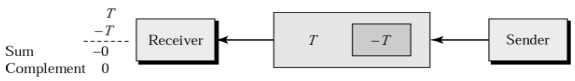
Name	Polynomial	Application
CRC-8	$x^8 + x^2 + x + 1$	**ATM header**
CRC-10	$x^{10} + x^9 + x^5 + x^4 + x^2 + 1$	**ATM AAL**
ITU-16	$x^{16} + x^{12} + x^5 + 1$	**HDLC**
ITU-32	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$	**LANs**

Checksum



 U2.31

Data Unit and Checksum



 U2.32

Cont ….

Note:

The sender follows these steps:

- *The unit is divided into k sections, each of n bits.*
- *All sections are added using one's complement to get the sum.*
- *The sum is complemented and becomes the checksum.*
- *The checksum is sent with the data.*

 U2.33

Cont ....

Note:

The receiver follows these steps:

- *The unit is divided into k sections, each of n bits.*
- *All sections are added using one's complement to get the sum.*
- *The sum is complemented.*
- *If the result is zero, the data are accepted: otherwise, rejected.*

 U2.34

Cont ....

Suppose the following block of 16 bits is to be sent using a checksum of 8 bits.

10101001 00111001

The numbers are added using one's complement

	10101001
	00111001

Sum	11100010
Checksum	**00011101**
The pattern sent is	10101001 00111001 **00011101**

 U2.35

Cont ....

Now suppose the receiver receives the pattern sent in Example 7 and there is no error.

10101001 00111001 00011101

When the receiver adds the three sections, it will get all 1s, which, after complementing, is all 0s and shows that there is no error.

	10101001
	00111001
	00011101
Sum	11111111
Complement	**00000000** means that the pattern is OK.

 U2.36

Cont ….

Now suppose there is a burst error of length 5 that affects 4 bits.

10101**111 11**111001 00011101

When the receiver adds the three sections, it gets

	10101111
	11111001
	00011101
Partial Sum	**1** 11000101
Carry	**1**
Sum	11000110
Complement	**00111001** **the pattern is corrupted.**

Cont ….

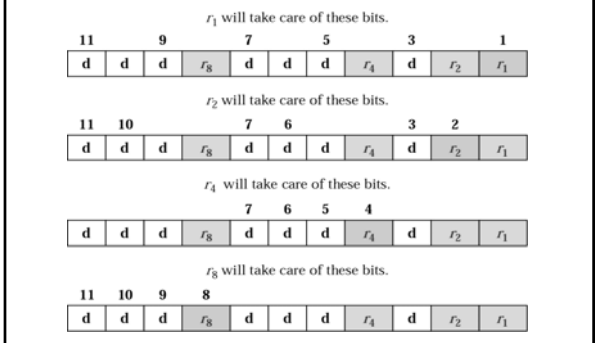
Table 10.2 Data and redundancy bits

Number of data bits m	Number of redundancy bits r	Total bits m + r
1	2	3
2	3	5
3	3	6
4	3	7
5	4	9
6	4	10
7	4	11

Positions of Redundancy Bits

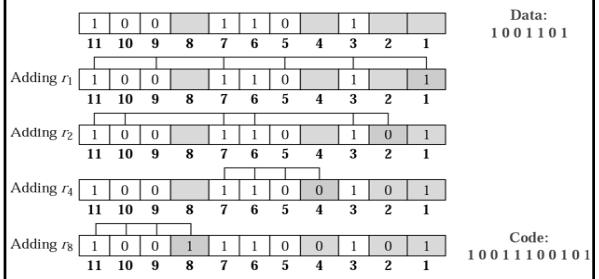
11	10	9	8	7	6	5	4	3	2	1
d	**d**	**d**	r_8	**d**	**d**	**d**	r_4	**d**	r_2	r_1

Redundancy Bits Calculation



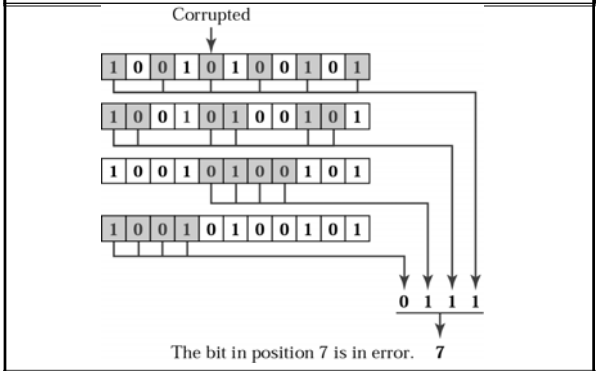
 U2.40

Example of Redundancy



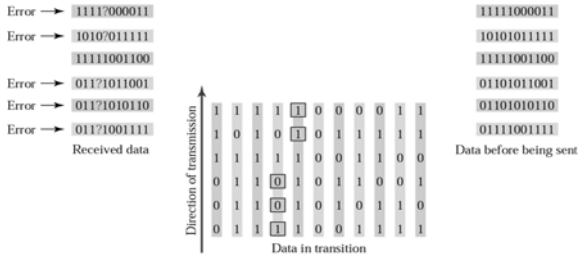
 U2.41

Error Detection using Hamming



 U2.42

Burst Error Correction Example



 U2.43

Conclusion

- Errors can be single bit or burst errors
- Three common redundancy methods are parity check, CRC and checksum
- Errors can be corrected by retransmission
- Hamming code is error correction through retransmission

 U2.44

Topic

Data Link Control and Protocols

 U2.45

Learning Objectives

- To introduce the protocols for error and flow control.
- To discuss Stop and wait, Go back N and selective repear ARQ
- To discuss concept of piggybacking and pipelining
- To discuss HDLC protocol and its various frames

 U2.46

Cont ….

Note:

Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.

 U2.47

Cont ….

Note:

Error control in the data link layer is based on automatic repeat request, which is the retransmission of data.

 U2.48

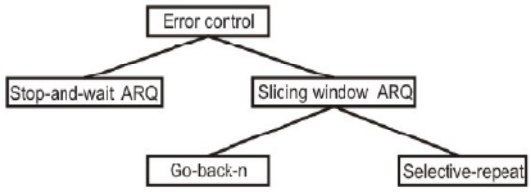
Cont ....

Error Control Techniques

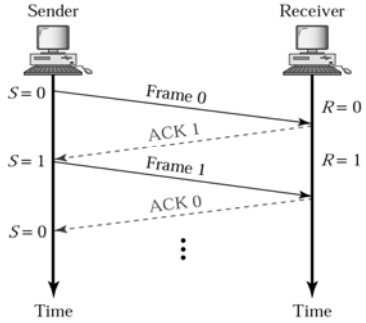
When an error is detected in a message, the receiver sends a request to the transmitter to retransmit the ill-fated message or packet.

The most popular retransmission scheme is known as Automatic-Repeat-Request (ARQ). Such schemes, where receiver asks transmitter to re-transmit if it detects an error, are known as reverse error correction techniques.

Cont ....



Normal Operation



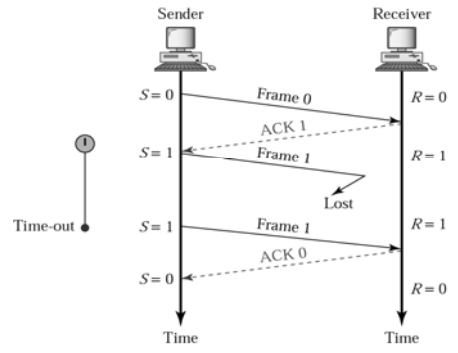
Cont ….

In Stop-and-Wait ARQ, which is simplest among all protocols, the sender (say station A) transmits a frame and then waits till it receives positive acknowledgement (ACK) or negative acknowledgement (NACK) from the receiver (say station B).

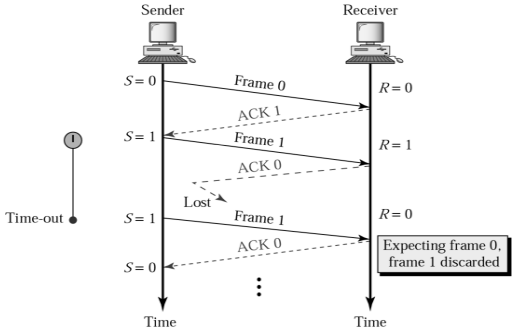
Station B sends an ACK if the frame is received correctly, otherwise it sends NACK.

Station A sends a new frame after receiving ACK; otherwise it retransmits the old frame, if it receives a NACK.

Stop-and-Wait ARQ, Lost Frame



Stop-and-Wait ARQ, Lost ACK

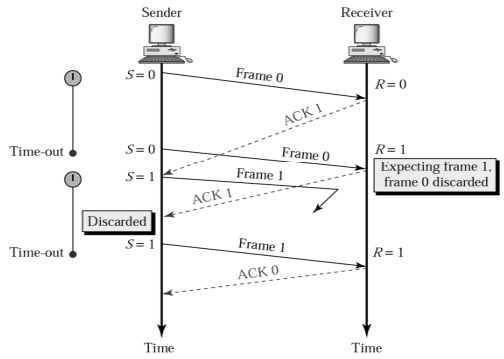


Cont ….

Note:

In Stop-and-Wait ARQ, numbering frames prevents the retaining of duplicate frames.

Stop-and-Wait , Delayed ACK

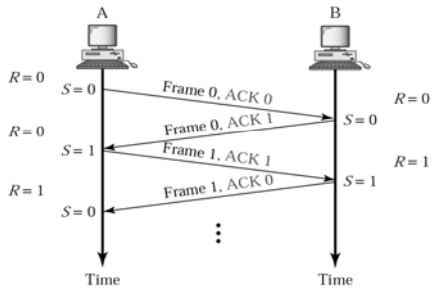


Cont ….

Note:

Numbered acknowledgments are needed if an acknowledgment is delayed and the next frame is lost.

Piggy Backing



 U2.58

Cont ….

What is piggybacking? What is its advantage?

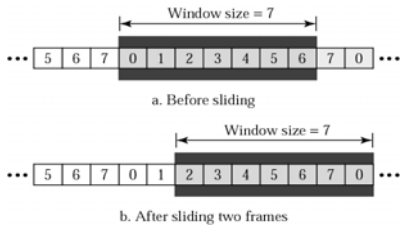
In practice, the link between receiver and transmitter is full duplex and usually both transmitter and receiver stations send data to each over.

So, instead of sending separate acknowledgement packets, a portion (few bits) of the data frames can be used for acknowledgement. This phenomenon is known as piggybacking.

The piggybacking helps in better channel utilization. Further, multi-frame acknowledgement can be done.

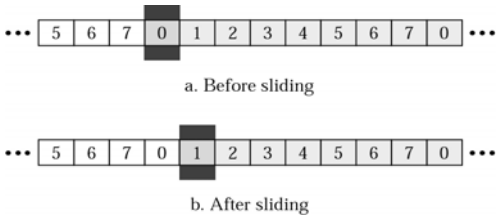
 U2.59

Sender sliding Window Go Back N

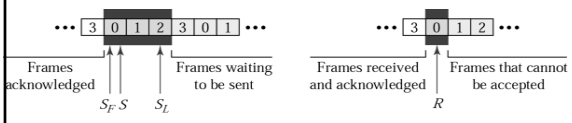


 U2.60

Receiver Sliding Window



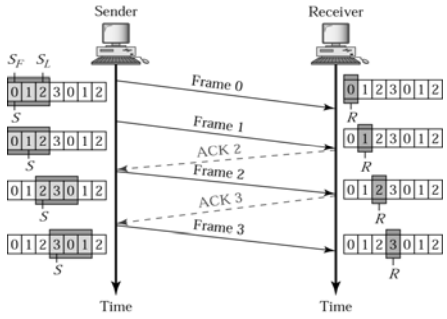
Control Variables



Cont ….

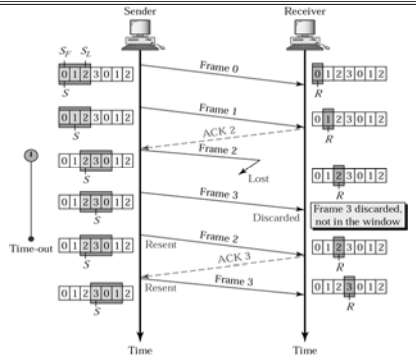
- The most popular ARQ protocol is the go-back-N ARQ, where the sender sends the frames continuously without waiting for acknowledgement.
- That is why it is also called as *continuous ARQ*. As the receiver receives the frames, it keeps on sending ACKs or a NACK, in case a frame is incorrectly received.
- When the sender receives a NACK, it retransmits the frame in error plus all the succeeding frames as shown in Fig..
- Hence, the name of the protocol is go-back-N ARQ. If a frame is lost, the receiver sends NAK after receiving the next frame

Go-Back-N , Normal Operation



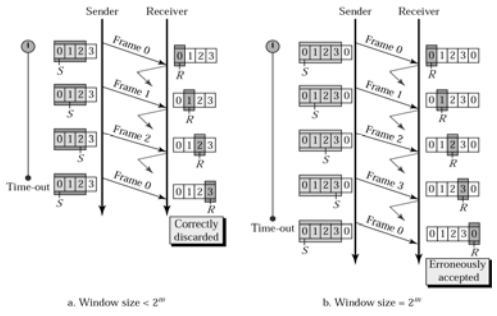
 U2.64

Go-Back-N , Lost Frame



 U2.65

Go-Back-N : Sender Window Size



 U2.66

Cont ….

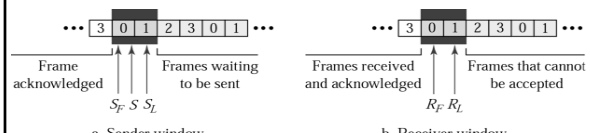
Note:

In Go-Back-N ARQ, the size of the sender window must be less than 2m; the size of the receiver window is always 1.

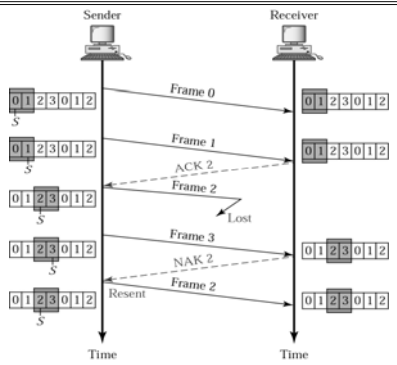
Cont ….

- The selective-repetitive ARQ scheme retransmits only those for which NAKs are received or for which timer has expired, this is shown in the Fig
- This is the most efficient among the ARQ schemes, but the sender must be more complex so that it can send out-of-order frames.
- The receiver also must have storage space to store the post-NAK frames and processing power to reinsert frames in proper sequence.

Selective Repeat



Selective Repeat , Lost Frame



 U2.70

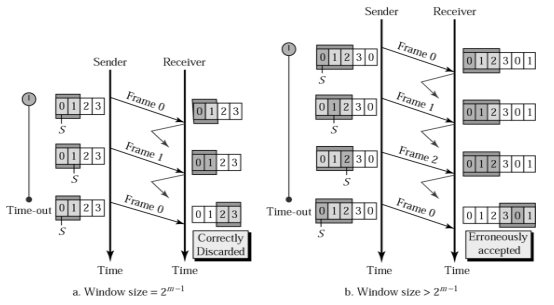
Cont ....

Note:

In Selective Repeat ARQ, the size of the sender and receiver window must be at most one-half of 2^m.

 U2.71

Selective Repeat



 U2.72

Selective Repeat

How the inefficiency of Stop-and-Wait protocol is overcome in sliding window protocol?

- The Stop-and-Wait protocol is inefficient when large numbers of small packets are send by the transmitter since the transmitter has to wait for the acknowledgement of each individual packet before sending the next one.
- This problem can be overcome by sliding window protocol. In sliding window protocol multiple frames (up to a fixed number of frames) are send before receiving an acknowledgement from the receiver.

 U2.73

HDLC

- HDLC is a bit-oriented protocol. It was developed by the International Organization for Standardization (ISO).
- It falls under the ISO standards ISO 3309 and ISO 4335.
- It has found itself being used throughout the world. It has been so widely implemented because it supports both half-duplex and full-duplex communication lines, point-to-point (peer to peer) and multi-point networks, and switched or non-switched channels.
- HDLC supports several modes of operation, including a simple sliding-window mode for reliable delivery.

 U2.74

HDLC

HDLC specifies the following three types of stations for data link control:
Primary Station
Secondary Station
Combined Station

 U2.75

HDLC

Primary Station

- Within a network using HDLC as its data link protocol, if a configuration is used in which there is a primary station, it is used as the controlling station on the link.
- It has the responsibility of controlling all other stations on the link (usually secondary stations).
- primary issues *commadnds* and secondary issues *responses*.
- Despite this important aspect of being on the link, the primary station is also responsible for the organization of data flow on the link. It also takes care of error recovery at the data link level (layer 2 of the OSI model).

 U2.76

HDLC

Secondary Station

- If the data link protocol being used is HDLC, and a primary station is present, a secondary station must also be present on the data link. The secondary station is under the control of the primary station.
- It has no ability, or direct responsibility for controlling the link. It is only activated when requested by the primary station.
- It only responds to the primary station. The secondary station's frames are called responses. It can only send response frames when requested by the primary station. A primary station maintains a separate logical link with each secondary station.

 U2.77

HDLC

Combined Station

- A combined station is a combination of a primary and secondary station. On the link, all combined stations are able to send and receive commands and responses without any permission from any other stations on the link.
- HDLC also defines three types of configurations for the three types of stations. The word configuration refers to the relationship between the hardware devices on a link.

 U2.78

HDLC

Following are the three configurations defined by HDLC:

Unbalanced Configuration
Balanced Configuration
Symmetrical Configuration

The unbalanced configuration in an HDLC link consists of a primary station and one or more secondary stations. The unbalanced condition arises because one station controls the other stations.

The balanced configuration in an HDLC link consists of two or more combined stations. Each of the stations has equal and complimentary responsibility compared to each other.

 U2.79

HDLC

This third type of configuration is not widely in use today. It consists of two independent point-to-point

 U2.80

HDLC

HDLC Operational Modes

- A mode in HDLC is the relationship between two devices involved in an exchange; the mode describes who controls the link. Exchanges over unbalanced configurations are always conducted in normal response mode.
- Exchanges over symmetric or balanced configurations can be set to specific mode using a frame design to deliver the command. HDLC offers three different modes of operation. These three modes of operations are:

Normal Response Mode (NRM)
Asynchronous Response Mode (ARM)
Asynchronous Balanced Mode (ABM)

 U2.81

HDLC

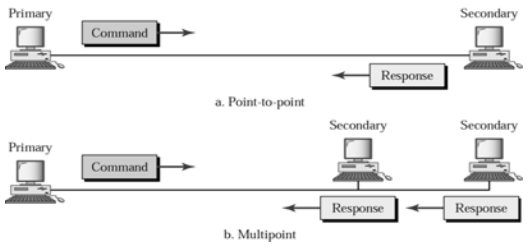
Normal Response Mode

- This is the mode in which the primary station initiates transfers to the secondary station.
- The secondary station can only transmit a response when, and only when, it is instructed to do so by the primary station.
- In other words, the secondary station must receive explicit permission from the primary station to transfer a response.
- After receiving permission from the primary station, the secondary station initiates its transmission.

HDLC

- This transmission from the secondary station to the primary station may be much more than just an acknowledgment of a frame.
- It may in fact be more than one information frame.
- Once the last frame is transmitted by the secondary station, it must wait once again from explicit permission to transfer anything, from the primary station.
- Normal Response Mode is only used within an unbalanced configuration.

NRM



ARM

Asynchronous Response Mode

- In this mode, the primary station doesn't initiate transfers to the secondary station.
- In fact, the secondary station does not have to wait to receive explicit permission from the primary station to transfer any frames.
- The frames may be more than just acknowledgment frames.
- They may contain data, or control information regarding the status of the secondary station.

 U2.85

ARM

This mode can reduce overhead on the link, as no frames need to be transferred in order to give the secondary station permission to initiate a transfer.

However, some limitations do exist.

Due to the fact that this mode is asynchronous, the secondary station must wait until it detects and idle channel before it can transfer any frames.

This is when the ARM link is operating at half-duplex.

 U2.86

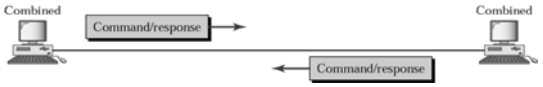
SBM

Synchronous Balanced Mode

- This mode is used in case of combined stations.
- There is no need for permission on the part of any station in this mode.
- This is because combined stations do not require any sort of instructions to perform any task on the link.

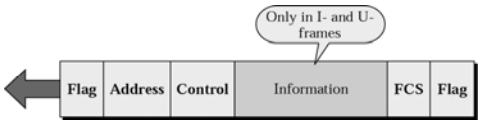
 U2.87

ABM



 U2.88

HDLC Frame



 U2.89

HDLC Frame

The Flag field

- Every frame on the link must begin and end with a flag sequence field (F). Stations attached to the data link must continually listen for a flag sequence.
- The flag sequence is an octet looking like 01111110. Flags are continuously transmitted on the link between frames to keep the link active. Two other bit sequences are used in HDLC as signals for the stations on the link. These two bit sequences are:
- Seven 1's, but less than 15 signal an abort signal. The stations on the link know there is a problem on the link.
- 15 or more 1's indicate that the channel is in an idle state.

 U2.90

HDLC Frame

The Address field

- The address field (A) identifies the primary or secondary stations involvement in the frame transmission or reception.
- Each station on the link has a unique address.
- In an unbalanced configuration, the A field in both commands and responses refer to the secondary station.
- In a balanced configuration, the command frame contains the destination station address and the response frame has the sending station's address.

 U2.91

HDLC Frame

The Control field

•HDLC uses the control field (C) to determine how to control the communications process.

•This field contains the commands, responses and sequences numbers used to maintain the data flow accountability of the link, defines the functions of the frame and initiates the logic to control the movement of traffic between sending and receiving stations.

 U2.92

HDLC Frame

There three control field formats:

Information Transfer Format: The frame is used to transmit end-user data between two devices.

Supervisory Format: The control field performs control functions such as acknowledgment of frames, requests for re-transmission, and requests for temporary suspension of frames being transmitted. Its use depends on the operational mode being used.

Unnumbered Format: This control field format is also used for control purposes. It is used to perform link initialization, link disconnection and other link control functions.

 U2.93

HDLC Frame

The Poll/Final Bit (P/F)

- The 5th bit position in the control field is called the **poll/final bit, or P/F bit**. It can only be recognized when it is set to 1. If it is set to 0, it is ignored. The poll/final bit is used to provide dialogue between the primary station and secondary station.
- The primary station uses P=1 to acquire a status response from the secondary station. The P bit signifies a poll. The secondary station responds to the P bit by transmitting a data or status frame to the primary station with the P/F bit set to F=1.
- The F bit can also be used to signal the end of a transmission from the secondary station under Normal Response Mode.

 U2.94

HDLC Frame

The Information field or Data field

- This field is not always present in a HDLC frame. It is only present when the Information Transfer Format is being used in the control field.
- The information field contains the actually data the sender is transmitting to the receiver in an I-Frame and network management information in U-Frame.

The Frame check Sequence field
This field contains a 16-bit, or 32-bit cyclic redundancy check bits.

 U2.95

HDLC Frame

HDLC Commands and Responses

Information transfer format command and response (I-Frame) The function of the information command and response is to transfer sequentially numbered frames, each containing an information field, across the data link.

 U2.96

HDLC Frame

Supervisory format command and responses (S-Frame)

- Supervisory (S) commands and responses are used to perform numbered supervisory functions such as acknowledgment, polling, temporary suspension of information transfer, or error recovery.
- Frames with the S format control field cannot contain an information field.
- A primary station may use the S format command frame with the P bit set to 1 to request a response from a secondary station regarding its status.

 U2.97

HDLC Frame

Format commands and responses are as follows:

- **Receive Ready (RR)** is used by the primary or secondary station to indicate that it is ready to receive an information frame and/or acknowledge previously received frames.
- **Receive Not Ready (RNR)** is used to indicate that the primary or secondary station is not ready to receive any information frames or acknowledgments.

 U2.98

HDLC Frame

Format commands and responses are as follows:

- **Reject (REJ)** is used to request the retransmission of frames.
- **Selective Reject (SREJ)** is used by a station to request retransmission of specific frames. An SREJ must be transmitted for each erroneous frame; each frame is treated as a separate error. Only one SREJ can remain outstanding on the link at any one time.

 U2.99

HDLC Frame

Unnumbered Format Commands and responses (U-Frame)

- The unnumbered format commands and responses are used to extend the number of data link control functions.
- The unnumbered format frames have 5 modifier bits, which allow for up to 32 additional commands and 32 additional response functions.
- 13 command functions, and 8 response functions

 U2.100

HDLC Frame

Set Normal Response Mode (SNRM) places the secondary station into NRM. NRM does not allow the secondary station to send any unsolicited frames. Hence the primary station has control of the link.

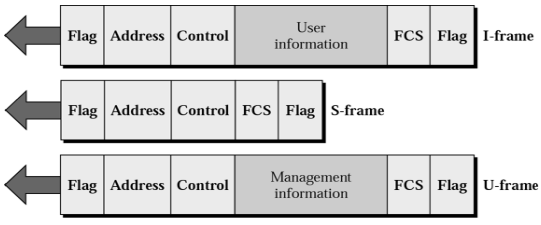
Set Asynchronous Response Mode (SARM) allows a secondary station to transmit frames without a poll from the primary station.

Set Asynchronous Balanced Mode (SABM) sets the operational mode of the link to ABM.

Disconnect (DISC) places the secondary station in to a disconnected mode.

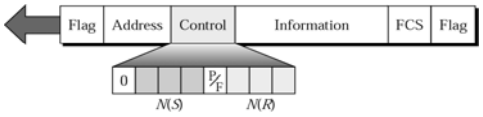
 U2.101

HDLC Frame Types

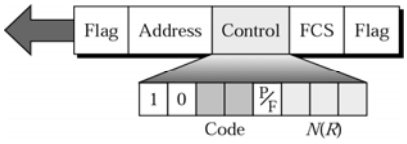


 U2.102

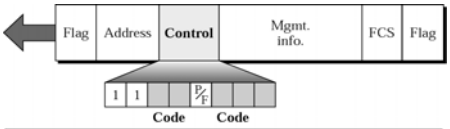
I-frame



S-Frame Control field in HDLC



Cont ….



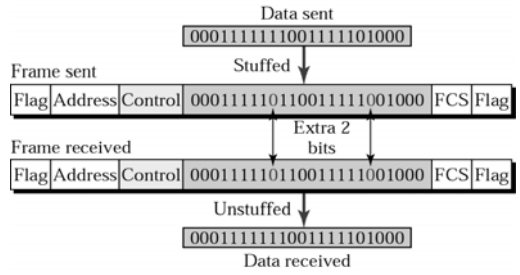
Code		Command	Response
00	001	SNRM	
11	011	SNRME	
11	100	SABM	DM
11	110	SABME	
00	000	UI	UI
00	110		UA
00	010	DISC	RD
10	000	SIM	RIM
00	100	UP	
11	001	RSET	
11	101	XID	XID
10	001		FRMR

Cont ….

Command/response	Meaning
SNRM	Set normal response mode
SNRME	Set normal response mode (extended)
SABM	Set asynchronous balanced mode
SABME	Set asynchronous balanced mode (extended)
UP	Unnumbered poll
UI	Unnumbered information
UA	Unnumbered acknowledgment
RD	Request disconnect
DISC	Disconnect
DM	Disconnect mode
RIM	Request information mode
SIM	Set initialization mode
RSET	Reset
XID	Exchange ID
FRMR	Frame reject

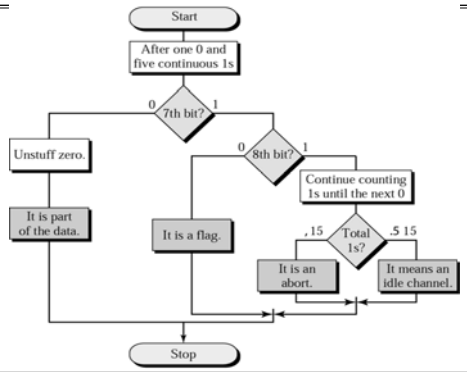
 U2.106

Bit Stuffing and Removal



 U2.107

Bit Stuffing in HDLC



 U2.108

Conclusion

- Flow control is the regulation of the sender's data so that receiver buffer does not become overwhelmed.
- Stop and Wait the sender sends a frame and waits for acknowledgment
- In Go back N and Selective Repeat multiple frames can be sent at the same time
- HDLC is a protocol that implements ARQ mechanisms

 U2.109

TOPIC

Multiple Access

 U2.110

Switching

- When there are many devices, it is necessary to develop suitable mechanism for communication between any two devices.
- In the switched network methodology, the network consists of a set of interconnected nodes, among which information is transmitted from source to destination via different routes, which is controlled by the switching mechanism.

 U2.111

Switching

- The end devices that wish to communicate with each other are called stations. The switching devices are called nodes. Some nodes connect to other nodes and some are to connected to some stations.
- The switching performed by different nodes can be categorized into the following three types:
  - Circuit Switching
  - Packet Switching
  - Message Switching

 U2.112

Circuit Switching

- Communication via circuit switching implies that there is a dedicated communication path between the two stations.
- The path is a connected through a sequence of links between network nodes.
- On each physical link, a logical channel is dedicated to the connection.
- Circuit switching is commonly used technique in telephony, where the caller sends a special message with the address of the callee (i.e. by dialing a number) to state its destination.

 U2.113

Circuit Switching

It involved the following three distinct steps:

Circuit Establishment: *To establish an end-to-end connection before any transfer of data.*

Some segments of the circuit may be a dedicated link, while some other segments may be shared.

Data transfer:

- Transfer data is from the source to the destination.
- The data may be analog or digital, depending on the nature of the network.
- The connection is generally full-duplex.

 U2.114

Circuit Switching

Circuit disconnect:

- Terminate connection at the end of data transfer.
- Signals must be propagated to deallocate the dedicated resources.

Thus the actual physical electrical path or circuit between the source and destination host must be established before the message is transmitted.

This connection, once established, remains exclusive and continuous for the complete duration of information exchange and the circuit becomes disconnected only when the source wants to do so.

 U2.115

Message Switching

- In this switching method, a different strategy is used, where instead of establishing a dedicated physical line between the sender and the receiver, the message is sent to the nearest directly connected switching node.
- This node stores the message, checks for errors, selects the best available route and forwards the message to the next intermediate node.

 U2.116

Message Switching

The line becomes free again for other messages, while the process is being continued in some other nodes.

Due to the mode of action, this method is also known as *store-and-forward technology where the message hops from node to node to its final destination. Each node stores the full message, checks for errors and forwards it.*

In this switching technique, more devices can share the network bandwidth, as compared with circuit switching technique.

 U2.117

Message Switching

Temporary storage of message reduces traffic congestion to some extent.

Higher priority can be given to urgent messages, so that the low priority messages are delayed while the urgent ones are forwarded faster.

Through broadcast addresses one message can be sent to several users.

Last of all, since the destination host need not be active when the message is sent, message switching techniques improve global communications.

 U2.118

Message Switching

- Each network node receives and stores the message
- Determines the next leg of the route, and
- Queues the message to go out on that link.

Advantages:

- Line efficiency is greater (sharing of links).
- Data rate conversion is possible.
- Even under heavy traffic, packets are accepted, possibly with a greater delay in delivery.
- Message priorities can be used, to satisfy the requirements, if any.

Disadvantages:

- Message of large size monopolizes the link and storage

 U2.119

Packet Switching

- The basic approach is not much different from message switching. It is also based on the same 'store-and-forward' approach. However, to overcome the limitations of message switching, messages are divided into subsets of equal length called *packets.*
- In packet switching approach, data are transmitted in short packets (few Kbytes). A long message is broken up into a series of packets

 U2.120

Packet Switching

- Main difference between Packet switching and Circuit Switching is that the communication lines are not dedicated to passing messages from the source to the destination.
- In Packet Switching, different messages (and even different packets) can pass through different routes, and when there is a "dead time" in the communication between the source and the destination, the lines can be used by other sources.

 U2.121

Packet Switching

- Main difference between Packet switching and Circuit Switching is that the communication lines are not dedicated to passing messages from the source to the destination.
- In Packet Switching, different messages (and even different packets) can pass through different routes, and when there is a "dead time" in the communication between the source and the destination, the lines can be used by other sources.

© Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi-63 by Vishal Jain U2.122

Packet Switching

- There are two basic approaches commonly used to packet Switching: **virtual-circuit packet switching and datagram packet switching.**
- In virtual-circuit packet switching a virtual circuit is made before actual data is transmitted, but it is different from circuit switching in a sense that in circuit switching the call accept signal comes only from the final destination to the source while in case of virtual-packet switching this call accept signal is transmitted between each adjacent intermediate node

 U2.123

Packet Switching

- There are two basic approaches commonly used to packet Switching: **virtual-circuit packet switching and datagram packet switching.**
- In virtual-circuit packet switching a virtual circuit is made before actual data is transmitted, but it is different from circuit switching in a sense that in circuit switching the call accept signal comes only from the final destination to the source while in case of virtual-packet switching this call accept signal is transmitted between each adjacent intermediate node

Packet Switching

- An initial setup phase is used to set up a route between the intermediate nodes for all the packets passed during the session between the two end nodes.
- In each intermediate node, an entry is registered in a table to indicate the route for the connection that has been set up.
- Thus, packets passed through this route, can have short headers, containing only a *virtual circuit identifier (VCI), and not their destination.*
- *Each intermediate node passes the packets according to the information that was stored in it, in the setup phase.*

Packet Switching

Datagram Packet Switching Networks

- This approach uses a different, more dynamic scheme, to determine the route through the network links.
- Each packet is treated as an independent entity, and its header contains full information about the destination of the packet.
- The intermediate nodes examine the header of the packet, and decide to which node to send the packet so that it will reach its destination.

Packet Switching

- Thus, in this method, the packets don't follow a pre-established route, and the intermediate nodes (the routers) don't have pre-defined knowledge of the routes that the packets should be passed through.
- Packets can follow different routes to the destination, and delivery is not guaranteed (although packets usually do follow the same route, and are reliably sent).

 U2.127

Packet Switching

- Due to the nature of this method, the packets can reach the destination in a different order than they were sent, thus they must be sorted at the destination to form the original message.
- This approach is time consuming since every router has to decide where to send each packet.
- The main implementation of Datagram Switching network is the Internet, which uses the IP network protocol.

 U2.128

Packet Switching

Advantages :

- Call setup phase is avoided (for transmission of a few packets, datagram will be faster).
- Because it is more primitive, it is more flexible.
- Congestion/failed link can be avoided (more reliable).

Problems:

- Packets may be delivered out of order.
- If a node crashes momentarily, all of its queued packets are lost.

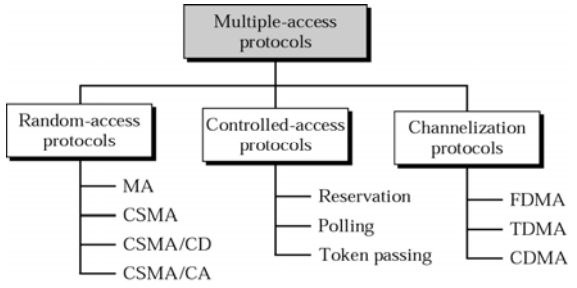
 U2.129

Switching

Circuit Switching	Datagram Packet	Virtual Circuit Packet
Dedicated path	No dedicated path	No dedicated path
Path established for entire conversation	Route established for each packet	Route established for entire conversation
Call set up delay	Packet transmission delay	Call set up delay, Packet transmission delay
Overload may block call set up	Overload increases packet delay	Overload may block call set up and increases packet delay
No speed or code conversion	Speed or code conversion	Speed or code conversio
Fixed bandwidth	Dynamic bandwidth	Dynamic bandwidth
No overhead bits after call set up	Overhead bits in each packet	Overhead bits in each packet

 U2.130

Multiple-Access Protocols



 U2.131

Random Access

- In random access or contention methods, no station is superior to another station and none is assigned the control over another.
- No station permits, or does not permit, another station to send.
- The decision to send data depends on the state of the medium (busy or idle).
- In random access method, each station has the right to the medium without being controlled by any other station.
- However, if more than one station tries to send, there is an access conflict- collision- and the frames will be either destroyed and modified.

 U2.132

Random Access

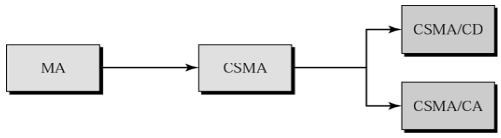
MA

CSMA

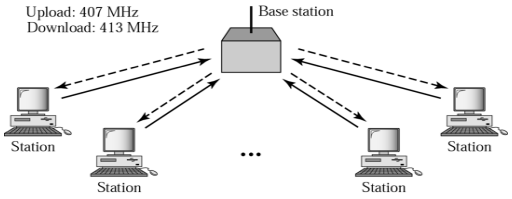
CSMA/CD

CSMA/CA

Random-access methods



ALOHA network



ALOHA Network

•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.

•It was designed for a radio (Wireless LAN) , but it can be used on any shared medium.

•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.

ALOHA network

Pure ALOHA

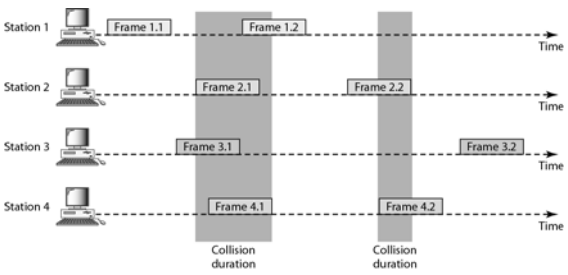
•The original ALOHA protocol is called pure ALOHA.

•The idea is that each station sends a frame whenever it has a frame to send.

•However, since there is only one channel to share, there is the possibility of collision between frames from different stations.

•We need to mention that even if one bit of a frame coexists on the channel with one bit from another frame, there is collision and both will be destroyed.

ALOHA Network



ALOHA Network

- The pure ALOHA protocol relies on acknowledgment from the receiver.
- When a station sends a frame, it expects the receiver to send an acknowledgement .
- If the acknowledgment does not arrive after a time-out period, the station assumes that the frame has been destroyed and resends the frame.

 U2.139

ALOHA network

A collision involves two or more stations.

If all these stations try to resend their frames after the time-out, the frame will collide again.

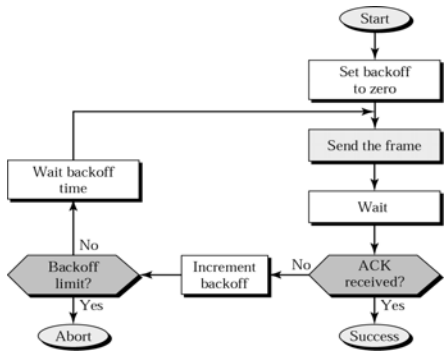
Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame.

The randomness will help avoid more collisions.

We call this time the back-off time.

 U2.140

Procedure for ALOHA protocol

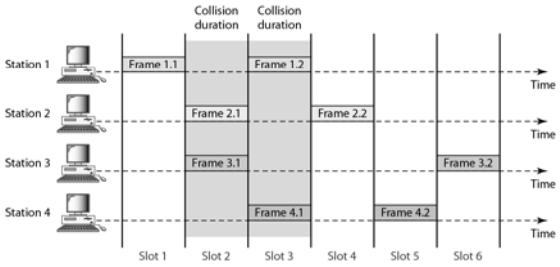


 U2.141

ALOHA Network

Slotted ALOHA

In slotted ALOHA we devide the time into slots and force the station to send only at the beginning of the time slot.



 U2.142

Collision in 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.

 U2.143

Collision in CSMA

•In this scheme, a node having data to transmit first listens to the medium to check whether another transmission is in progress or not.

•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.*

 U2.144

Collision in CSMA

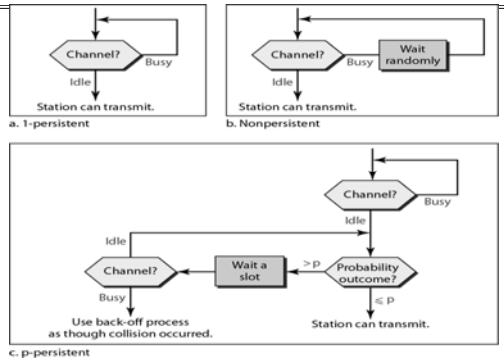
There are three variations of this basic scheme as outlined below.

(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.

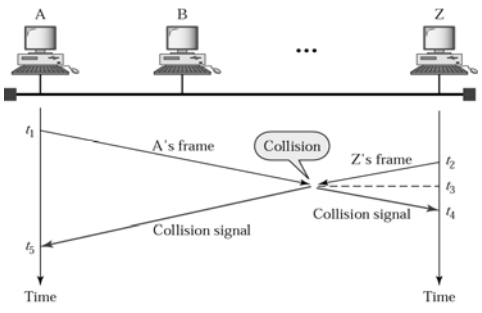
(ii) Non-persistent CSMA: If the channel is sensed free, the node starts sending the packet. Otherwise, the node waits for a random amount of time and then monitors the channel.

(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*.

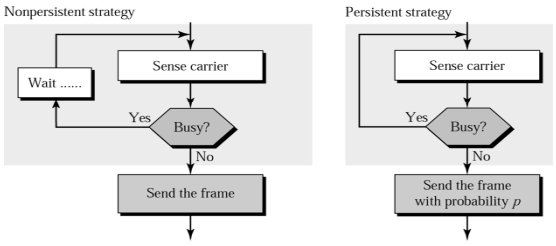
Persistence Strategies



Collision in CSMA



Persistence strategies



 U2.148

CSMA/CD

•The CSMA method does not specify the procedure following a collision.

•Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.

•In this method, a station monitors the medium after it sends a frame to see if the transmission was successful.

•If so, the station is finished..

•If, however, there is a collision, the frame is sent again.

 U2.149

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.

 U2.150

CSMA/CD

•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.*

CSMA/CD

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.

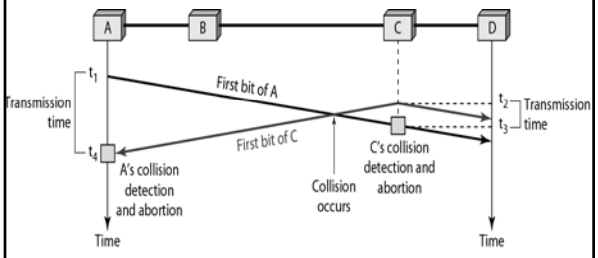
(ii) After transmitting the jamming signal, the node waits for a random amount of time and then transmission is resumed.

CSMA/CD

- 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.

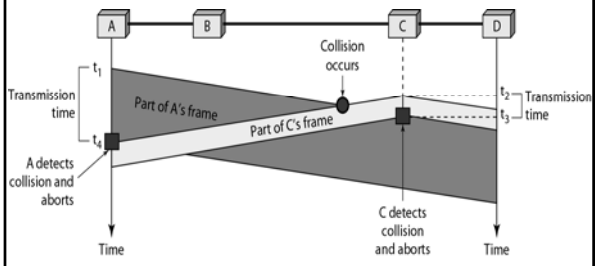
CSMA/CD

Collision of the first bit in CSMA/CD

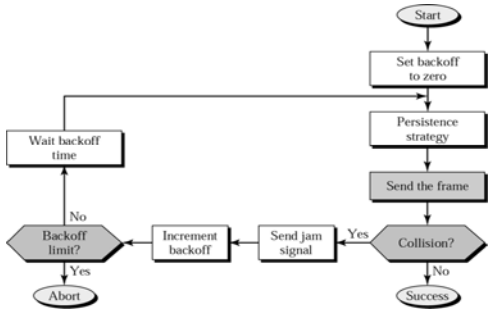


CSMA/CD

Collision and abortion in CSMA/CD



CSMA/CD procedure



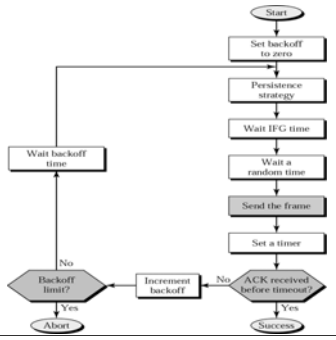
CSMA/CA procedure

•Carrier sense multiple access with collision avoidance (CSMA/CA) is CSMA with procedures that avoid a collision.

•In CSMA/CA, the IFS (interframe space) can also be used to define the priority of a station or a frame.

•In CSMA/CA, if the station finds the channel busy, it does not restart the timer of the contention window; it stops the timer and restarts it when the channel becomes idle.

CSMA/CA procedure



Comparison

How performance is improved in CSMA/CD protocol compared to CSMA protocol?

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.

Control Access

Reservation

Polling

Token Passing

Reservation access method

In Reservation method, a station needs to make a reservation before sending data.

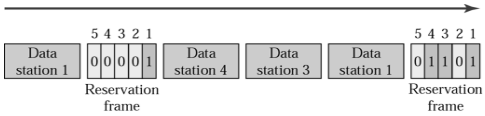
Time to divided into intervals, a reservation frame precedes the data frame sent in that interval

If there are N stations in the system, there are exactly N reservation minislots in the reservation frame.

When a station needs to send a data frame, it makes a reservation in its own minislot.

The station that have made reservations can send their data frames after the reservation frame.

Reservation access method



Polling

Polling works with topologies in which one device is designated as primary station and the other devices are secondary stations.

All data exchanges must be made through the primary device even when the ultimate destination is a secondary device.

The primary device controls the link; the secondary devices follow its instructions.

It is up to the primary device to determine which device is allowed to use the channel at a given time.

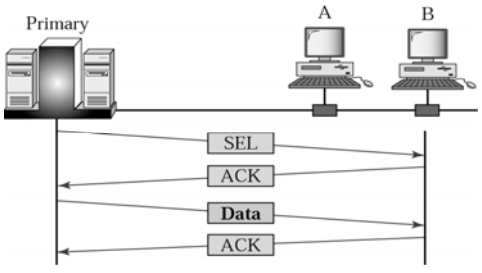
Select

•The select function is used whenever the primary device has something to send.

•The primary must alert the secondary to the upcoming transmission and wait for an ACK of the secondary ready status .

•Before sending the data, the primary creates and transmits a select (SEL) frame, one field of which includes the address of the intended secondary.

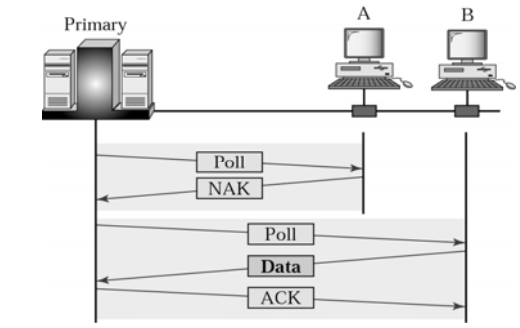
Select



Poll

- The poll function is used by the primary device to solicit information from the secondary devices.
- When the primary is ready to receive data, it must ask (poll) each device in turn if it has anything to send.
- When the first secondary is approached, it responds either with NAK frame if it has nothing to send.
- Or with data if it does.
- If the response is negative then primary asks to other secondary station.

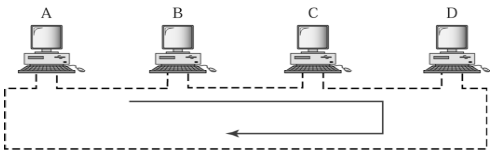
Poll



Token-passing network

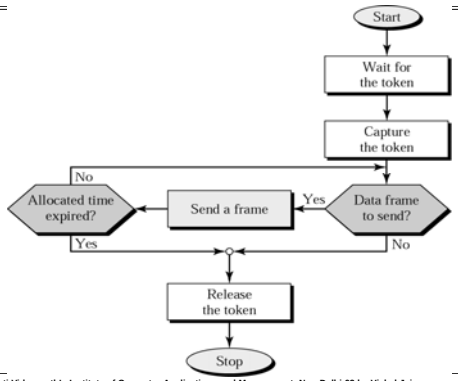
- In token passing method, the station in network are organized in a logical ring.
- A special packet called a token circulates through the ring.
- The possession of the token gives the station the right to access the channel and sends its data.
- When a station has something to send data , it waits until it receives the token from its predecessor.

Token-passing network



 U2.169

Token-passing procedure



 U2.170

Channelization

FDMA

TDMA

CDMA

 U2.171

Note:

In FDMA, the bandwidth is divided into channels.

 U2.172

FDMA

- Frequency Division Multiple Access
- The available bandwidth is divided into frequency bands.
- Each station is allocated a band to send its data.
- In other words, each band is reserved for a specific station, and it belongs to the station all the time.
- Each station also uses a bandpass filter to confine the transmitter frequencies.
- To prevent station interferences, the allocated bands are separated from one another by small guard bands.

 U2.173

Note:

In TDMA, the bandwidth is just one channel that is timeshared.

 U2.174

Note:

In CDMA, one channel carries all transmissions simultaneously.

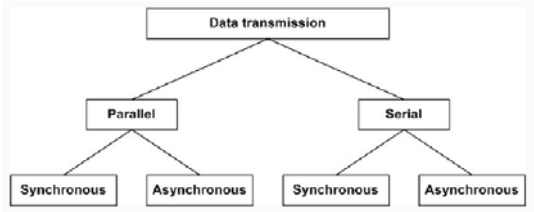
Conclusion

- Medium Access control can be random acess, controlled or channelised.
- In CSMA station must listen to the medium first
- CSMA/CD is CSMA with post collision procedure
- CSMA/CA is CSMA with procedure that avoids collision

Interface of media

To send signal through the transmission media, it is necessary to develop suitable mechanism for interfacing data terminal equipments (DTEs), which are the sources of data, to the data circuit terminating equipments (DCEs), which converts data to signal and interfaces with the transmission media.

Interface of media



 U2.178

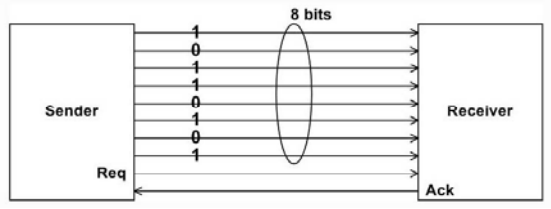
Interface of media

Parallel Transmission

Parallel transmission involves grouping several bits, say n, together and sending all the n bits at a time.
Figure shows how parallel transmission occurs for n = 8.
This can be accomplishes with the help of eight wires bundled together in the form of a cable with a connector at each end. Additional wires, such as request (req) and acknowledgement (ack) are required for asynchronous transmission.

 U2.179

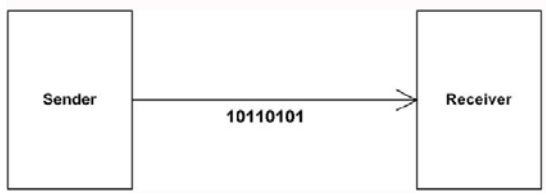
Parallel



 U2.180

Serial

Serial transmission involves sending one data bit at a time. Figure shows how serial transmission occurs. It uses a pair of wire for communication of data in bit-serial form.



 U2.181

Serial

Serial mode of communication widely used because of the following advantages:

• Reduced cost of cabling: Lesser number of wires is required as compared to parallel connection
• Reduced cross talk: Lesser number of wires result in reduced cross talk
• Availability of suitable communication media
• Inherent device characteristics: Many devices are inherently serial in nature
• Portable devices like PDAs, etc use serial communication to reduce the size of the connector

 U2.182

Serial

•There are two basic approaches for serial communication to achieve synchronization of data transfer between the source-destination pair. These are referred to as – **asynchronous** and **synchronous**.
•In the first case, data are transmitted in small sizes, say character by character, to avoid timing problem and make data transfer self-synchronizing.
•However, it is not very efficient because of large overhead.
• To overcome this problem, synchronous mode is used.
•In synchronous mode, a block with large number of bits can be sent at a time. However, this requires tight synchronization between the transmitter and receiver clocks.

 U2.183

Synchronization

•Data sent by a sender in bit-serial form through a medium must be correctly interpreted at the receiving end.
•This requires that the beginning, the end and logic level and duration of each bit as sent at the transmitting end must be recognized at the receiving end.
•There are three synchronization levels: *Bit, Character and Frame.* Moreover, to achieve synchronization, two approaches known as *asynchronous* and *synchronous* transmissions are used.

 U2.184

Synchronization

•Data sent by a sender in bit-serial form through a medium must be correctly interpreted at the receiving end.
•This requires that the beginning, the end and logic level and duration of each bit as sent at the transmitting end must be recognized at the receiving end.
•There are three synchronization levels: *Bit, Character and Frame.* Moreover, to achieve synchronization, two approaches known as *asynchronous* and *synchronous* transmissions are used.
•Frame synchronization is the process by which incoming frame alignment signals (i.e., distinctive bit sequences) are identified, i.e. distinguished from data bits, permitting the data bits within the frame to be extracted for decoding or retransmission.

 U2.185

Synchronization

•Data sent by a sender in bit-serial form through a medium must be correctly interpreted at the receiving end.
•This requires that the beginning, the end and logic level and duration of each bit as sent at the transmitting end must be recognized at the receiving end.
•There are three synchronization levels: *Bit, Character and Frame.* Moreover, to achieve synchronization, two approaches known as *asynchronous* and *synchronous* transmissions are used.
•Frame synchronization is the process by which incoming frame alignment signals (i.e., distinctive bit sequences) are identified, i.e. distinguished from data bits, permitting the data bits within the frame to be extracted for decoding or retransmission.

 U2.186

Synchronization

Synchronous communication (bit-oriented)

•Timing is recovered from the signal itself (by the carrier if the signal is analog, or by regular transitions in the data signal or by a separate clock line if the signal is digital). Scrambling is often used to ensure frequent transitions needed. The data transmitted may be of any bit length, but is often constrained by the frame transfer protocol (data link or MAC protocol).
•Bit-oriented framing only assumes that bit synchronization has been achieved by the underlying hardware, and the incoming bit stream is scanned at all possible bit positions for special patterns generated by the sender.

 U2.187

Synchronization

•The sender uses a special pattern (a flag pattern) to delimit frames (one flag at each end), and has to provide for data transparency by use of bit stuffing (see below). A commonly used flag pattern is HDLC's 01111110 flag
•The bit sequence 01111110 is used for both preamble and postamble for the purpose of synchronization.

 U2.188

Synchronization

Bit stuffing: If the flag pattern appears anywhere in the header or data of a frame, then the receiver may prematurely detect the start or end of the received frame.
•To overcome this problem, the sender makes sure that the frame body it sends has no flags in it at any position (note that since there is no character synchronization,
•The flag pattern can start at any bit location within the stream). It does this by *bit stuffing*, inserting an extra bit in any pattern that is beginning to look like a flag.

 U2.189

Synchronization

•In HDLC, whenever 5 consecutive 1's are encountered in the data, a 0 is inserted after the 5th 1, regardless of the next bit in the data.
•On the receiving end, the bit stream is piped through a shift register as the receiver looks for the flag pattern. If 5 consecutive 1's followed by a 0 is seen, then the 0 is dropped before sending the data on (the receiver destuffs the stream). If 6 1's and a 0 are seen,
•It is a flag and either the current frame are ended or a new frame is started, depending on the current state of the receiver. If more than 6 consecutive 1's are seen, then the receiver has detected an invalid pattern, and usually the current frame, if any, is discarded.

 U2.190

Synchronization

Bit oriented (a) Data to be sent to the peer, (b) Data after being bit stuffed.

 U2.191

Synchronization

Asynchronous communication (word-oriented)
•In asynchronous communication, small, fixed-length words (usually 5 to 9 bits long) are transferred without any clock line or clock is recovered from the signal itself.

•Each word has a start bit (usually as a 0) before the first data bit of the word and a stop bit (usually as a 1) after the last data bit of the word.

•The receiver's local clock is started when the receiver detects the 1-0 transition of the start bit, and the line is sampled in the middle of the fixed bit intervals (a bit interval is the inverse of the data rate).

 U2.192

Synchronization

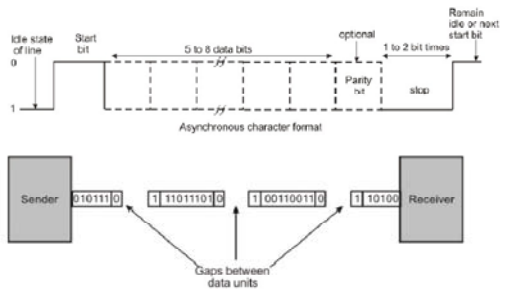
•The sender outputs the bit at the agreed-upon rate, holding the line in the appropriate state for one bit interval for each bit, but using its own local clock to determine the length of these bit intervals.

•The receiver's clock and the sender's clock may not run at the same speed, so that there is a relative clock drift (this may be caused by variations in the crystals used, temperature, voltage, etc.).

•If the receiver's clock drifts too much relative to the sender's clock, then the bits may be sampled while the line is in transition from one state to another, causing the receiver to misinterpret the received data.

•There can be variable amount of gap between two frames

Synchronization



Synchronization

•Most commonly, a DLE (data link escape) character is used to signal that the next character is a control character, with DLE SOH (start of header) used to indicate the start of the frame (it starts with a header), DLE STX (start of text) used to indicate the end of the header and start of the data portion, and DLE ETX (end of text) used to indicate the end of the frame.

•A serious problem occurs with this method when binary data, such as object program are being transmitted.

•It may easily happen when the characters for **DLE STX or DLE ETX** occur in the data, which will interfere with the framing. One way to overcome this problem is to use character stuffing discussed below.

Synchronization

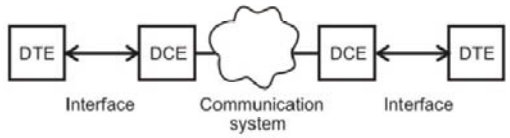
a) A C B

b) DLE STX A C B DLE ETX

To represent start of text

To represent end of text

DTE-DCE interface



Topic

Local Area Networks: Ethernet

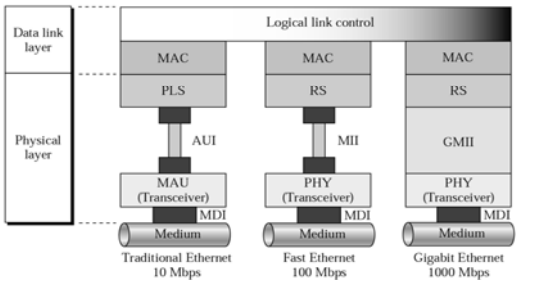
Learning Objectives

- To introduce the three generation of ethernet
- To describe the different stages in these three generations
- Traditional Ethernet
- Fast Ethernet
- Gigabit Ethernet

 U2.199

Three generations of Ethernet

AUI: Attachment Unit Interface
MAC: Media Access Control
MAU: Medium Attachment Unit
MDI: Medium-Dependent Interface
MII: Medium-Independent Interface
GMII: Gigabit Medium-Independent Interface
PHY: Physical Layer Entity
PLS: Physical Layer Signaling
RS: Reconciliation Signaling



 U2.200

Traditional Ethernet

MAC Sublayer

Physical Layer

Physical Layer Implementation

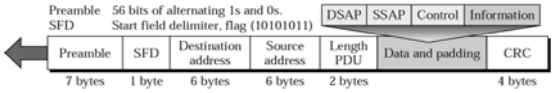
Bridged Ethernet

Switched Ethernet

Full-Duplex Ethernet

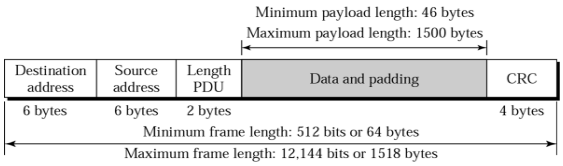
 U2.201

MAC frame



 U2.202

Minimum and maximum length



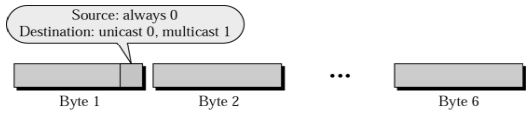
 U2.203

Ethernet addresses in hexadecimal notation

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

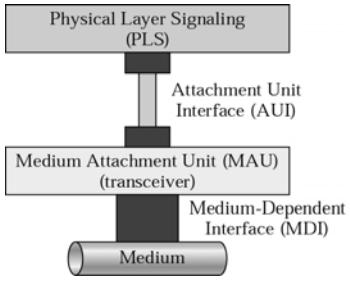
 U2.204

Unicast and multicast addresses



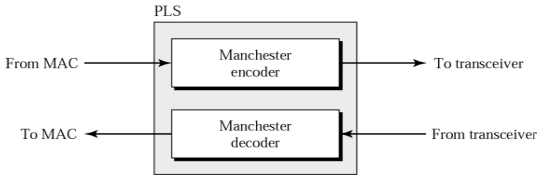
 U2.205

Physical layer



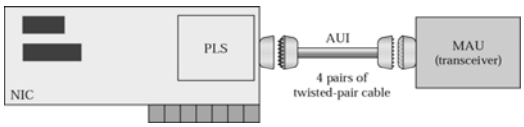
 U2.206

PLS

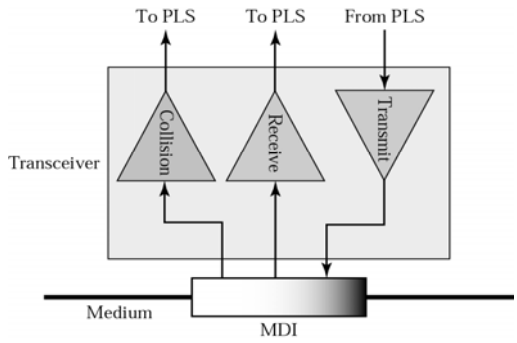


 U2.207

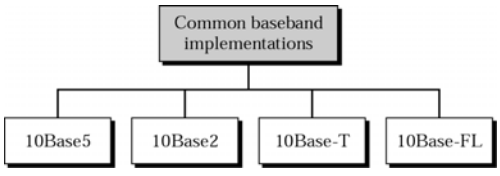
AUI



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

 U2.211

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.

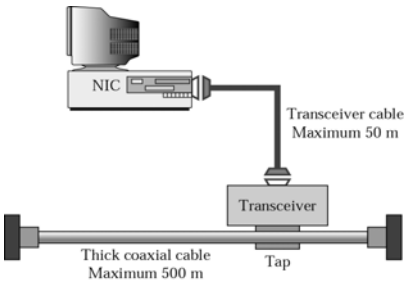
•The Category 5e (CAT5e) cable supports Gigabit Ethernet.

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

•Ethernet adapters interfaces directly with a computer's system bus. The cables, in turn, utilize connectors that in many cases look like the RJ-45 connector used with modern telephones.

 U2.212

Connection of a station to the medium using 10Base5



 U2.213

Connection of a station to the medium using 10Base5

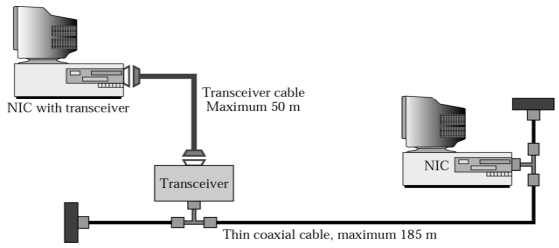
Fast Ethernet

In the mid-1990s, Fast Ethernet technology matured and met its design goals of

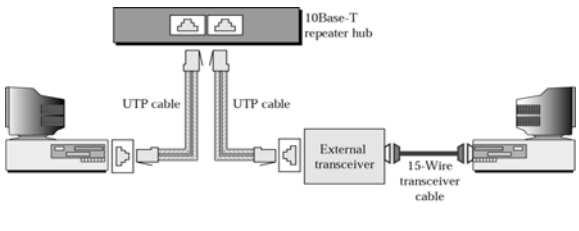
a) increasing the performance of traditional Ethernet while
b) b) avoiding the need to completely re-cable existing Ethernet networks.

Fast Ethernet comes in two major varieties:
100Base-T (using unshielded twisted pair cable)
100Base-FX (using fiber optic cable)

Connection of stations to the medium using 10Base2



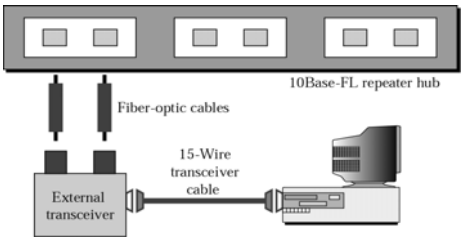
Connection of stations to the medium using 10Base-T



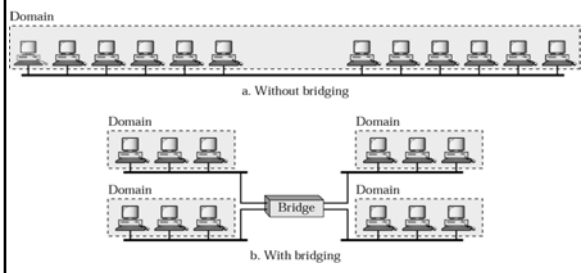
Connection of stations to the medium using 10Base-FL

- 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.

Connection of stations to the medium using 10Base-FL



Collision domains in a nonbridged and bridged network



Switched Ethernet

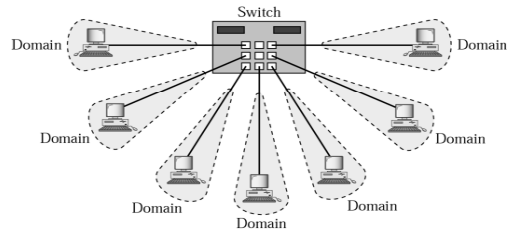
Switched Ethernet

•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.

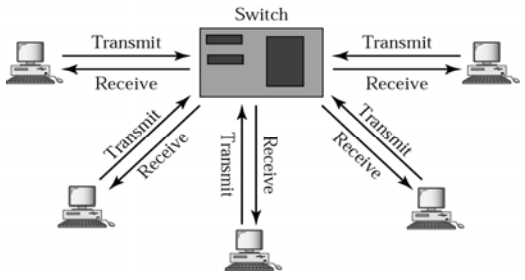
 U2.220

Switched Ethernet



 U2.221

Full-duplex switched Ethernet



 U2.222

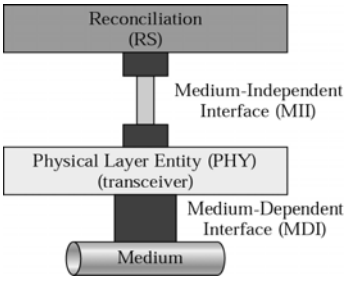
Fast Ethernet

MAC Sublayer

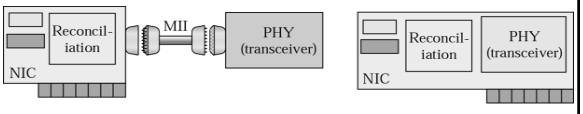
Physical Layer

Physical Layer Implementation

Fast Ethernet Physical Layer



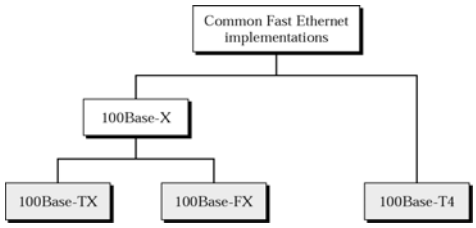
MII



a. MII is needed for external transceiver

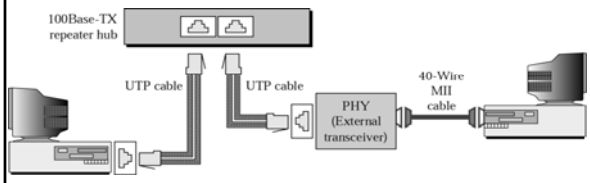
b. MII is not needed for internal transceiver

Fast Ethernet Implementations



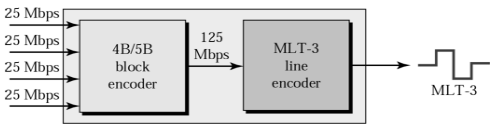
 U2.226

100Base-TX Implementation



 U2.227

Encoding and decoding in 100Base-TX



 U2.228

Gigabit Ethernet

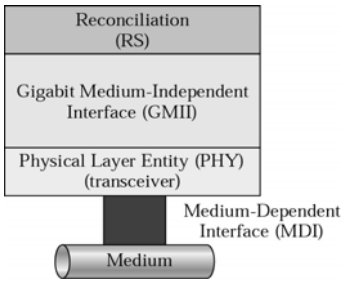
MAC Sublayer

Physical Layer

Physical Layer Implementation

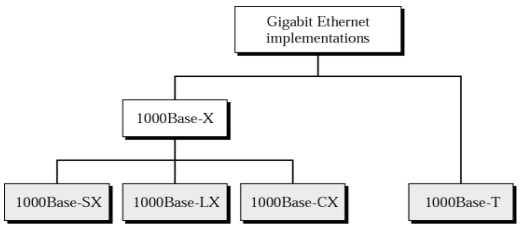
 U2.229

Physical Layer in Gigabit Ethernet



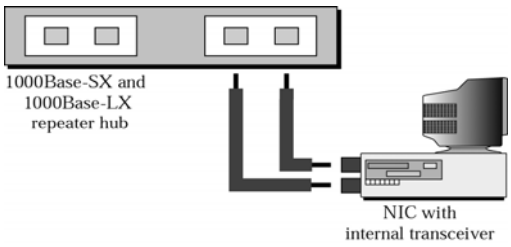
 U2.230

Gigabit Ethernet Implementations



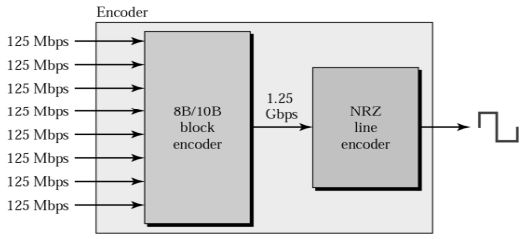
 U2.231

1000Base-X Implementation



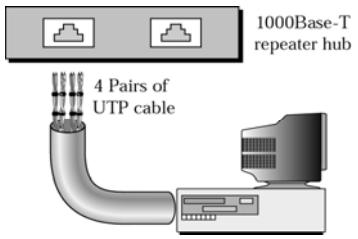
 U2.232

Encoding in 1000Base-X



 U2.233

1000Base-T Implementation



 U2.234

Conclusion

- Medium Access control can be random acess, controlled or channelised.
- In CSMA station must listen to the medium first
- CSMA/CD is CSMA with post collision procedure
- CSMA/CA is CSMA with procedure that avoids collision

 U2.235

Topic

Wireless LANs

 U2.236

IEEE 802.11

Architecture

Physical Layer

MAC Layer

Addressing Mechanism

 U2.237

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. This makes the use of cables, or wired LANs, impractical if not impossible. Wireless LAN can provide users mobility, which is likely to increase productivity, user convenience and various service opportunities

 U2.238

Wireless LANs

Installation speed and simplicity: Wireless LANs are very easy to install. There is no requirement for wiring every workstation and every room. This ease of installation makes wireless LANs inherently flexible.

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.

 U2.239

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. Long-term cost-benefits are greater in dynamic environment requiring frequent moves and changes.

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.

 U2.240

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)

 U2.241

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.

 U2.242

IEEE 802.11 Architecture

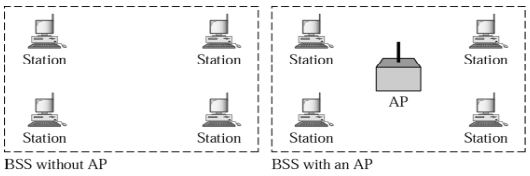
In this architecture, stations can form a network without the need of an AP.

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.**

 U2.243

BSSs



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.

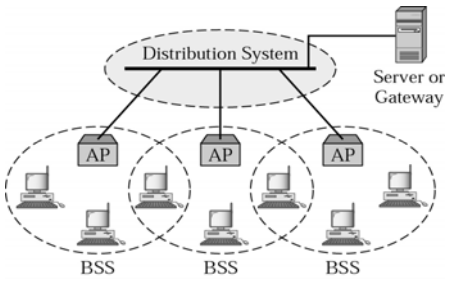
IEEE 802.11 Architecture

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.

ESS



 U2.247

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.

 U2.248

Station Types

IEEE 802.11, defines three types ios atations based on their mobility in a wireless Lan

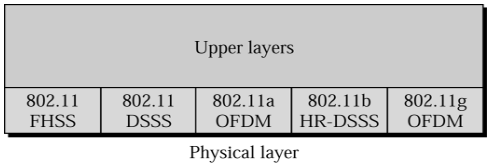
- **No-transition** – A station with no-transition mobility is either stationary or moving only inside a BSS
- **BSS-transition** – A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS.
- **ESS-transition** – A station with ESS-transition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

 U2.249

Physical Layer Specifications

Multiplexing Techniques

Physical Layer Specifications



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.
- 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.

FHSS

•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.

 U2.253

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***.

 U2.254

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.

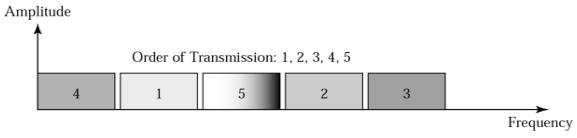
 U2.255

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.

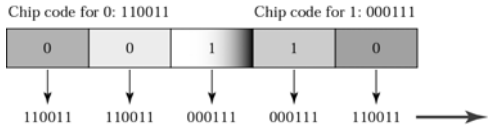
 U2.256

FHSS



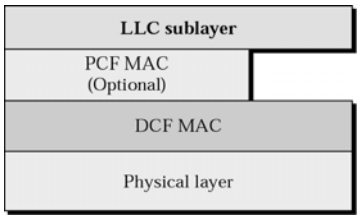
 U2.257

DSSS



 U2.258

MAC layers in IEEE 802.11 standard



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.

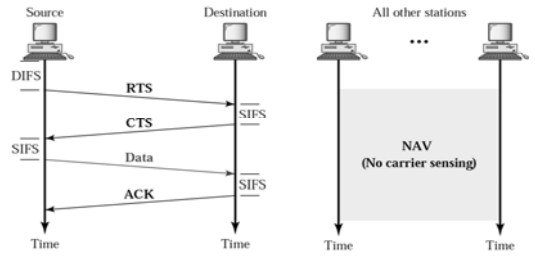
•Hidden station problem

•Signal fading – if distance is great

CSMA/CA flowchart

 U2.262

CSMA/CA and NAV



 U2.263

CSMA/CA Process

1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.
   a. The channel use a persistence strategy with back-off until the channel is idle.
   b. After the station is found to be idle, the station waits for a period of time called distribution interframe space (DIFS); then the station sends a control frame called the request to send (RTS).

 U2.264

CSMA/CA Process

2. After receiving the RTS and waiting a period of time called the short interframe space (SIFS) , the destination sends a control frame, called the clear to send (CTS), to the source station. This control frame indicates that the destination station is ready to receive data.
3. The source station sends data after waiting an amount of time equal to SIFS.
4. The destination station, after waiting an amount of time equal to SIFS, sends an ACK to show that the frame has been received.
5. ACK is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination.

 U2.265

CSMA/CA process

On the other hand, the lack of collision in CSMA/CD is a kind of indication to the source that data have arrived.

 U2.266

NAV

When a station send a RTS frame, it includes the duration of time that it needs to occupy the channel.

The stations that are affected by this transmission create a time called a network allocation vector (NAV) that shows how much time must pass before these stations are allowed to check the channel for idleness.

Each time a station accesses the system and sends an RTS frame, other stations start their NAV.

In other words, each station, before sensing the physical medium to see if it is idle, first checks its NAV to see if it has expired.

 U2.267

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.

PCF

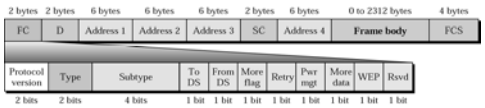
To give priority to PCF over DCF, another set of interframe spaces has been defined : PIFS and SIFS.

SIFS is as same as DCF

PIFS (PCF IFS) – is shorter than the DIFS.

This means that if, at the same time, a station wants to use only DCF and an AP wants to use PCF, the AP has priority.

Frame Format



Frame format

FC – Frame Control – The FC field is used to define the type of frame and some control information.
D – in all frames (data frames, control frames, management frames) except one, this field defines the duration of the transmission. That is used to set the value of NAV. In control frame, this field defines the ID of the frame.
Addresses – To DS and from DS
Sequence control - defines sequence number of the frame to be used in flow control.
Frame body – data
FCS - CRC

 U2.271

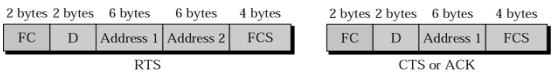
Subfields in FC field

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.
More data	When set to 1, means station has more data to send.
WEP	Wired equivalent privacy. When set to 1, means encryption implemented.
Rsvd	Reserved.

 U2.272

Control Frames

Control frames are used for accessing the channel and acknowledging frames.



 U2.273

Cont ….

Table Values of subfields in control frames

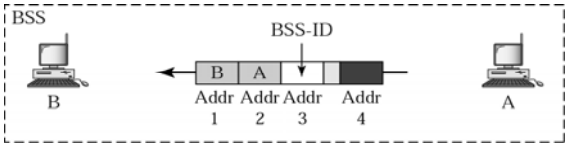
Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

Cont ….

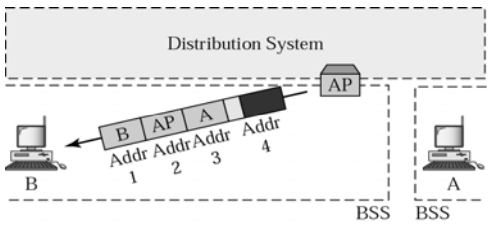
Table Subfields in FC field

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

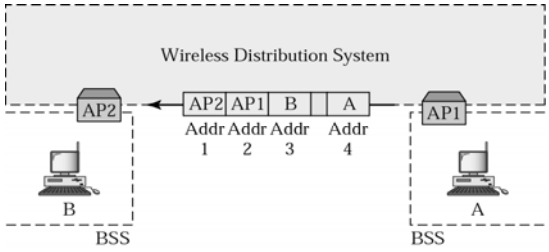
Addressing Mechanism: Case 1



Addressing Mechanism: Case 2



Addressing Mechanism: Case 4



Bluetooth

Architecture

Radio Layer

Baseband Layer

L2CAP Layer

Other Upper Layers

Bluetooth

- Bluetooth wireless technology is a short-range radio technology, which is developed for Personal Area Network (PAN).
- Bluetooth is a standard developed by a group of electronics manufacturers that allows any sort of electronic equipment -- from computers and cell phones to keyboards and headphones -- to make its own connections, without wires, cables or any direct action from a user. It is an ad hoc type network operable over a small area such as a room.

 U2.280

Bluetooth

Bluetooth wireless technology makes it possible to transmit signals over short distances between telephones, computers and other devices and there by simplify communication and synchronization between devices.

. It is a global standard that:

- Eliminates wires and cables between both stationary and mobile devices
- Facilitates both data and voice communication
- Offers the possibility of ad hoc networks and delivers the ultimate synchronicity between all your personal devices

 U2.281

Bluetooth

Bluetooth is a dynamic standard where devices can automatically find each other, establish connections, and discover what they can do for each other on an ad hoc basis.

Bluetooth is intended to be a standard that works at two levels:

- It provides agreement at the physical level -- Bluetooth is a radio-frequency standard.
- It also provides agreement at the next level up, where products have to agree on when bits are sent, how many will be sent at a time and how the parties in a conversation can be sure that the message received is the same as the message sent.

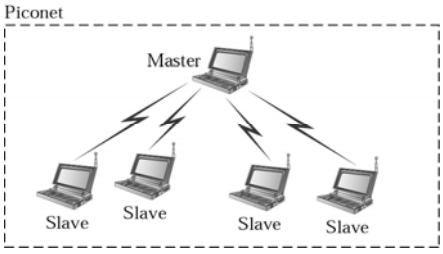
 U2.282

Bluetooth

There are two types of topology for Bluetooth – Piconet, Scatternet. The Piconet is a small ad hoc network of devices (normally 8 stations) as shown in Fig. It has the following features:

- One is called Master and the others are called Slaves
- All slave stations synchronizes their clocks with the master
- Possible communication - One-to-one or one-to-many
- There may be one station in parked state
- Each piconet has a unique hopping pattern/ID
- Each master can connect to 7 simultaneous or 200+ inactive (parked) slaves per piconet

Piconet

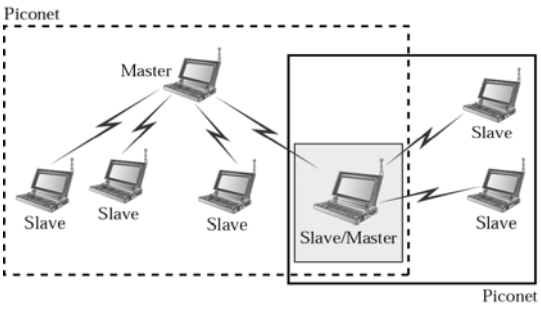


Scatternet

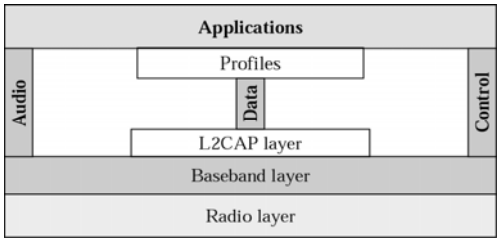
By making one slave as master of another Piconet, Scatternet is formed by combining several Piconets as shown in Fig. Key features of the scatternet topology are mentioned below:

• A Scatternet is the linking of multiple co-located piconets through the sharing of common master or slave devices.
• A device can be both a master and a slave.
• Radios are symmetric (same radio can be master or slave).
• High capacity system, each piconet has maximum capacity (720 Kbps)

Scatternet



Bluetooth Layers



Bluetooth Layers

The Bluetooth architecture, showing all the major layers in the Bluetooth system, are depicted in the Fig.

The layers below can be considered to be different hurdles in an obstacle course.

This is because all the layers function one after the other. One layer comes into play only after the data has been through the previous layer.

Bluetooth Layers

• **Radio:** The Radio layer defines the requirements for a Bluetooth transceiver operating in the 2.4 GHz ISM band.

• **Baseband:** The Baseband layer describes the specification of the Bluetooth Link Controller (LC), which carries out the baseband protocols and other low-level link routines. It specifies Piconet/Channel definition, "Low-level" packet definition, Channel sharing

• **LMP:** The Link Manager Protocol (LMP) is used by the Link Managers (on either side) for link set-up and control.
• **HCI:** The Host Controller Interface (HCI) provides a command interface to the Baseband Link Controller and Link Manager, and access to hardware status and control registers.

 U2.289

Bluetooth Layers

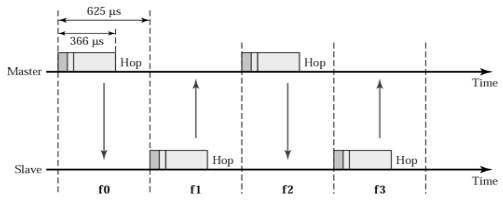
• **L2CAP:** Logical Link Control and Adaptation Protocol (L2CAP) supports higher level protocol multiplexing, packet segmentation and reassembly, and the conveying of quality of service information.

• **RFCOMM:** The RFCOMM protocol provides emulation of serial ports over the L2CAP protocol. The protocol is based on the ETSI standard TS 07.10.

• **SDP:** The Service Discovery Protocol (SDP) provides a means for applications to discover, which services are provided by or available through a Bluetooth device. It also allows applications to determine the characteristics of those available services.

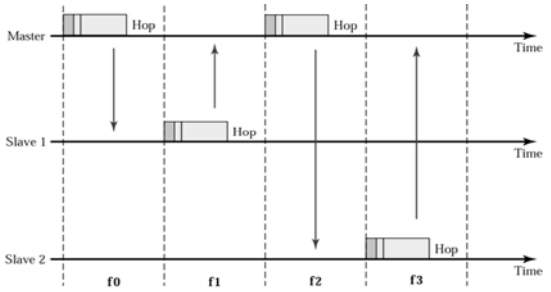
 U2.290

Single-Slave Communication



 U2.291

Multiple-Slave Communication



 U2.292

Conclusion

- Medium Access control can be random access, controlled or channelised.
- In CSMA station must listen to the medium first
- CSMA/CD is CSMA with post collision procedure
- CSMA/CA is CSMA with procedure that avoids collision

 U2.293

Summary

- Medium Access control can be random acess, controlled or channelised.
- In CSMA station must listen to the medium first
- CSMA/CD is CSMA with post collision procedure
- CSMA/CA is CSMA with procedure that avoids collision

 U2.294

Review Questions (OBJ)

1. In cyclic redundancy checking, the divisor is _____ the CRC.
A) The same size as
B) one bit less than
C) one bit more than
D) none of the above

2. The _____of errors is more difficult than the _____.
A) correction; detection
B) detection; correction
C) creation; correction
D) creation; detection

Review Questions (OBJ)

3. The checksum of 1111 and 1111 is _____.
A) 1111
B) 0000
C) 1110
D) 0111

4. The divisor in a cyclic code is normally called the _____.
A) degree
B) generator
C) redundancy
D) none of the above

Review Questions (OBJ)

5. In a Go-Back-N ARQ, if the window size is 63, what is the range of sequence numbers?
A) 0 to 63
B) 0 to 64
C) 1 to 63
D) 1 to 64

6. In Go-Back-N ARQ, if frames 4, 5, and 6 are received successfully, the receiver may send an ACK _____ to the sender.
A) 5
B) 6
C) 7
D) any of the above

Review Questions (OBJ)

7. HDLC is an acronym for _____.
A) High-duplex line communication
B) High-level data link control
C) Half-duplex digital link combination
D) Host double-level circuit
8. Both Go-Back-N and Selective-Repeat Protocols use a _____.
A) sliding frame
B) sliding window
C) sliding packet
D) none of the above

Review Questions (OBJ)

9. In Selective Repeat ARQ, if 5 is the number of bits for the sequence number, then the maximum size of the send window must be _____
A) 15
B) 16
C) 31
D) 1

10. ARQ stands for _____.
A) Automatic repeat quantization
B) Automatic repeat request
C) Automatic retransmission request
D) Acknowledge repeat request

Review Questions (Short)

1. What is advantage of controlled access over random access?
2. How do two persistence strategies differ?
3. What is purpose of Jam signal in CSMA/CD?
4. Why is token passing a controlled access procedure?
5. Compare and contrast Go Back N and Selective repeat
6. Define piggybacking and its usefulness
7. What is access method used in wireless lans?
8. Find the checksum of the following bi sequence. Assume 8-bit segment size
   10010011 10010011 1001100 01001101

Review Questions (Short)

9. How are a lost acknowledgement a lost frame handled at the sender site in Go-Back-N ARQ ?
10. What are the various layers involved in Gigabit Ethernet. Explain
11. What is Frequency Hopping Spread Spectrum . Explain.
12. Construct the Hamming code for the bit sequence 1001101.
13. What is the relationship between AMPS and D-AMPS in Mobile Phones?
14. Explain the procedure of CSMA/CD

 U2.301

Review Questions (Long)

1. Describe the services provided by Data Link Layer
2. Define the frame format for HDLC? Describe all the options for all three frames in detail?
3. Compare flow control and error control ?
4. Describe various types of messages in ICMP protocol.
5. Compare and contrast IPV4 and IPV6.
6. Differentiate between Go-back n and Selective repeat .sliding window?
7. Explain the layering of Gigabit Ethernet
8. What is purpose of NAV

 U2.302

Recommended reading

1. Forozun, Data Communication and Networking, TMH
2. Tanenbaum , A computer Networks: Prentice Hall
3. Stallings , High speed Networks :Prentice Hall
4. Comer D. Computer Networks: Prentice hall
5. Kurose, J and ross , Computer Networking : Addison Wesley

 U2.303