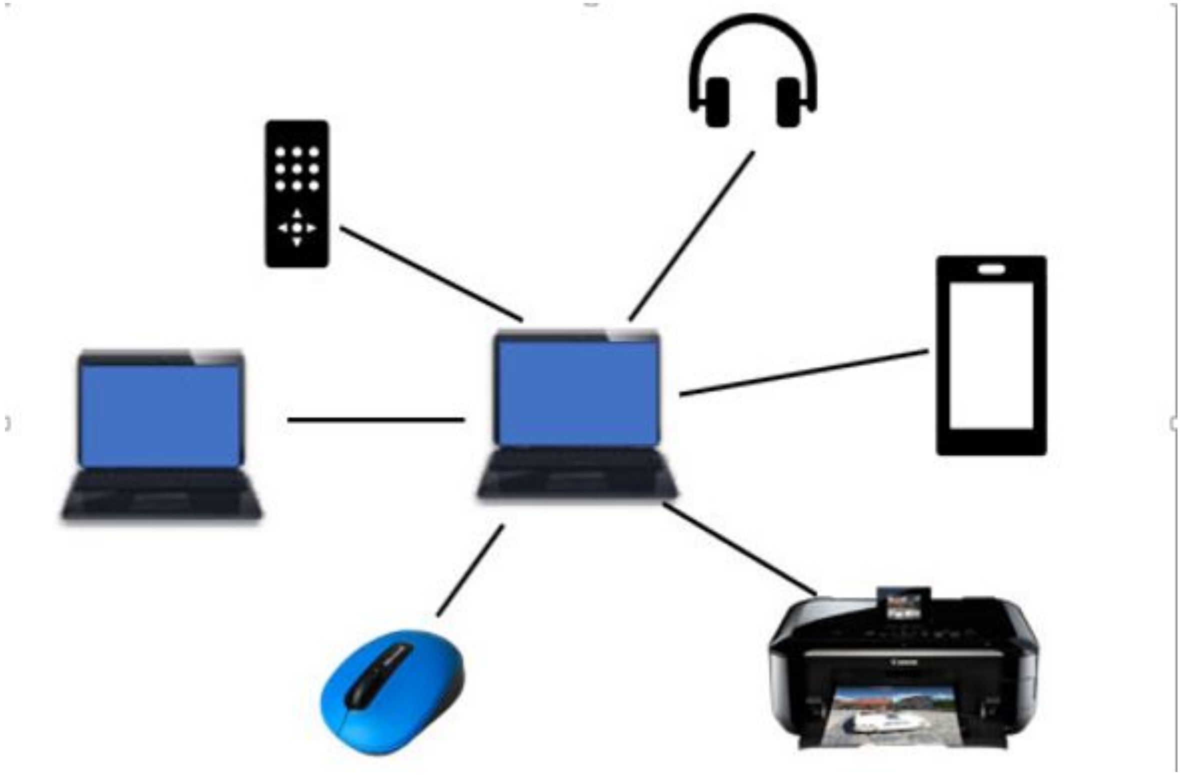
UNIT 2

Getting Connected



By Adithya D A (ADA)
Assistant Professor, AI and ML
BMSCE ,Bangalore.

Chapter Outline

- Perspectives on Connecting nodes
- Encoding
- Framing
- Error Detection
- Reliable Transmission
- Ethernet and Multiple Access Networks
- Wireless Networks

Chapter Goal

- Exploring different communication medium over which we can send data
- Understanding the issue of encoding bits onto transmission medium so that they can be understood by the receiving end
- Discussing the matter of delineating the sequence of bits transmitted over the link into complete messages that can be delivered to the end node
- Discussing different technique to detect transmission errors and take the appropriate action

Chapter Goal (contd.)

- Discussing the issue of making the links reliable in spite of transmission problems
- Introducing Media Access Control Problem
- Introducing Carrier Sense Multiple Access (CSMA) networks
- Introducing Wireless Networks with different available technologies and protocol

Perspectives on Connecting

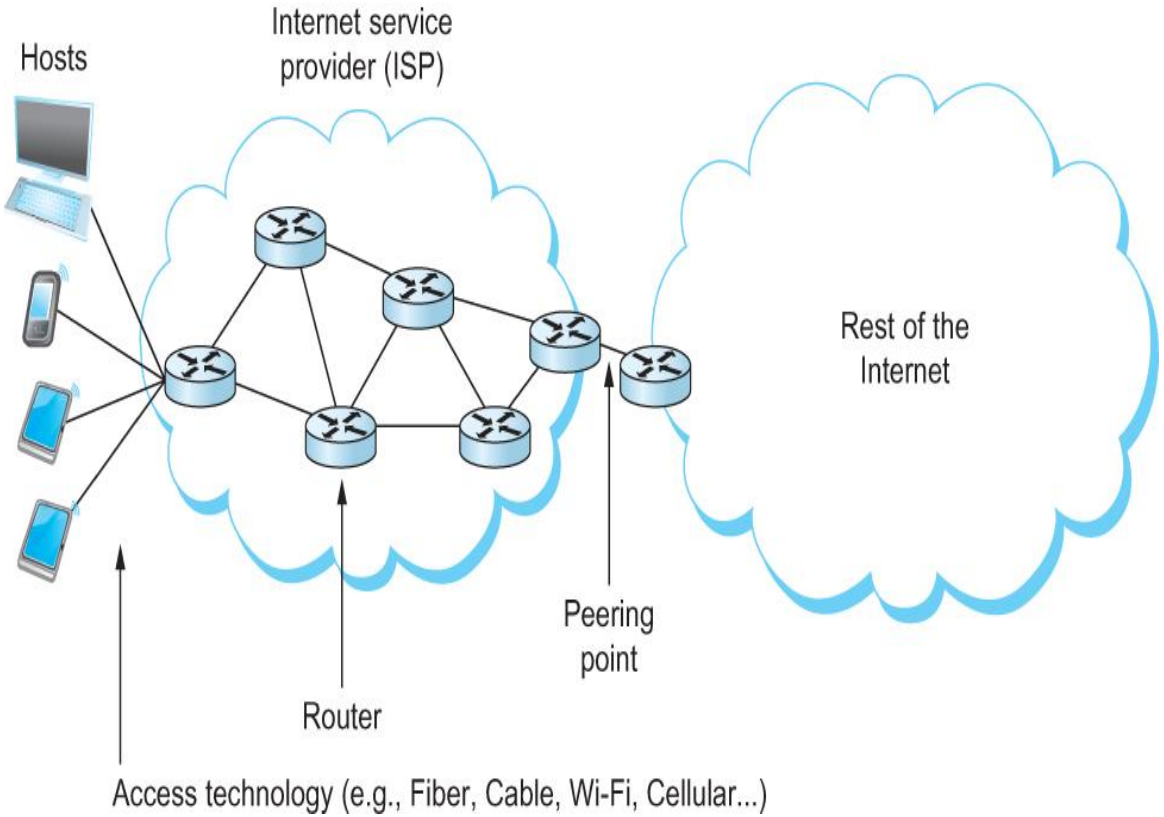

Hosts
Internet service provider (ISP)
Rest of the Internet
Peering point
Router
Access technology (e.g., Fiber, Cable, Wi-Fi, Cellular...)

FIGURE 2 : An end-user's view of the Internet.

- Figure 2.1 illustrates various types of links as seen by a typical end-user of today's Internet. On the left, we see a variety of end-user devices ranging from mobile phones to PDAs to full-fledged computers connected by various means to an Internet Service Provider.
- While those links might be of any type mentioned above, or some other type, they all look the same in this picture—a straight line connecting a device to a router. Also, there are some links that connect routers together inside the ISP and a link that connects the ISP to the "rest of the Internet,"

- By the end of this chapter, we'll understand how to send complete packets over just about any sort of link, no matter what physical medium is involved.

Perspectives on Connecting

- **How do we make all these different types of link look sufficiently alike to end users and routers? Essentially, we have to deal with all the physical limitations and shortcomings of links that exist in the real world.**
- **We sketched out some of these issues in the opening problem statement for this chapter.**

- **Issues:**
  - The first issue is that links are made of some physical material that can propagate signals (such as radio waves or other sorts of electromagnetic radiation), but what we really want to do is send bits.
  - we'll look at how to encode bits for transmission on a physical medium, followed by the other issues.
  - **By the end of this chapter, we'll understand how to send complete packets over just about any sort of link, no matter what physical medium is involved.**

Link Capacity and Shannon-Hartley Theorem

- Shannon-Hartley Theorem : Gives the upper bound to the capacity of a link in terms of bits per second (bps) as a function of signal-to-noise ratio of the link measured in decibels (dB) and bandwidth of channel measured in hertz(hz)
- As an example, we can apply the Shannon-Hartley theorem to determine the rate at which a dial-up modem can be expected to transmit binary data over a voice-grade phone line without suffering from too high an error rate.
- The theorem is typically given by the following formula:
- $C = B \log2 (1 + S/N)$
- where C is the achievable channel capacity measured in bits per second.
- B is the bandwidth of the channel in Hz.
- S is the average signal power and
- N is the average noise power.

Classes of Links

- One way to characterize links, then, is by the medium they use :
- 1. Typically copper wire in some form (as in Digital Subscriber Line (DSL) and coaxial cable),
- 2.Optical fiber (as in both commercial fiber-to-the home services and many long-distance links in the Internet’s backbone), or Air/free space (for wireless links).
- 3.Another important link characteristic is the frequency Measured in hertz, with which the electromagnetic waves oscillate
- Wave length : Distance between the adjacent pair of maxima or minima of a wave measured in meters is called wavelength.
- Modulation :involves modifying the signals in terms of their frequency, amplitude, and phase.

Classes of Links.

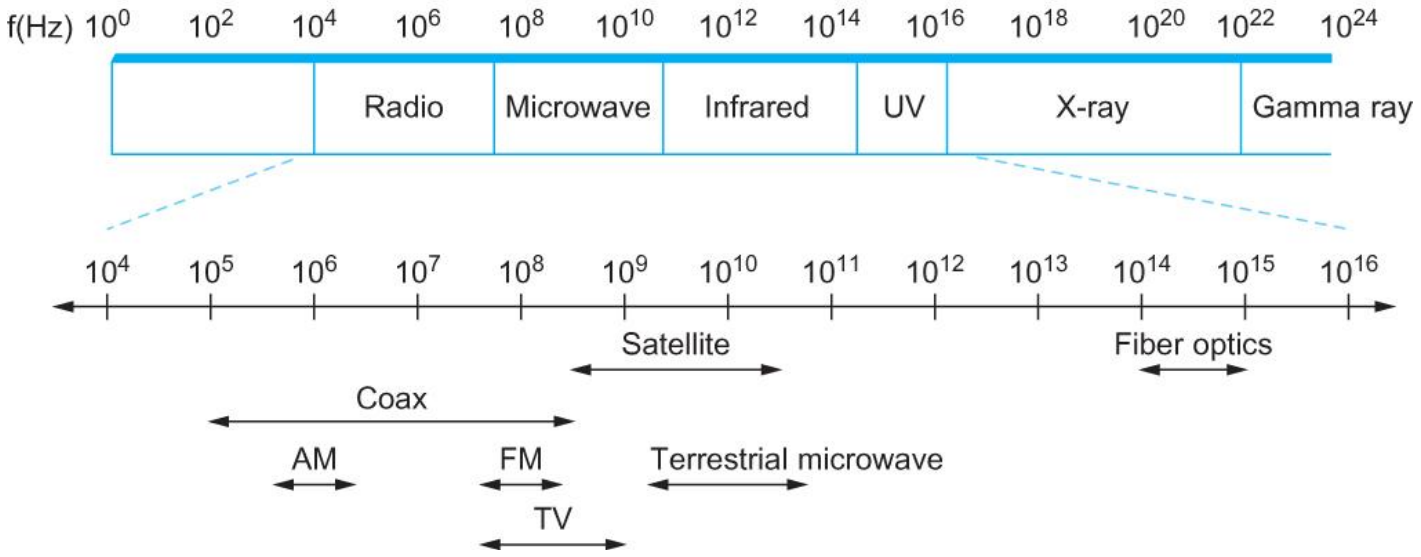
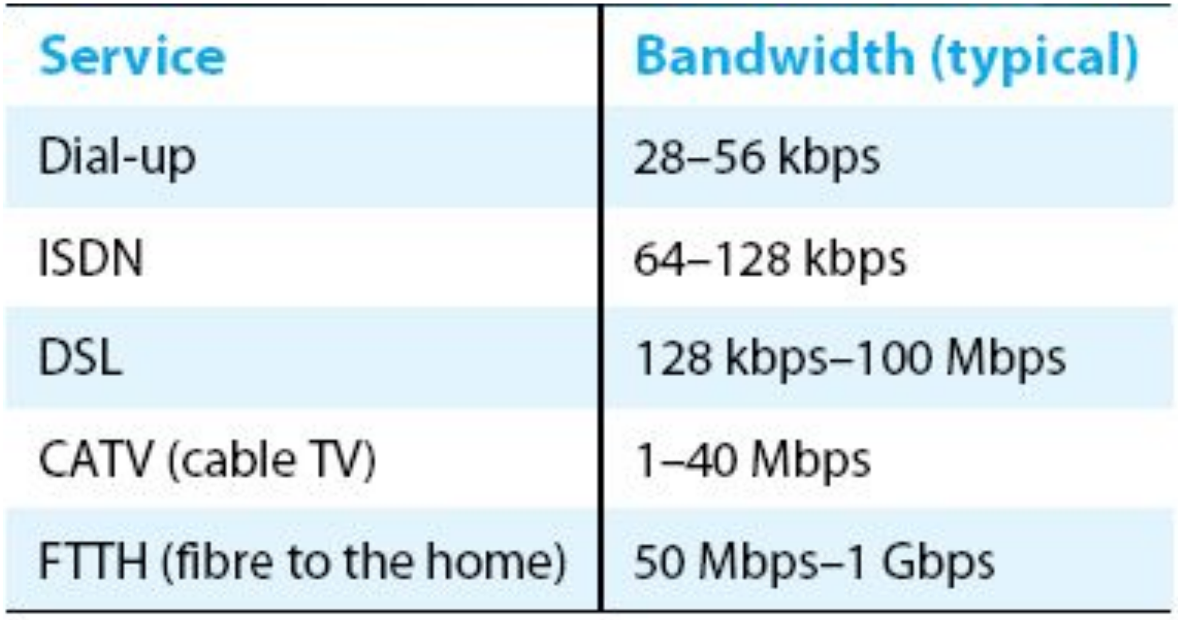


Figure depicts the electromagnetic spectrum and shows which media are commonly used to carry which frequency bands.



Service	Bandwidth (typical)
Dial-up	28–56 kbps
ISDN	64–128 kbps
DSL	128 kbps–100 Mbps
CATV (cable TV)	1–40 Mbps
FTTH (fibre to the home)	50 Mbps–1 Gbps

ISDL : Integrated Services Digital Network.
DSL : Digital subscriber Line

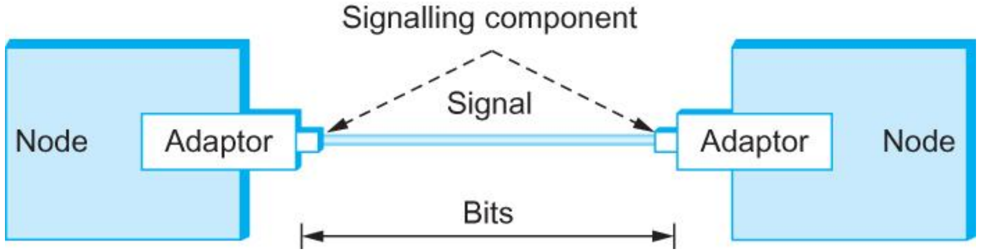
Table 2.1 Common Services Available to Connect Your Home

1.Encoding (NRZ, NRZI, MANCHESTER, 4B/5B)

- Encoding : is **the process of converting the data or a given sequence of characters, symbols, alphabets etc**., into a specified format, for the secured transmission of data.

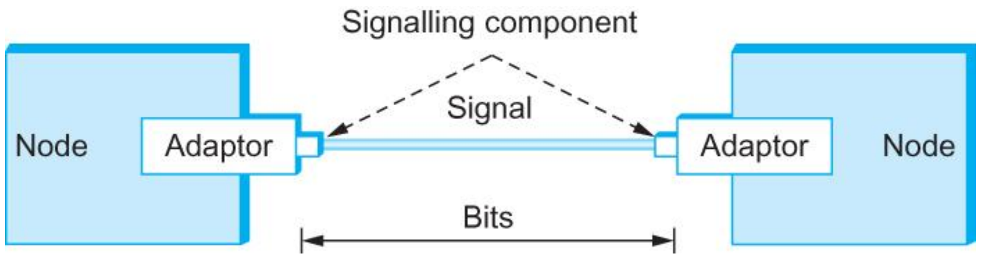
The task, therefore, is to encode the binary data that the source node wants to send into the signals that the links are able to carry and then to decode the signal back into the corre- sponding binary data at the receiving node.

Most of the functions discussed in this chapter are performed by a net-work adaptor—a piece of hardware that connects a node to a link. The network adaptor contains a signaling component that actually encodes bits into signals at the sending node and decodes signals into bits at the receiving node.



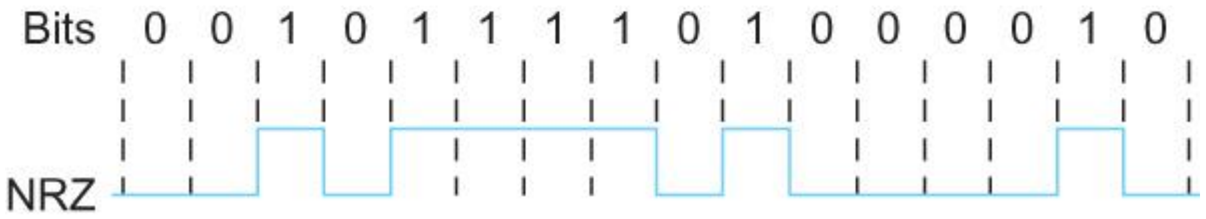
1 . Non-return to zero (NRZ) :

To map the data value 1 onto the high signal and the data value 0 onto the low signal. This is exactly the mapping used by an encoding scheme called, cryptically enough, non-return to zero (NRZ).



Signals travel between signaling components; bits flow between adaptors

For example, Figure 2.4 schematically depicts the NRZ-encoded signal (bottom) that corresponds to the transmission of a particular sequence of bits (top).



NRZ encoding of a bit stream

For example, Figure 2.4 schematically depicts the NRZ-encoded signal (bottom) that corresponds to the transmission of a particular sequence of bits (top).

Encoding

- Problem with NRZ
  - Baseline wander
    - The receiver keeps an average of the signals it has seen so far
    - Uses the average to distinguish between low and high signal
    - When a signal is significantly low than the average, it is 0, else it is 1
    - Too many consecutive 0’s and 1’s cause this average to change, making it difficult to detect

Problem with NRZ

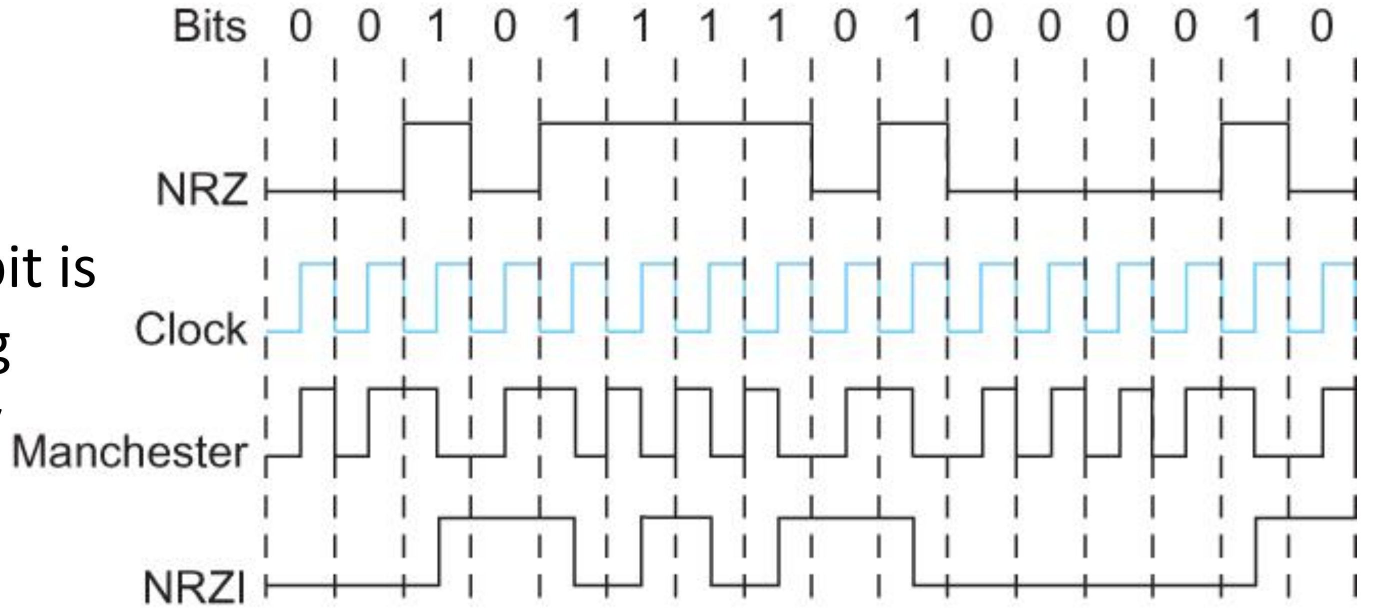
Clock recovery

- Frequent transition from high to low or vice versa are necessary to enable clock recovery
- Both the sending and decoding process is driven by a clock
- Every clock cycle, the sender transmits a bit and the receiver recovers a bit
- The sender and receiver have to be precisely synchronized

2. NRZI

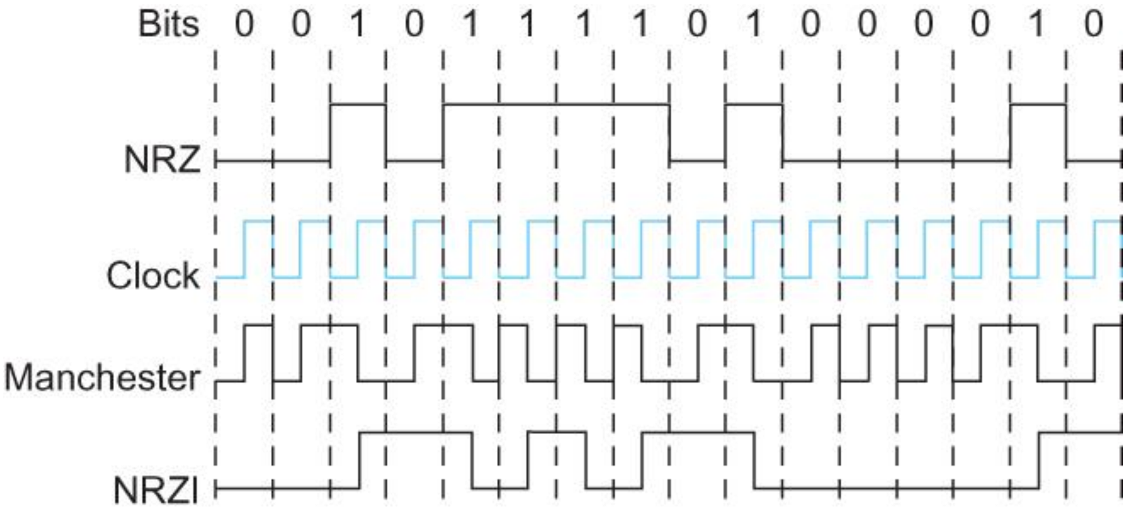
- Non Return to Zero Inverted
- Sender makes a transition from the current signal to encode 1 and stay at the current signal to encode 0
- Solves for consecutive 1’s

NRZI maps binary signals to physical signals during transmission. If a data bit is 1, NRZI transitions at the clock boundary. If a data bit is 0, there is no transition. NRZI may have long series of 0s or 1s, resulting in clock recovery difficulties.



3.Manchester encoding

- Manchester encoding
  - Merging the clock with signal by transmitting Ex-OR of the NRZ encoded data and the clock
  - Clock is an internal signal that alternates from low to high, a low/high pair is considered as one clock cycle
  - In Manchester encoding
    - 0: low□ high transition
    - 1: high□ low transition



- Problem with Manchester encoding
    - Doubles the rate at which the signal transitions are made on the link
        - Which means the receiver has half of the time to detect each pulse of the signal
    - The rate at which the signal changes is called the link’s baud rate
    - In Manchester the bit rate is half the baud rate

4 . 4B/5B encoding

- 4B/5B encoding
  - Insert extra bits into bit stream so as to break up the long sequence of 0’s and 1’s
  - Every 4-bits of actual data are encoded in a 5- bit code that is transmitted to the receiver
  - 5-bit codes are selected in such a way that each one has no more than one leading 0(zero) and no more than two trailing 0’s.
  - No pair of 5-bit codes results in more than three consecutive 0’s

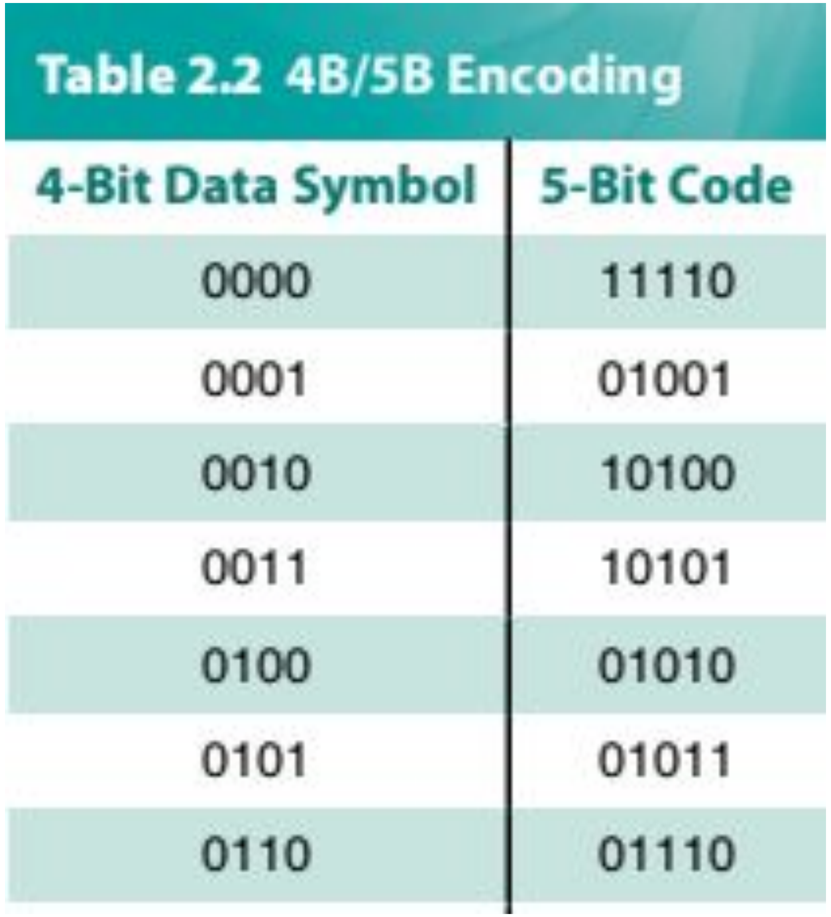


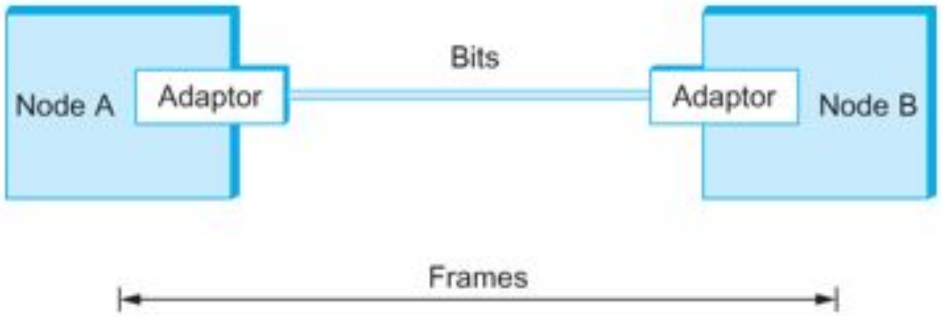
Table 2.2 4B/5B Encoding

4-Bit Data Symbol	5-Bit Code
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110

2. Framing(Framing is a point-to-point connection between two computers or devices consists of a wire in which data is transmitted as a stream of bits)

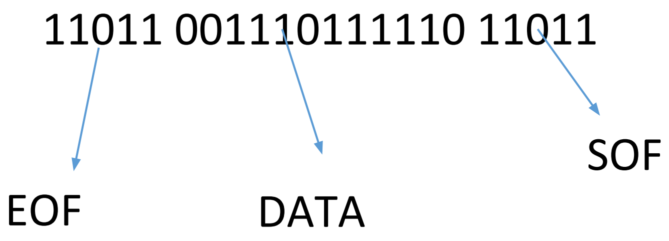
- We are focusing on packet-switched networks, which means that blocks of data (called *frames* at this level), not bit streams, are exchanged between nodes.
- It is the network adaptor that enables the nodes to exchange frames.

- It is the network adaptor that enables the nodes to exchange frames.



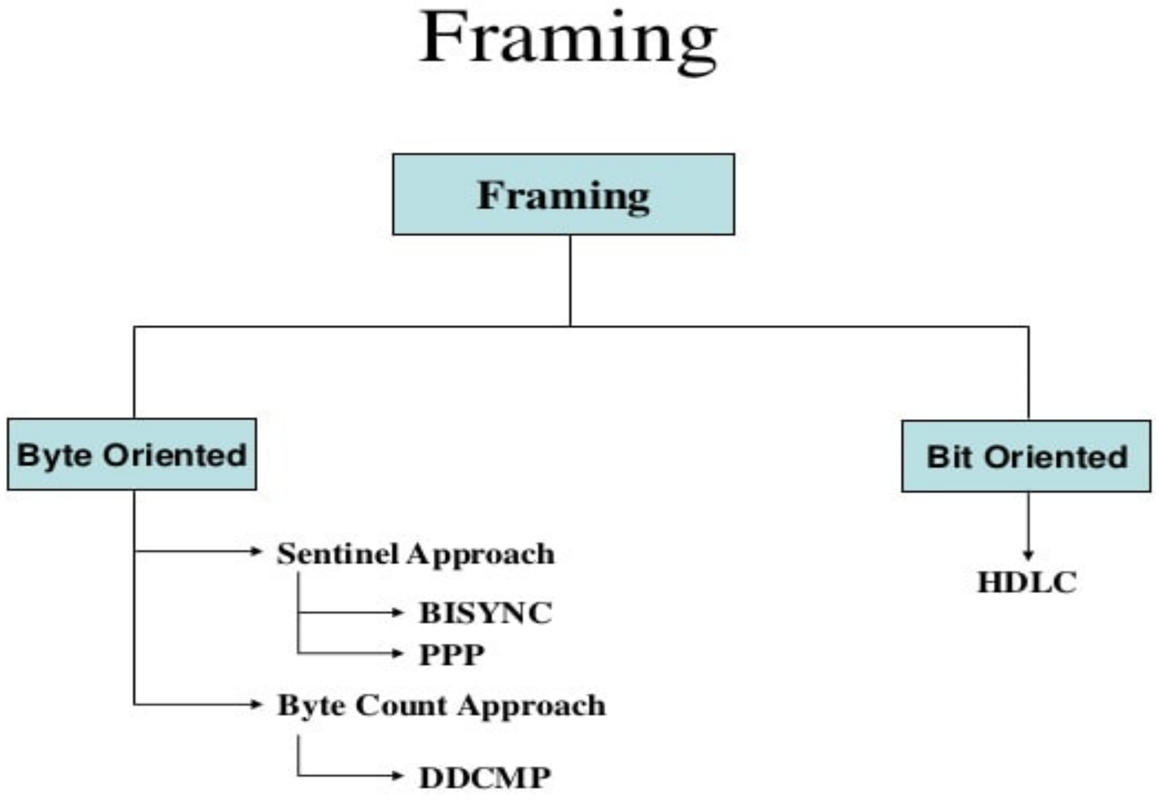
Bits flow between adaptors, frames between hosts

Bits Flow Between Adaptors
Frames flow between nodes/hosts



- When node A wishes to transmit a frame to node B, it tells its adaptor to transmit a frame from the node’s memory. This results in a sequence of bits being sent over the link.
- The adaptor on node B then collects together the sequence of bits arriving on the link and deposits the corresponding frame in B’s memory.
- Recognizing exactly what set of bits constitute a frame—that is, determining where the frame begins and ends—is the central challenge faced by the adaptor

Types of Framing.



Framing

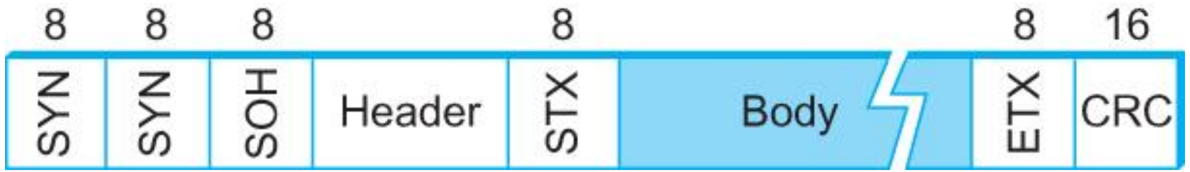
- **Byte-oriented Protocols(BISYNC, PPP, DDCMP)**
- one of the oldest approaches to framing—it has its roots in connecting terminals to mainframes—is to view each frame as a collection of bytes (characters) rather than a collection of bits.

  - To view each frame as a collection of bytes (characters) rather than bits
  - BISYNC (Binary Synchronous Communication) Protocol
    - Developed by IBM (late 1960)
  - Point-to-Point Protocol(PPP)
  - DDCMP (Digital Data Communication Protocol)
    - Used in DECNet (Digital Equipment Corporation’s)

BISYNC (Binary Synchronous Communication) Protocol

- BISYNC – sentinel approach
  - Frames transmitted beginning with leftmost field
  - Beginning of a frame is denoted by sending a special SYN (synchronize) character
  - Data portion of the frame is contained between special sentinel character STX (start of text) and ETX (end of text)
  - SOH : Start of Header
  - CRC: Cyclic Redundancy Check

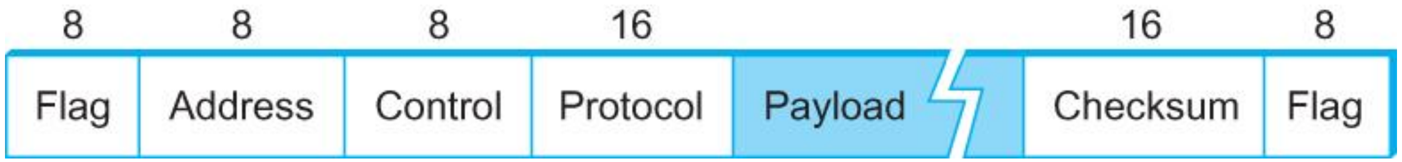
(which is used to detect transmission errors;)



BISYNC Frame Format

Point-to-Point Protocol(PPP)

- Recent PPP which is commonly run over Internet links uses sentinel approach
  - Special start of text character denoted as Flag
    - 0 1 1 1 1 1 1 0
  - Address, control : default numbers
  - Protocol for demux : IP / IPX
  - Payload : negotiated (1500 bytes) - the portion of the transmitted data packet which holds the actual message(variable in length)
  - Checksum : for error detection

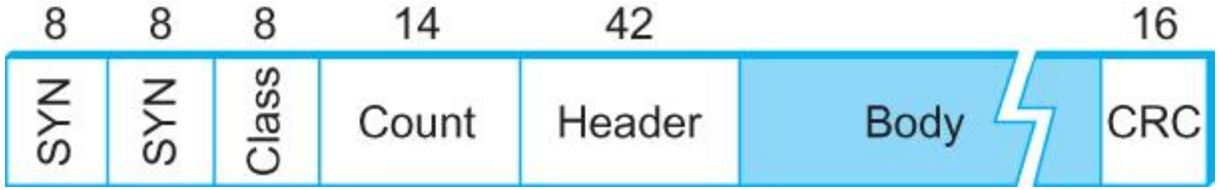


8	8	8	16		16	8
Flag	Address	Control	Protocol	Payload	Checksum	Flag

PPP Frame Format

DDCMP (Digital Data Communication Protocol)

- Byte-counting approach
  - DDCMP
  - *count* : how many bytes are contained in the frame body
  - If *count* is corrupted
    - Framing error
  - A class field of 8 bits.

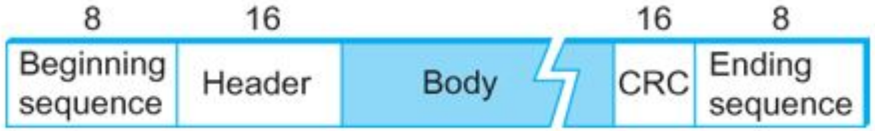


DDCMP Frame Format

- Bit-oriented Protocol

- Bit-oriented Protocol
  - HDLC : High Level Data Link Control
    - Beginning and Ending Sequences

      0 1 1 1 1 1 1 0



HDLC Frame Format

- HDLC Protocol
    - On the sending side, any time five consecutive 1’s have been transmitted from the body of the message (i.e. excluding when the sender is trying to send the distinguished 0111110 sequence)
        - The sender inserts 0 before transmitting the next bit

- HDLC Protocol
  - On the receiving side
    - 5 consecutive 1’s
      - Next bit 0 : Stuffed, so discard it

        1 : Either End of the frame marker

        Or Error has been introduced in the bitstream

        Look at the next bit

        If 0 (0111110) □ End of the frame marker

        If 1 (0111111) □ Error, discard the whole frame

        The receiver needs to wait for next

        01111110 before it can start

        receiving again

Error Detection

- Bit errors are introduced into frames
  - Because of electrical interference and thermal noises
- Detecting Error
- Correction Error
- Two approaches when the recipient detects an error
  - Notify the sender that the message was corrupted, so the sender can send again.
    - If the error is rare, then the retransmitted message will be error-free
  - Using some error correct detection and correction algorithm, the receiver reconstructs the message

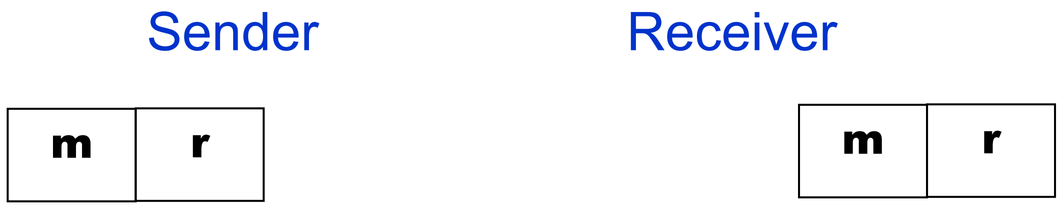
Error Detection

- Common technique for detecting transmission error
  - Two Dimensional Parity (BISYNC)
  - Checksum (IP)
  - Cyclic redundancy check (CRC)

- Basic Idea of Error Detection
  - To add redundant information to a frame that can be used to determine if errors have been introduced
  - Imagine (Extreme Case)
    - Transmitting two complete copies of data
      - Identical □ No error
      - Differ □ Error
      - Poor Scheme ???
        - n bit message, n bit redundant information
        - Error can go undetected
    - In general, we can provide strong error detection technique
      - k redundant bits, n bits message, k << n
      - In Ethernet, a frame carrying up to 12,000 bits of data requires only 32-bit CRC

Error Detection

- Extra bits are redundant
  - They add no new information to the message
  - Derived from the original message using some algorithm
  - Both the sender and receiver know the algorithm



Sender

Receiver

Receiver computes *r* using *m*

If they match, no error

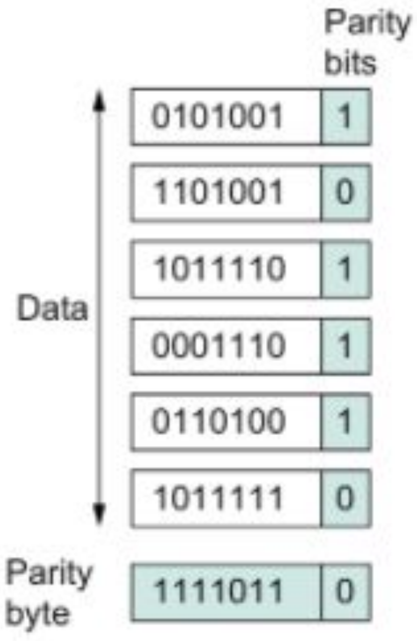
Two-dimensional parity

- Two-dimensional parity is exactly what the name suggests
- It is based on “simple” (one-dimensional) parity, which usually involves adding one extra bit to a 7-bit code to balance the number of 1s in the byte. For example,
  - Odd parity sets the eighth bit to 1 if needed to give an odd number of 1s in the byte, and
  - Even parity sets the eighth bit to 1 if needed to give an even number of 1s in the byte

Two-dimensional parity

- Two-dimensional parity does a similar calculation for each bit position across each of the bytes contained in the frame
- Two-dimensional parity catches all 1-, 2-, and 3-bit errors and most 4-bit errors

Two Dimensional Parity



0101001	1
1101001	0
1011110	1
0001110	1
0110100	1
1011111	0
1111011	0

Two Dimensional Parity

Internet Checksum Algorithm

- Not used at the link level
- Add up all the words that are transmitted and then transmit the result of that sum
  - The result is called the checksum
- The receiver performs the same calculation on the received data and compares the result with the received checksum
- If any transmitted data, including the checksum itself, is corrupted, then the results will not match, so the receiver knows that an error occurred

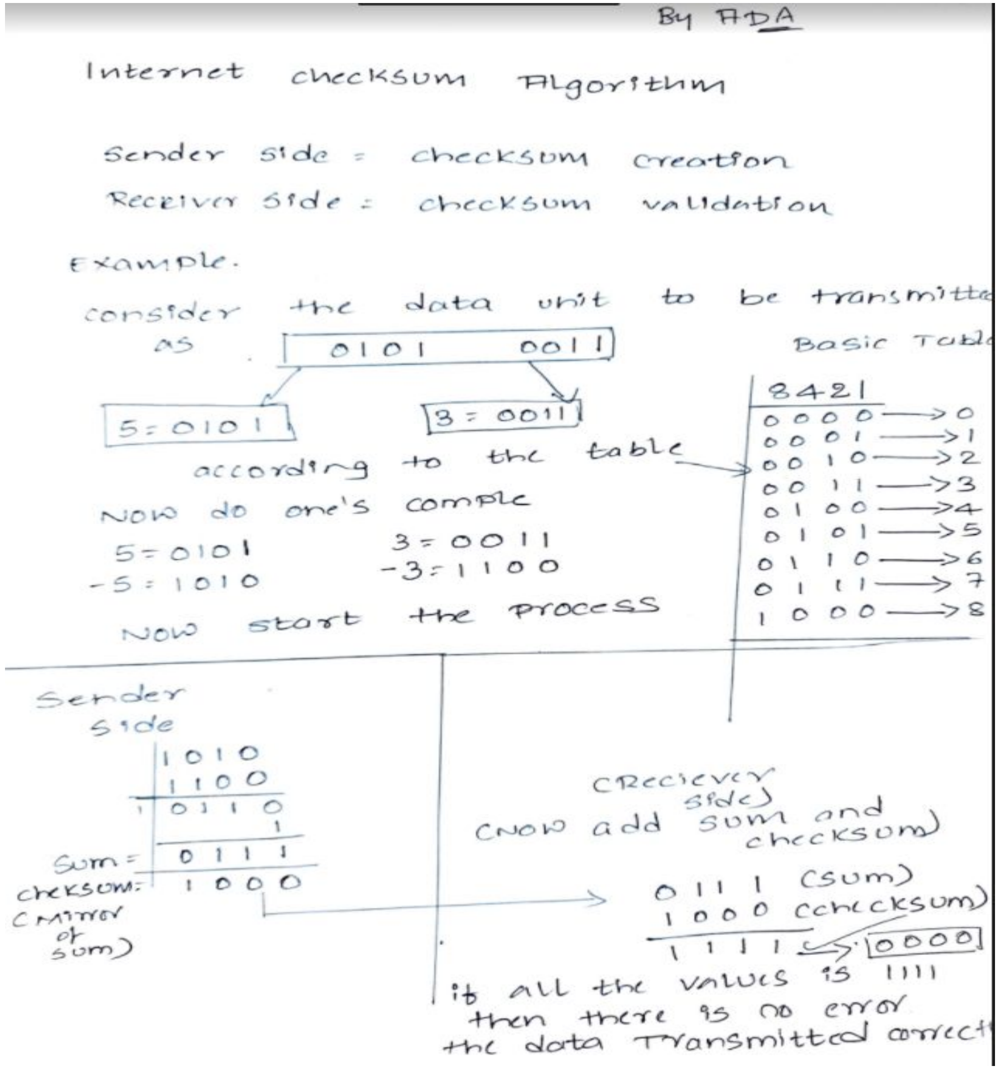
Internet Checksum Algorithm

- In ones complement arithmetic, a negative integer −x is represented as the complement of x;
  - Each bit of x is inverted.
- When adding numbers in ones complement arithmetic, a carryout from the most significant bit needs to be added to the result.

Internet Checksum Algorithm

- Consider, for example, the addition of −5 and −3 in ones complement arithmetic on 4-bit integers
  - +5 is 0101, so −5 is 1010; +3 is 0011, so −3 is 1100
- If we add 1010 and 1100 ignoring the carry, we get 0110
- In ones complement arithmetic, the fact that this operation caused a carry from the most significant bit causes us to increment the result, giving 0111, which is the ones complement representation of −8 (obtained by inverting the bits in 1000), as we would expect

Internet Checksum Algorithm



By ADA

Internet checksum Algorithm

Sender side = checksum creation

Receiver side = checksum validation

Example.

consider the data unit to be transmitte as

0101 0011

5 = 0101 3 = 0011

according to the table

Basic Tabl

8421	
0000	→ 0
0001	→ 1
0010	→ 2
0011	→ 3
0100	→ 4
0101	→ 5
0110	→ 6
0111	→ 7
1000	→ 8

Now do one's comple

5 = 0101 3 = 0011

-5 = 1010 -3 = 1100

Now start the process

Sender side

```
          1010
          1100
        -------
        1 0110
             1
        -------
Sum =     0111
        -------
cheksum = 1000
(Mirror
 of
 sum)
```

(Reciever side)

(Now add sum and checksum)

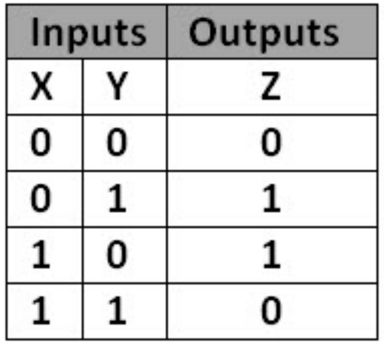
```
  0111  (sum)
  1000  (checksum)
  ----
  1111  -> 0000
```

if all the values is 1111 then there is no error the data Transmitted correct

Cyclic Redundancy Check (CRC)

1. Find the Length of Divisor ‘L’
2. Appended “L-1” bits to the original message
3. Perform Binary division operation
4. Remainder of division is CRC

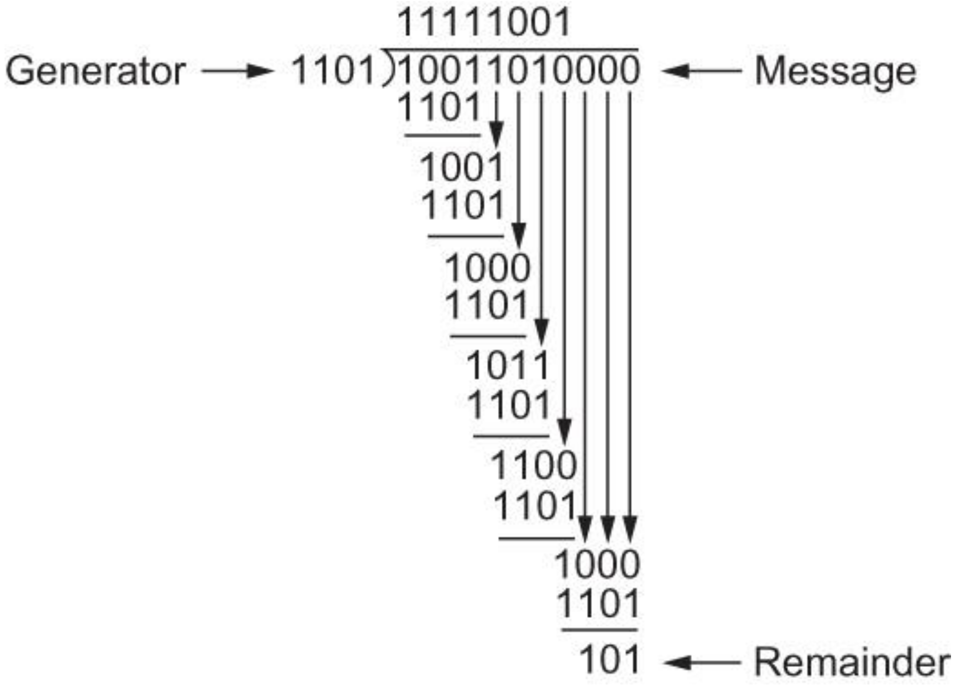
Remember XOR table to solve the CRC



Inputs		Outputs
X	Y	Z
0	0	0
0	1	1
1	0	1
1	1	0

XOR Table

Find CRC for 10011010 with divisor 1101



CRC = 101
Data Transmitted =
100110010**101**

- Six generator polynomials that have become international standards are:
  - CRC-8 = x^8+x^2+x+1
  - CRC-10 = $x^{10}+x^9+x^5+x^4+x+1$
  - CRC-12 = $x^{12}+x^{11}+x^3+x^2+x+1$
  - CRC-16 = $x^{16}+x^{15}+x^2+1$
  - CRC-CCITT = $x^{16}+x^{12}+x^5+1$
  - CRC-32 = $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$

Reliable Transmission

- CRC is used to detect errors.
- Some error codes are strong enough to correct errors.
- The overhead is typically too high.
- **Corrupt frames must be discarded.**
- **A link-level protocol that wants to deliver frames reliably must recover from these discarded frames.**
- **This is accomplished using a combination of two fundamental mechanisms**
  - **Acknowledgements and Timeouts**

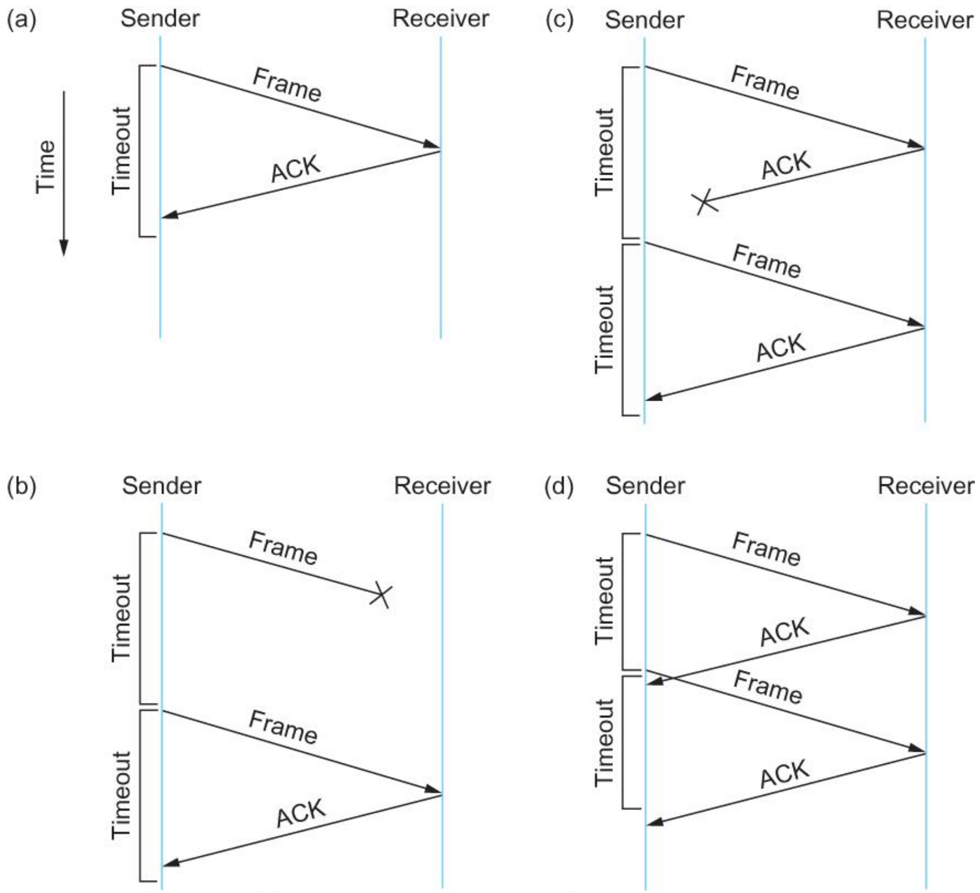
- An *acknowledgement* (ACK for short) is a small control frame that a protocol sends back to its peer saying that it has received the earlier frame.
    - A control frame is a frame with header only (no data).
- The receipt of an *acknowledgement* indicates to the sender of the original frame that its frame was successfully delivered.

- If the sender does not receive an *acknowledgment* after a reasonable amount of time, then it retransmits the original frame.
- The action of waiting a reasonable amount of time is called a ***timeout*.**
- The general strategy of using *acknowledgements* and *timeouts* to implement reliable delivery is sometimes called **Automatic Repeat reQuest (ARQ).**

Stop and Wait Protocol

- Idea of stop-and-wait protocol is straightforward
  - After transmitting one frame, the sender waits for an acknowledgement before transmitting the next frame.
  - If the acknowledgement does not arrive after a certain period of time, the sender times out and retransmits the original frame

Stop and Wait Protocol

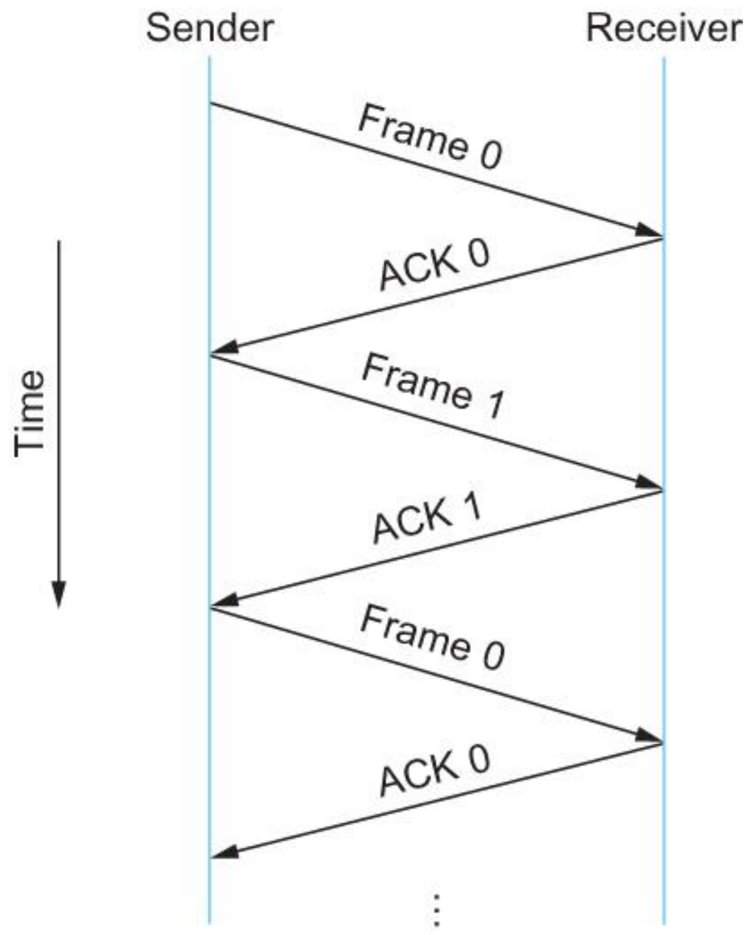


Timeline showing four different scenarios for the stop-and-wait algorithm.

(a) The ACK is received before the timer expires; (b) the original frame is lost; (c) the

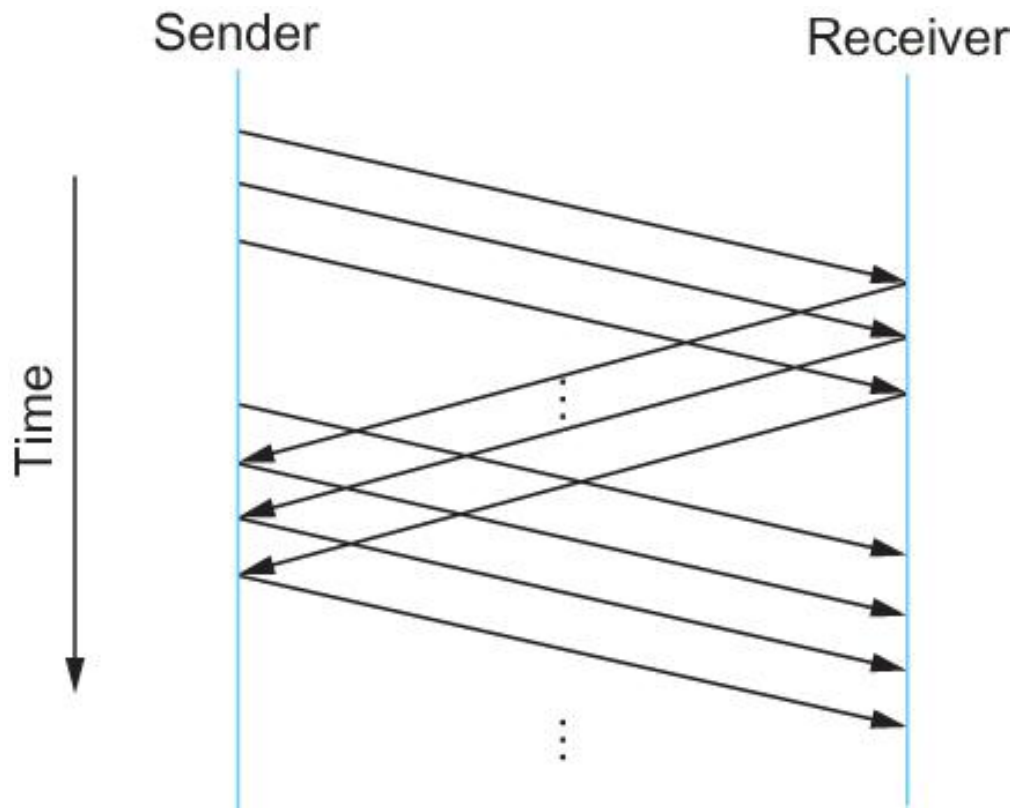
- If the acknowledgment is lost or delayed in arriving
    - The sender times out and retransmits the original frame, but the receiver will think that it is the next frame since it has correctly received and acknowledged the first frame
    - As a result, duplicate copies of frames will be delivered

- How to solve this
    - Use 1 bit sequence number (0 or 1)
    - When the sender retransmits frame 0, the receiver can determine that it is seeing a second copy of frame 0 rather than the first copy of frame 1 and therefore can ignore it (the receiver still acknowledges it, in case the first acknowledgement was lost)



Timeline for stop-and-wait with 1-bit sequence number

Sliding Window Protocol



Timeline for Sliding Window Protocol

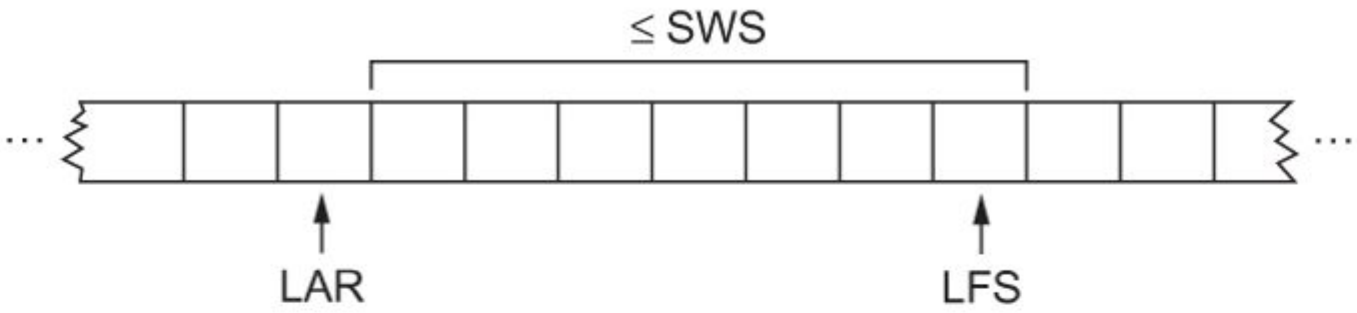
Sliding Window Protocol

- Sender assigns a sequence number denoted as SeqNum to each frame.
    - Assume it can grow infinitely large

- Sender maintains three variables
    - Sending Window Size (SWS)
        - Upper bound on the number of outstanding (unacknowledged) frames that the sender can transmit
    - Last Acknowledgement Received (LAR)
        - Sequence number of the last acknowledgement received
    - Last Frame Sent (LFS)
        - Sequence number of the last frame sent

- Sender also maintains the following invariant

  $$\text{LFS} - \text{LAR} \leq \text{SWS}$$

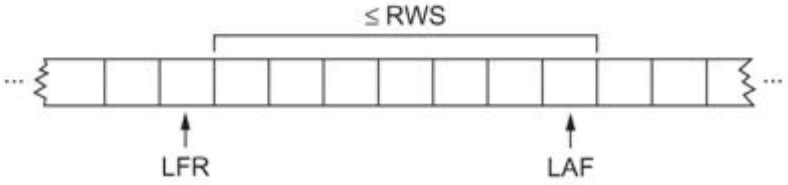


Sliding Window on Sender

- When an acknowledgement arrives
  - the sender moves LAR to right, thereby allowing the sender to transmit another frame
- Also the sender associates a timer with each frame it transmits
  - It retransmits the frame if the timer expires before the ACK is received
- Note that the sender has to be willing to buffer up to SWS frames

- Receiver maintains three variables
  - Receiving Window Size (RWS)
    - Upper bound on the number of out-of-order frames that the receiver is willing to accept
  - Largest Acceptable Frame (LAF)
    - Sequence number of the largest acceptable frame
  - Last Frame Received (LFR)
    - Sequence number of the last frame received
- Receiver also maintains the following invarian

$$\text{LAF} - \text{LFR} \le \text{RWS}$$



Sliding Window on Receiver

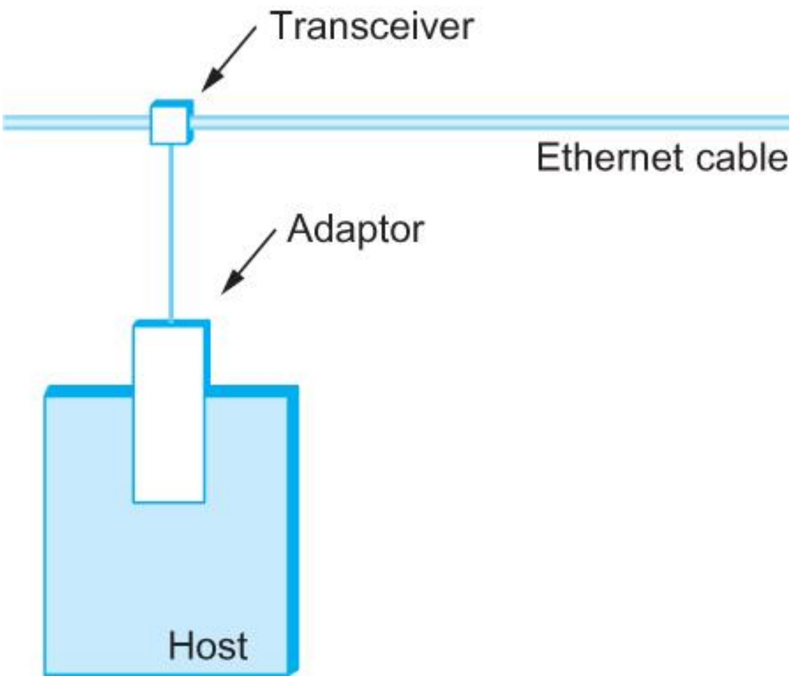
Concurrent Logical Channels

- One important consequence of this approach is that the frames sent over a given link are not kept in any particular order. The protocol also implies nothing about flow control.
- The idea underlying the ARPANET protocol, which we refer to as concurrent logical channels, is to multiplex several logical channels onto a single point-to-point link and to run the stop-and-wait algorithm on each of these logical channels.
- There is no relationship maintained among the frames sent on any of the logical channels, yet because a different frame can be outstanding on each of the several logical channels the sender can keep the link full.

Ethernet

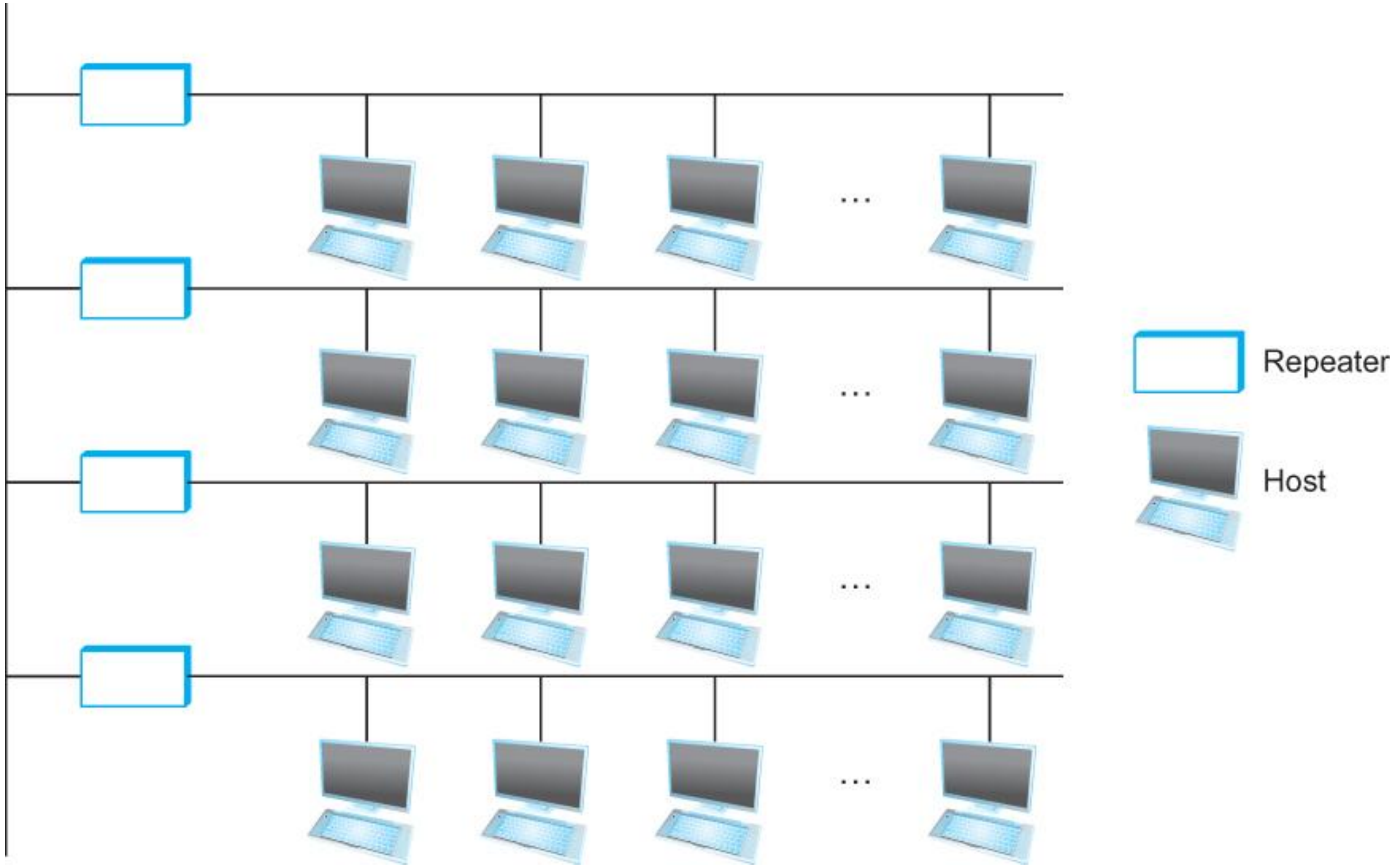
- **Ethernet is a family of wired computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN).**
  - Uses ALOHA (packet radio network) as the root protocol
    - Developed at the University of Hawaii to support communication across the Hawaiian Islands.
    - For ALOHA the medium was atmosphere, for Ethernet the medium is a coax cable.
  - DEC and Intel joined Xerox to define a 10-Mbps Ethernet standard in 1978.
  - This standard formed the basis for IEEE standard 802.3
  - More recently 802.3 has been extended to include a 100-Mbps version called Fast Ethernet and a 1000-Mbps version called Gigabit Ethernet.

- An Ethernet segment is implemented on a coaxial cable of up to 500 m.
  - This cable is similar to the type used for cable TV except that it typically has an impedance of 50 ohms instead of cable TV’s 75 ohms.
- Hosts connect to an Ethernet segment by tapping into it.
- A transceiver (a small device directly attached to the tap) detects when the line is idle and drives signal when the host is transmitting.
- The transceiver also receives incoming signal.
- The transceiver is connected to an Ethernet adaptor which is plugged into the host.
- The protocol is implemented on the adaptor.



Ethernet transceiver and adaptor

- Multiple Ethernet segments can be joined together by *repeaters.*
- A *repeater* is a device that forwards digital signals.
- No more than four repeaters may be positioned between any pair of hosts.
  - An Ethernet has a total reach of only 2500 m.



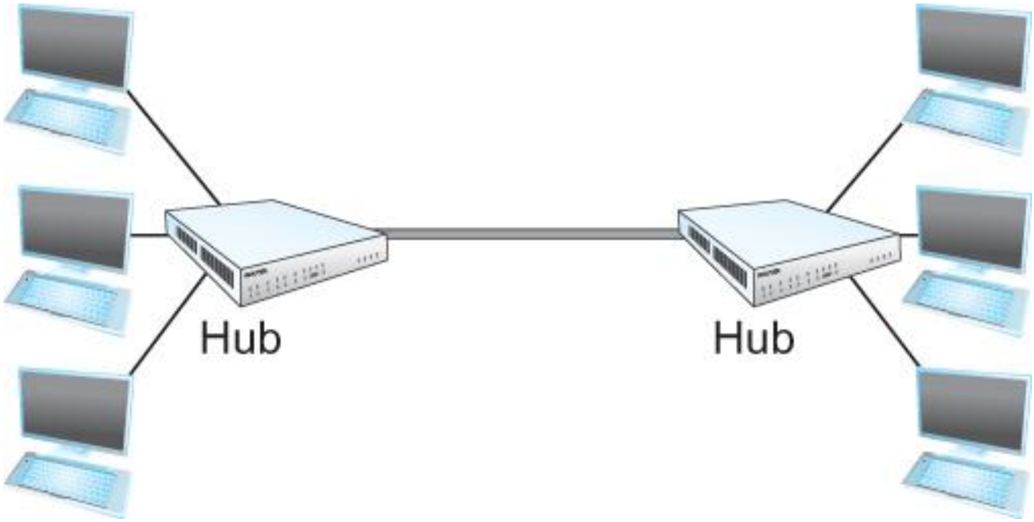
Ethernet repeater

Ethernet

- Any signal placed on the Ethernet by a host is broadcast over the entire network
    - Signal is propagated in both directions.
    - Repeaters forward the signal on all outgoing segments.
    - Terminators attached to the end of each segment absorb the signal.
- Ethernet uses Manchester encoding scheme.
    - **New Technologies in Ethernet**
        - Instead of using coax cable, an Ethernet can be constructed from a thinner cable known as 10Base2 (the original was 10Base5)
            - 10 means the network operates at 10 Mbps
            - Base means the cable is used in a baseband system
            - 2 means that a given segment can be no longer than 200 m

Ethernet Hub

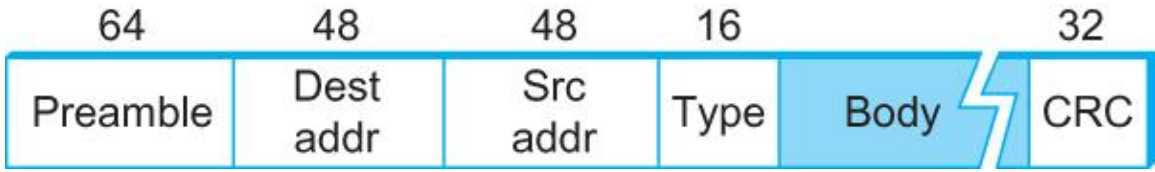
- New Technologies in Ethernet
  - Another cable technology is 10BaseT
    - T stands for twisted pair
    - Limited to 100 m in length
  - With 10BaseT, the common configuration is to have several point to point segments coming out of a multiway repeater, called *Hub*



Ethernet Hub

Access Protocol for Ethernet

- The algorithm is commonly called Ethernet’s Media Access Control (MAC).
  - It is implemented in Hardware on the network adaptor.
- Frame format
  - Preamble (64bit): allows the receiver to synchronize with the signal (sequence of alternating 0s and 1s).
  - Host and Destination Address (48bit each).
  - Packet type (16bit): acts as demux key to identify the higher level protocol.
  - Data (up to 1500 bytes)
    - Minimally a frame must contain at least 46 bytes of data.
    - Frame must be long enough to detect collision.
  - CRC (32bit)



Ethernet Frame

Ethernet Frame Format

Ethernet Addresses

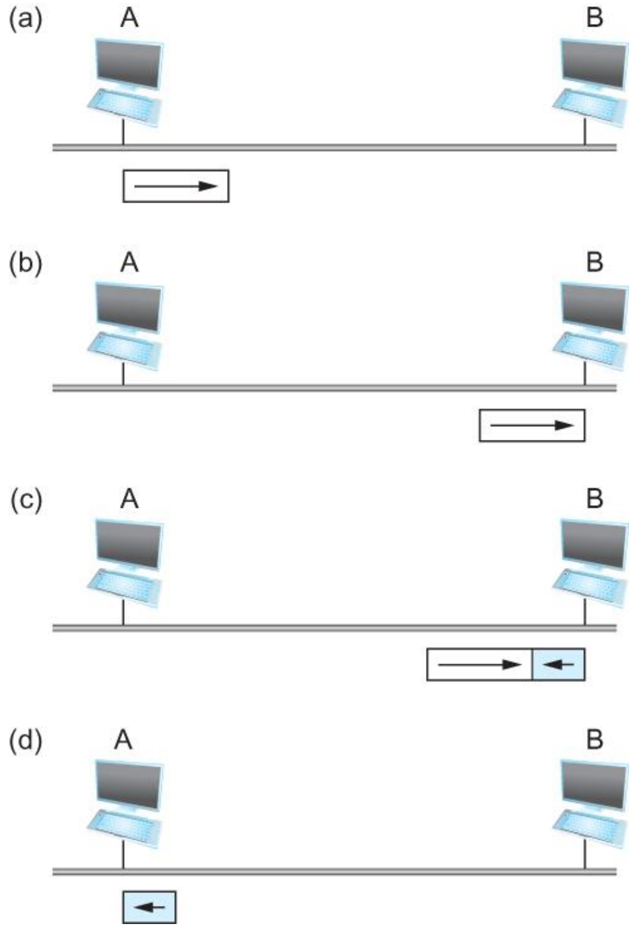
- Each host on an Ethernet (in fact, every Ethernet host in the world) has a unique Ethernet Address.
- The address belongs to the adaptor, not the host.
    - It is usually burnt into ROM.
- Ethernet addresses are typically printed in a human readable format
    - As a sequence of six numbers separated by colons.
    - Each number corresponds to 1 byte of the 6 byte address and is given by a pair of hexadecimal digits, one for each of the 4-bit nibbles in the byte
    - Leading 0s are dropped.
    - For example
    - 00001000 00000000 00101011 11100100 10110001 00000010

- To ensure that every adaptor gets a unique address, each manufacturer of Ethernet devices is allocated a different prefix that must be prepended to the address on every adaptor they build
    - AMD has been assigned the 24bit prefix 8:0:20

- To summarize, an Ethernet adaptor receives all frames and accepts
    - Frames addressed to its own address
    - Frames addressed to the broadcast address
    - Frames addressed to a multicast addressed if it has been instructed

Ethernet Transmitter Algorithm

- A begins transmitting a frame at time *t*
- *d* denotes the one link latency
- The first bit of A’s frame arrives at B at time *t* + *d*
- Suppose an instant before host A’s frame arrives, host B begins to transmit its own frame
- B’s frame will immediately collide with A’s frame and this collision will be detected by host B
- Host B will send the 32-bit jamming sequence
- Host A will not know that the collision occurred until B’s frame reaches it, which will happen at *t* + 2 * *d*
- Host A must continue to transmit until this time in order to detect the collision
    - Host A must transmit for *2* * *d* to be sure that it detects all possible collisions

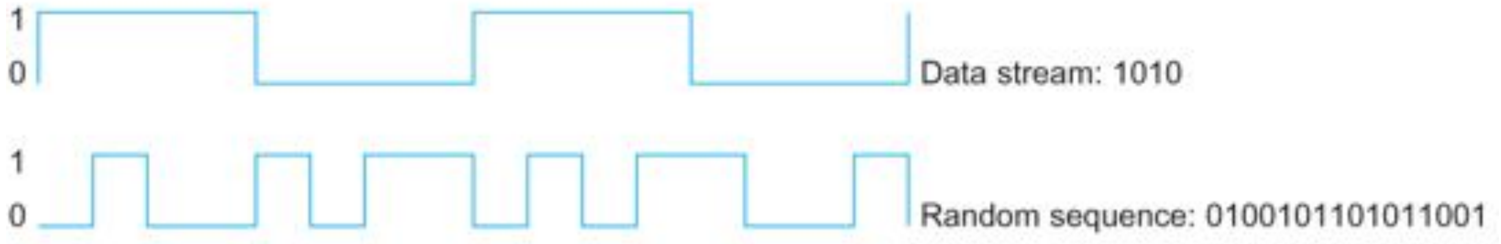


Worst-case scenario: (a) A sends a frame at time *t; (b) A's frame arrives*
at B at time *t + d; (c) B begins transmitting at time t + d and collides with A's frame;*
(d) B's runt (32-bit) frame arrives at A at time *t + 2d.*

Wireless Links

- Wireless links transmit electromagnetic signals
  - Radio, microwave, infrared
- Wireless links all share the same “wire” (so to speak)
  - The challenge is to share it efficiently without unduly interfering with each other
  - Most of this sharing is accomplished by dividing the “wire” along the dimensions of frequency and space
- Exclusive use of a particular frequency in a particular geographic area may be allocated to an individual entity such as a corporation

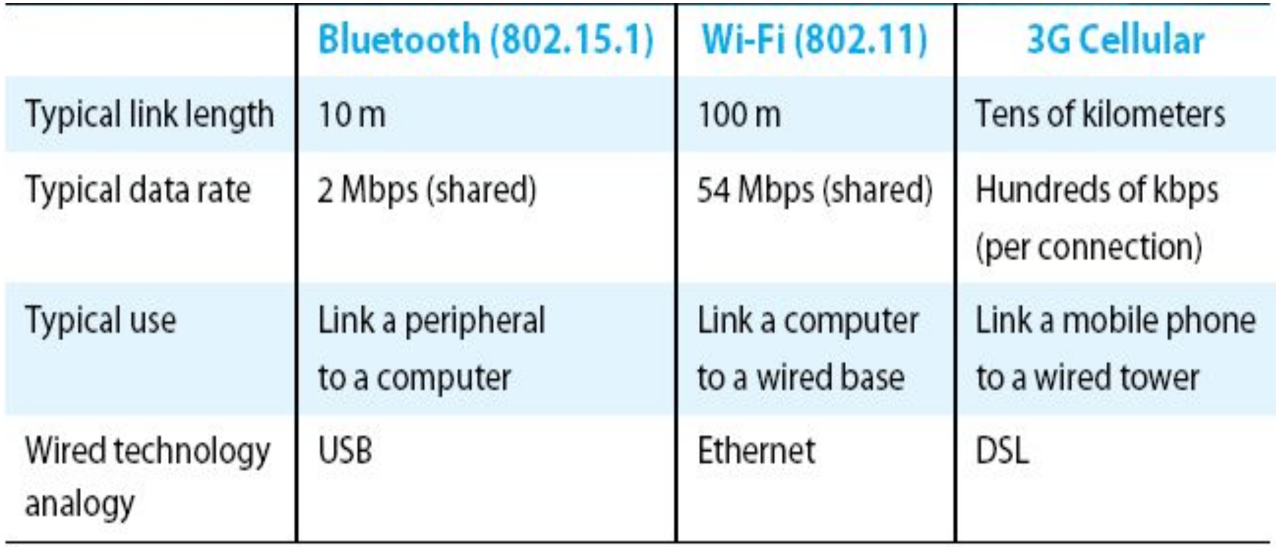
- These allocations are determined by government agencies such as FCC (Federal Communications Commission) in USA
- Specific bands (frequency) ranges are allocated to certain uses.
    - Some bands are reserved for government use
    - Other bands are reserved for uses such as AM radio, FM radio, televisions, satellite communications, and cell phones
    - Specific frequencies within these bands are then allocated to individual organizations for use within certain geographical areas.
    - Finally, there are several frequency bands set aside for “license exempt” usage
        - Bands in which a license is not needed



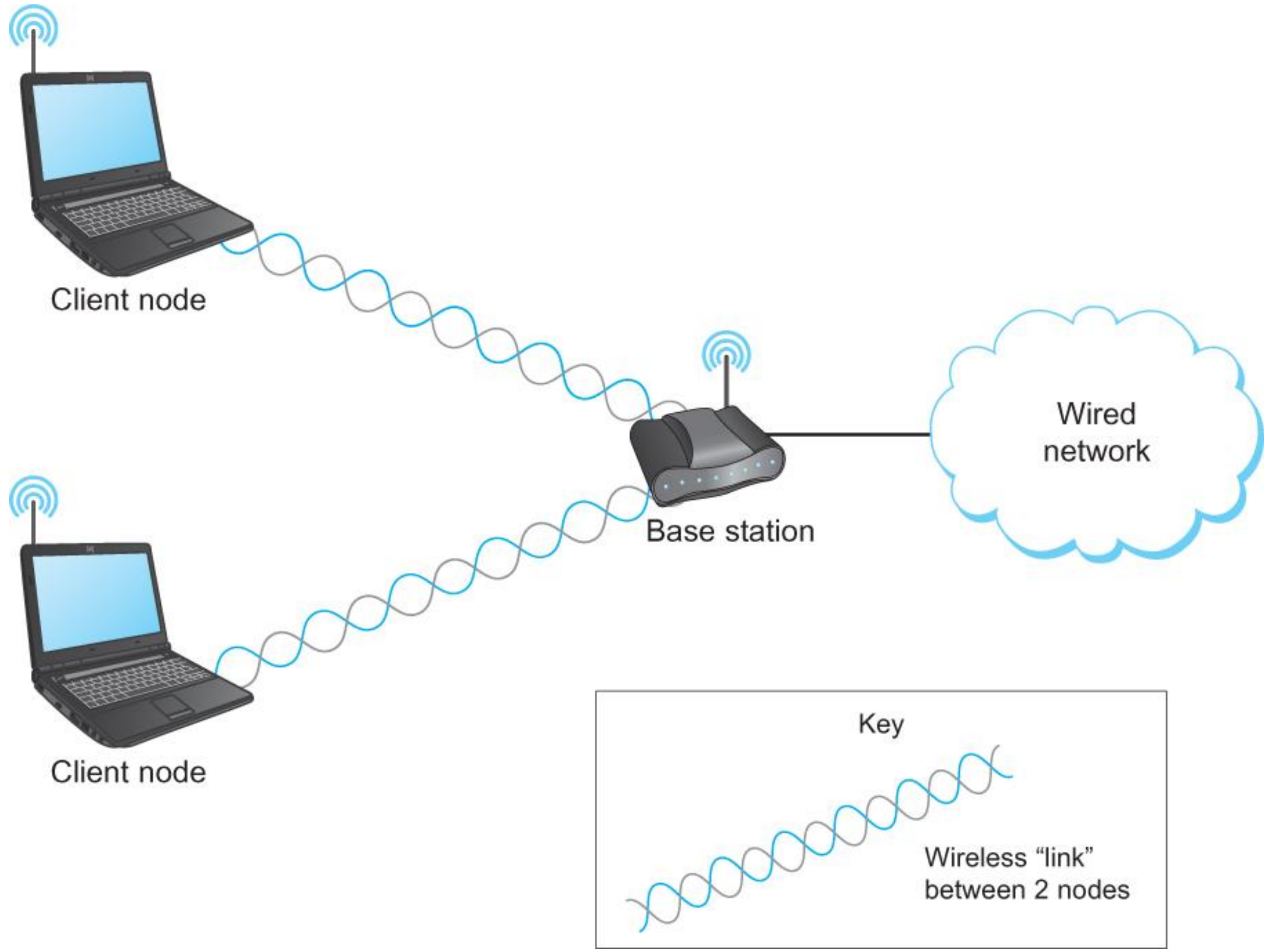
Example 4-bit chipping sequence

- Wireless technologies differ in a variety of dimensions
  - How much bandwidth they provide
  - How far apart the communication nodes can be

- Four prominent wireless technologies
  - Bluetooth
  - Wi-Fi (more formally known as 802.11)
  - WiMAX (802.16)
  - 3G cellular wireless



	Bluetooth (802.15.1)	Wi-Fi (802.11)	3G Cellular
Typical link length	10 m	100 m	Tens of kilometers
Typical data rate	2 Mbps (shared)	54 Mbps (shared)	Hundreds of kbps (per connection)
Typical use	Link a peripheral to a computer	Link a computer to a wired base	Link a mobile phone to a wired tower
Wired technology analogy	USB	Ethernet	DSL



A wireless network using a base station

- Three levels of mobility for clients
  - No mobility: the receiver must be in a fix location to receive a directional transmission from the base station (initial version of WiMAX)
  - Mobility is within the range of a base (Bluetooth)
  - Mobility between bases (Cell phones and Wi-Fi)

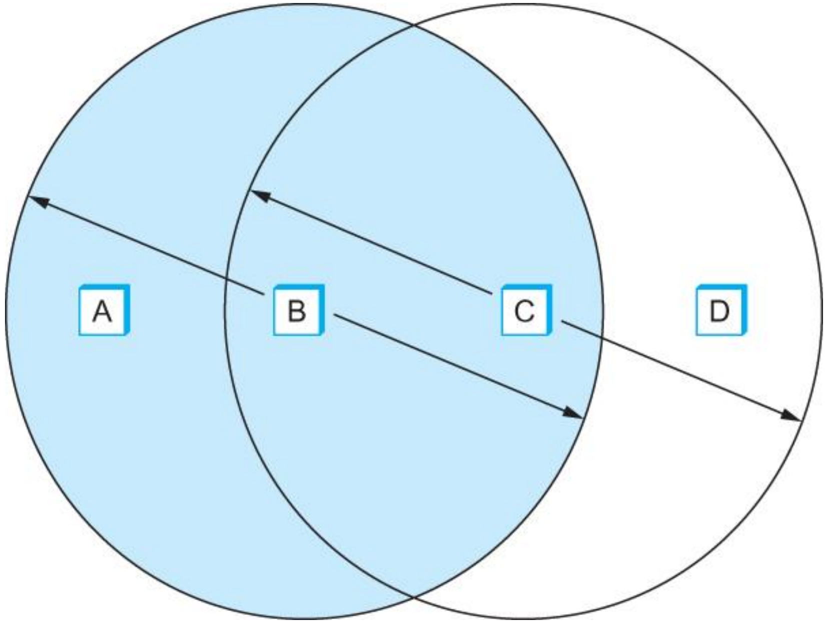
IEEE 802.11
IEEE stands for Institute of Electrical and Electronics Engineers

- Also known as Wi-Fi
- Like its Ethernet and token ring siblings, 802.11 is designed for use in a limited geographical area (homes, office buildings, campuses)
  - Primary challenge is to mediate access to a shared communication medium – in this case, signals propagating through space
- 802.11 supports additional features
  - power management and
  - security mechanisms

- Original 802.11 standard defined two radio-based physical layer standard
    - One using the frequency hopping
        - Over 79 1-MHz-wide frequency bandwidths
    - Second using direct sequence
        - Using 11-bit chipping sequence
    - Both standards run in the 2.4-GHz and provide up to 2 Mbps
- Then physical layer standard 802.11b was added
    - Using a variant of direct sequence 802.11b provides up to 11 Mbps
    - Uses license-exempt 2.4-GHz band
- Then came 802.11a which delivers up to 54 Mbps using OFDM
    - 802.11a runs on license-exempt 5-GHz band
- Most recent standard is 802.11g which is backward compatible with 802.11b
    - Uses 2.4 GHz band, OFDM and delivers up to 54 Mbps

IEEE 802.11 – Collision Avoidance

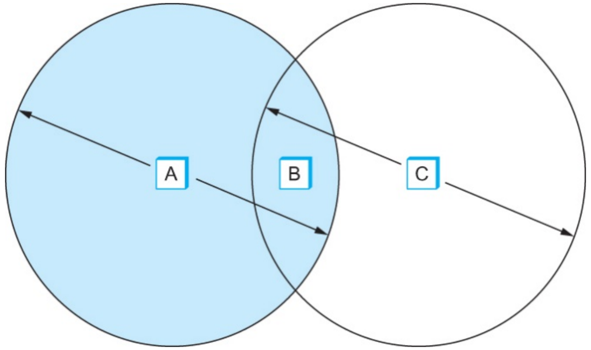
- Consider the situation in the following figure where each of four nodes is able to send and receive signals that reach just the nodes to its immediate left and right
  - For example, B can exchange frames with A and C, but it cannot reach D
  - C can reach B and D but not A



Same as Wi-Fi Limited to distance

- Suppose both A and C want to communicate with B and so they each send it a frame.
  - A and C are unaware of each other since their signals do not carry that far
  - These two frames collide with each other at B
    - But unlike an Ethernet, neither A nor C is aware of this collision
  - A and C are said to *hidden nodes* with respect to each other

The "Hidden Node" Problem. Although A and C are hidden from each other, their signals can collide at B. (B's reach is not shown.)



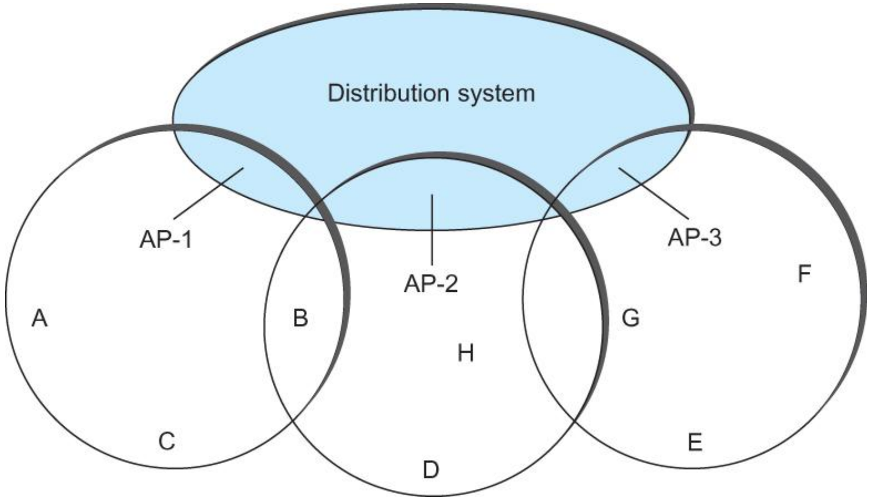
IEEE 802.11 – Distribution System

- 802.11 is suitable for an ad-hoc configuration of nodes that may or may not be able to communicate with all other nodes.
- Nodes are free to move around
- The set of directly reachable nodes may change over time
- To deal with this mobility and partial connectivity,
  - 802.11 defines additional structures on a set of nodes
  - Instead of all nodes being created equal,
    - some nodes are allowed to roam
    - some are connected to a wired network infrastructure

      - they are called *Access Points* (AP) and they are connected to each other by a so-called *distribution system*

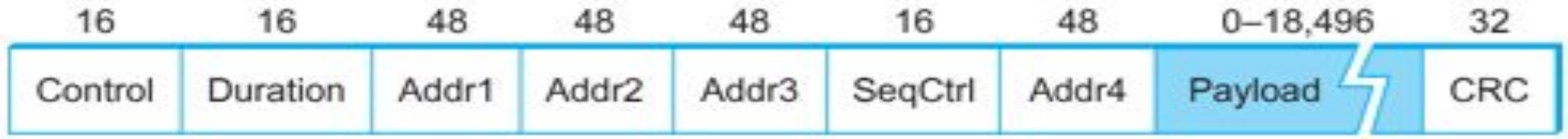
IEEE 802.11 – Distribution System

- Following figure illustrates a distribution system that connects three access points, each of which services the nodes in the same region
- Each of these regions is analogous to a cell in a cellular phone system with the APIs playing the same role as a base station
- The distribution network runs at layer 2 of the ISO architecture



IEEE 802.11 – Frame Format IEEE:

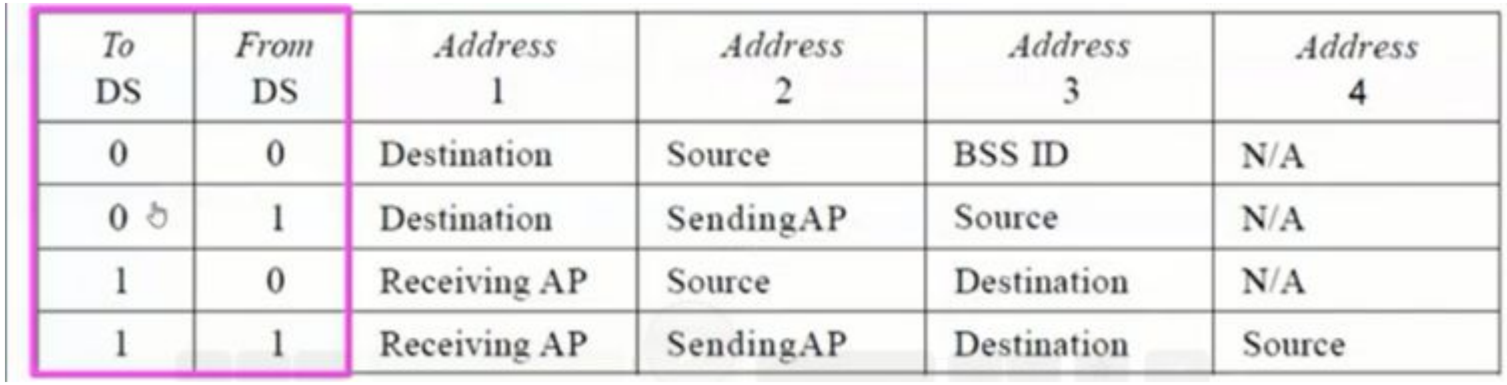
- Source and Destinations addresses: each 48 bits
- Data: up to 2312 bytes
- CRC: 32 bit
- Control field: 16 bits
  - Contains three subfields (of interest)
    - 6 bit **Type** field: indicates whether the frame is an RTS(ready to send) or CTS(clear to send) frame or being used by the scanning algorithm
    - A pair of 1 bit fields : called **To Distrusted steam DS** and From Distributed stream(**FromDS)**



16	16	48	48	48	16	48	0–18,496	32
Control	Duration	Addr1	Addr2	Addr3	SeqCtrl	Addr4	Payload	CRC

Frame Format

- Control : it Contains Control information of the frame
- Duration : it specifies the time period for which the frame and its acknowledgment occupy the channel
- Sequence : Field that stores the frame numbers
- CRC :- used to check the error Detection   BSSID :Basic Service Set ,AP: Access point



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

Fig : Standard IEEE 802.11 To DS to From Ds Table.

- Frame contains four addresses
- How these addresses are interpreted depends on the settings of the **ToDS** and **FromDS** bits in the frame’s Control field
- This is to account for the possibility that the frame had to be forwarded across the distribution system which would mean that,
  - the original sender is not necessarily the same as the most recent transmitting node
- Same is true for the destination address
- Simplest case
  - When one node is sending directly to another, both the DS bits are 0, Addr1 identifies the target node, and Addr2 identifies the source node

- Most complex case
  - Both DS bits are set to 1
    - Indicates that the message went from a wireless node onto the distribution system, and then from the distribution system to another wireless node
  - With both bits set,
    - Addr1 identifies the ultimate destination,
    - Addr2 identifies the immediate sender (the one that forwarded the frame from the distribution system to the ultimate destination)
    - Addr3 identifies the intermediate destination (the one that accepted the frame from a wireless node and forwarded across the distribution system)
    - Addr4 identifies the original source

- Addr1: E, Addr2: AP-3, Addr3: AP-1, Addr4: A

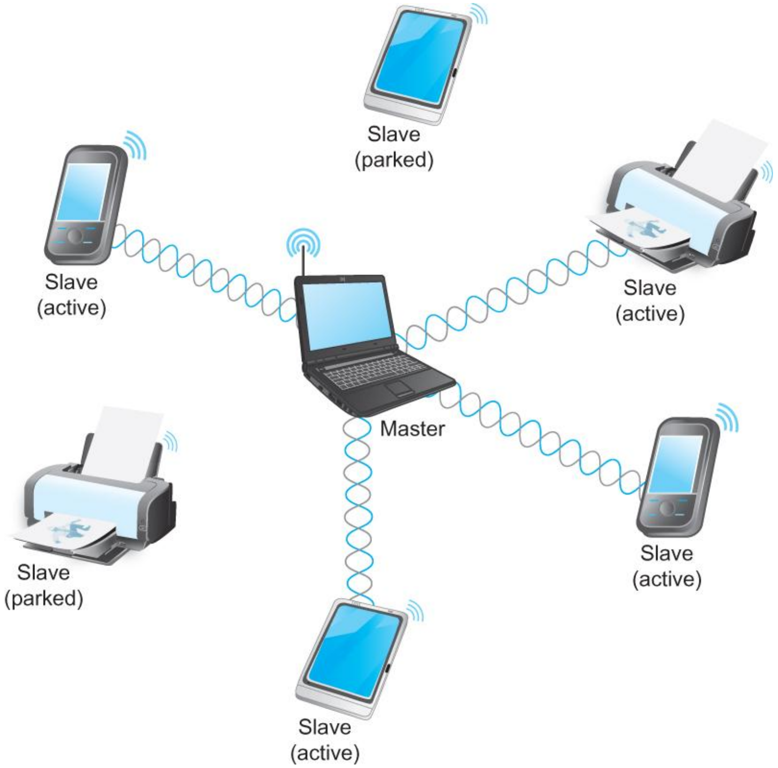
Bluetooth

- Used for very short range communication between mobile phones, PDAs, notebook computers and other personal or peripheral devices
- Operates in the license-exempt band at 2.45 GHz
- Has a range of only 10 m
- Communication devices typically belong to one individual or group
    - Sometimes categorized as Personal Area Network (PAN)
- Version 2.0 provides speeds up to 2.1 Mbps
- Power consumption is low

Bluetooth

- **Bluetooth is a short-range wireless technology standard that is used for exchanging data between fixed and mobile devices over short distances**
- Bluetooth is specified by an industry consortium called the Bluetooth Special Interest Group
- It specifies an entire suite of protocols, going beyond the link layer to define application protocols, which it calls *profiles*, for a range of applications
  - There is a profile for synchronizing a PDA with personal computer
  - Another profile gives a mobile computer access to a wired LAN
- The basic Bluetooth network configuration is called a *piconet*
  - Consists of a master device and up to seven slave devices
  - Any communication is between the master and a slave
  - The slaves do not communicate directly with each other
  - A slave can be *parked*: set to an inactive, low-power state
  - **Slave are printer , mobile etc**

Bluetooth


Slave
(parked)
Slave
(active)
Slave
(active)
Master
Slave
(parked)
Slave
(active)
Slave
(active)

ZigBee

- ZigBee is a new technology that competes with Bluetooth
- Devised by the ZigBee alliance and standardized as IEEE 802.15.4
- It is designed for situations where the bandwidth requirements are low and power consumption must be very low to give very long battery life
- It is also intended to be simpler and cheaper than Bluetooth, making it financially feasible to incorporate in cheaper devices such as a wall switch that wirelessly communicates with a ceiling-mounted fan.

Summary

- We introduced the many and varied type of links that are used to connect users to existing networks, and to construct large networks from scratch.
- We looked at the five key issues that must be addressed so that two or more nodes connected by some medium can exchange messages with each other
  - Encoding
  - Framing
  - Error Detecting
  - Reliability
  - Multiple Access Links
    - Ethernet
    - Wireless 802.11, Bluetooth