Computer Networks
Unit II – Physical Layer

Note: Material for this presentations are taken from Internet and books and only being used for student reference

Outline

- Introduction of LAN; MAN;WAN; PAN,Ad-hoc Network
- Topologies
- Network Architectures
- OSI Model
- TCP/IP Model
- Design issues for Layers
- **Transmission Mediums**
- Network Devices
- Manchester and Differential Manchester Encodings;
- IEEE802.11: Frequency Hopping (FHSS) and Direct Sequence (DSSS)

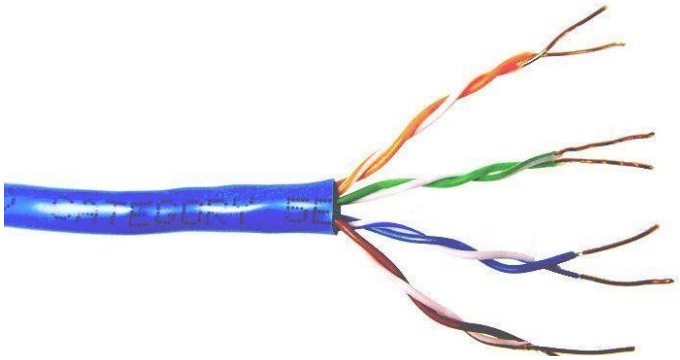
Transmission Mediums

- CAT5, 5e, 6
- OFC and
- Radio Spectrum,

Common network cable types

- Coaxial cable

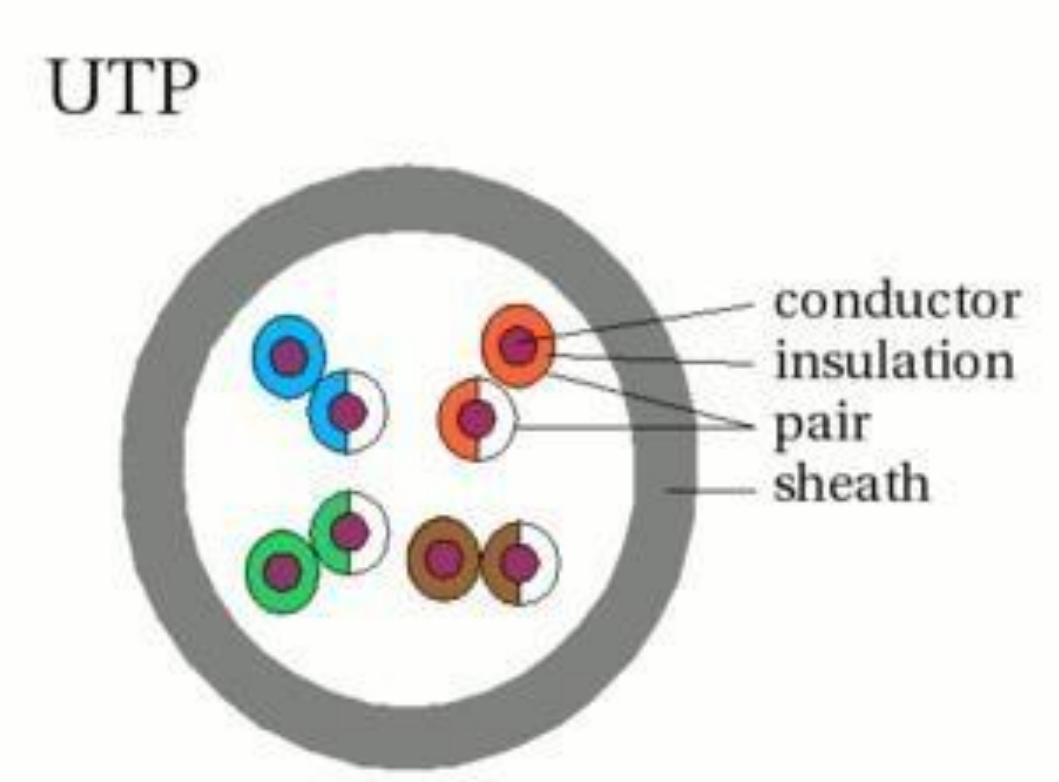
- Unshielded twisted pair



- Fiber optic

UTP (Unshielded Twisted Pair) characteristics

- Unshielded
- Twisted (why?) pairs of insulated conductors
- Covered by insulating sheath



UTP categories

Category 1	Voice only (Telephone)
Category 2	Data to 4 Mbps (Localtalk)
Category 3	Data to 10Mbps (Ethernet)
Category 4	Data to 20Mbps (Token ring)
Category 5 Category 5e	Data to 100Mbps (Fast Ethernet) Data to 1000Mbps (Gigabit Ethernet)
Category 6	Data to 2500Mbps (Gigabit Ethernet)

Categories of UTP: CAT 5

- 100 MHz Bandwidth
- 24.0 dB Attenuation (dB-decibel-Primarily used to express signal strength and power level)
- 100 ohms Impedance
- Used for high-speed data transmission
- Used in 10BaseT (10 Mbps) Ethernet & Fast Ethernet (100 Mbps)

Categories of UTP: CAT 5e

- 150 MHz Bandwidth
- 24.0 dB Attenuation
- 100 ohms Impedance
- Transmits high-speed data
- Used in Fast Ethernet (100 Mbps), Gigabit Ethernet (1000 Mbps) & 155 Mbps ATM
- For runs of up to 90 meters
- Solid core cable ideal for structural installations (PVC or Plenum)
- Stranded cable ideal for patch cables
- Terminated with RJ-45 connectors

Categories of UTP: CAT 6

- 250 MHz Bandwidth
- 19.8 dB Attenuation
- 100 ohms Impedance
- Transmits high-speed data
- Used in Gigabit Ethernet (1000 Mbps) & 10 Gig Ethernet (10000 Mbps)

Comparison between CAT5,5e and 6

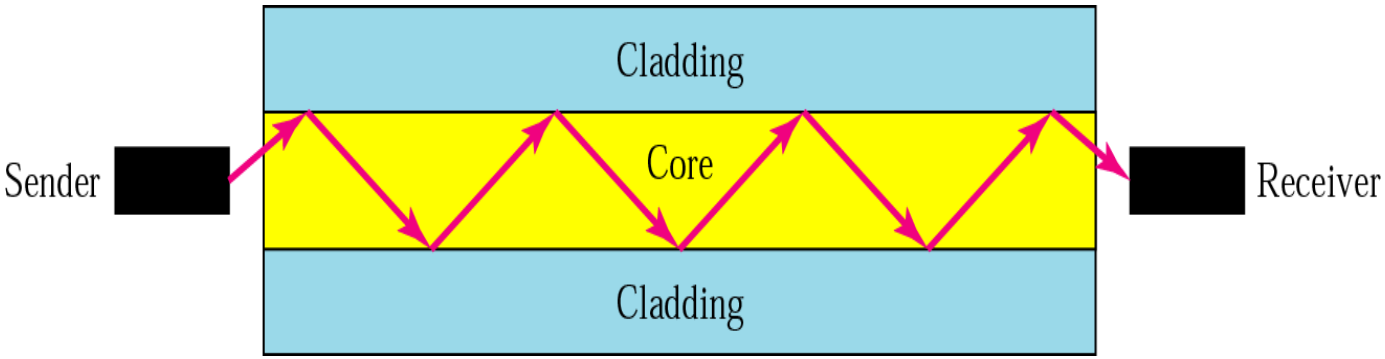
	CAT5	CAT5e	CAT6
Frequency	100 MHz	100 MHz	250 MHz
Attenuation (min. at 100 MHz)	22 dB	22 dB	19.8 dB
Characteristic Impedance	100 ohms = 15%	100 ohms = 15%	100 ohms = 15%
NEXT (min. at 100 MHz)	32.3 dB	35.3 dB	44.3 dB
PS-NEXT (min. at 100 MHz)	NA	32.3 dB	42.3 dB
EL-FEXT (min. at 100 MHz)	NA	23.8 dB	27.8 dB
PS-ELFEXT (min. at 100 MHz)	NA	20.8 dB	24.8 dB
PS-ANEXT (min. at 500 MHz)	--	--	--
PS-AELFEXT (min. at 500 MHz)	16 dB	20.1 dB	20.1 dB
Return Loss (min. at 100 MHz)	16 dB	20.1 dB	20.1 dB
Delay Skew (max. per 100m)	NA	45 ns	45 ns
Networks Supported	100BASE-T	1000BASE-T	1000BASE-TX

OFC- Optical fiber cable

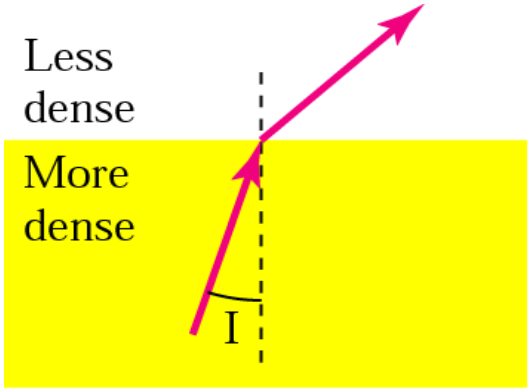
- An **optical fiber cable**, also known as **fiber optic cable**, is an assembly similar to an electrical cable, but containing one or more optical fibers that are used to carry light.
- The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed.
- Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Fiber Media

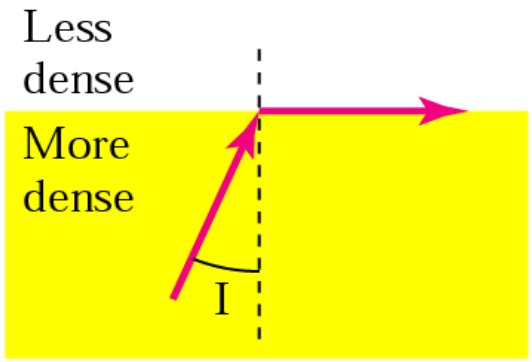
- Optical fibers use light to send information through the optical medium.
- It uses the principal of total internal reflection.
- Modulated light transmissions are used to transmit the signal.



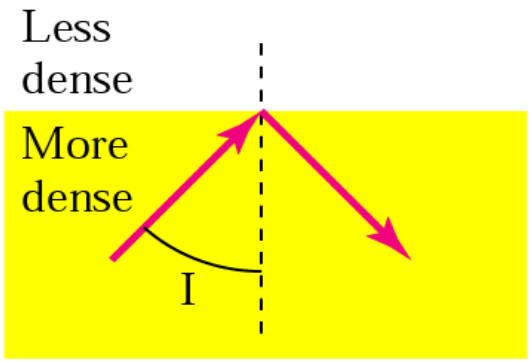
Total Internal Reflection



I < critical angle,
refraction



I = critical angle,
refraction



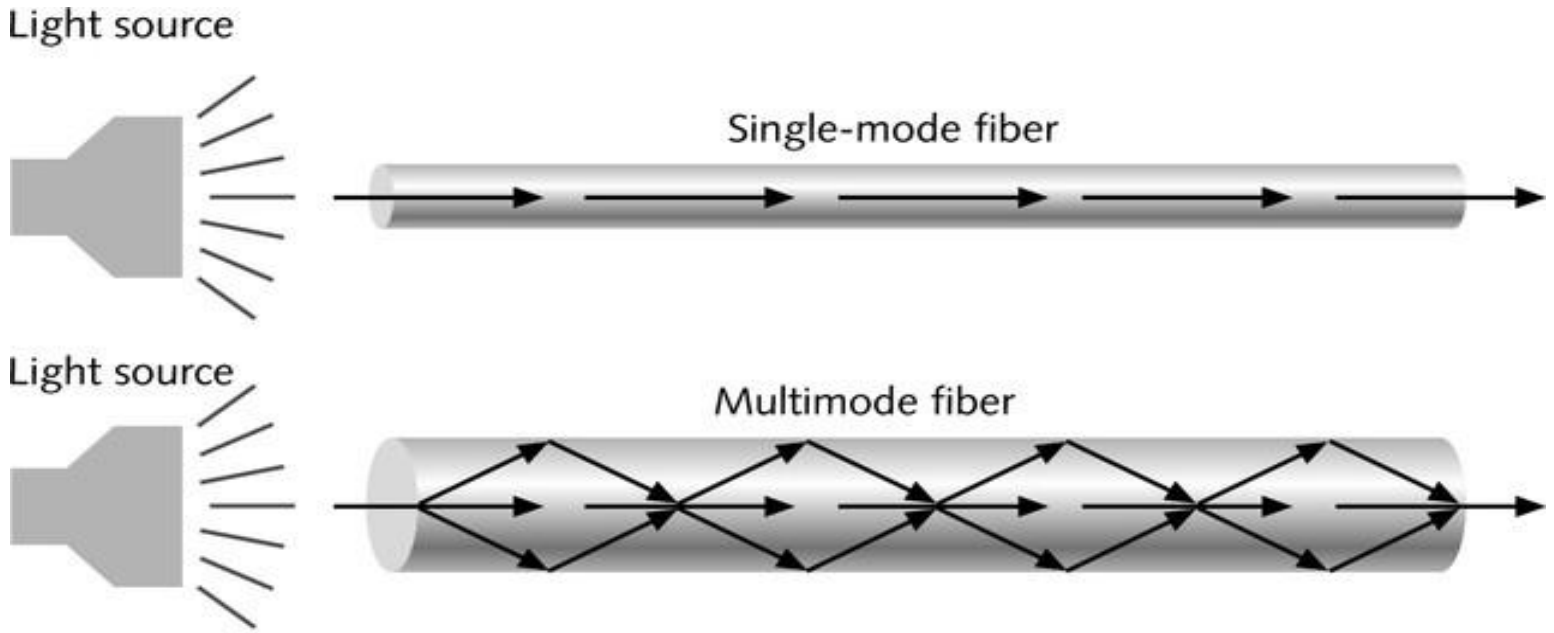
I > critical angle,
reflection

Fiber Media

- Light travels through the optical media by the way of total internal reflection.
- Modulation scheme used is intensity modulation.
- Two types of Fiber media :
  1. Multimode
  2. Singlemode
- Multimode Fiber can support less bandwidth than Singlemode Fiber.
- Singlemode Fiber has a very small core and carry only one beam of light. It can support Gbps data rates over > 100 Km without using repeaters.

Single and Multimode Fiber

- Single-mode fiber
  - Carries light pulses along single path
  - Uses Laser Light Source
- Multimode fiber
  - Many pulses of light generated by LED travel at different angles

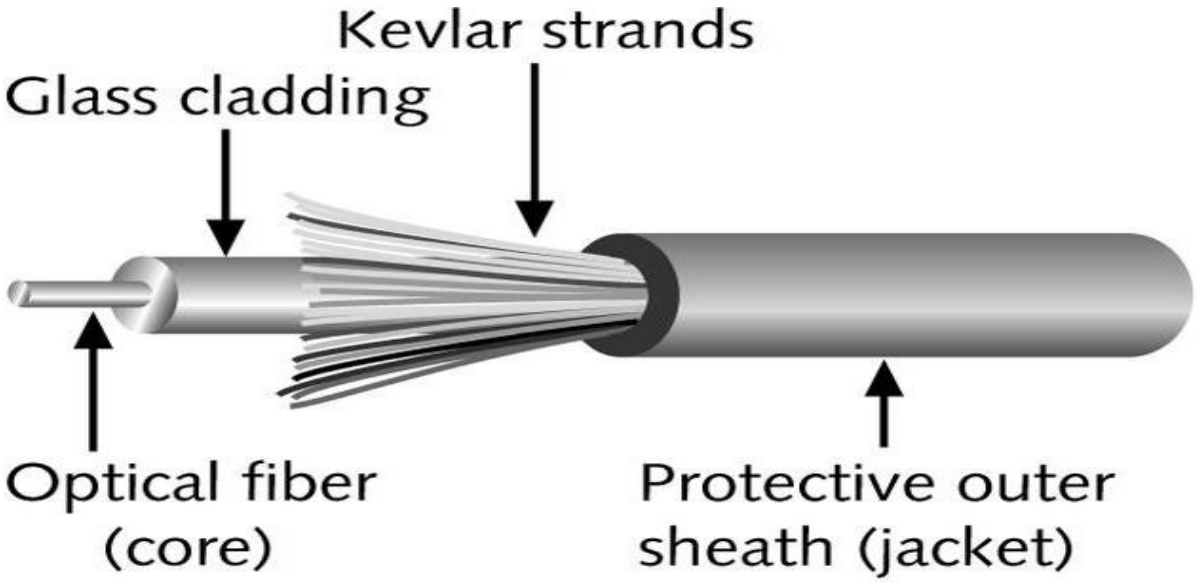


Fiber Media

- The bandwidth of the fiber is limited due to the dispersion effect.
- Distance Bandwidth product of a fiber is almost a constant.
- Fiber optic cables consist of multiple fibers packed inside protective covering.
- 62.5/125 μm (850/1310 nm) multimode fiber
- 50/125 μm (850/1310 nm) multimode fiber
- 10 μm (1310 nm) single-mode fiber

Fiber-Optic Cable

- Contains one or several glass fibers at its core
- Surrounding the fibers is a layer called cladding

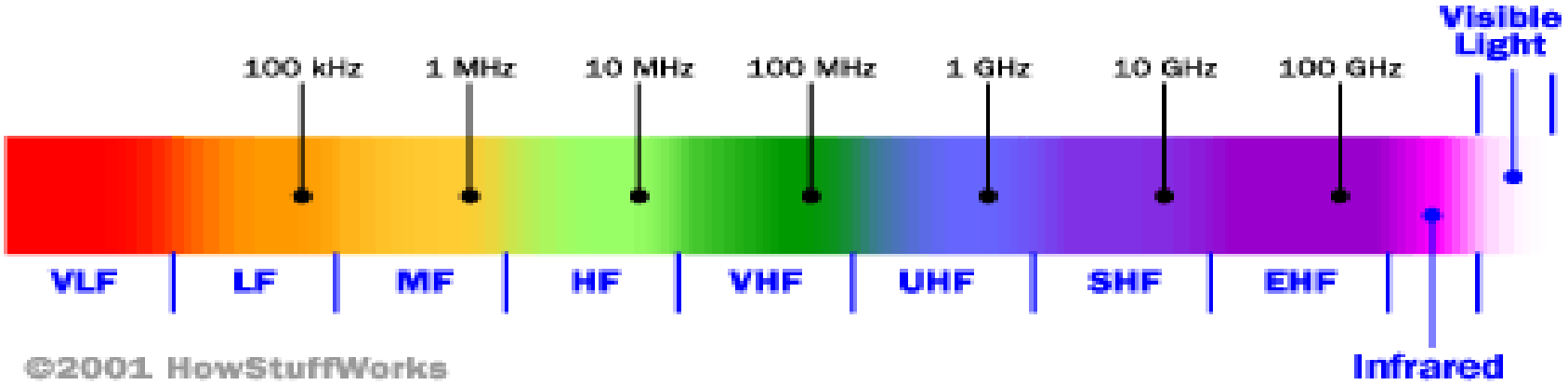


Fiber Optic Cable

- FO Cable may have 1 to over 1000 fibers

Radio Spectrum

- The **radio spectrum** is the part of the electromagnetic spectrum from 3 Hz to 3000 GHz (3 THz).
- Electromagnetic waves in this frequency range, called radio waves, are extremely widely used in modern technology, particularly in telecommunication.
- Coordinated by an international body, the International Telecommunication Union (ITU)



Frequency Band

Band	Range	Propagation	Application
VLF	3–30 KHz	Ground	Long-range radio navigation
LF	30–300 KHz	Ground	Radio beacons and navigational locators
MF	300 KHz–3 MHz	Sky	AM radio
HF	3–30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF	30–300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF	3–30 GHz	Line-of-sight	Satellite communication
EHF	30–300 GHz	Line-of-sight	Long-range radio navigation

Outline

- Introduction of LAN; MAN;WAN; PAN,Ad-hoc Network
- Topologies
- Network Architectures
- OSI Model
- TCP/IP Model
- Design issues for Layers
- Transmission Mediums
- **Network Devices**
- Manchester and Differential Manchester Encodings;
- IEEE802.11: Frequency Hopping (FHSS) and Direct Sequence (DSSS)

Devices and the layers at which they operate

Layer	Name of Layer	Device
3	Network	Routers, layer 3 switches
2	Data Link	Switches, bridges, NIC's
1	Physical	Hubs, Repeaters

Network Devices:

- Bridge
- Switch
- Router
- Brouter and
- Access Point

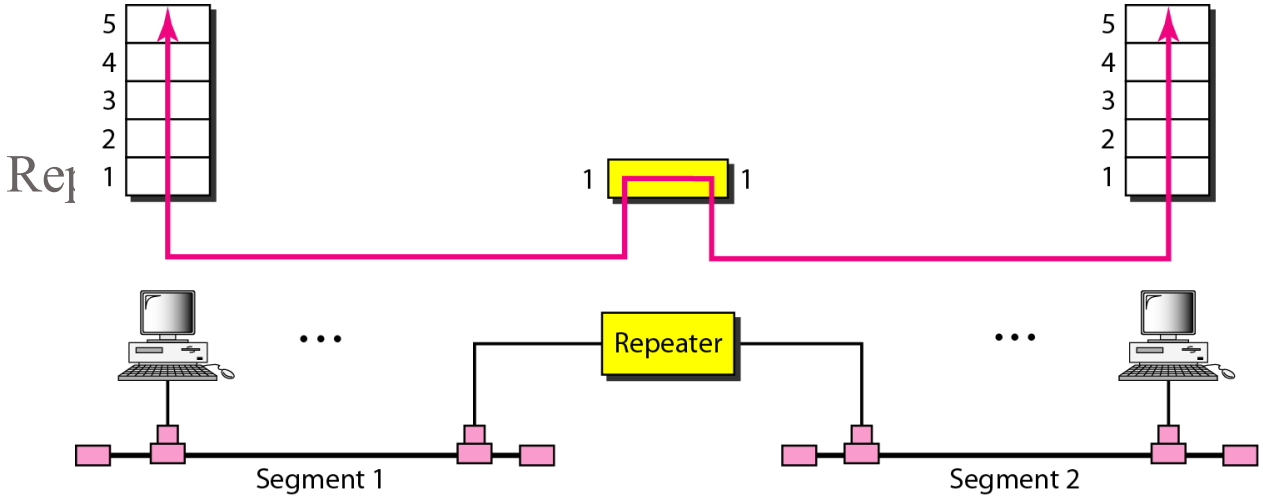
Hubs

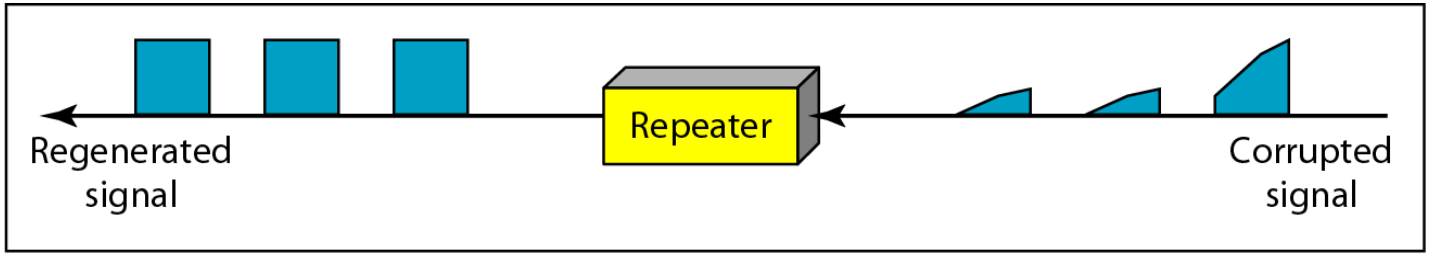
- A hub is used as a central point of connection among media segments.
- Cables from network devices plug in to the ports on the hub.
- Types of HUBS :
  - A **passive hub** is just a connector. It connects the wires coming from different branches.
  - The signal pass through a passive hub without regeneration or amplification.
  - Connect several networking cables together
  - **Active hubs or Multiport repeaters-** They regenerate or amplify the signal before they are retransmitted.

Repeaters

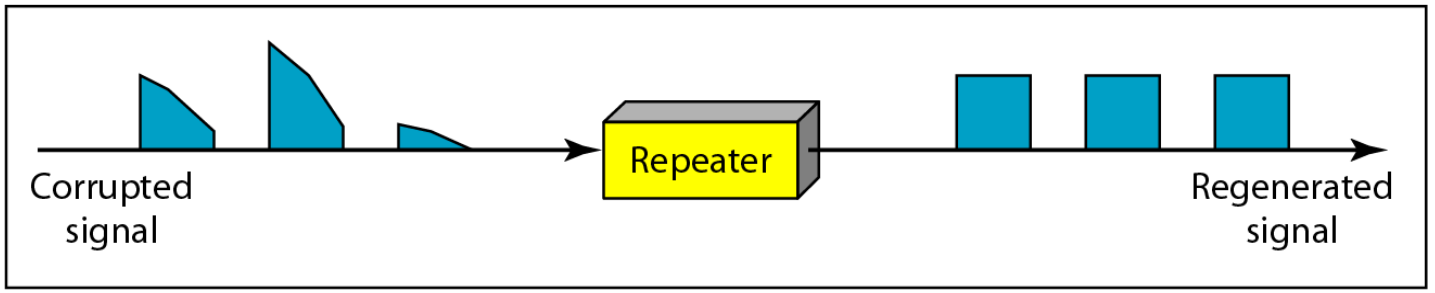
- A repeater is a device that operates only at the PHYSICAL layer.
- A repeater can be used to increase the length of the network by eliminating the effect of attenuation on the signal.
- It connects two segments of the same network, overcoming the distance limitations of the transmission media.
- A repeater forwards every frame it has no filtering capability.
- A repeater is a regenerator, not an amplifier.
- Repeaters can connect segments that have the same access method. (CSMA/CD, Token Passing, Polling, etc.)

Optic fiber repeater





a. Right-to-left transmission.



b. Left-to-right transmission.

Function of a repeater

Switches

- A **network switch** is a computer networking device that connects devices together on a computer network by using packet switching to receive, process, and forward data to the destination device.
- Unlike less advanced network hubs, a network switch forwards data only to the devices that need to receive it, rather than broadcasting the same data out of each of its ports.
- It uses Ethernet (MAC Address) address.

Store and Forward Switches

- Do error checking on each frame after the entire frame has arrived into the switch
- If the error checking algorithm determines there is no error, the switch looks in its MAC address table for the port to which to forward the destination device
- Highly reliable because doesn't forward bad frames
- Slower than other types of switches because it holds on to each frame until it is completely received to check for errors before forwarding

Cut Through Switch

- Faster than store and forward because doesn't perform error checking on frames
- Reads address information for each frame as the frames enter the switch
- After looking up the port of the destination device, frame is forwarded
- Forwards bad frames
  - Performance penalty because bad frames can't be used and replacement frames must be sent which creates additional traffic

Unmanaged/Intelligent switches

- Unmanaged – provides LAN's with all the benefits of switching Fine in small networks

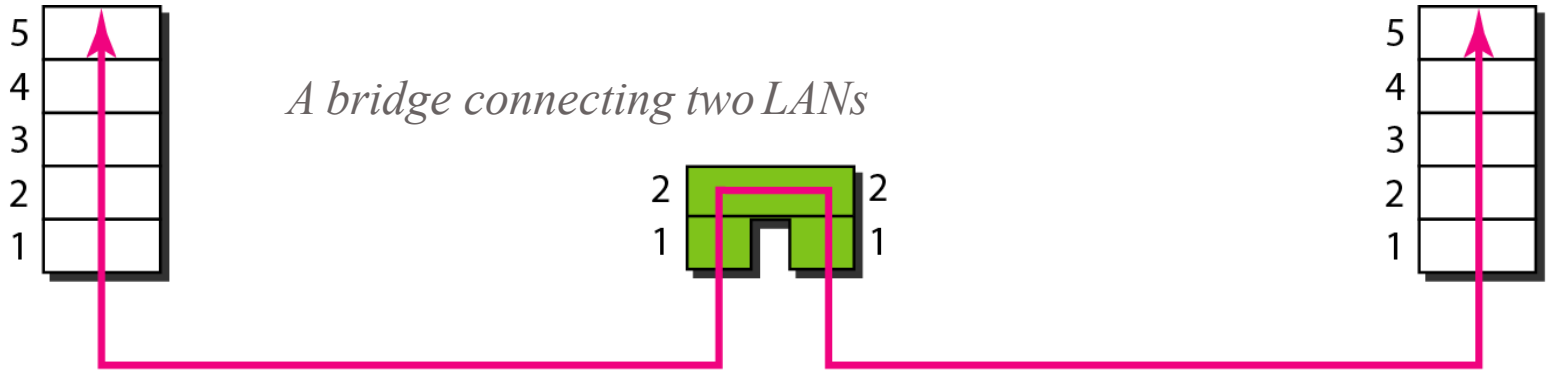
- Intelligent switches tracks and reports LAN performance statistics. Have a database ASIC (application specific integrated circuit) on board to collect and store data which you view through a software interface

Comparison of Hub and Switch

Basis for Comparison	Hub	Switch
Layer	Physical layer. Layer 1 devices	Data Link Layer. Layer 2
Function	To connect a network of personal computers together, they can be joined through a central hub.	Allow to connect multiple device and port can be manage,Vlan can create security also can apply
Data Transmission	Electrical signal or bits	Frame (L2 Switch) Frame &Packet (L3 switch)
Ports	4/12 ports	Switch is multi port Bridge. 24/48 ports
Device Type	Passive Device (Without Software)	Active Device (With Software) & Networking device
Used in	LAN	LAN
Transmission Mode	Half duplex	Half/Full duplex
Broadcast Domain	Hub has one Broadcast Domain.	Switch has one broadcast domain
Definition	An electronic device that connects many network device together so that devices can exchange data	A network switch is a computer networking device that is used to connect many devices together on a computer network. A switch is considered more advanced than a hub because a switch will on send msg to device that needs or request it
Speed	10Mbps	10/100 Mbps, 1 Gbps
Collisions	Collisions occur in setups using hubs.	No collisions occur in a full-duplex switch.
Address Used	Uses MAC address	Uses MAC address

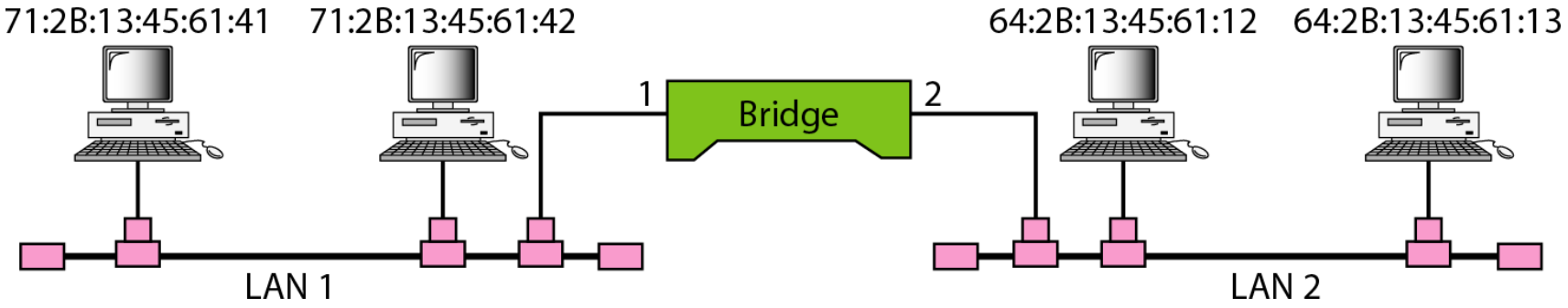
Bridges

- Operates in both the PHYSICAL and the data link layer.
- As a PHYSICAL layer device, it regenerates the signal it receives.
- As a data link layer device, the bridge can check the PHYSICAL/MAC addresses(source and destination) contained in the frame.
- A bridge has a table used in filtering decisions.
- It can check the destination address of a frame and decide if the frame should be forwarded or dropped.
- If the frame is to be forwarded, the decision must specify the port.
- A bridge has a table that maps address to ports.
- Limit or filter traffic keeping local traffic local yet allow connectivity to other parts (segments).



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

Bridge Table

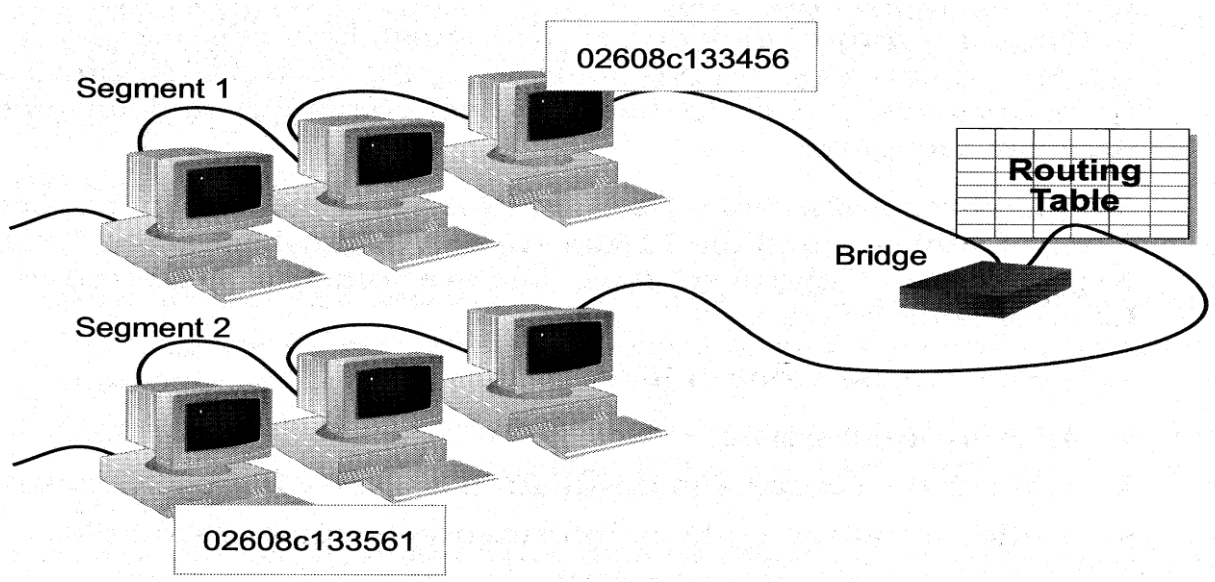


A bridge does not change the physical (MAC) addresses in a frame.

How Bridges Work

Bridges work at the Media Access Control

- Routing table is built to record the segment no. of address
- If destination address is in the same segment as the source address, stop transmit
- Otherwise, forward to the other segment



Characteristics of Bridges

Routing Tables

- Contains one entry per station of network to which bridge is connected.
- Is used to determine the network of destination station of a received packet.

Filtering

- Is used by bridge to allow only those packets destined to the remote network.
- Packets are filtered with respect to their destination and multicast addresses.

Forwarding

- the process of passing a packet from one network to another.

Learning Algorithm

- the process by which the bridge learns how to reach stations on the internetwork.

Types of Bridges

Transparent Bridge

- Also called learning bridges
- Build a table of MAC addresses as frames arrive
- Ethernet networks use transparent bridge
- Duties of transparent bridge are : Filtering frames,
- forwarding and blocking

Source Routing Bridge

- Used in Token Ring networks
- Each station should determine the route to the destination when it wants to send a frame and therefore include the route information in the header of frame.
- Addresses of these bridges are included in the frame.
- Frame contains not only the source and destination address but also the bridge addresses.

Advantages And Disadvantages Of Bridges

- Advantages of using a bridge
  - Extend physical network
  - Reduce network traffic with minor segmentation
  - Creates separate collision domains
  - Reduce collisions
  - Connect different architecture
- Disadvantages of using bridges
  - Slower that repeaters due to filtering
  - Do not filter broadcasts
  - More expensive than repeaters

Comparison of Switch and Bridge

Switch	Bridge
• A switch when compared to bridge has • multiple ports. • Switches can perform error checking before forwarding data. • Switches are very efficient by not forwarding packets that error-ed out or forwarding good packets selectively to correct devices only. • Switches can support both layer 2 (based on MAC Address) and layer 3 (Based on IP address) depending on the type of switch. • Usually large networks use switches instead of hubs to connect computers within the same subnet.	• Bridge has a single incoming and outgoing port. • A bridge maintains a MAC address table for both LAN segments it is connected to. • Bridge filters traffic on the LAN by looking at the MAC address. • Bridge looks at the destination of the packet before forwarding unlike a hub. • It restricts transmission on other LAN segment if destination is not found. • Bridges are used to separate parts of a network that do not need to communicate • regularly, but need to be connected.

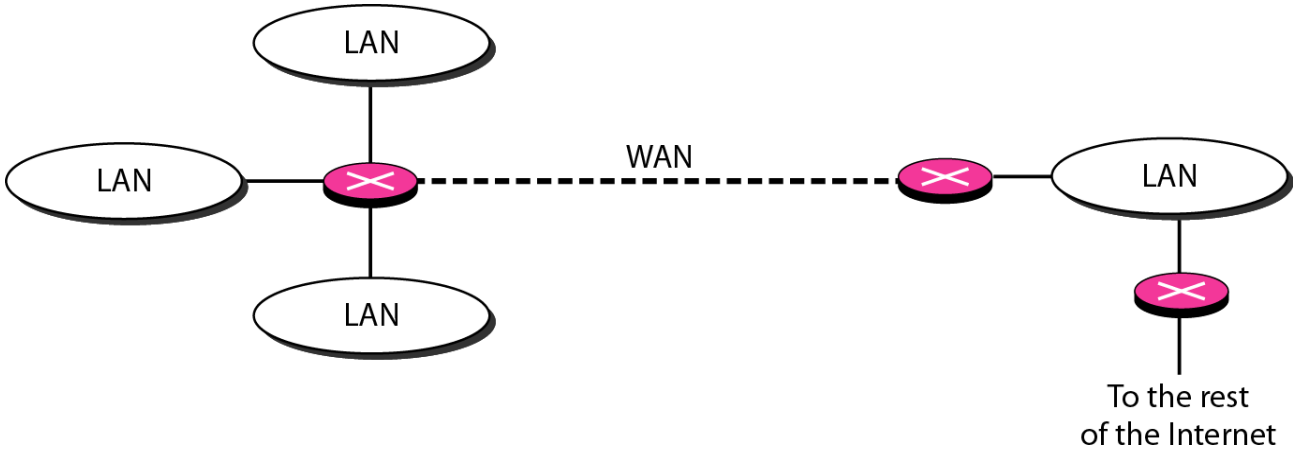
Two and Three layer switches

- Two layer switch operate at PHY and data link layer
- Three layer switch operates at network layer
- Bridge is an example of two-layer switch.
- Bridge with few port can connect a few LANs
- Bridge with many port may be able to allocate a unique port to each station, with each station on its own independent entity. This means no competing traffic (no collision as we saw in Ethernet)

3-layer switches- Router

- Routes packets based on their logical addresses (host-to-host addressing)
- A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decision about the route.
- The routing tables are normally dynamic and are updated using routing protocols.

Routers connecting independent LANs and WANs



Advantages and Disadvantages of Routers

- Advantages
  - Routers

  -provide sophisticated routing, flow control, and traffic isolation

  -are configurable, which allows network manager to make policy based on routing decisions

  -allow active loops so that redundant paths are available
- Disadvantages
  - Routers
  - are protocol-dependent devices that must understand the protocol they are forwarding
  - can require a considerable amount of initial configuration.
  - are relatively complex devices, and generally are more expensive than bridges.

Routers versus Bridges

- Addressing
  - Routers are explicitly addressed.
  - Bridges are not addressed.
- Availability
  - Routers can handle failures in links, stations, and other routers.
  - Bridges use only source and destination MAC address, which does not guarantee delivery of frames.
- Message Size
  - » Routers can perform fragmentation on packets and thus handle different packet sizes.
  - » Bridges cannot do fragmentation and should not forwarda frame which is too big for the next LAN.
- Forwarding
  - » Routers forward a message to a specific destination.
  - » Bridges forward a message to an outgoing network.

Routers versus Bridges

- Priority
  - » Routers can treat packets according to priorities
  - » Bridges treat all packets equally.
- Error Rate
  - » Network layers have error-checking algorithms that examines each received packet.
  - » The MAC layer provides a very low undetected bit error rate.
- Security
  - » Both bridges and routers provide the ability to put "security walls" around specific stations.
  - » Routers generally provide greater security than bridges because
    - – they can be addressed directly and
    - – they use additional data for implementing security.

Brouters: Bridging Routers

- Combine features of bridges and routers.
- Capable of establishing a bridge between two networks as well as routing some messages from the bridge networks to other networks.
- Are sometimes called (Layer 2/3) switches and are a combination of bridge/router hardware and software.

Gateway

- Interchangeably used term router and gateway
- Connect two networks above the network layer of OSI model.
- Are capable of converting data frames and network protocols into the format needed by another network.
- Provide for translation services between different computer protocols.
- **Transport gateways** make a connection between two networks at the **transport layer.**
- **Application gateways** connect two parts of an application in the **application layer**, e.g., sending email between two machines using different mail formats
- Broadband-modem-router is one e.g of gateway

Access Point

- In computer **networking**, a wireless **access point** (WAP) is a **networking** hardware **device** that allows a Wi-Fi **device** to connect to a wired **network**. The WAP usually connects to a router (via a wired **network**) as a standalone **device**, but it can also be an integral component of the router itself.

Access Point

- Access Point(AP) units serve areas of a building, similar to base units of cordless telephones except each AP can connect to many computers. APs serve as network bridges between the wired and wireless portions of the network.

Outline

- Introduction of LAN; MAN;WAN; PAN,Ad-hoc Network
- Topologies
- Network Architectures
- OSI Model
- TCP/IP Model
- Design issues for Layers
- Transmission Mediums
- Network Devices
- **Manchester and Differential Manchester Encodings;**
- IEEE802.11: Frequency Hopping (FHSS) and Direct Sequence (DSSS)

Encoding

Coding is the process of embedding clocks into a given data stream and producing a signal that can be transmitted over a selected medium.

Transmitter is responsible for "encoding" i.e. inserting clocks into data according to a selected coding scheme

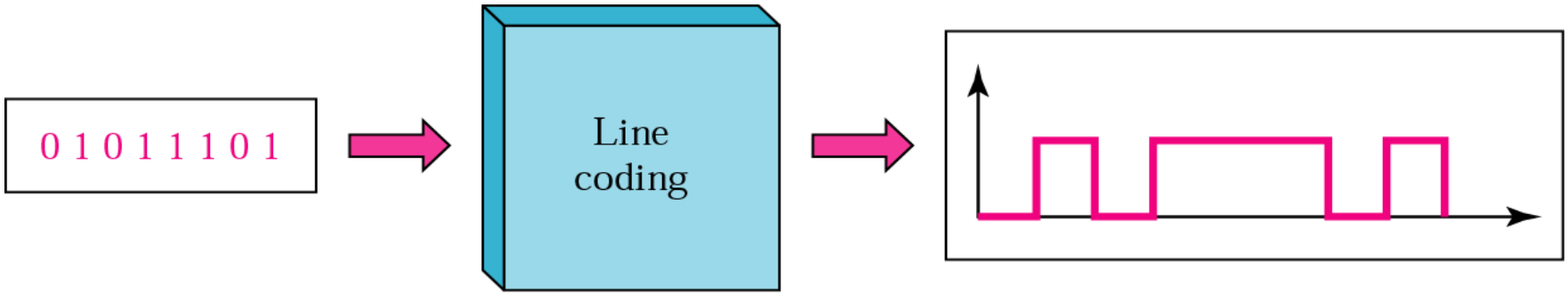
Receiver is responsible for "decoding" i.e. separating clocks and data from the incoming embedded stream.

A signal needs to be manipulated in such a way so that it contains identifiable changes that are recognizable to the sender and receiver.

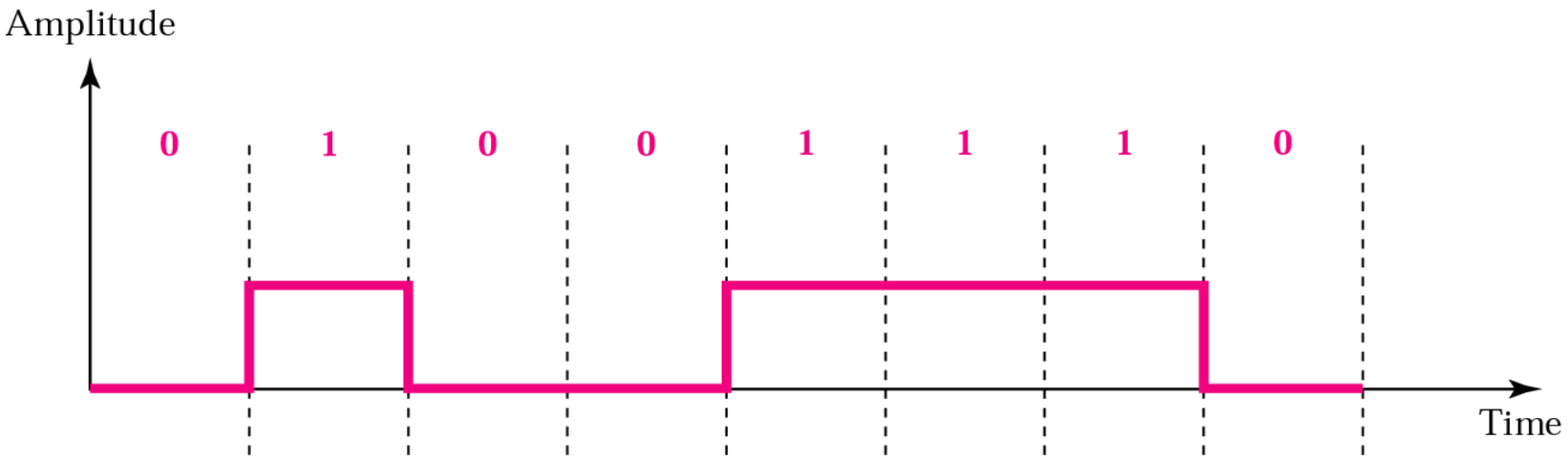
There are 4 possible encoding techniques that can be used on the data: Digital-to-digital, Digital-to-Analog, Analog-to-analog, Analog-to-digital.

Digital-to-Digital Encoding

- The binary signals created by your computer (DTE) are translated into a sequence of voltage pulses that can be sent through the transmission medium.
- Binary signals have two basic parameters: amplitude and duration.
- As the number of bits sent per unit of time increases, the bit duration decreases.
- The three most common methods of encoding used are: *unipolar* , *polar* , and *bipolar* .

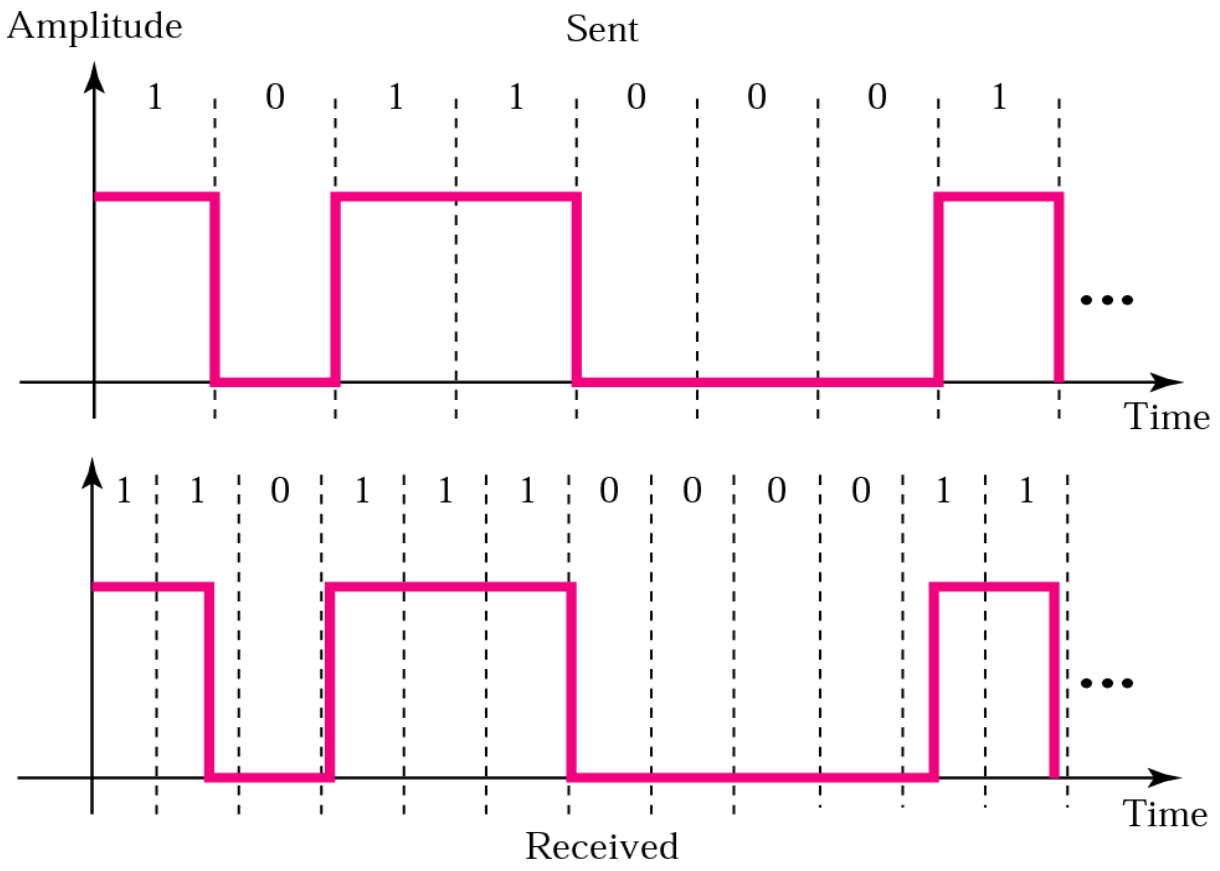


UNIPOLAR ENCODING

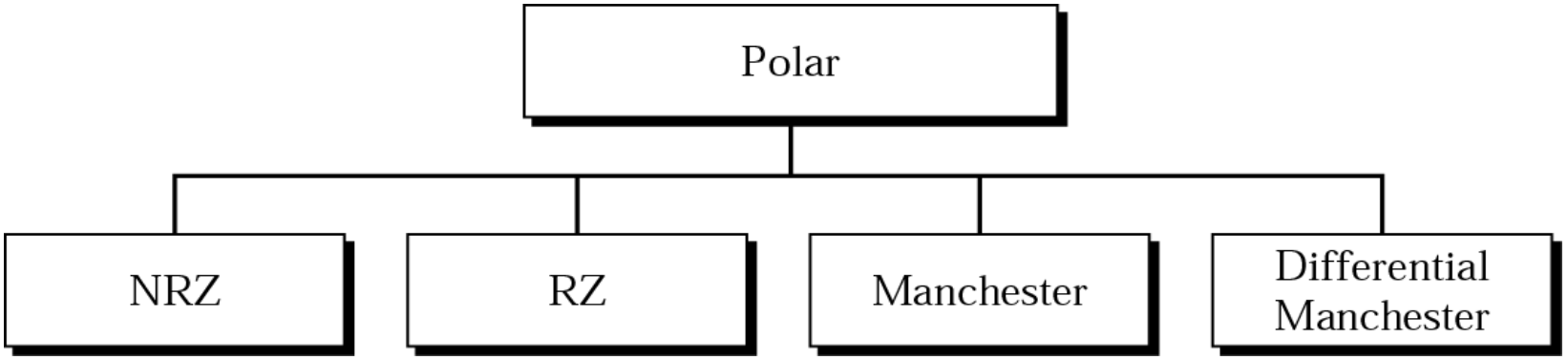


Unipolar encoding uses only one voltage level.

Lack of synchronization



POLAR ENCODING



Polar encoding uses two voltage levels (positive and negative).

Manchester

(or diphase or biphase encoding)

This code is self-clocking

Provides a *transition* for every bit in the *middle* of the bit cell. This transition is used only to provide clocking.

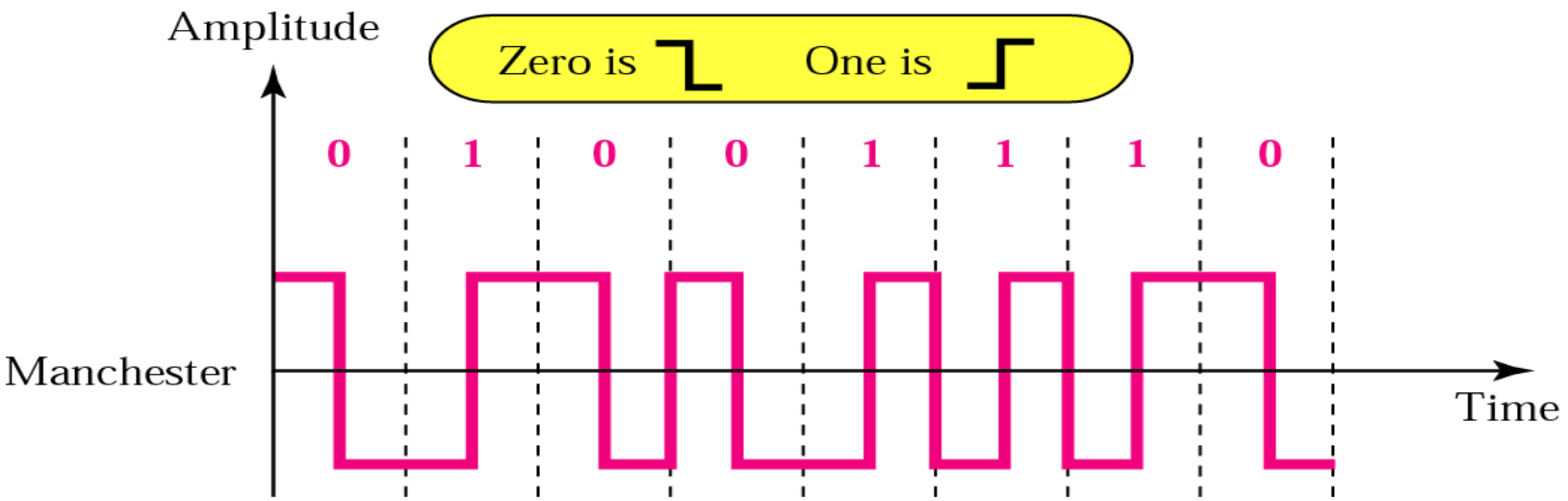
+ve to -ve transition for a "0" bit

-ve to +ve transition for a "1" bit

Residual DC component is eliminated by having both polarities for every bit.

This scheme is used in Ethernet and IEEE 802.3 compliant LANs

Manchester Encoding

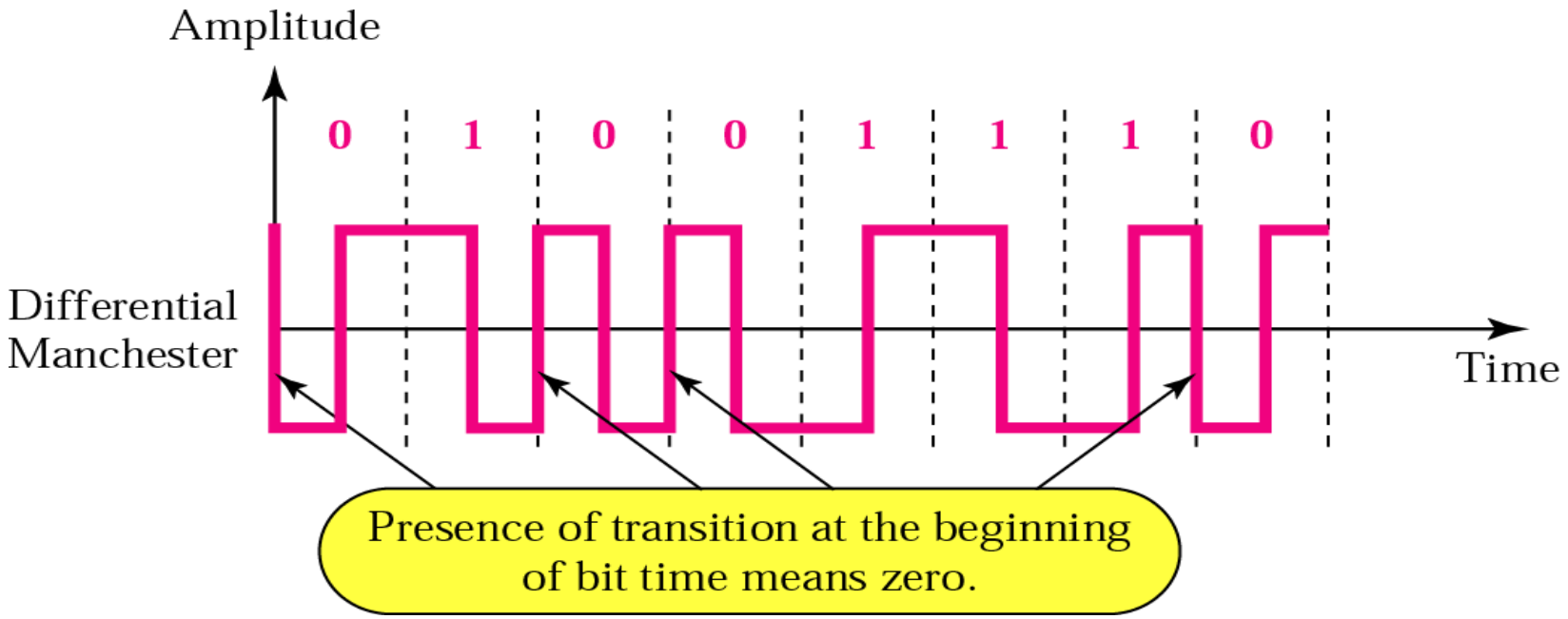


In Manchester encoding, the transition at the middle of the bit is used for both synchronization and bit representation.

Differential Manchester Coding

- Code is self-clocking
- *Transition* for every bit in the *middle* of the bit cell
- *Transition* at the beginning of the bit cell if the next bit is " *0* "
- *NO Transition* at the beginning of the bit cell if the next bit is " *1* "
- *Used in Token Ring or IEEE 802.5-compliant LANs.*

Differential Manchester encoding



In differential Manchester encoding, the transition at the middle of the bit is used only for synchronization. The bit representation is defined by the inversion or noninversion at the beginning of the bit.

Outline

- Introduction of LAN; MAN;WAN; PAN,Ad-hoc Network
- Topologies
- Network Architectures
- OSI Model
- TCP/IP Model
- Design issues for Layers
- Transmission Mediums
- Network Devices
- Manchester and Differential Manchester Encodings;
- **IEEE802.11: Frequency Hopping (FHSS) and Direct Sequence (DSSS)**

IEEE 802 Standards

Number	Topic
802.1	Overview and architecture of LANs
802.2 ↓	Logical link control
802.3 *	Ethernet
802.4 ↓	Token bus (was briefly used in manufacturing plants)
802.5	Token ring (IBM's entry into the LAN world)
802.6 ↓	Dual queue dual bus (early metropolitan area network)
802.7 ↓	Technical advisory group on broadband technologies
802.8 †	Technical advisory group on fiber optic technologies
802.9 ↓	Isochronous LANs (for real-time applications)
802.10 ↓	Virtual LANs and security
802.11 *	Wireless LANs
802.12 ↓	Demand priority (Hewlett-Packard's AnyLAN)
802.13	Unlucky number. Nobody wanted it
802.14 ↓	Cable modems (defunct: an industry consortium got there first)
802.15 *	Personal area networks (Bluetooth)
802.16 *	Broadband wireless
802.17	Resilient packet ring

The important ones are marked with *. The ones marked with ↓ are hibernating. The one marked with † gave up.

IEEE 802.11 Wireless LAN Standard

IEEE developed the first internationally recognized wireless LAN standard – **IEEE 802.11** in 1997

Scope of IEEE 802.11 is limited to **Physical and Data Link Layers.**

IEEE 802.11 Standards

- 802.11a (OFDM Waveform)
- 802.11b
- 802.11g
- 802.11n
- 802.11ac
- 802.11ad
- 802.11af
- 802.11ah
- 802.11ai
- 802.11aj
- 802.11aq
- 802.11ax

Physical Media of 802.11 Standard

Frequency-hopping spread spectrum	• Operating in 2.4 GHz ISM band • Lower cost, power consumption • Most tolerant to signal interference
Direct-sequence spread spectrum	• Operating in 2.4 GHz ISM band • Supports higher data rates • More range than FH or IR physical layers
Infrared	• Lowest cost • Lowest range compared to spread spectrum • Doesn't penetrate walls, so no eavesdropping

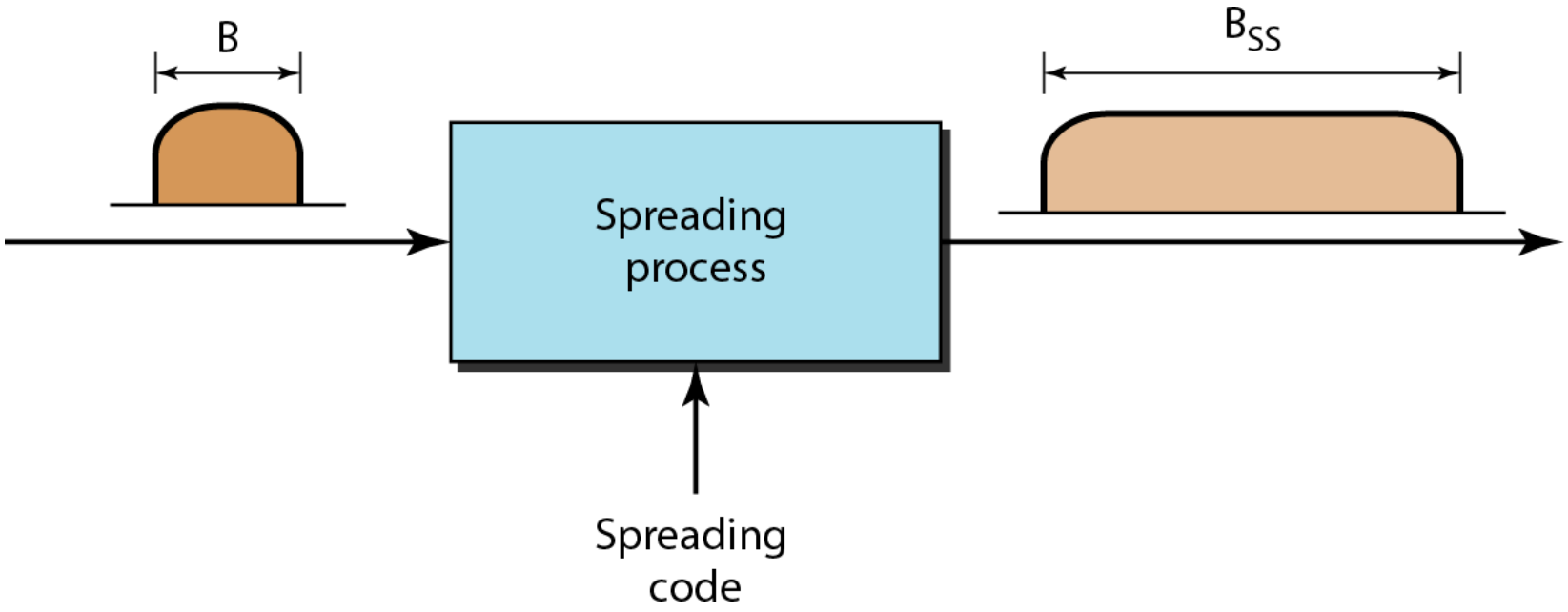
What is meant by Spread Spectrum

Spread spectrum is a form of wireless communications in which the **frequency of the transmitted signal is varied**.This results in a much greater bandwidth than the signal (Bss >> B)

This technique decreases the potential interference to other receivers while achieving privacy.

Two types of Spread Spectrum- FHSS and DSSS

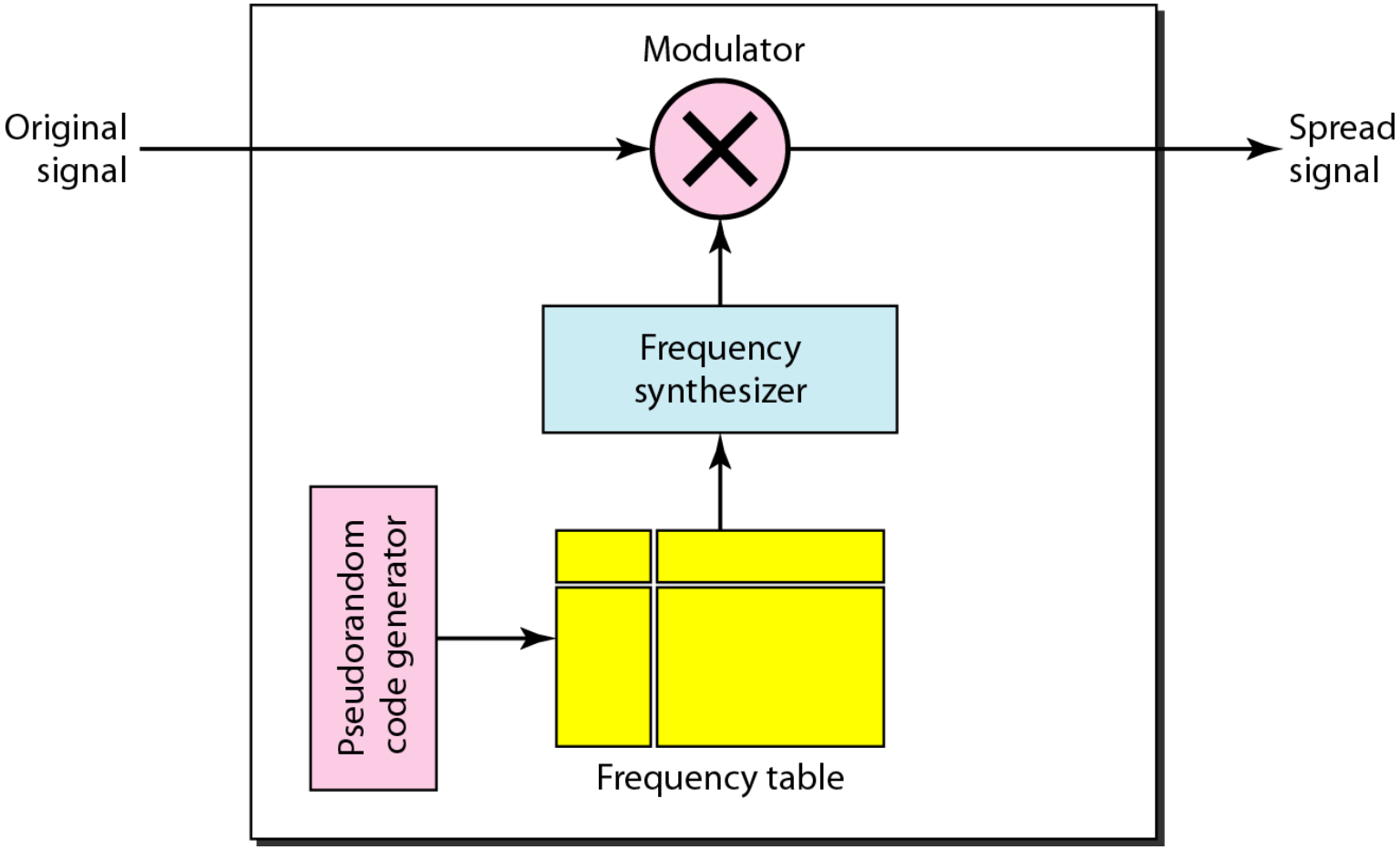
Spread spectrum



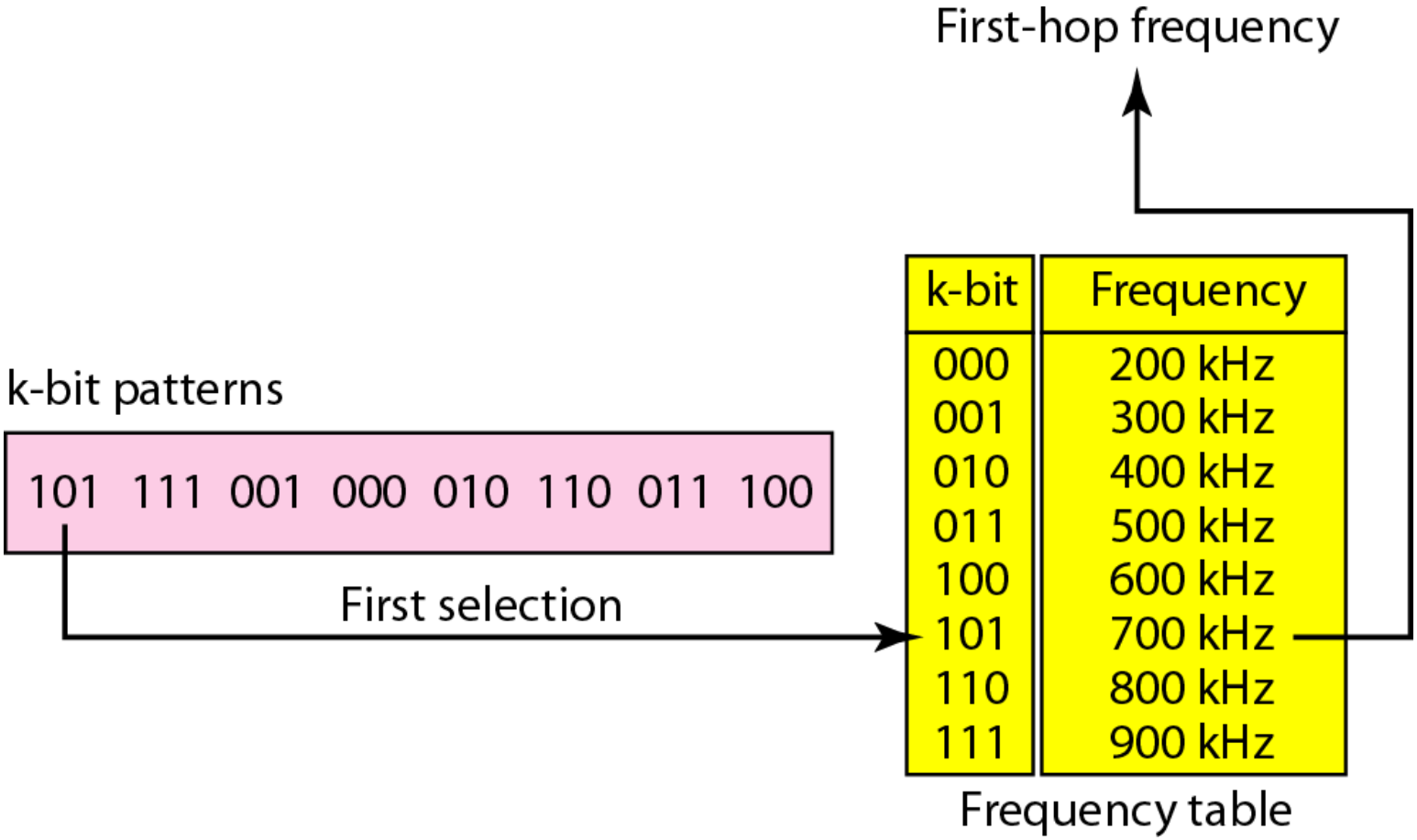
Frequency Hopping Spread Spectrum (FHSS)

- Signal is broadcast over seemingly random series of radio frequencies
- Signal hops from frequency to frequency at fixed intervals
- Receiver, hopping between frequencies in synchronization with transmitter, picks up message
- Advantages
  - Efficient utilization of available bandwidth
  - Eavesdropper hear only unintelligible blips
  - Attempts to jam signal on one frequency succeed only at knocking out a few bits

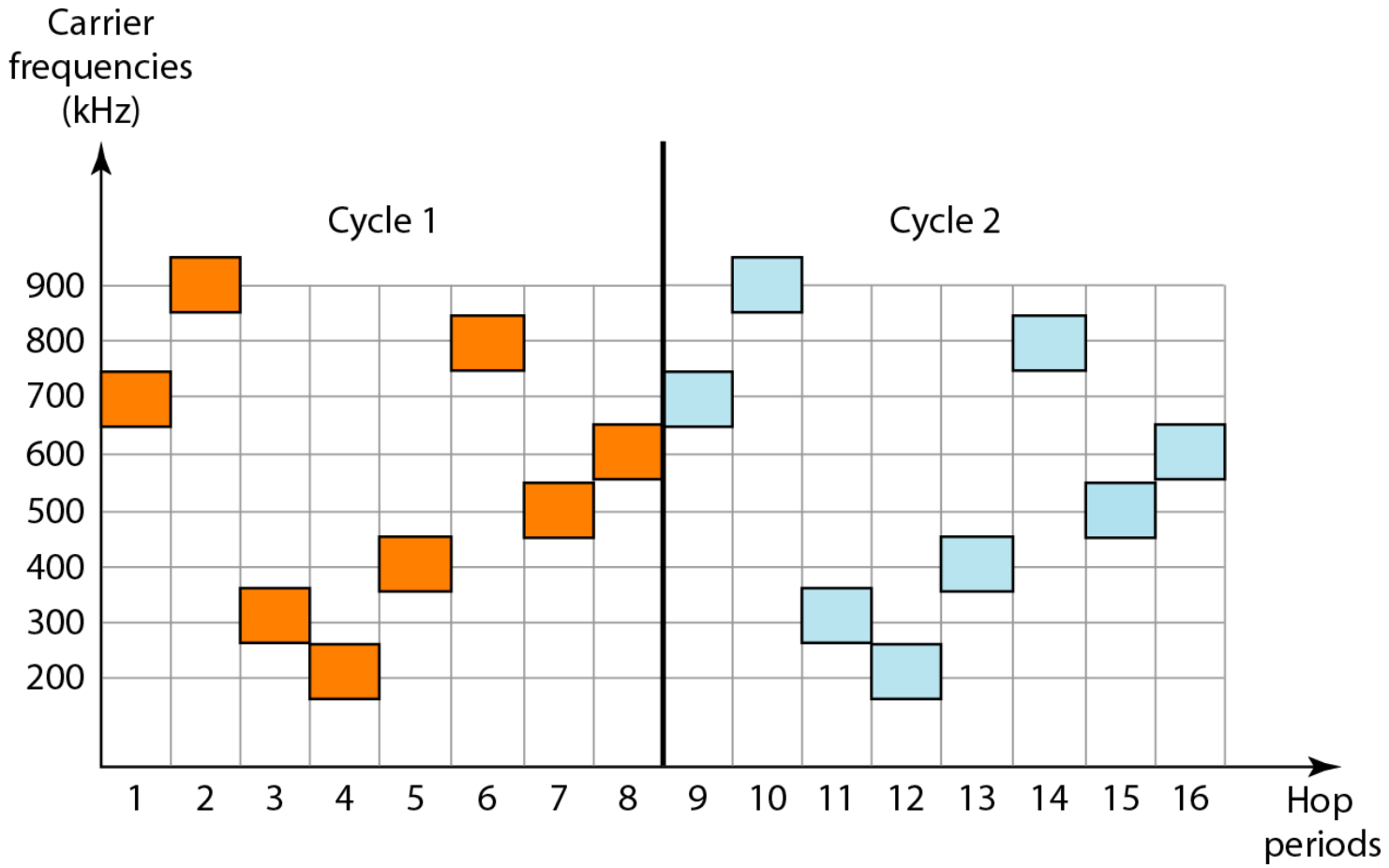
Frequency hopping spread spectrum (FHSS)



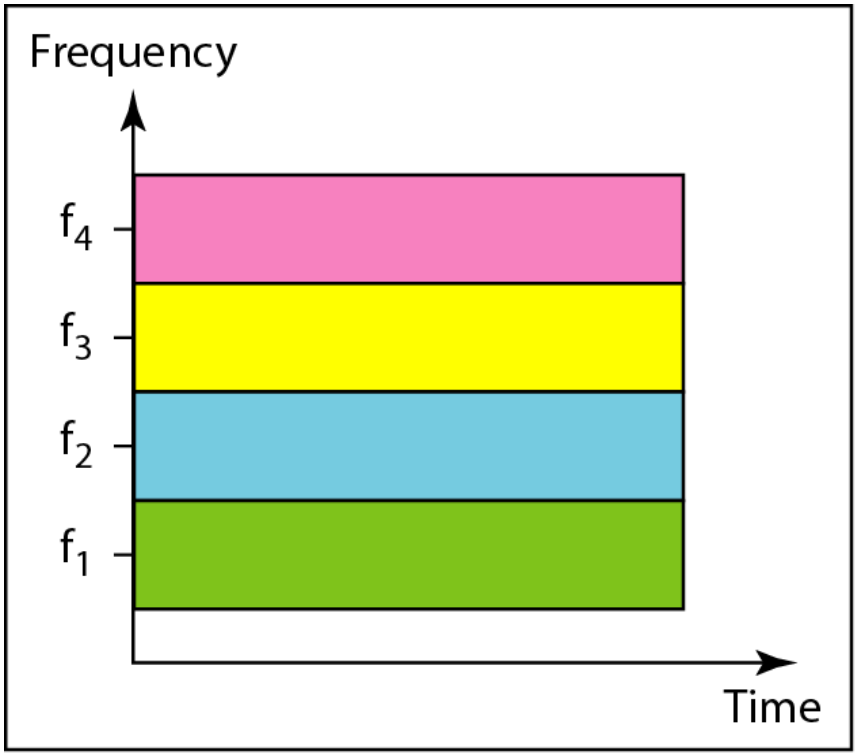
Frequency hopping spread spectrum (FHSS)



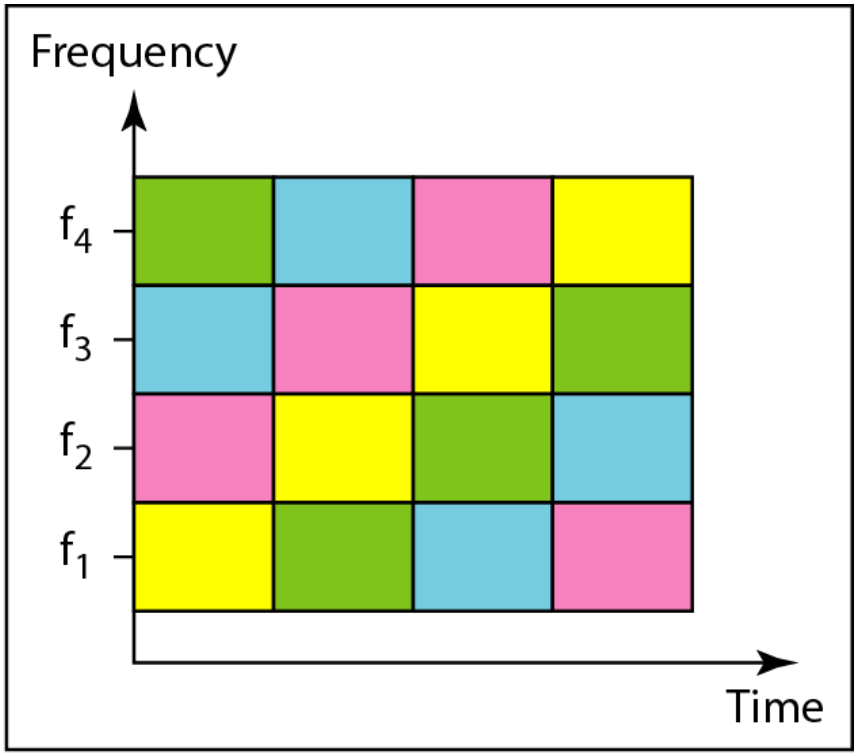
FHSS cycles


Carrier frequencies (kHz)
Cycle 1
Cycle 2
900
800
700
600
500
400
300
200
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
Hop periods

Bandwidth sharing difference between FDM and FHSS



a. FDM

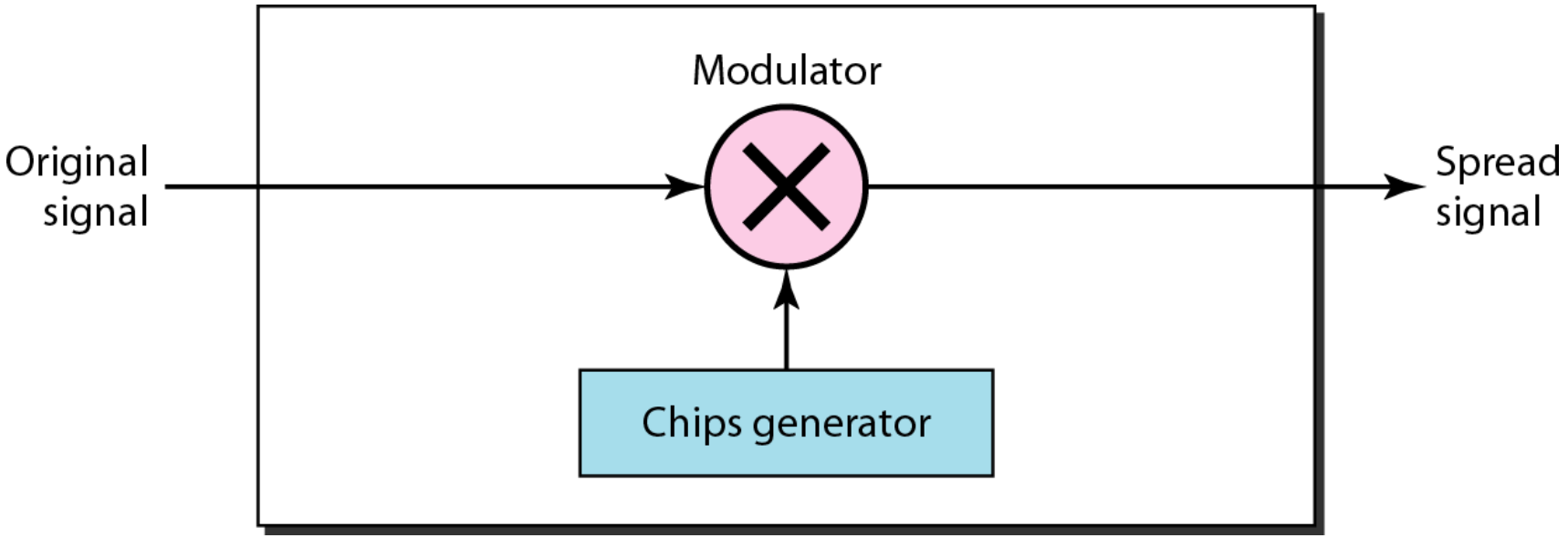


b. FHSS

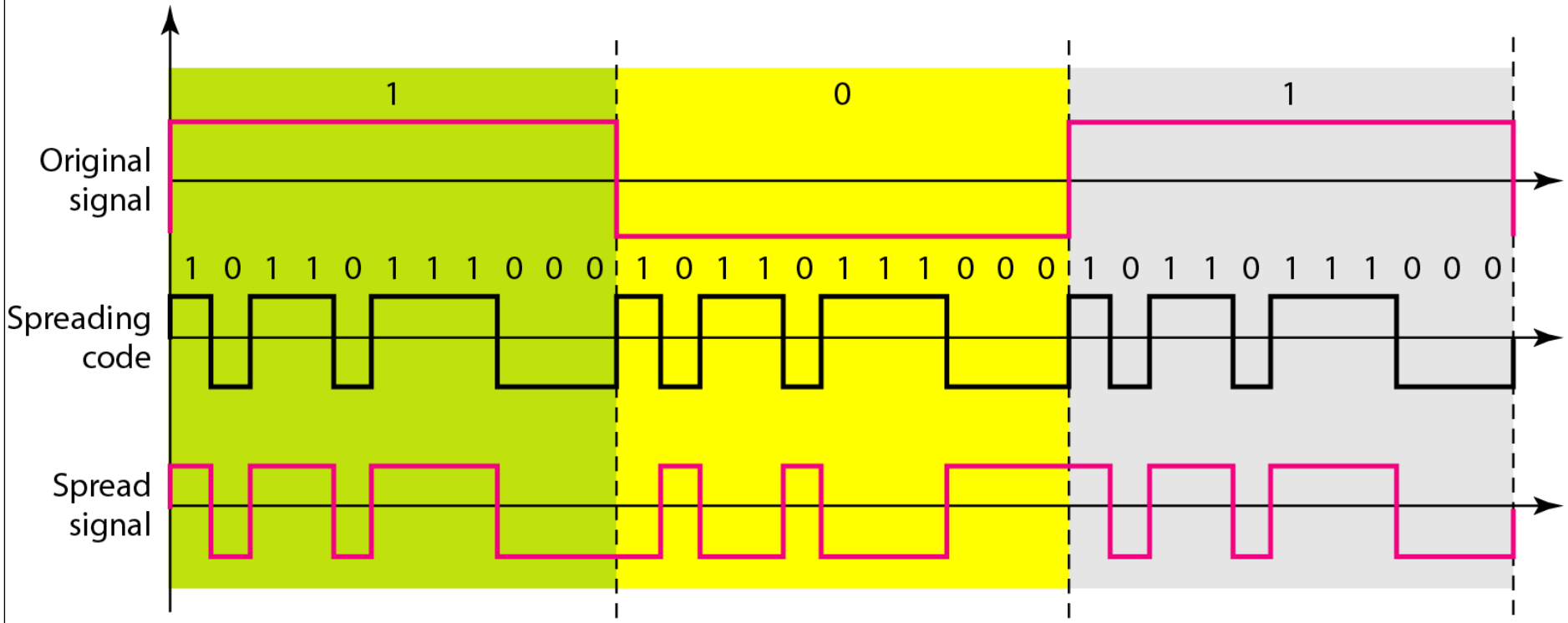
Direct Sequence Spread Spectrum (DSSS)

- Each bit in original signal is represented by multiple bits in the transmitted signal
- Spreading code spreads signal across a wider frequency band
- DSSS is the only physical layer specified for the 802.11b specification
  - 802.11a and 802.11b differ in use of chipping method
  - 802.11a uses 11-bit barker chip
  - 802.11b uses 8-bit complimentary code keying (CCK) algorithm

Direct Sequence Spread Spectrum (DSSS)



DSSS example



FHSS Vs DSSS

- FH systems use a radio carrier that "hops" from frequency to frequency in a pattern known to both transmitter and receiver
  - Easy to implement
  - Resistance to noise
  - Limited throughput (2-3 Mbps @ 2.4 GHz)
- DS systems use a carrier that remains fixed to a specific frequency band. The data signal is spread onto a much larger range of frequencies (at a much lower power level) using a specific encoding scheme.
  - Much higher throughput than FH (11 Mbps)
  - Better range
  - Less resistant to noise (made up for by redundancy – it transmits at least 10 fully redundant copies of the original signal at the same time)

Outline

- Introduction of LAN; MAN;WAN; PAN,Ad-hoc Network
- Topologies
- Network Architectures
- OSI Model
- TCP/IP Model
- Design issues for Layers
- Transmission Mediums
- Network Devices
- Manchester and Differential Manchester Encodings;
- IEEE802.11: Frequency Hopping (FHSS) and Direct Sequence (DSSS)

References

Websites:

- http://www.studytonight.com/computer-networks/
- https://cs.fit.edu/~pkc/classes/dc/slides/ch3.ppt
- https://www.techopedia.com/2/29090/networks/lanwanman-an-overview-of-network-types
- https://www.slideshare.net/ENGMSHARI/adhoc-networks
- http://www.businessdictionary.com/definition/distributed-network-architecture-DNA.html
- https://en.wikipedia.org/wiki/Optical_fiber_cable
- https://en.wikipedia.org/wiki/Radio_spectrum
- https://www.slideshare.net/rupinderj/networking-devices-12807479
- https://en.wikipedia.org/wiki/Wireless_access_point
- https://www.slideshare.net/LukaXavi/data-encoding

Text Books:

- Andrew S.Tenenbaum, "Computer Networks",5th Edition, PHI, ISBN 81-203-2175-8.
- Fourauzan B., "Data Communications and Networking", 5th Edition, Tata McGraw-Hill, Publications, 2006