Presentation on

Wireless Lans And Pans

(Embedded Systems - ECE)

I -M.TECH I -Semester (AUTONOMOUS-R18)

Prepared by,

Ms. C. Devisupraja

Assistant Professor

UNIT-1

WIRELESS SYSTEMS

CONTENTS

- *INTRODUCTION*
- *1G TECHNOLOGY*
- *2GTECHNOLOGY*
- *MODELS OF 1G & 2G*
- *2.5 TECHNOLOGY*
- *3G*
- **TECHNOLOGY**
- *4G TECHNOLOGY*
- *5G TECHNOLOGY*
- **WIRELESS *APPLICATIONS***
- *WIRELESS SERVICES*
- *EVOLUTION FROM 1G TO 5G TECHNOLOGY*
- *CONCLUSION*

INTRODUCTION

WHAT IS WIRELESS ?

- The word wireless is dictionary defined “having no wires ” .
- In networking terminology , wireless is the term used to describe any computer network where there is no physical wired connection between sender and receiver, but rather the network is connected by radio waves and or microwaves to maintain communications.
- Wireless networking utilizes specific equipment such as NICs and Routers in place of wires (copper or optical fibre).

1G TECHNOLOGY

- 1G refers to the first generation of wireless telephone technology, mobile telecommunications which was first introduced in 1980s and completed in early 1990s.
  - It's Speed was upto 2.4kbps.
  - It allows the voice calls in 1 country. 1G network use Analog Signal.
- AMPS was first launched in USA in 1G mobile systems.

DRAWBACKS OF 1G

- *Poor Voice Quality*
- *Poor Battery Life*
- *Large Phone Size*
- *No Security*
- *Limited Capacity*
- *Poor Handoff Reliability*

1G Wireless System

2G TECHNOLOGY

- 2G technology refers to the 2nd generation which is based on GSM.
- It was launched in Finland in the year 1991.
- 2G network use digital signals.
- It's data speed was upto 64kbps.

- Features Includes:
- It enables services such as text messages, picture messages and (multi media message).
- It provides better quality and capacity .

DRAWBACKS OF 2G

- 2G requires strong digital signals to help mobile phones work. If there is no network coverage in any specific area , digital signals would weak.
- These systems are unable to handle complex data such as Videos.

2G Wireless System

WIRELESS MODELS OF 1G & 2G

2.5G TECHNOLOGY

- *2.5G is a technology between the second (2G) and third (3G) generation of mobile telephony.*
- *2.5G is sometimes described as 2G Cellular Technology combined with GPRS.*

Features Includes:

- *Phone Calls*
- *Send/Receive E-mail Messages*
- *Web Browsing*
- *Speed : 64-144 kbps*
- *Camera Phones*
- *Take a time of 6-9 mins. to download a 3 mins. Mp3 song*

3G TECHNOLOGY

- *3G technology refer to third generation which was introduced in year 2000s.*

- *Data Transmission speed increased from 144kbps- 2Mbps.*

- *Typically called Smart Phones and features increased its bandwidth and data transfer rates to accommodate web-based applications and audio and video files.*

FEATURES OF 3G TECHNOLOGY

- Providing Faster Communication
- Send/Receive Large Email Messages

•High Speed Web / More Security Video Conferencing / 3D Gaming

- TV Streaming/ Mobile TV/ Phone Calls
- Large Capacities and Broadband Capabilities
- 11 sec – 1.5 min. time to download a 3 min Mp3 song.

DRAWBACKS OF 3G TECHNOLOGY

- Expensive fees for 3G Licenses Services
- It was challenge to build the infrastructure for 3G
- High Bandwidth Requirement
- Expensive3G Phones.
- Large Cell Phones

4G TECHNOLOGY (Anytime ,Anywhere)

4G TECHNOLOGY (Anytime ,Anywhere)

- *4G technology refer to or short name of fourth Generation which was started from late 2000s.*
- *Capable of providing 100Mbps – 1Gbps speed.*
- *One of the basic term used to describe 4G is MAGIC.*

MAGIC:

- *Mobile Multimedia*
- *Anytime Anywhere*
- *Global Mobility Support*
- *Integrated Wireless Solution*
- *Customized Personal Services*

Also known as Mobile Broadband Everywhere.

4G (Anytime, Anywhere)

- ***The next generations of wireless technology that promises higher data rates and expanded multimedia services.***
- ***Capable to provide speed 100Mbps-1Gbps.***
- ***High QOS and High Security***
- ***Provide any kind of service at any time as per user requirements, anywhere.***

<u>Features Include:</u>

- ***More Security***
- ***High Speed***
- ***High Capacity***
- ***Low Cost Per-bit etc.***

DRAWBACKS OF 4G

- *Battery uses is more*
- *Hard to implement*
- *Need complicated hardware*
- *Expensive equipment required*

to implement next generation network.

COMPARISON BETWEEN 3G Vs 4G

Technology	3G	4G
Data Transfer Rate	3.1 MB/sec	100 MB/sec
Internet Services	Broadband	Ultra Broadband
Mobile - TV Resolution	Low	High
Bandwidth	5-20 MHz	100MHz
Frequency	1.6-2 GHz	2-8 GHz
Download and upload	5.8 Mbps	14 Mbps

WIRLESS MODELS OF 3G & 4G

5G TECHNOLOGY

- *5G technology refer to short name of fifth Generation which was started from late 2010s.*

- *Complete wireless communication with almost no limitations.*

- *It is highly supportable to WWWW (Wireless World Wide Web).*

BENEFITS OF 5G TECHNOLOGY

- *High Speed, High Capacity*
- *5G technology providing large broadcasting of data in Gbps .*
- *Multi - Media Newspapers, watch T.V programs with the clarity as to that of an HD Quality.*
- *Faster data transmission that of the previous generations.*
- *Large Phone Memory, Dialing Speed, clarity in Audio/Video.*
- *Support interactive multimedia , voice, streaming video, Internet and other*
- *5G is More Effective and More Attractive.*

COMPARISON BETWEEN 4G Vs 5G

Technology	4G(2000-10)	5G(2010-20)
Switching	Circuit/Packet	Circuit/Packet
Data Rate	Upto 20Mbps	Upto 1 Gbps
Technology	Combination of broadband LAN/WAN/PAN	Combination of broadband LAN/WAN/PAN

EVOLUTION OF 1G TO 5G TECHNOLOGY

WIRELESS APPLICATIONS

- Wireless applications are those which we use free space as the transmission medium & do not involve cabling like fibre or copper cables.

WIRELESS SERVICES

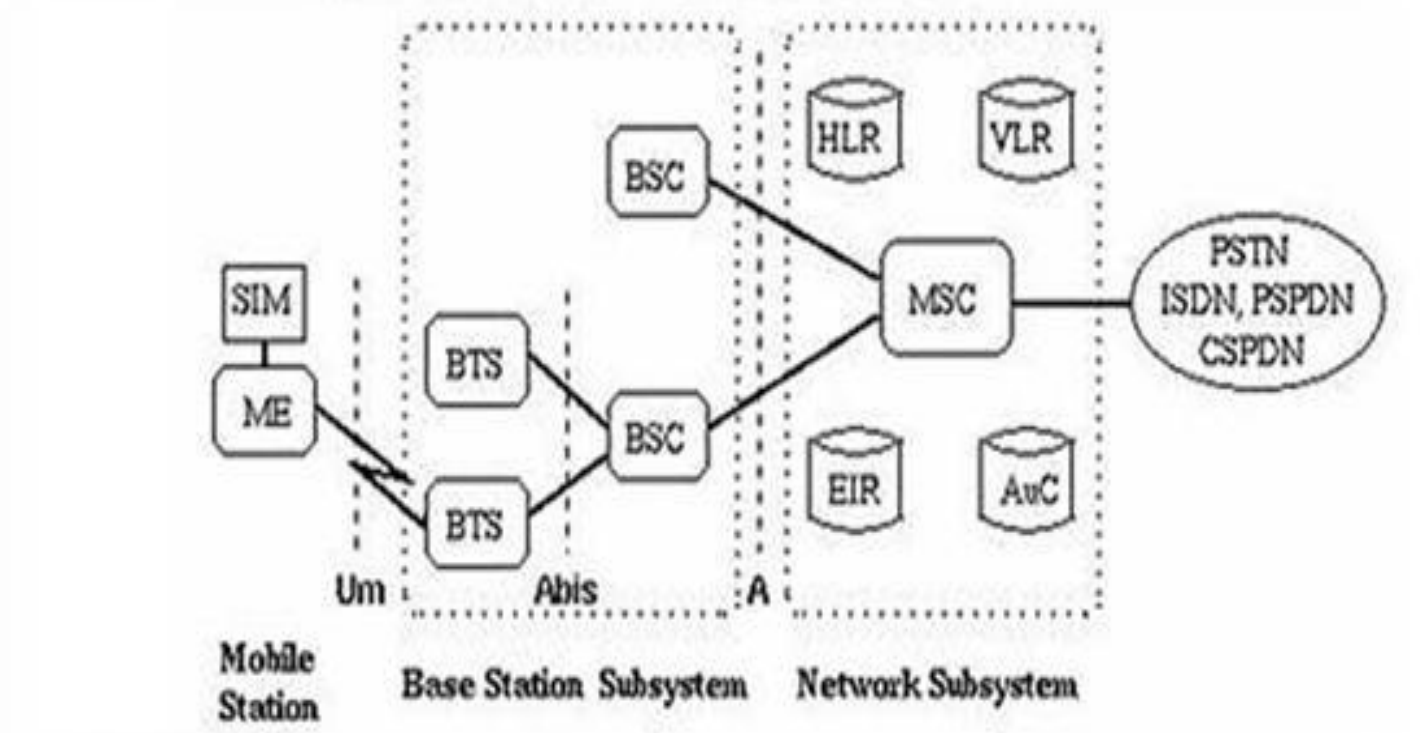
Wireless solution for:

- Business and Industry
- Schools , Colleges
- Doctors , Pilots
- Police and Vehicles etc.

CONCLUSION

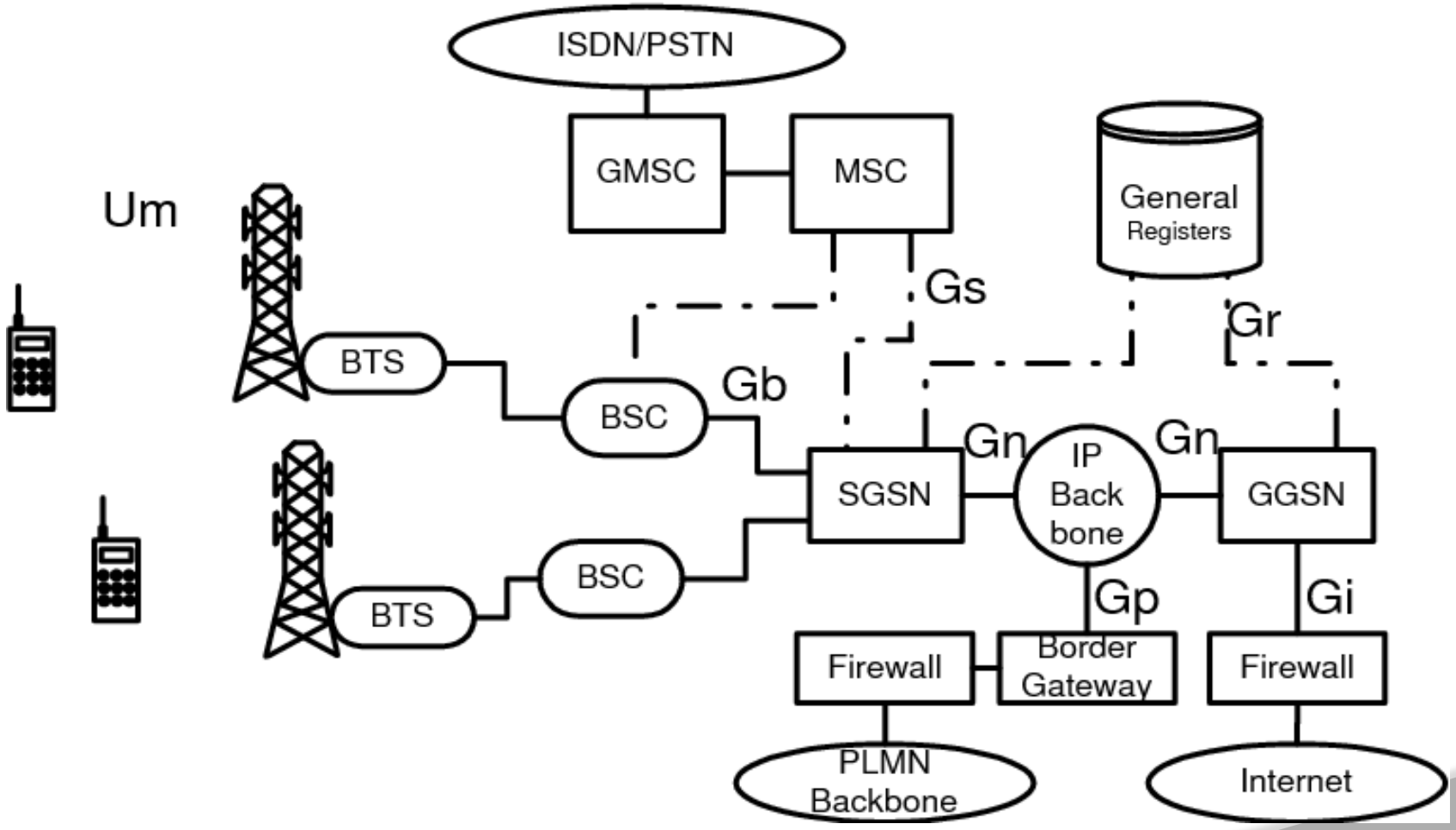
- All totally the best way to help all users is to use 5G as the next wireless system and in totally it is safety and secure for public, this the need that demands the solution.
- Today's wired society is going wireless and if it has problem, 5G is answer.
- 5G technology is going to give tough competition to Computers and Laptops.
- It will be available in the market 2020 at affordable cost with more reliability than previous mobiles.

GSM ARCHITECTURE

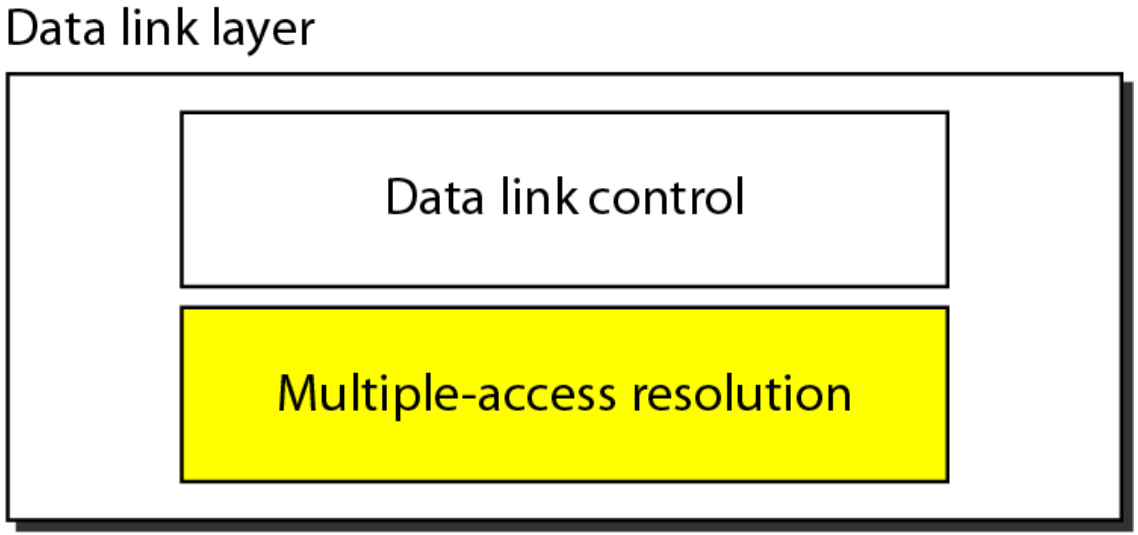


SIM Subscriber Identity Module
ME Mobile Equipment
BTS Base Transreceiver station
BSC Base Station Controller
HLR Home Location Register
VLR Vistor Location Register
MSC Mobile service switching center
EIR Equipment Identity Register
AuC Authentication Center

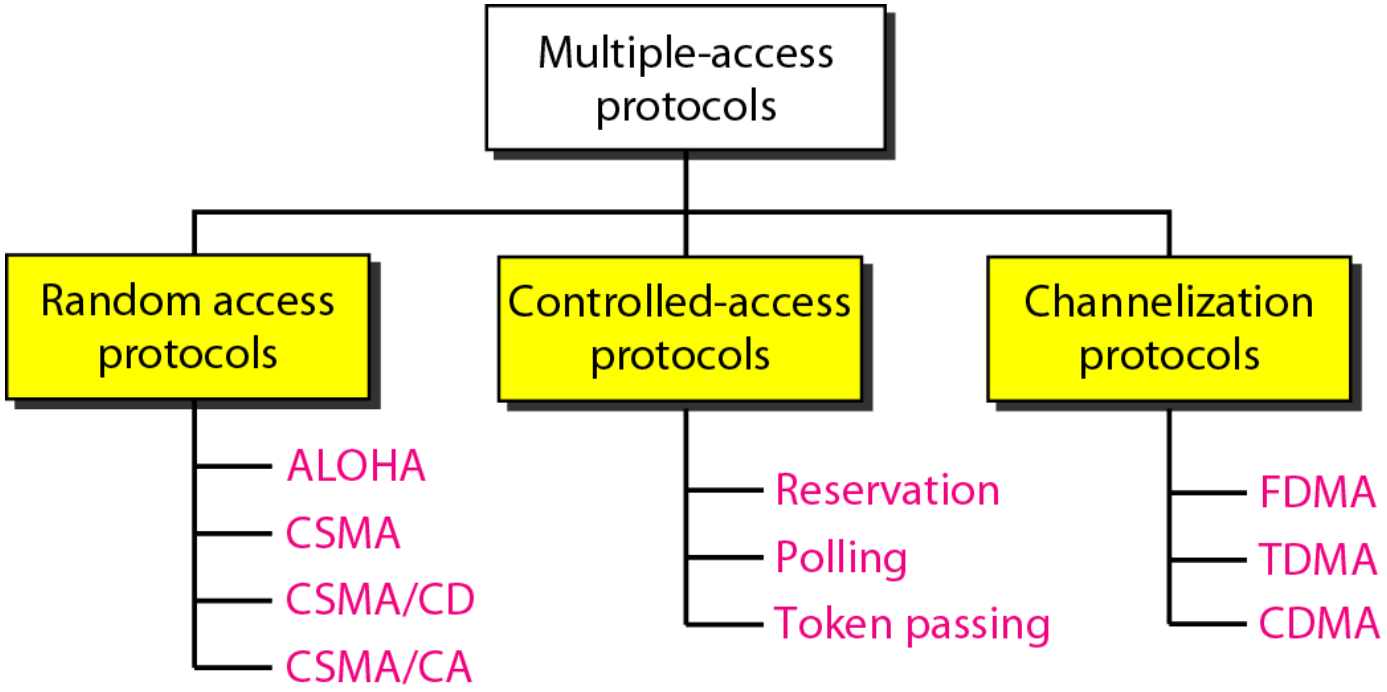
GPRS ARCHITECTURE



SUBLAYERS OF DATA LINK LAYER



TAXONOMY OF MULTIPLE-ACCESS PROTOCOLS



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. At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send.

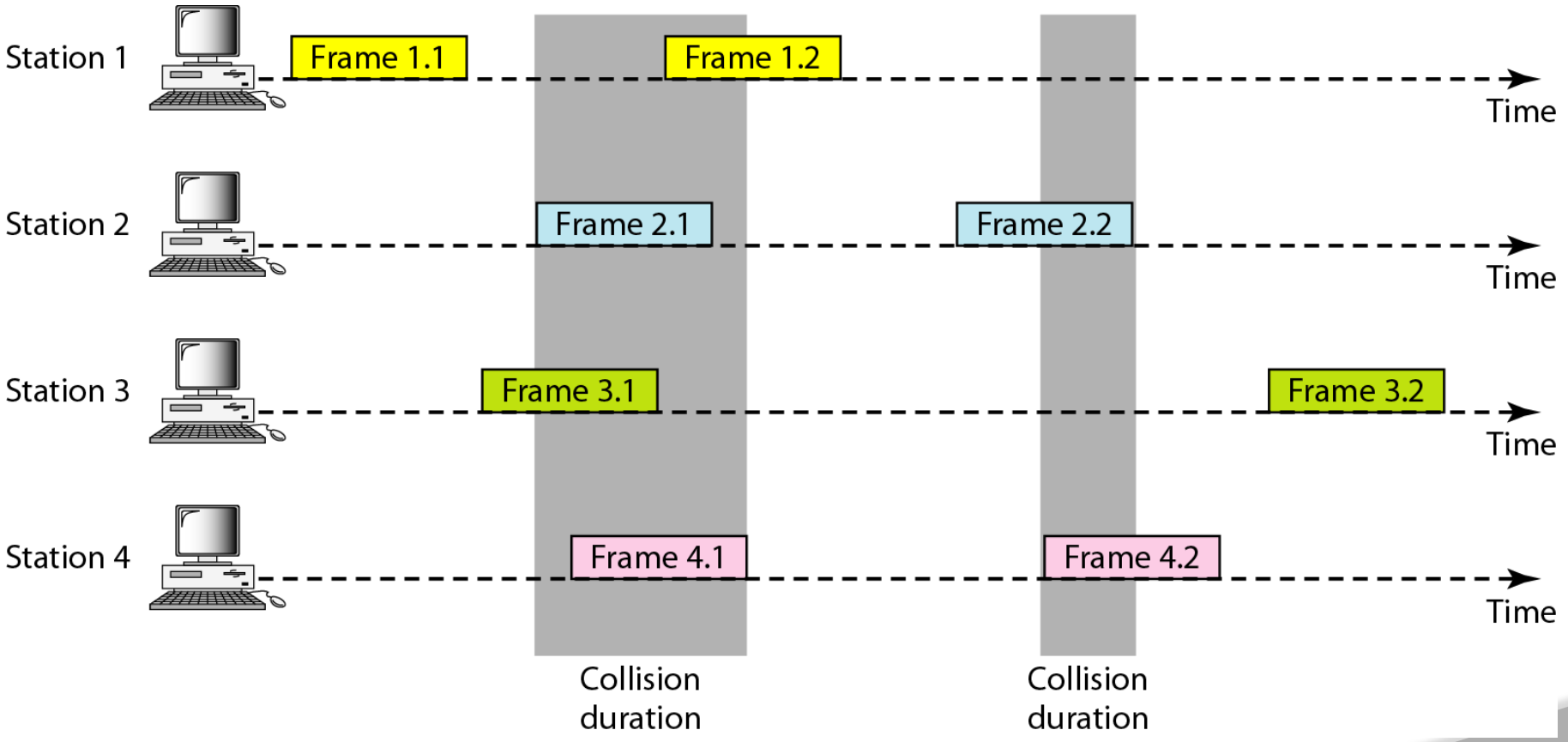
ALOHA

Carrier Sense Multiple Access

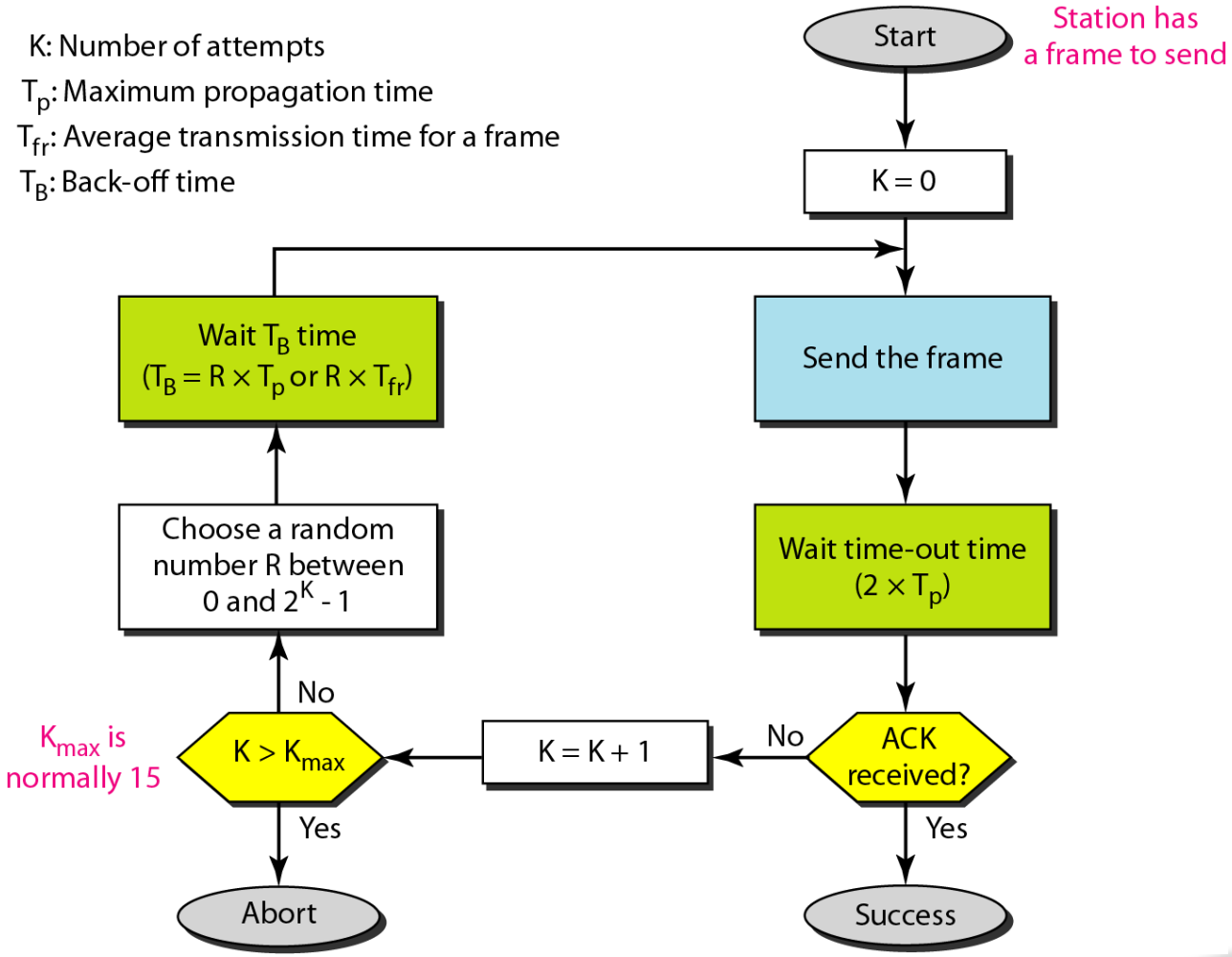
Carrier Sense Multiple Access with Collision Detection

Carrier Sense Multiple Access with Collision Avoidance

FRAMES IN A PURE ALOHA NETWORK



PROCEDURE FOR PURE ALOHA PROTOCOL



Example 1.1

The stations on a wireless ALOHA network are a maximum of 600 km apart. If we assume that signals propagate at 3×10^8 m/s, we find

$$Tp = (600 \times 10^5) / (3 \times 10^8) = 2 \text{ ms}.$$

Now we can find the value of T_B for different values of K .

a. For K = 1, the range is {0, 1}. The station needs to generate a random number with a value of 0 or 1. This means that T_B is either 0 ms (0 × 2) or 2 ms (1 × 2), based on the outcome of the random variable.

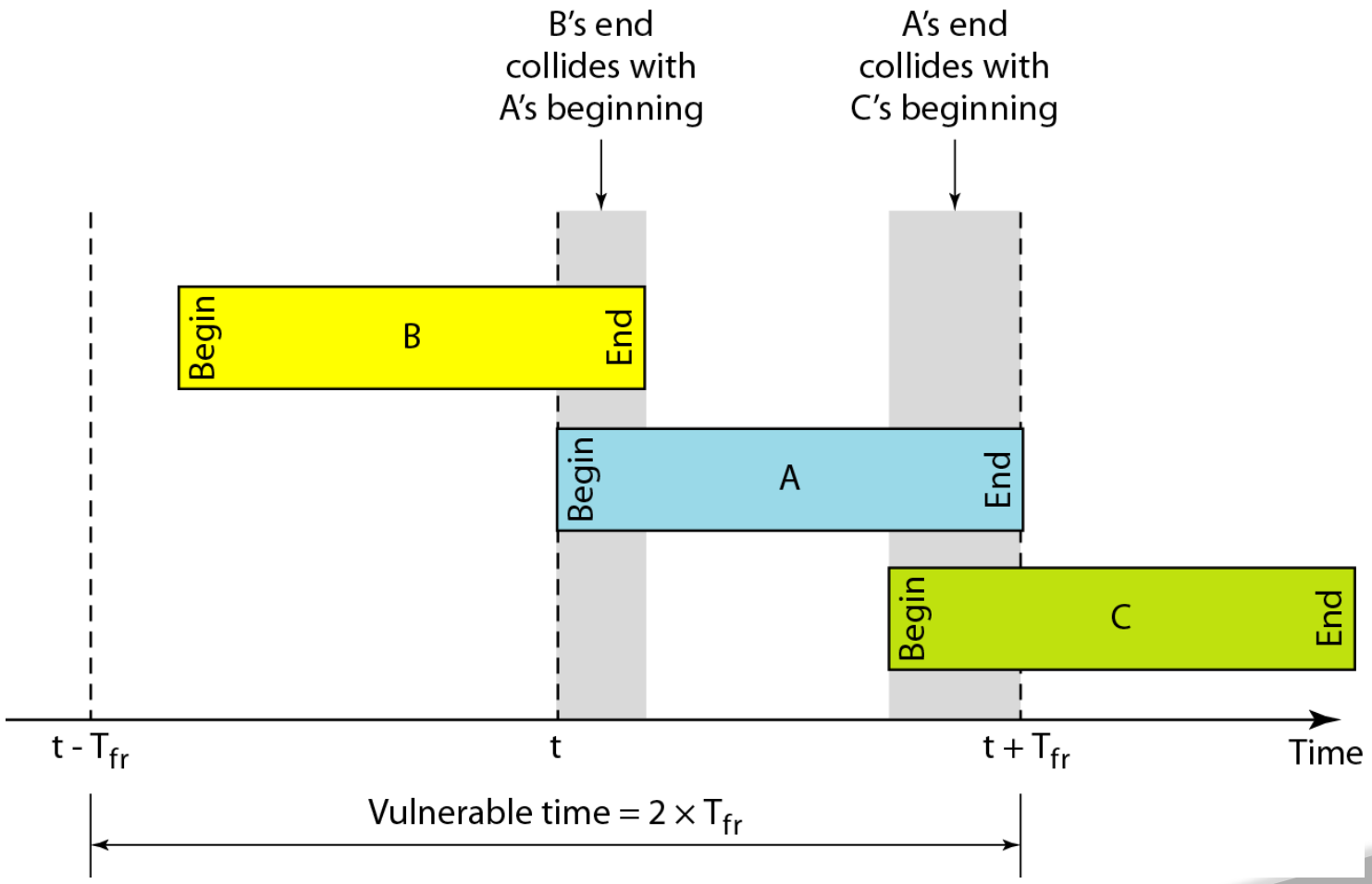
EXAMPLE 1.1 (CONTINUED)

b. For K = 2, the range is {0, 1, 2, 3}. This means that T_B can be 0, 2, 4, or 6 ms, based on the outcome of the random variable.

c. For K = 3, the range is {0, 1, 2, 3, 4, 5, 6, 7}. This means that T_B can be 0, 2, 4, . . . , 14 ms, based on the outcome of the random variable.

d. We need to mention that if K > 10, it is normally set to 10.

VULNERABLE TIME FOR PURE ALOHA PROTOCOL



EXAMPLE 1.2

A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the requirement to make this frame collision-free?

Solution

Average frame transmission time T_{fr} is 200 bits/200 kbps or 1 ms. The vulnerable time is 2×1 ms = 2 ms. This means no station should send later than 1 ms before this station starts transmission and no station should start sending during the one 1-ms period that this station is sending.

NOTE

The throughput for pure ALOHA is

$$S = G \times e^{-2G} .$$

The maximum throughput

$S_{max} = 0.184$ when $G = (1/2)$.

EXAMPLE 1.3

A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces

a. 1000 frames per second b. 500 frames per second

c. 250 frames per second.

Solution

The frame transmission time is 200/200 kbps or 1 ms.

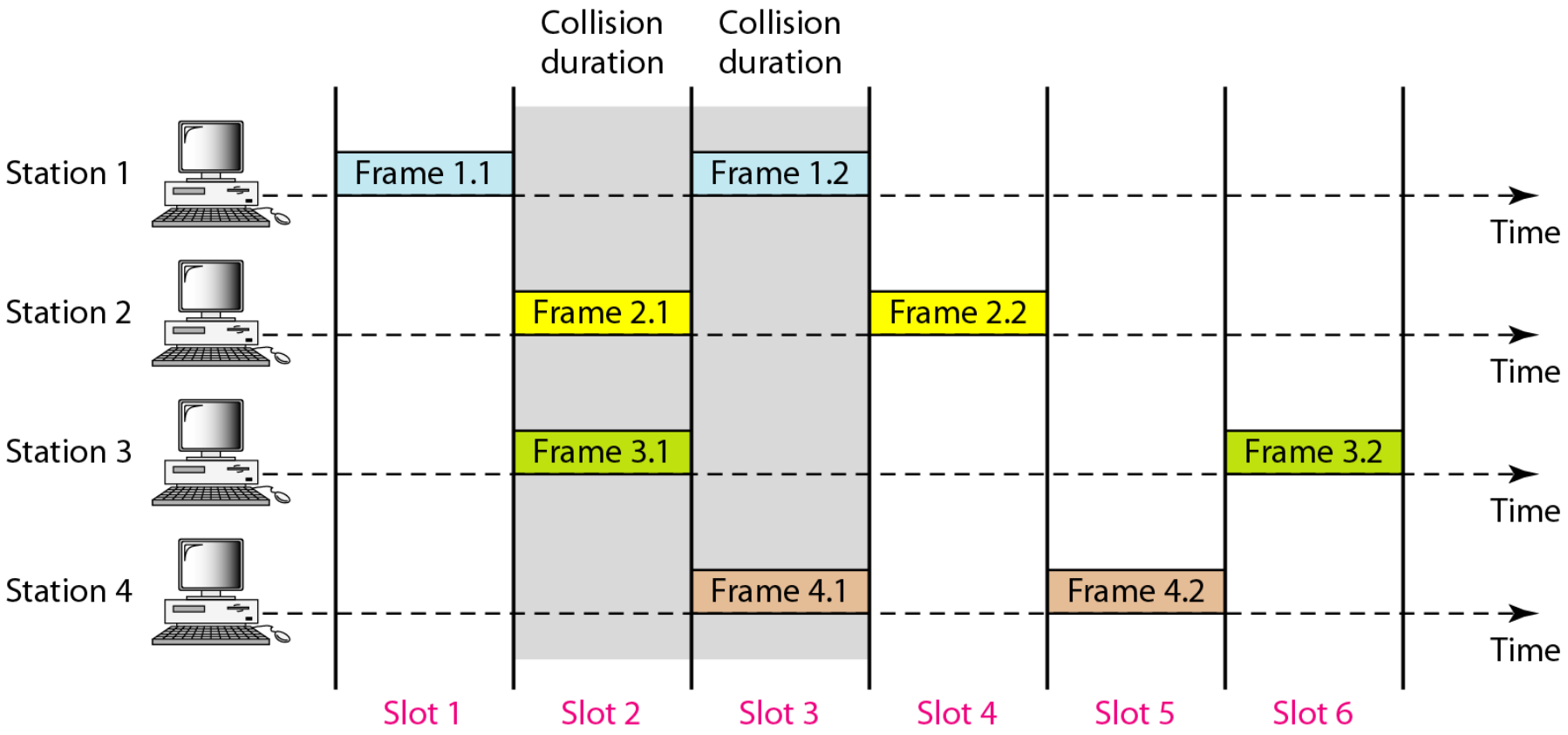
a. If the system creates 1000 frames per second, this is 1 frame per millisecond. The load is 1. In this case $S = G \times e^{-2G}$ or $S = 0.135$ (13.5 percent). This means that the throughput is $1000 \times 0.135 = 135$ frames. Only 135 frames out of 1000 will probably survive.

EXAMPLE 1.3

b. (1/2) frame per millisecond. The load is (1/2). In this case $S = G \times e^{-2G}$ or $S = 0.184$ (18.4 percent). This means that the throughput is $500 \times 0.184 = 92$ and that only 92 frames out of 500 will probably survive. Note that this is the maximum throughput case, percentagewise.

c. If the system creates 250 frames per second, this is (1/4) frame per millisecond. The load is (1/4). In this case $S = G \times e^{-2G}$ or $S = 0.152$ (15.2 percent). This means that the throughput is $250 \times 0.152 = 38$. Only 38 frames out of 250 will probably survive.

FRAMES IN A SLOTTED ALOHA NETWORK

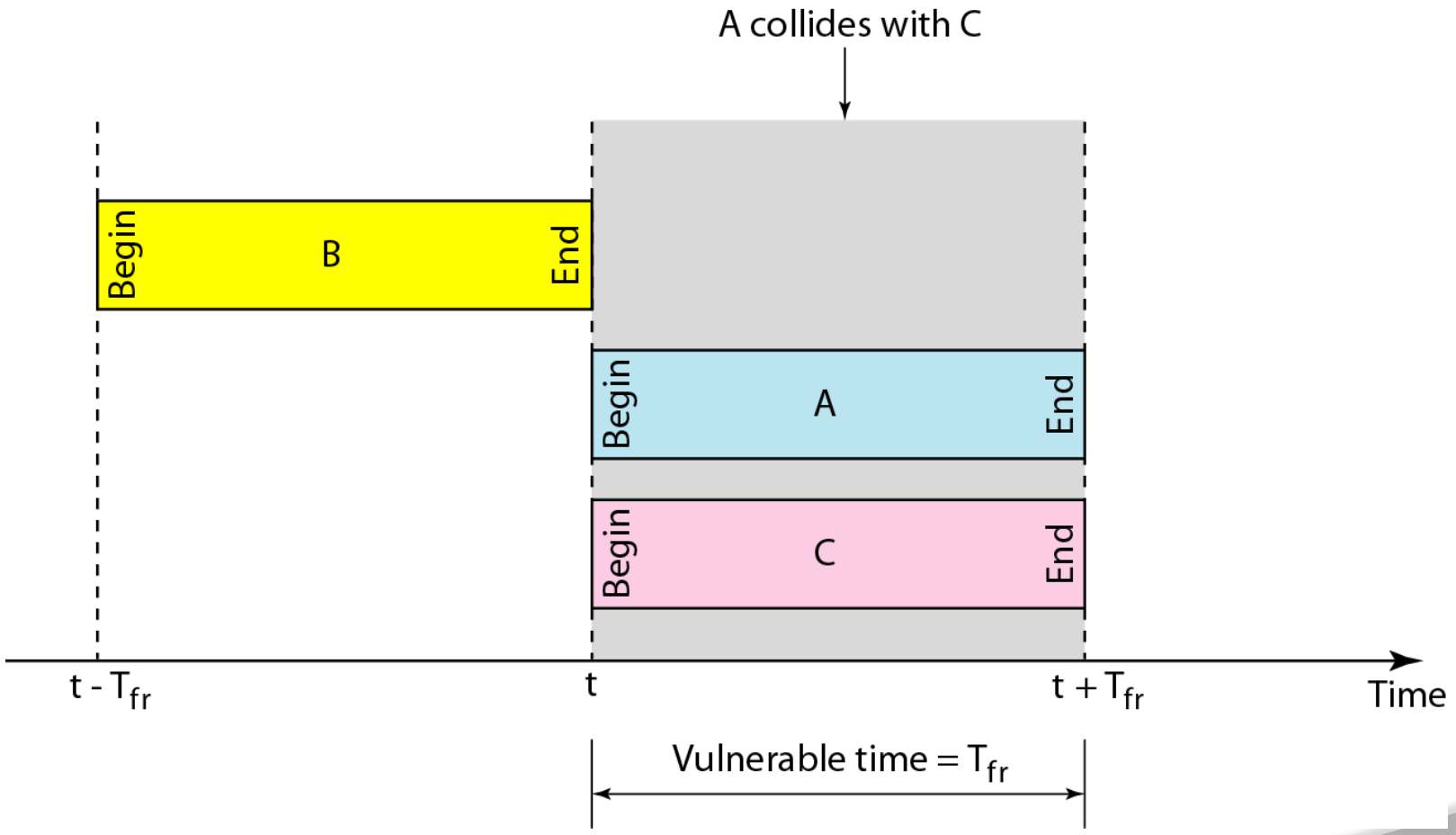


Note

The throughput for slotted ALOHA is $S = G \times e^{-G}$.

The maximum throughput $S_{max} = 0.368$ when $G = 1$.

VULNERABLE TIME FOR SLOTTED ALOHA PROTOCOL



EXAMPLE 1.4

A slotted ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces

a. 1000 frames per second b. 500 frames per second

c. 250 frames per second.

Solution

The frame transmission time is 200/200 kbps or 1 ms.

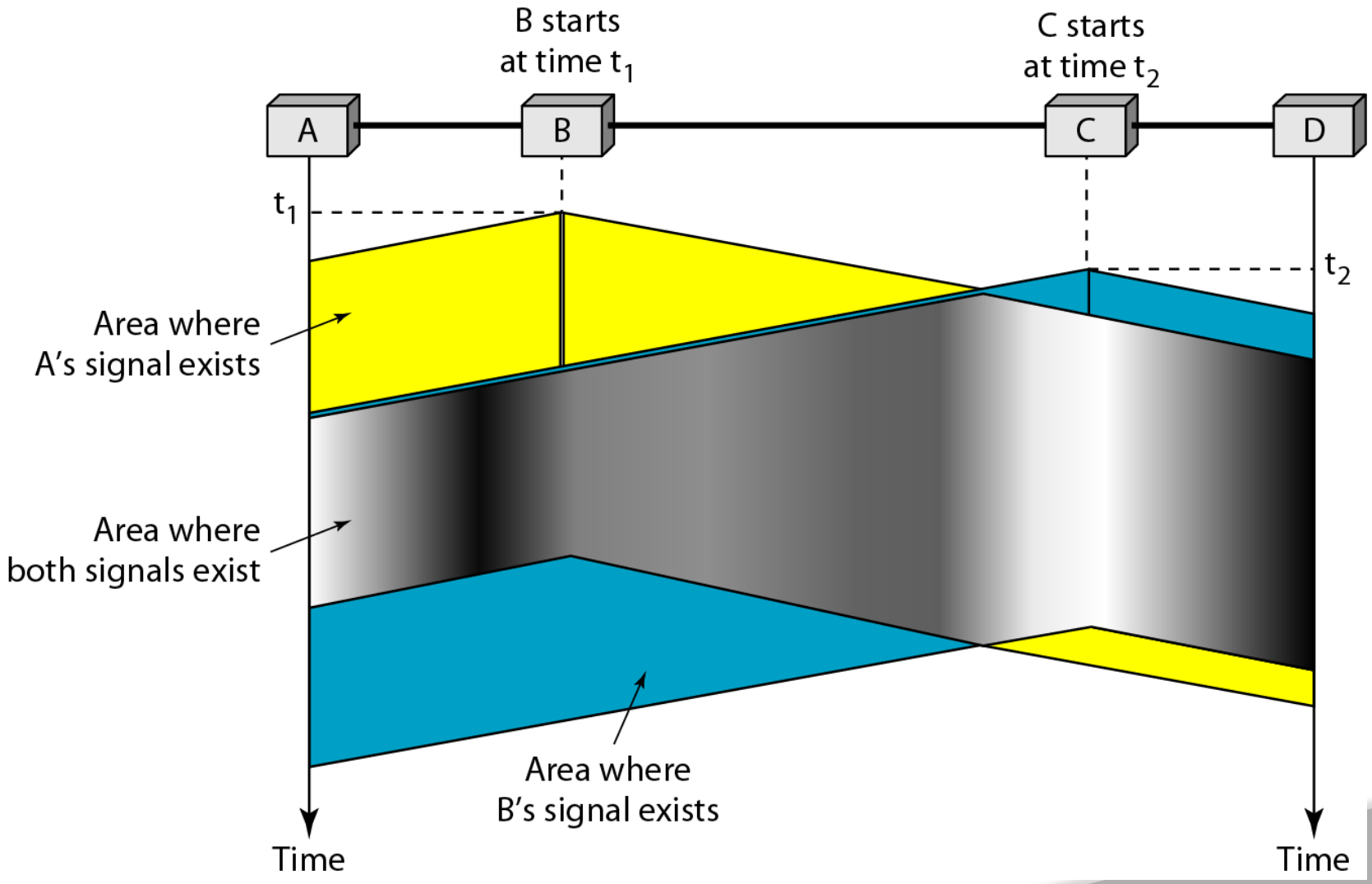
a. If the system creates 1000 frames per second, this is 1 frame per millisecond. The load is 1. In this case $S = G \times e^{-G}$ or $S = 0.368$ (36.8 percent). This means that the throughput is $1000 \times 0.0368 = 368$ frames. Only 386 frames out of 1000 will probably survive.

EXAMPLE 1.4 (CONTINUED)

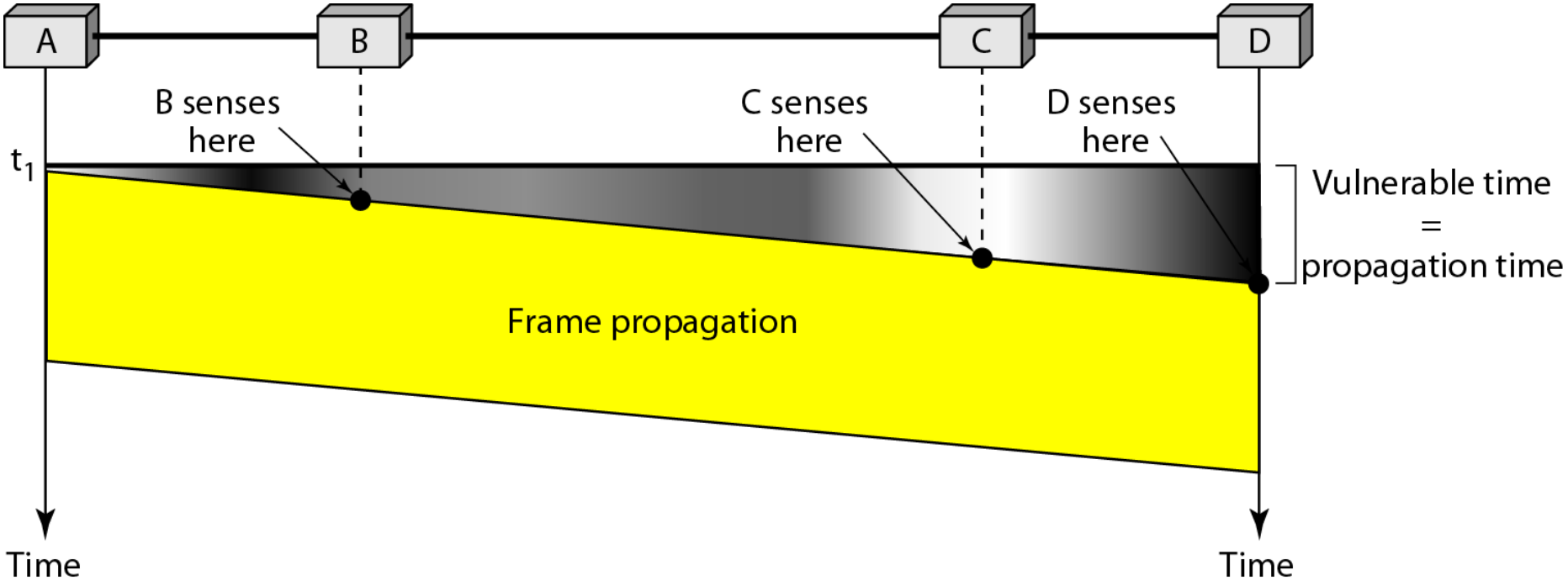
b. If the system creates 500 frames per second, this is (1/2) frame per millisecond. The load is (1/2). In this case $S = G \times e^{-G}$ or $S = 0.303$ (30.3 percent). This means that the throughput is $500 \times 0.0303 = 151$. Only 151 frames out of 500 will probably survive.

c. If the system creates 250 frames per second, this is (1/4) frame per millisecond. The load is (1/4). In this case $S = G \times e^{-G}$ or $S = 0.195$ (19.5 percent). This means that the throughput is $250 \times 0.195 = 49$. Only 49 frames out of 250 will probably survive.

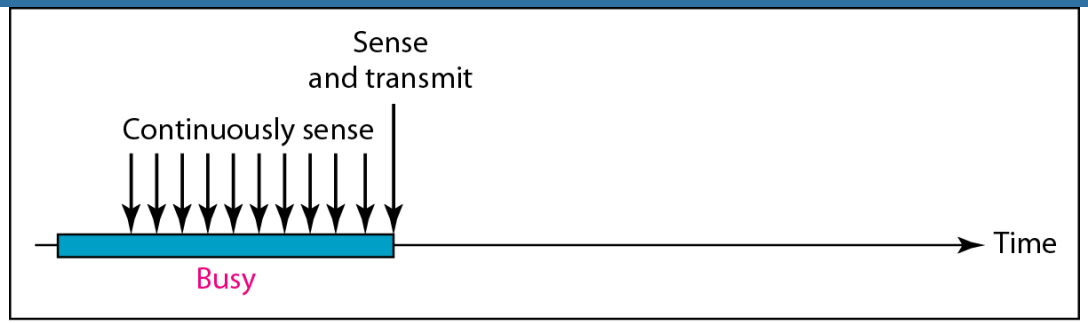
SPACE/TIME MODEL OF THE COLLISION IN CSMA



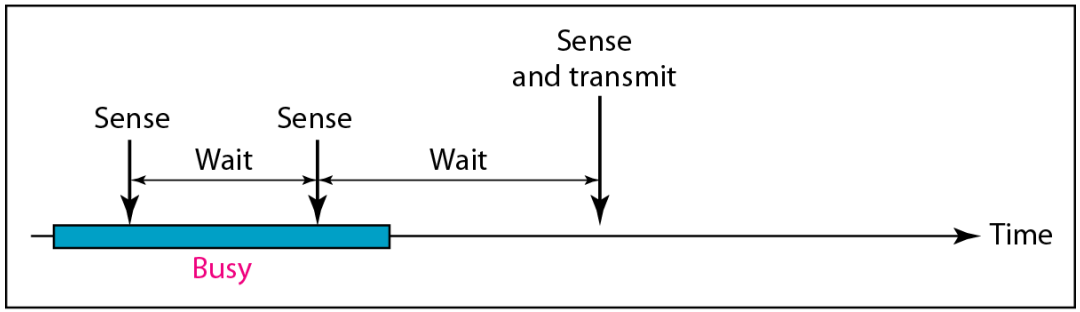
VULNERABLE TIME IN CSMA



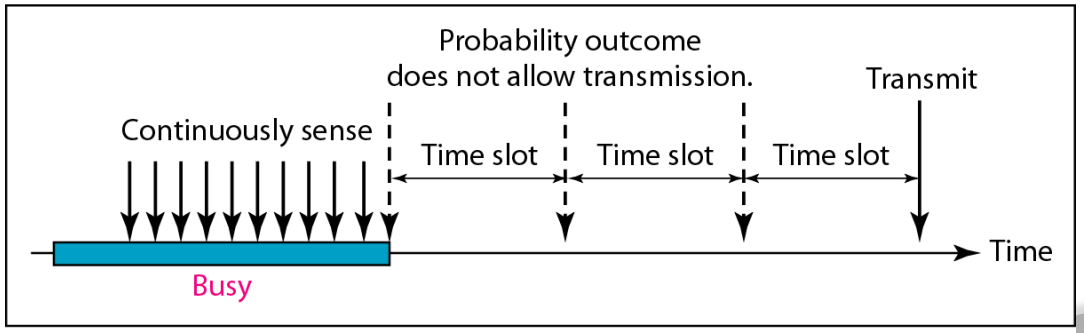
BEHAVIOR OF THREE PERSISTENCE METHODS



a. 1-persistent

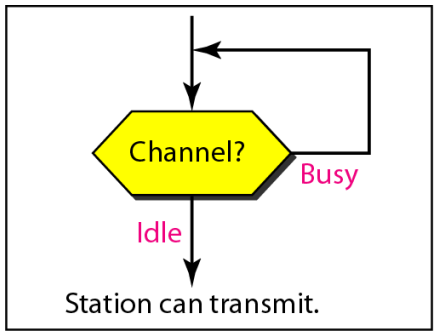


b. Nonpersistent

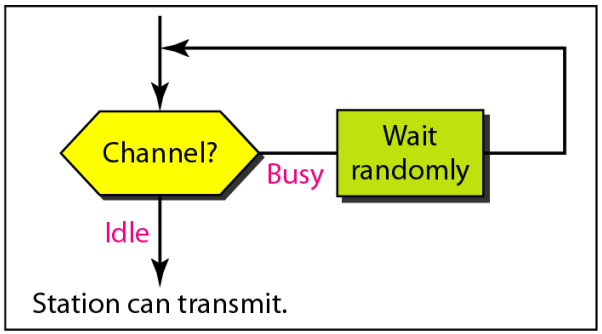


c. p-persistent

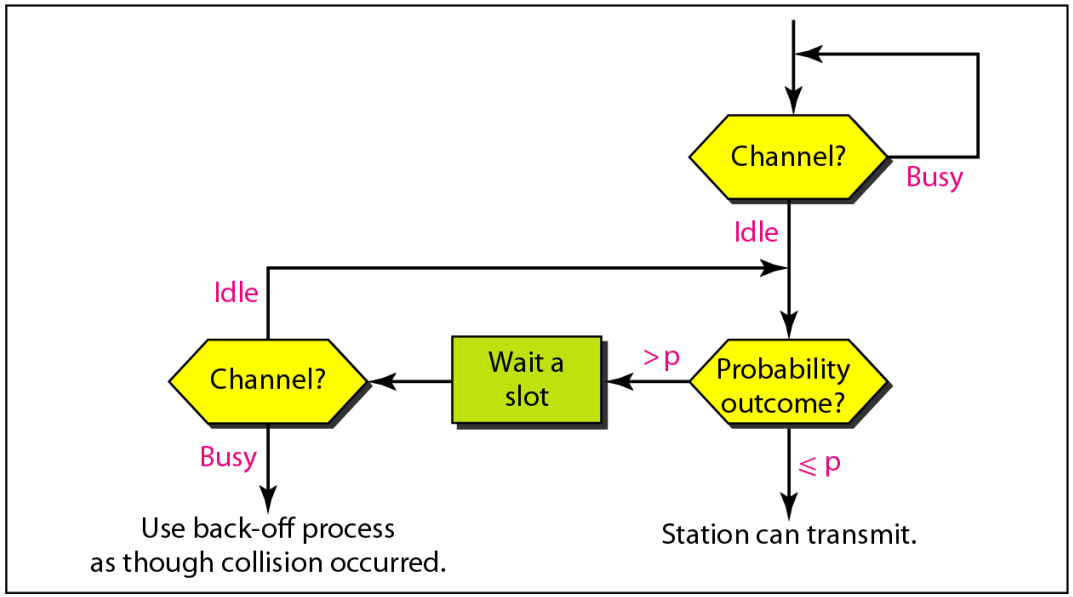
FLOW DIAGRAM FOR THREE PERSISTENCE METHODS



a. 1-persistent

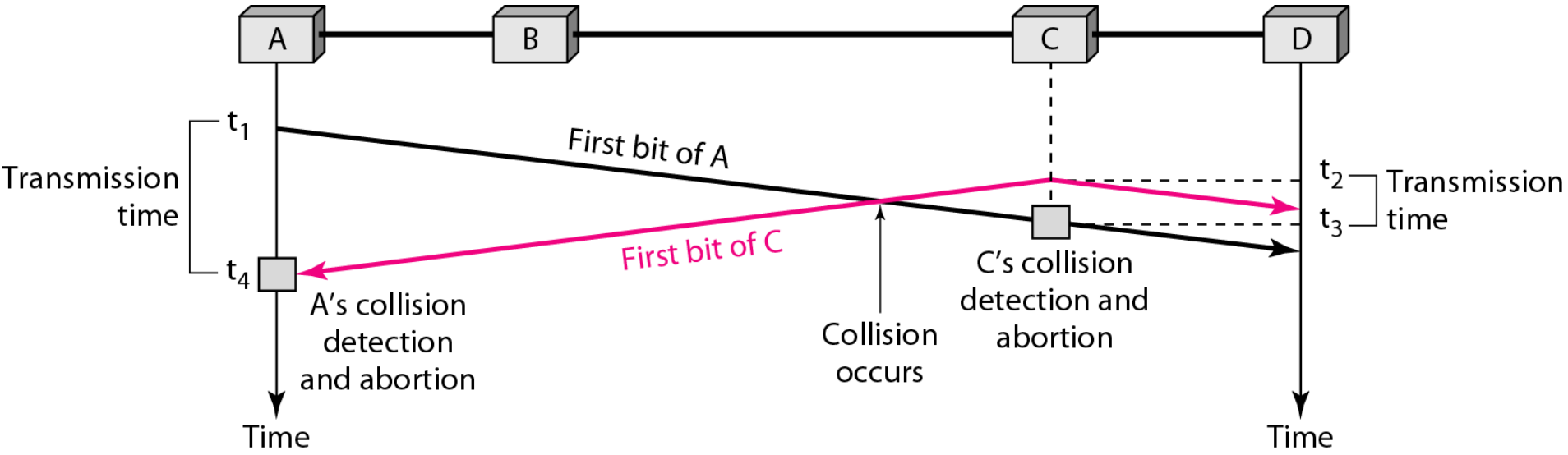


b. Nonpersistent

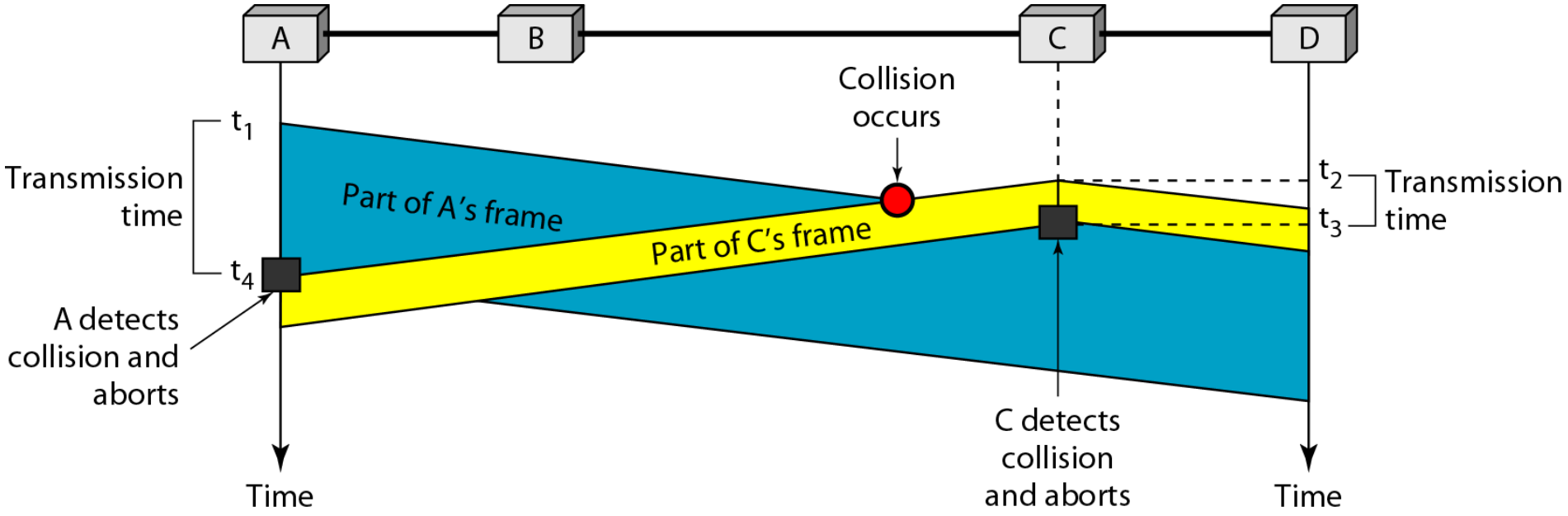


c. p-persistent

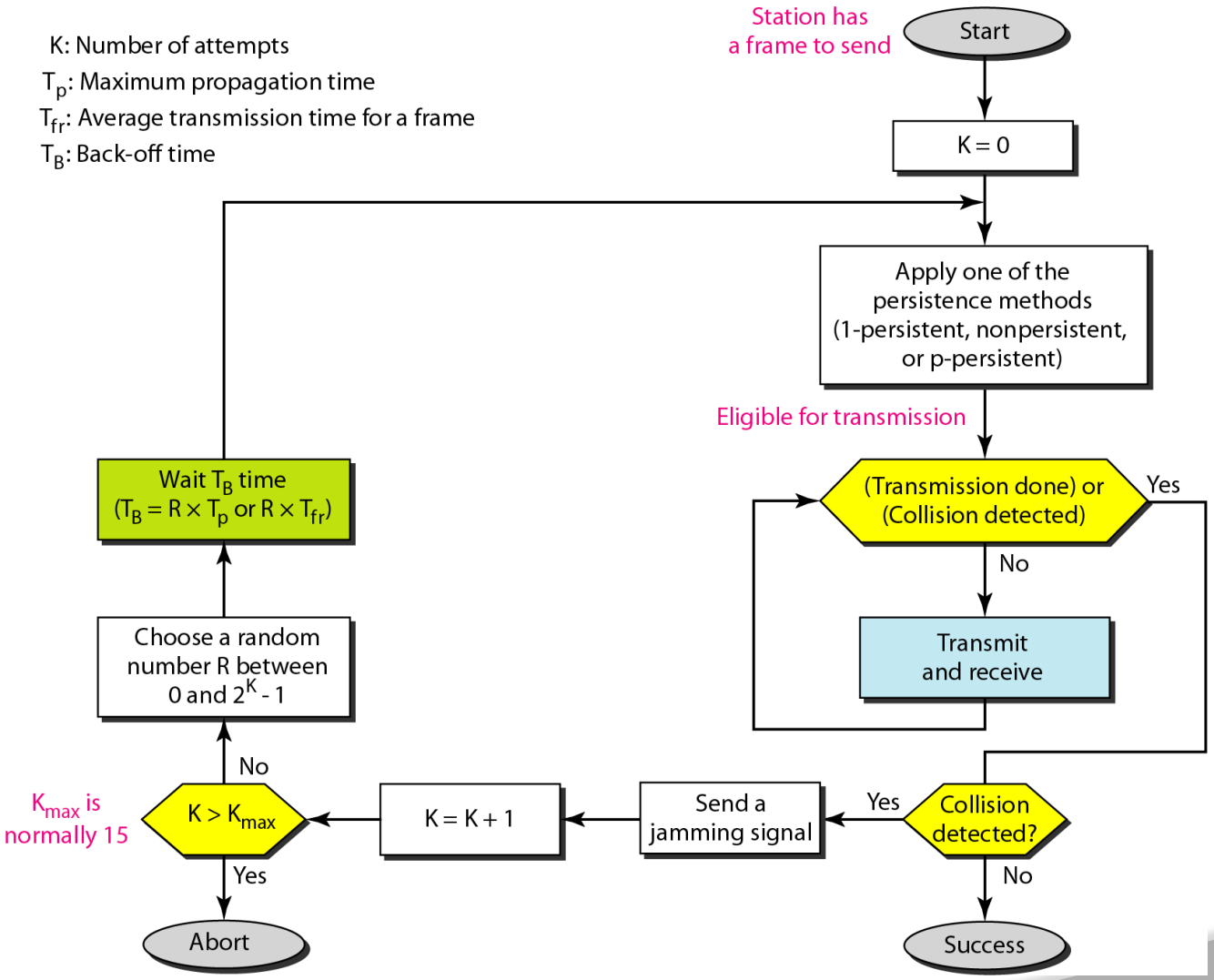
COLLISION OF THE FIRST BIT IN CSMA/CD



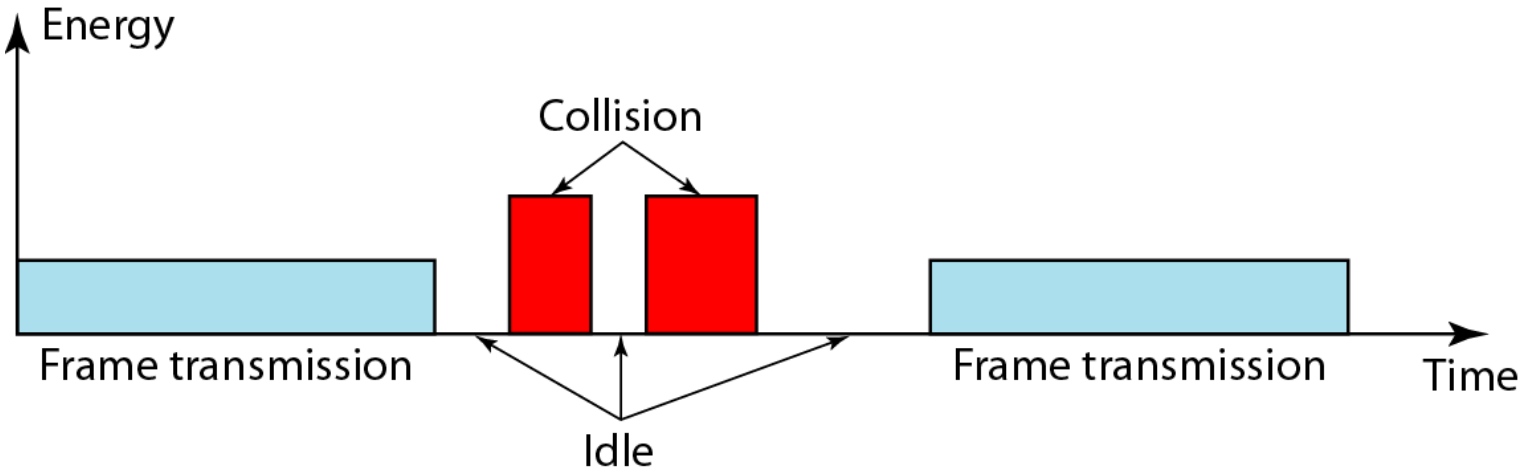
COLLISION AND ABORTION IN CSMA/CD



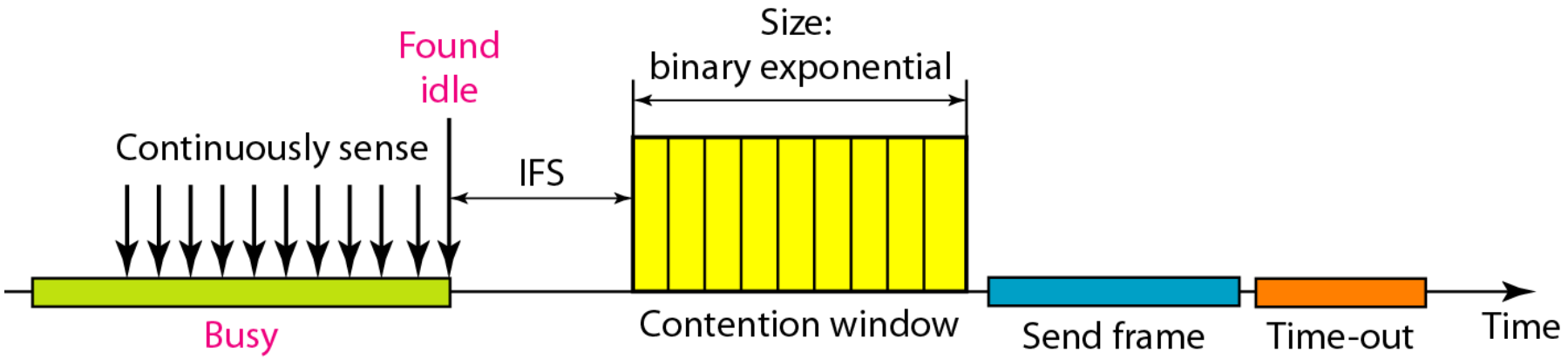
FLOW DIAGRAM FOR THE CSMA/CD



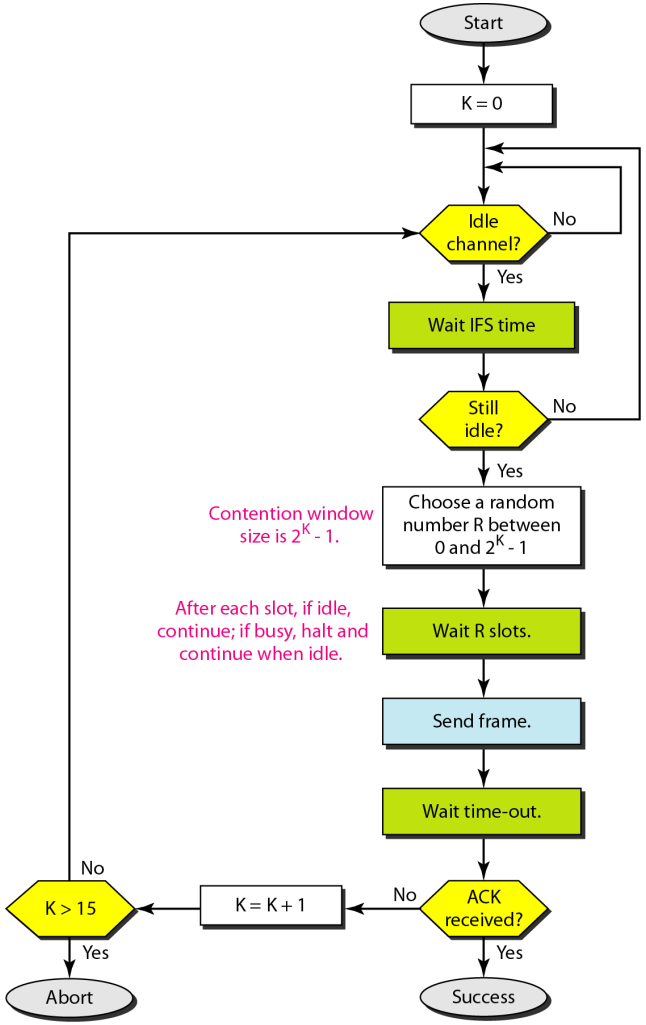
ENERGY LEVEL DURING TRANSMISSION, COLLISION



TIMING IN CSMA/CA



FLOW DIAGRAM FOR CSMA/CA



UNIT-2

WIRELESS LAN INTRODUCTION

- Wireless LAN stands for Wireless Local Area Network. It is also called LAWN (Local Area Wireless Network). WLAN is one in which a mobile user can connect to a Local Area Network (LAN) through a wireless connection.
- The IEEE 802.11 group of standards defines the technologies for wireless LANs. For path sharing, 802.11 standard uses the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance). It also uses an encryption method i.e. wired equivalent privacy algorithm.
- Wireless LANs provide high speed data communication in small areas such as building or an office. WLANs allow users to move around in a confined area while they are still connected to the network.
- In some instance wireless LAN technology is used to save costs and avoid laying cable, while in other cases, it is the only option for providing high-speed internet access to the public. Whatever the reason, wireless solutions are popping up everywhere.

WIRELESS LANS - IMPORTANCE

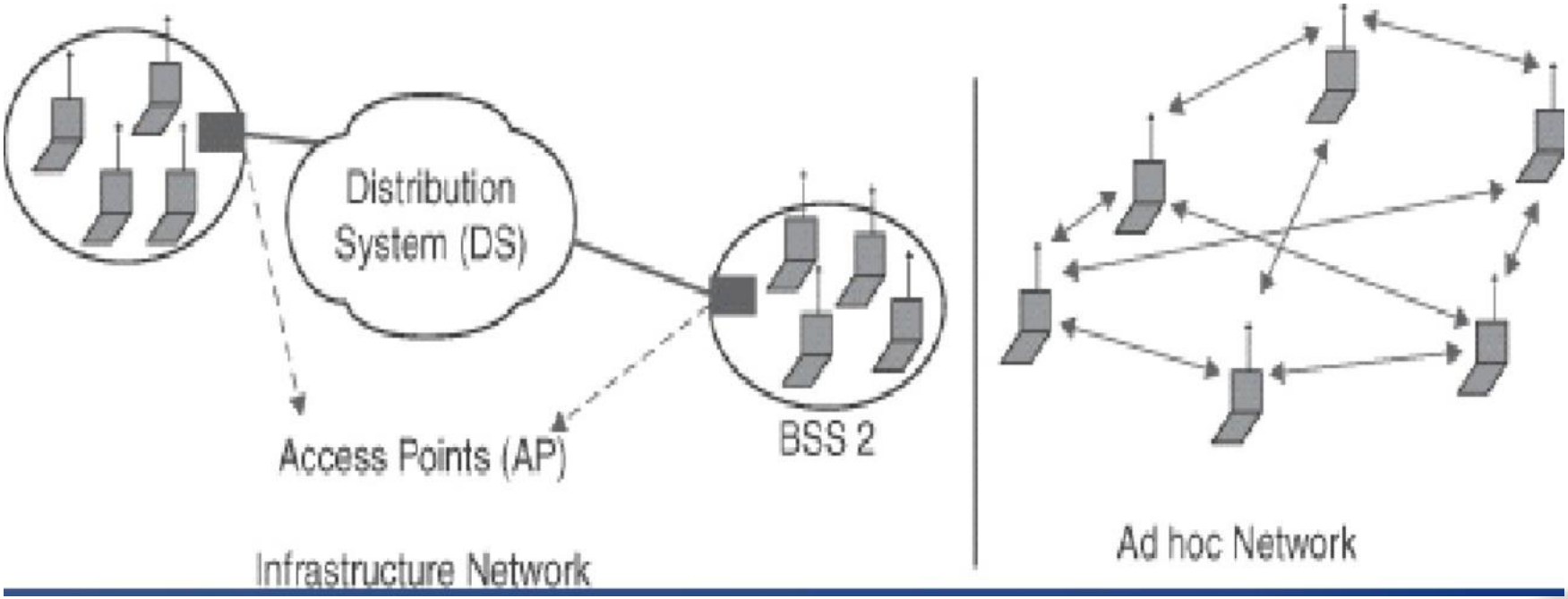
- Flexibility: Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.)
- Planning: Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.
- Design: Wireless networks allow for the design of independent, small devices which can for example be put into a pocket. Cables not only restrict users but also designers of small notepads, PDAs, etc.
- Robustness: Wireless networks can handle disasters, e.g., earthquakes, flood etc. whereas, networks requiring a wired infrastructure will usually break down completely in disasters.
- Ease of Use: Wireless LAN is easy to use and the users need very little new information to take advantage of WLANs.

WIRELESS LANS - IMPORTANCE

- Cost: The cost of installing and maintaining a wireless LAN is on average lower than the cost of installing and maintaining a traditional wired LAN, for two reasons.
- First, after providing wireless access to the wireless network via an access point for the first user, adding additional users to a network will not increase the cost.
- second, wireless LAN eliminates the direct costs of cabling and the labor associated with installing and repairing it.

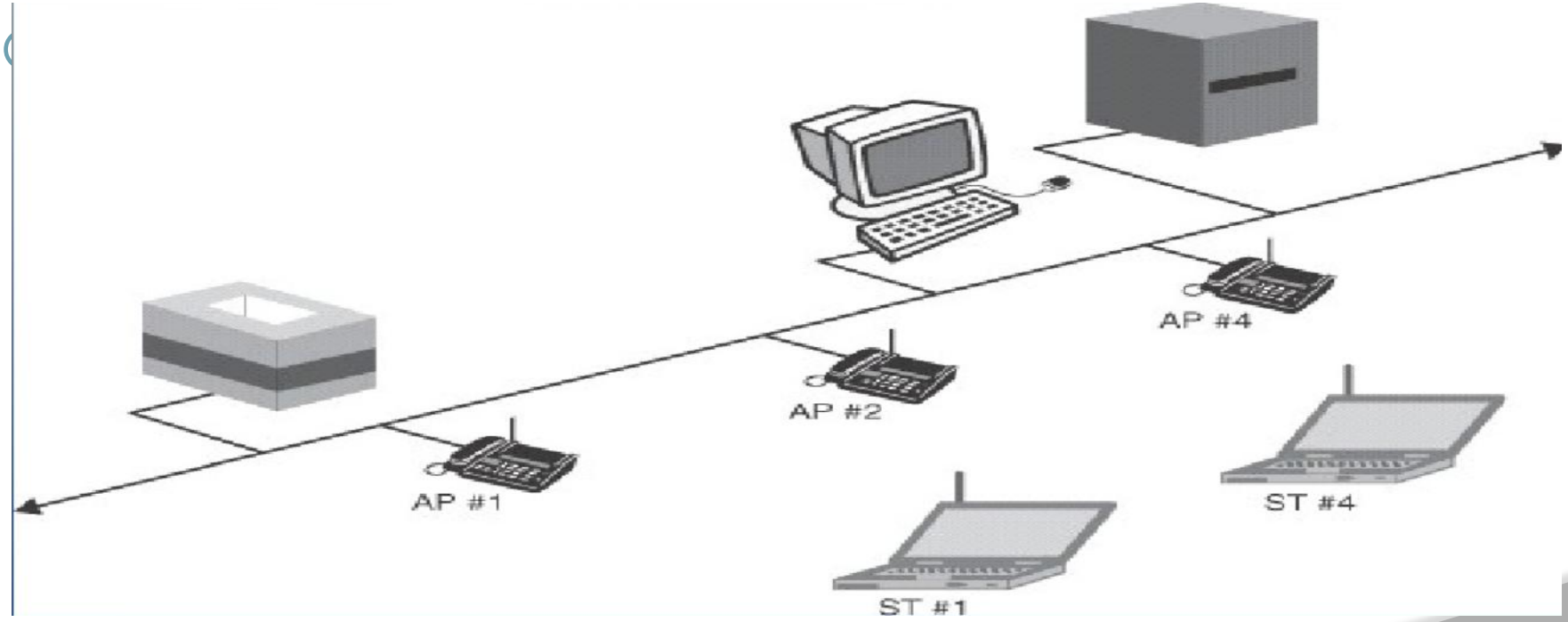
WLAN TOPOLOGIES - PEER-TO-PEER (ADHOC) TOPOLOGY

Peer-to-peer (adhoc) topology in which client devices in the same cell communicate with each other directly.



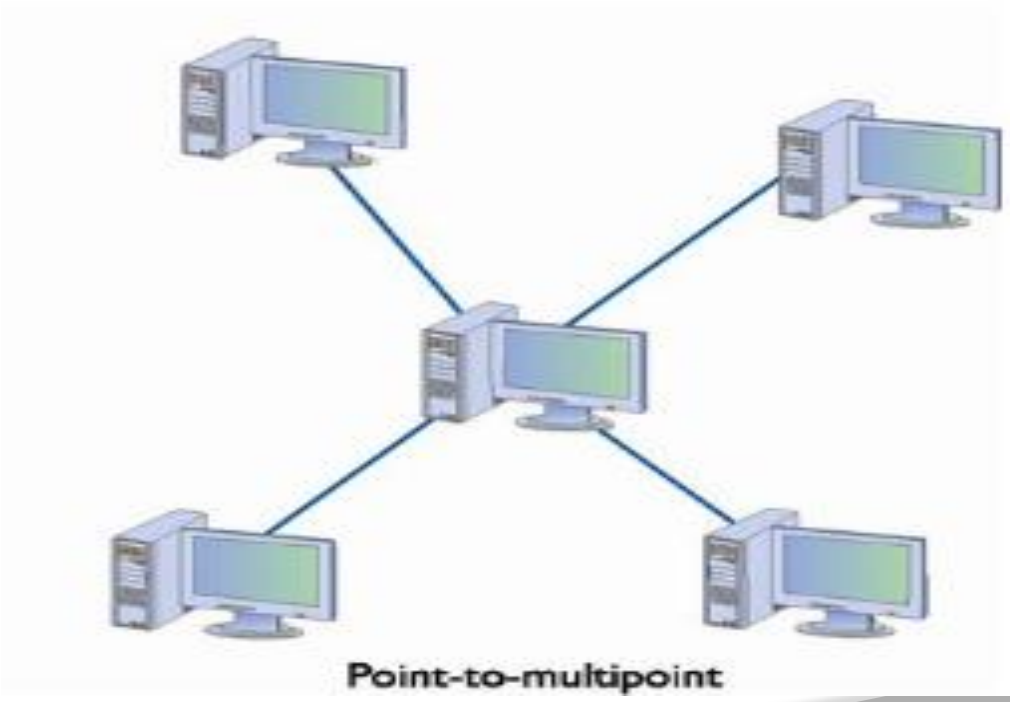
ACCESS POINT BASED TOPOLOGY

- Access point based topology uses access points to bridge traffic onto a wired (Ethernet/Token ring) or wireless backbone.



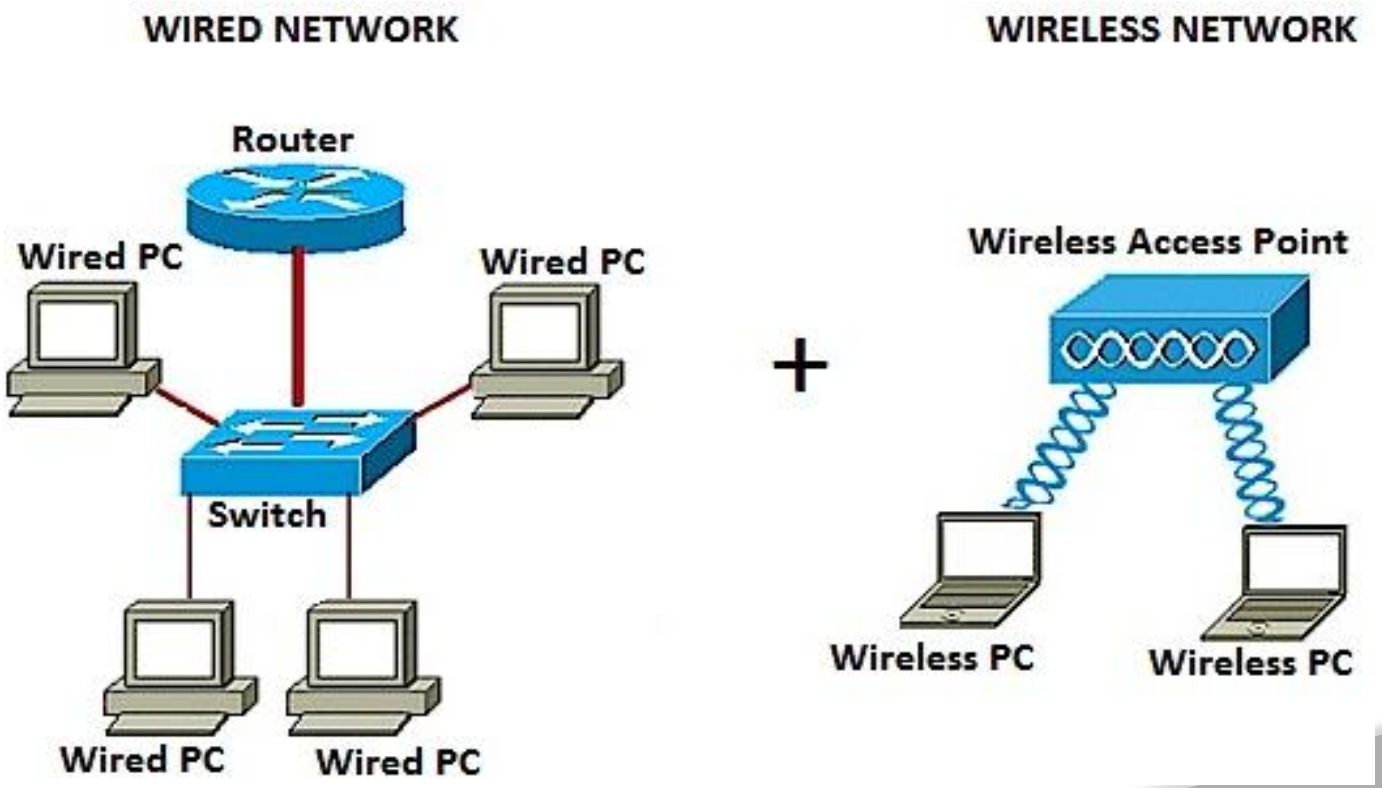
POINT-TO-MULTIPOINT TOPOLOGY

- Point-to-multipoint topology in which wireless bridges connect LANs in one building to LANs in another building even if the buildings are miles apart



TRANSMISSION TECHNIQUES:

- Wired Networks
- Wireless Networks

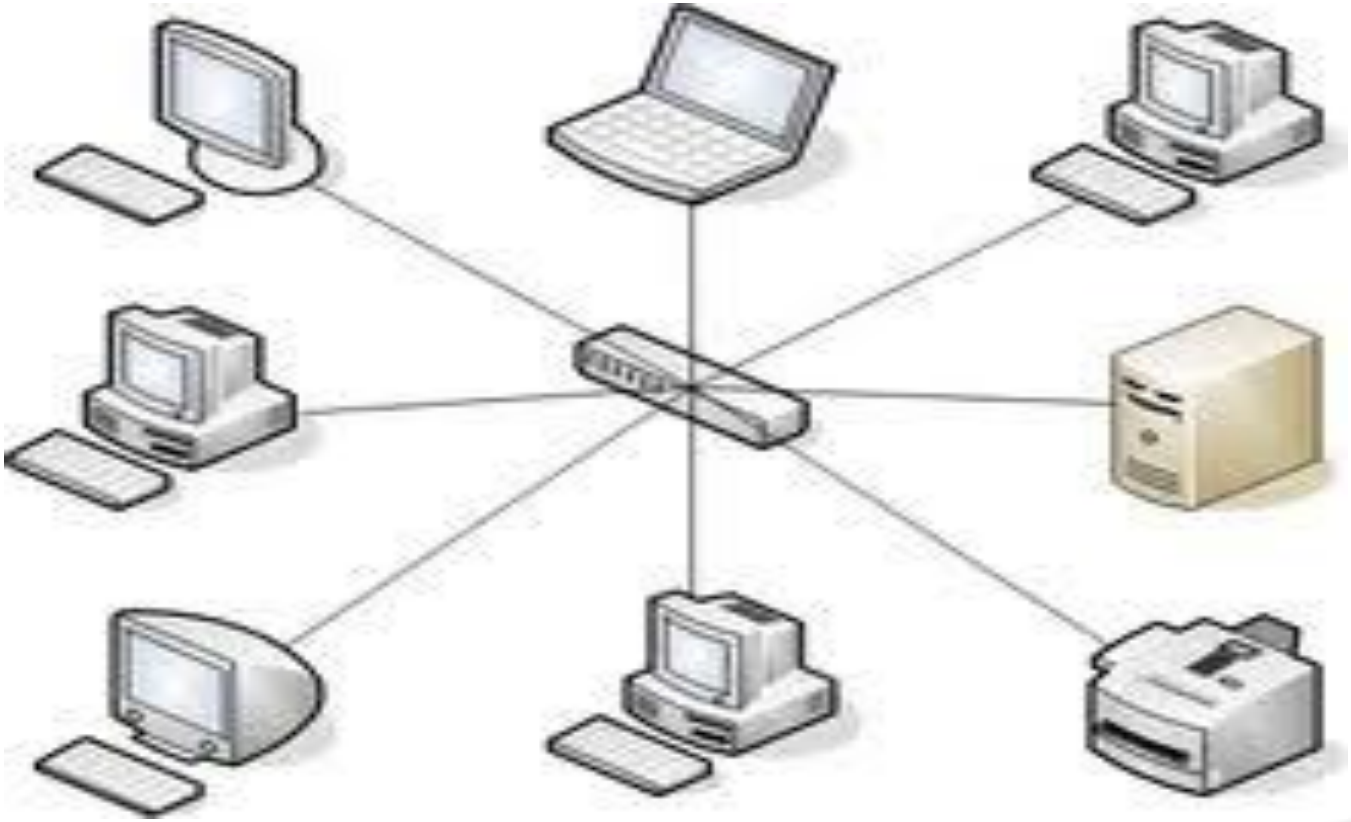


WIRED NETWORKS

- Wired networks, also called Ethernet networks, are the most common type of local area network (LAN) technology. A wired network is simply a collection of two or more computers, printers, and other devices linked by Ethernet cables. Ethernet is the fastest wired network protocol, with connection speeds of 10 megabits per second (Mbps) to 100 Mbps or higher.
- Wired networks can also be used as part of other wired and wireless networks. To connect a computer to a network with an Ethernet cable, the computer must have an Ethernet adapter (sometimes called a network interface card, or NIC). Ethernet adapters can be internal (installed in a computer) or external (housed in a separate case). Some computers include a built-in Ethernet adapter port, which eliminates the need for a separate adapter (Microsoft). There are three basic network topologies that are most commonly used today

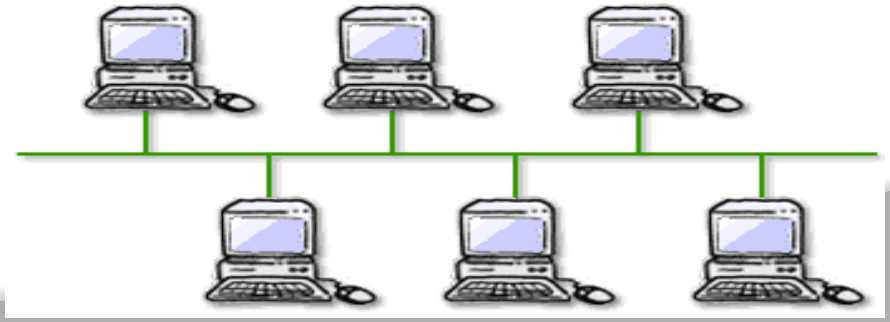
Wired Networks - Star network

- The star network, a general more simplistic type of topology, has one central hub that connects to three or more computers and the ability to network printers.
- This type can be used for small businesses and even home networks. The star network is very useful for applications where some processing must be centralized and some must be performed locally.
- The major disadvantage is the star network is its vulnerability. All data must pass through one central host computer and if that host fails the entire network will fail.



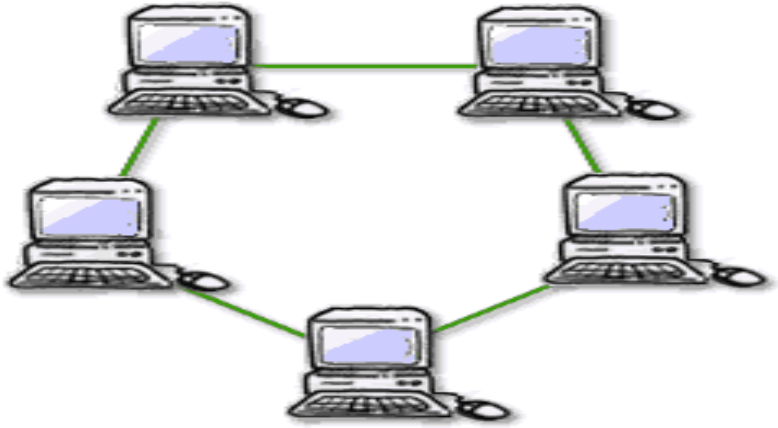
BUS NETWORK

- Bus network has no central computer and all computers are linked on a single circuit. This type broadcasts signals in all directions and it uses special software to identify which computer gets what signal.
- One disadvantage with this type of network is that only one signal can be sent at one time, if two signals are sent at the same time they will collide and the signal will fail to reach its destination.
- One advantage is that there is no central computer so if one computer goes down others will not be affected and will be able to send messages to one another.



Ring Network

- Similar to the bus network, the ring network does not rely on a central host computer either. Each computer in the network can communicate directly with any other computer, and each processes its own applications independently. A ring network forms a closed loop and data is sent in one direction only and if a computer in the network fails the data is still able to be transmitted.



WIRED NETWORK -OVERVIEW

- Typically the range of a wired network is within a 2,000-foot-radius. The disadvantage of this is that data transmission over this distance may be slow or nonexistent. The benefit of a wired network is that bandwidth is very high and that interference is very limited through direct connections.
- Wired networks are more secure and can be used in many situations; corporate LANs, school networks and hospitals. The biggest drawback to this type of network is that it must be rewired every time it is moved.

WIRELESS NETWORKS

- A wireless network, which uses high-frequency radio waves rather than wires to communicate between nodes, is another option for home or business networking. Individuals and organizations can use this option to expand their existing wired network or to go completely wireless.
- Wireless allows for devices to be shared without networking cable which increases mobility but decreases range.
- There are two main types of wireless networking i.e peer to peer or ad-hoc and infrastructure. (Wi-fi.com)

WIRELESS NETWORKS

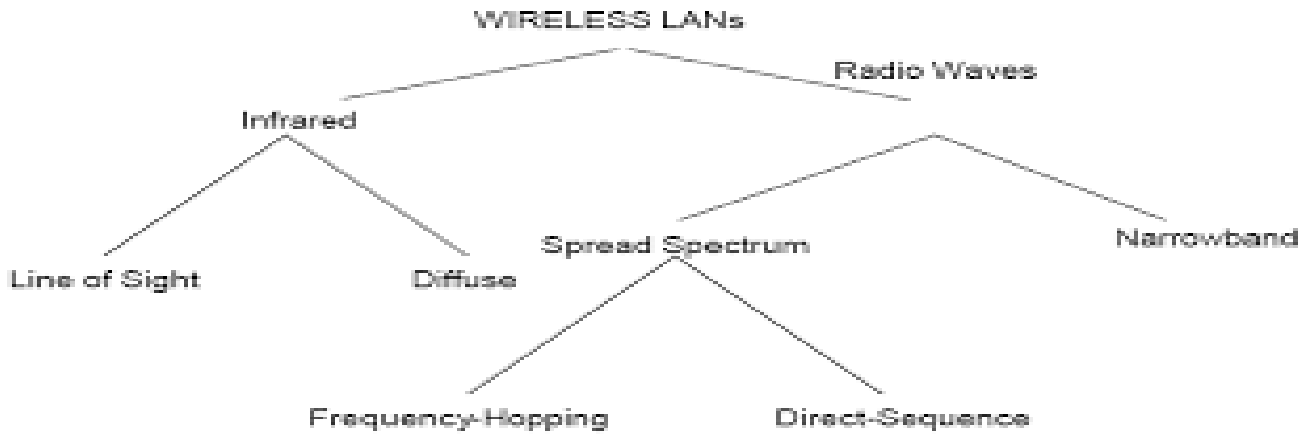
- An ad-hoc or peer-to-peer wireless network consists of a number of computers each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software.
- An infrastructure wireless network consists of an access point or a base station. In this type of network the access point acts like a hub, providing connectivity for the wireless computers. It can connect or bridge the wireless LAN to a wired LAN, allowing wireless computer access to LAN resources, such as file servers or existing Internet Connectivity

WIRELESS NETWORKS

- There are four basic types of transmissions standards for wireless networking. These types are produced by the Institute of Electrical and Electronic Engineers (IEEE). These standards define all aspects of radio frequency wireless networking. They have established four transmission standards; 802.11, 802.11a, 802.11b, 802.11g.
- The basic differences between these four types are connection speed and radio frequency. 802.11 and 802.11b are the slowest at 1 or 2 Mbps and 5.5 and 11Mbps respectively. They both operate off of the 2.4 GHz radio frequency. 802.11a operates off of a 5 GHz frequency and can transmit up to 54 Mbps and the 802.11g operates off of the 2.4 GHz frequency and can transmit up to 54 Mbps.

WLAN TECHNOLOGIES

- WLANs include the following technologies:
- Infrared
- UHF (narrowband)
- Spread spectrum
- Each implementation comes with its own advantages and disadvantages.



INFRARED TECHNOLOGY

- Infrared is an invisible band of radiation that exists at the lower end of the visible electromagnetic spectrum. This type of transmission is most effective when a clear line exists between the sender and receiver. Two type of infrared solutions are available:
- **Diffused beam** uses reflected rays to transmit/receive a data signal. Data rate for it is lower data rates in the 1-2 Mbps range.
- **Direct beam** which is more directional therefore it is more faster than diffused beam.

UHF NARROWBAND TECHNOLOGY

- UHF which has been around since the early 1980s normally transmit in the 430 to 470 MHz frequency range with systems who rarely use the 800 MHz range. The lower portion of this band (430-450 MHz) is called the unprotected or unlicensed band and the 450-470 MHz is referred to the protected or licensed band. In the unprotected band RF licenses are not granted for a specific frequencies and anyone is allowed to use any frequencies. The term narrowband is used to described this technology because the RF signal is sent in a very narrow bandwidth, typically 12.5 kHz or 25 Khz and power levels range from 1-2 watts in narrowband RF systems.

SPREAD SPECTRUM TECHNOLOGY

- Many WLANs use Spread Spectrum technology which is a wideband radio frequency technique that uses the entire allotted spectrum in a shared fashion. It spreads the transmission power over the entire usable spectrum. Spread Spectrum technology makes eavesdropping and jamming inherently difficult. Two modulation schemes are used in Spread Spectrum technology:
- **Direct sequence spread spectrum** (DSSS) generates a redundant bit pattern for each bit to be transmitted and the pattern is known as a spreading code. The longer the spreading code the greater the probability the data can be recovered.
- **Frequency Hopping spread spectrum** which uses a narrowband carrier that changes frequency in a pattern known to the sender and receiver. When properly synchronized the net effect is to maintain a single logical channel.

UNIT-3

WIRELESS LAN -802.11

Availability of low cost portable equipments are driving feature.

Advantage:

Mobility.

Installation speed and simplicity .

Installation flexibility.

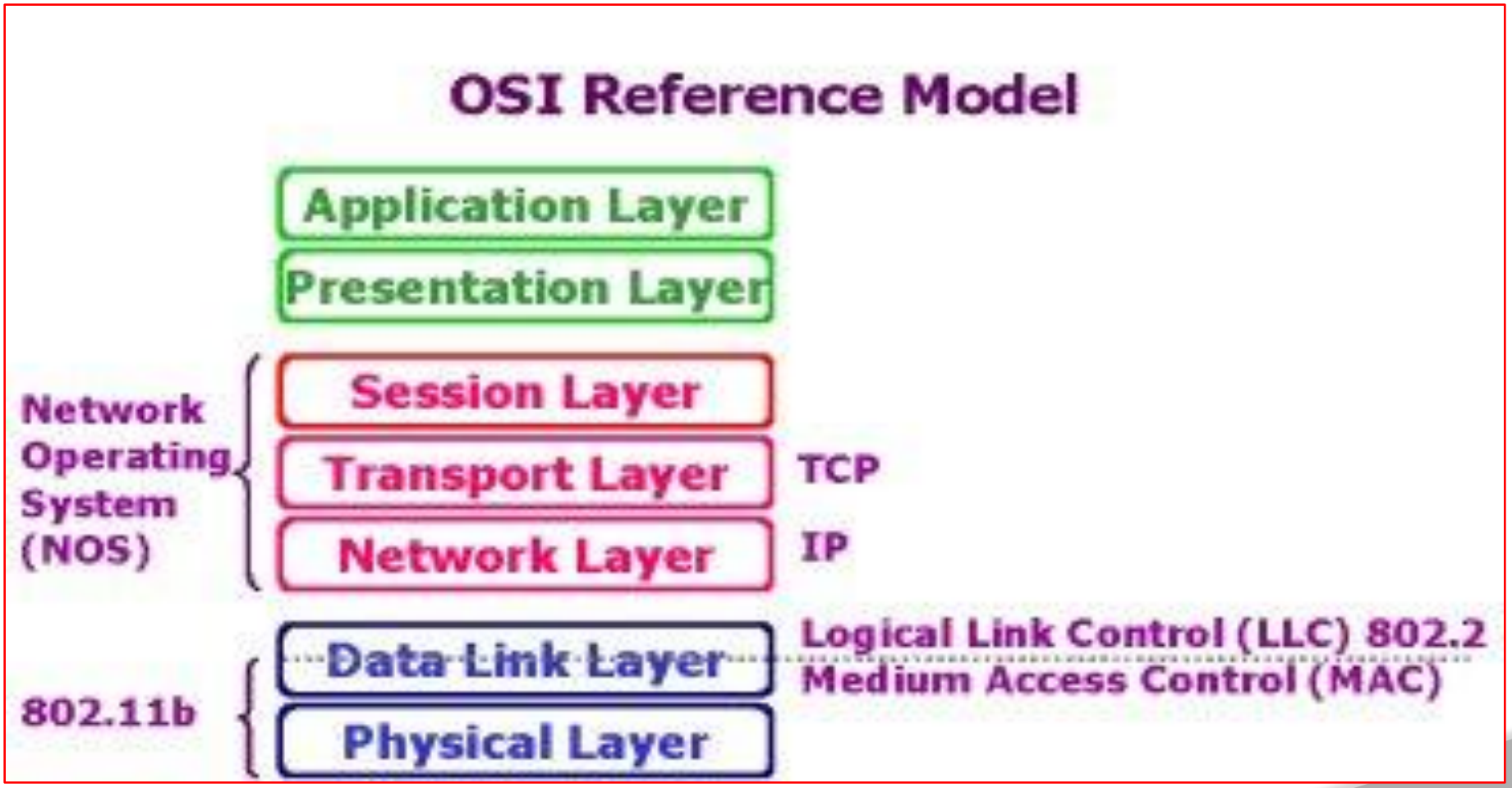
Reduced cost of ownership .

Scalability.

LIMITATION & CHALLENGES IN 802.11

- Lower reliability due to susceptibility of radio transmission to noise and interference.
- Fluctuation of the strength of the received signal through multiple paths causing fading.
- Vulnerable to eavesdropping leading to security problem.
- Limited data rate because of the use of spread spectrum transmission techniques enforced to ISM band users.

IEEE 802.11 IN OSI MODEL



COMPONENT IEEE 802.11 TECHNOLOGY

1-Transmission Medium.

2-Topolgy

3-Medium Access Control

TRANSMISSION MEDIUM

Three different Physical media:

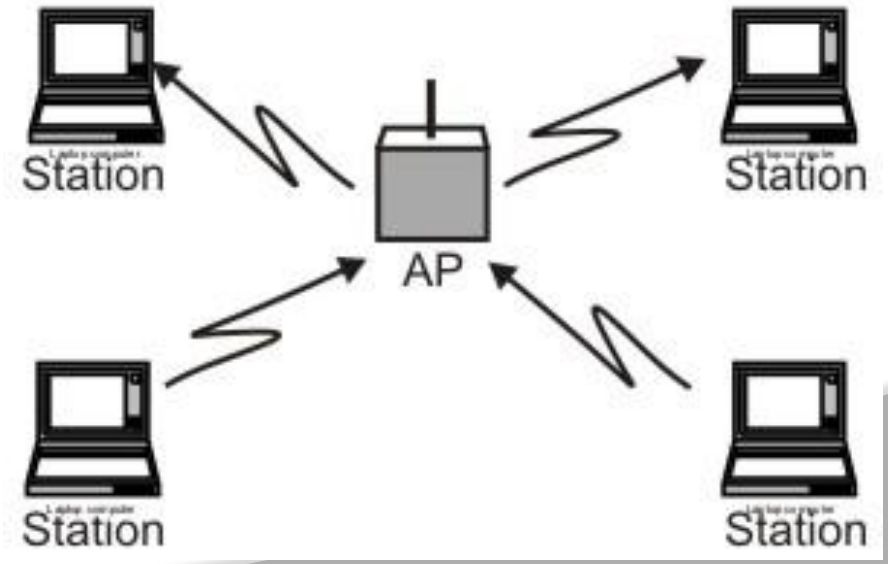
Spread Spectrum radio in 2.4 GHz ISM Band (2400 to 2483.5 MHz).

- **Frequency Hop (FH):** The 802.11 frequency hopping physical layer uses 79 non overlapping 1 MHz channels to transmit 1Mbps data signal.
- **Direct Sequence Spread Spectrum (DSSS):** The IEE 802.11 uses simple 11-Chip Barker sequence B11 [-1, +1, -1, -1, +1, -1, -1, -1, +1, +1, +1] with QPSK or BPSK modulation .
- **Infrared Signal** in the near visible range of 850 to 950 nanometers.

TOPOLOGY

- The 802.11 standard supports the formation of two different type of BSSs.
- The first type of BSS is known as Adhoc network, without access point.
- The second type of BSS is known as Infrastructure BSS , With An Access Point.

Adhoc Network

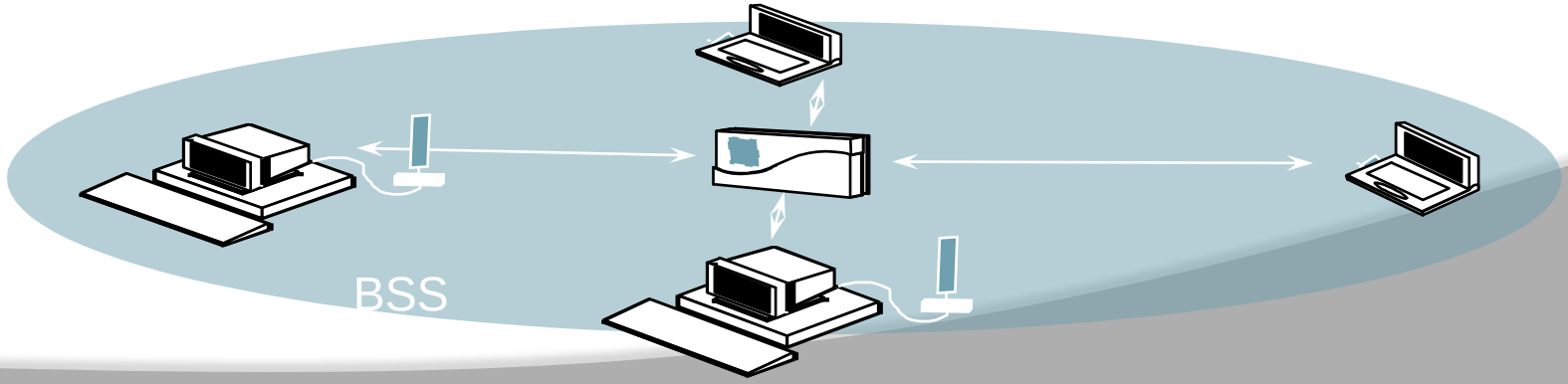


Infrastructure Type BSS

IEEE 802 .11 TERMINOLOGY

Basic Service Set (BSS):

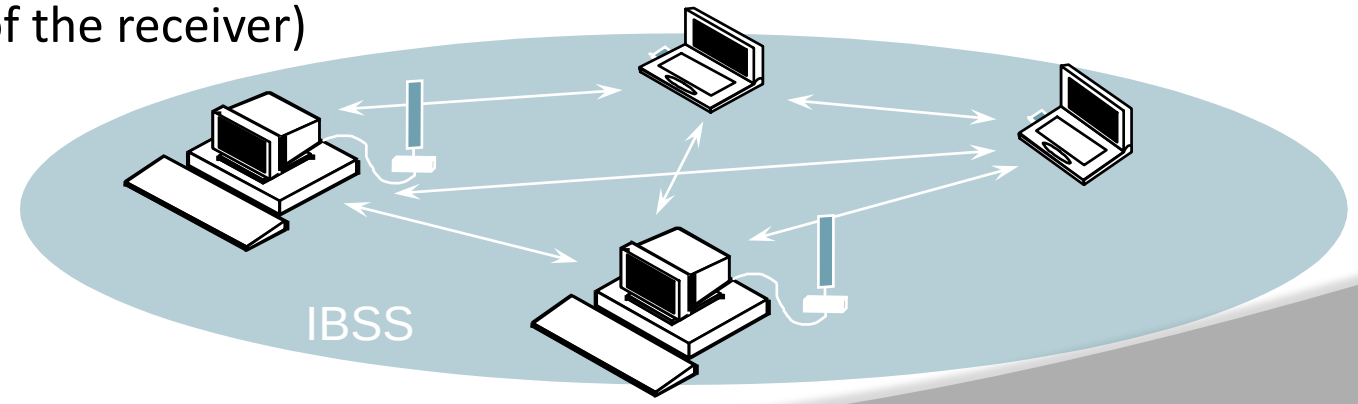
- A set of stations controlled by a single "Coordination Function" (=the logical function that determines when a station can transmit or receive).
- Similar to a "cell" in Cellular network terminology.
- A BSS can have an Access-Point (both in standalone networks and in building-wide configurations), or can run without and Access-Point (in standalone networks only).
- Station-to-Station traffic is relayed by the Access Point.



IEEE 802 .11 TERMINOLOGY

Independent Basic Service Set (IBSS):

- A Basic Service Set (BSS) which forms a self-contained network in which no access to a Distribution System is available.
- A BSS **without** an Access-Point.
- Station-to-station traffic flows directly without any relay action
- All stations in the cell will be able to receive frames transmitted by another station in the cell (filtering of traffic for subsequent processing is based on MAC address of the receiver)



IEEE 802 .11 TERMINOLOGY

Extended Service Set (ESS):

A set of one or more Basic Service Sets interconnected by a Distribution System (DS).

Traffic always flows via Access-Point.

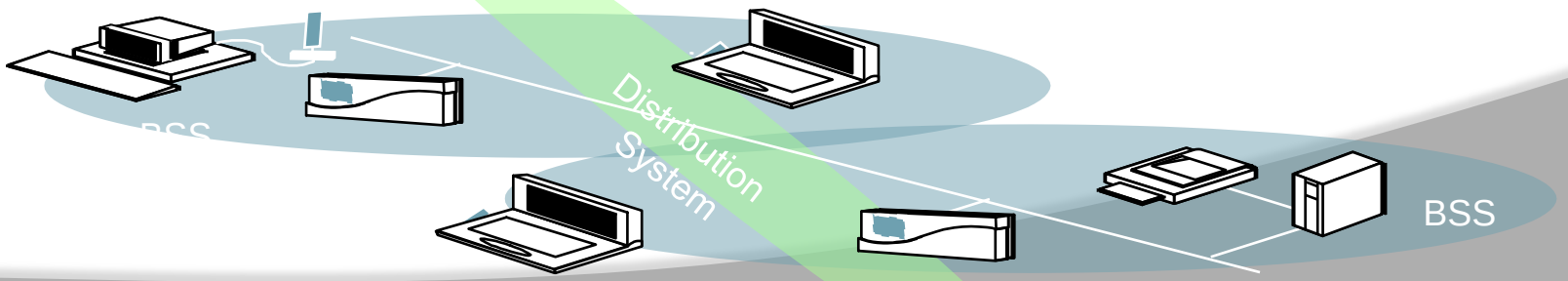
Distribution System (DS):

A system to interconnect a set of Basic Service Sets.

Integrated; A single Access-Point in a standalone network.

Wired; Using cable to interconnect the Access-Points.

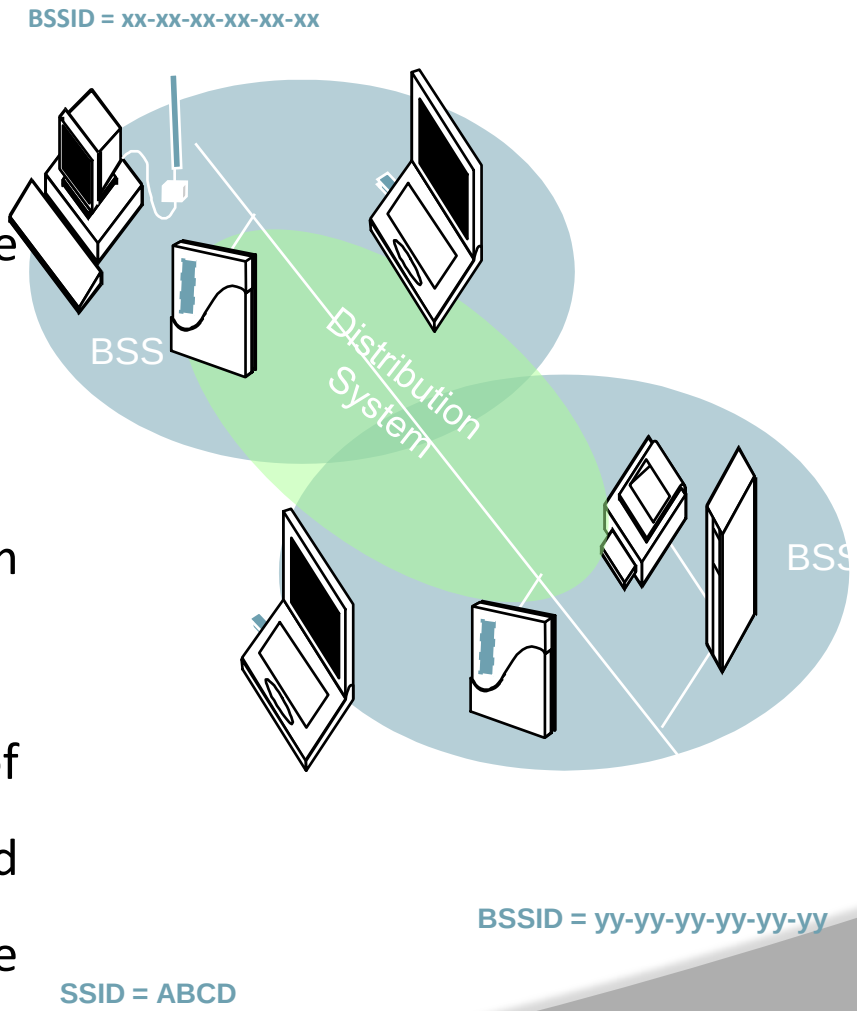
Wireless; Using wireless to interconnect the Access-Points.



IEEE 802 .11 TERMINOLOGY

Service Set Identifier (SSID):

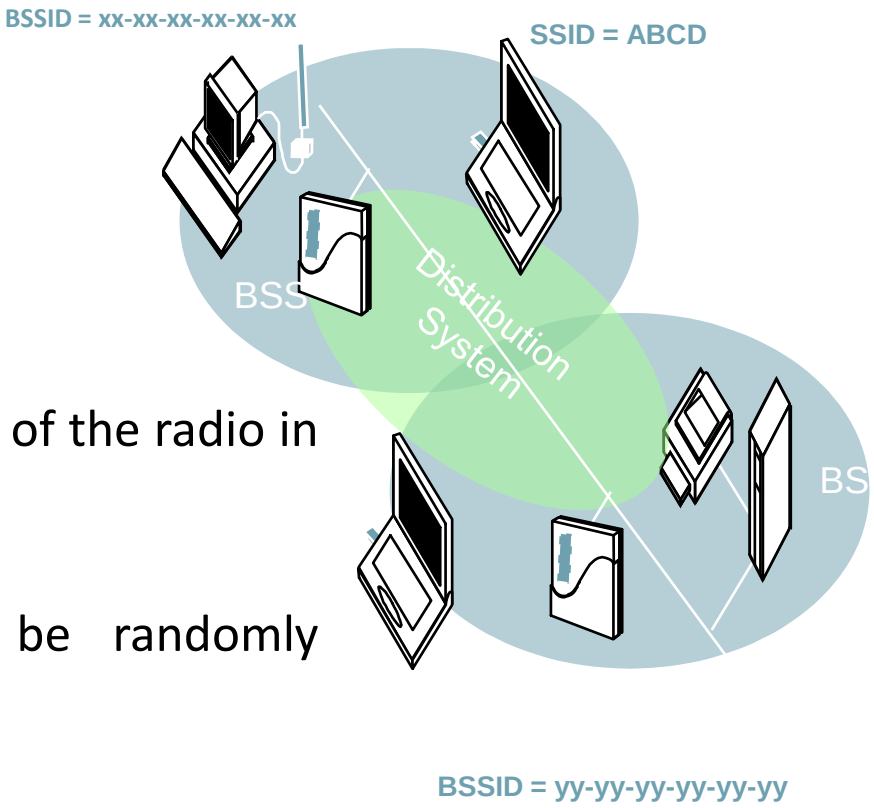
- "Network name"
- One network (ESS or IBSS) has one SSID
- 32 octets long string.
- Needed to separate one network from the other.
- Used during initial establishment of communication between stations and AP to allow stations to select the correct AP.



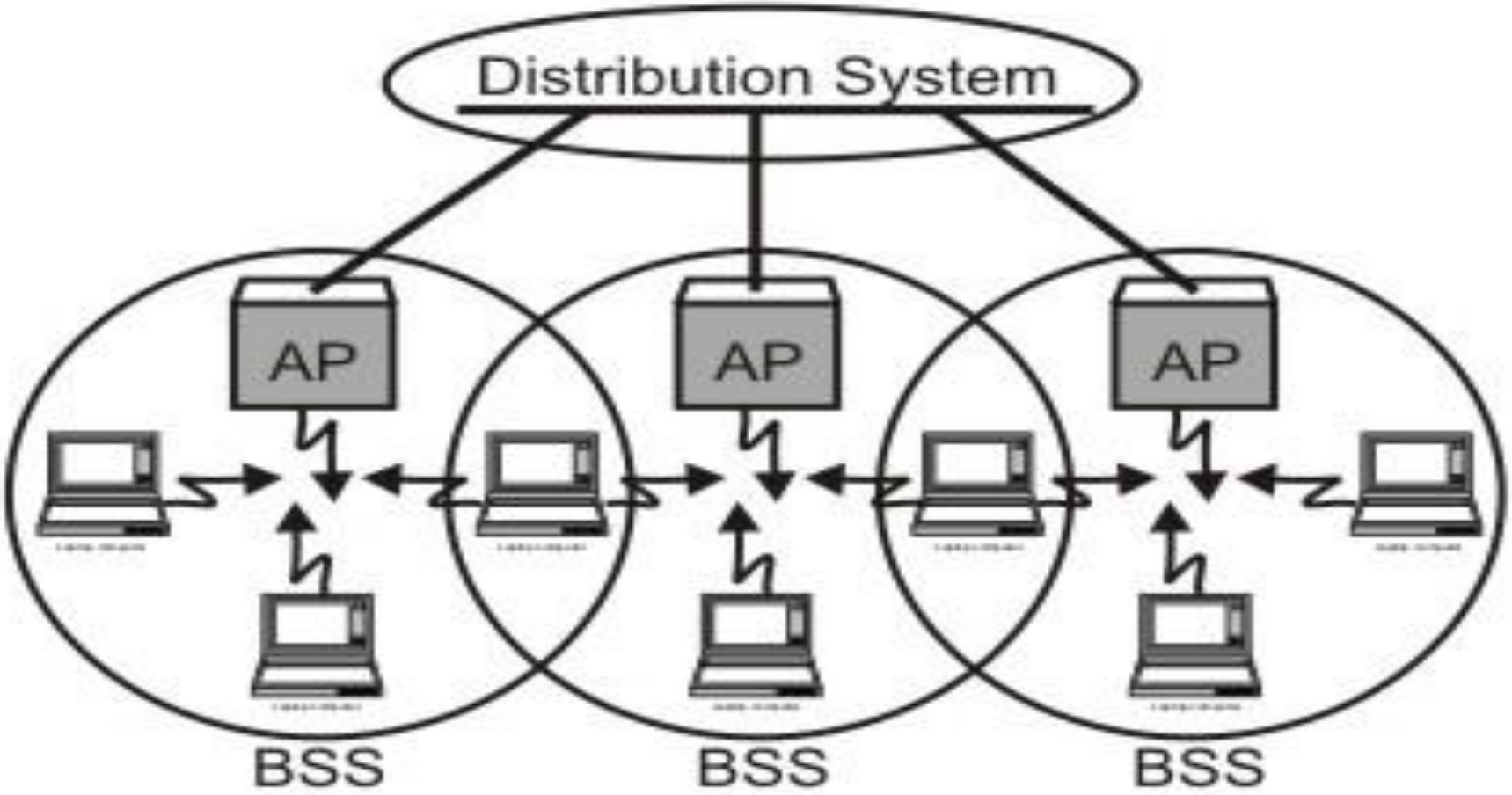
IEEE 802 .11 TERMINOLOGY

Basic Service Set Identifier (BSSID)

- "Cell identifier".
- One BSS has one BSSID .
- 6 octets long (MAC address format).
- In ESS is the same as the MAC address of the radio in the AP .
- In IBSS the value of BSSID will be randomly generated, and with local-bit on.
- Used as filter for multi-cast traffic and for traffic from other networks (in IBSS networks).
- Used during hand-over (roaming) to other AP, in identifying the "old" AP.



TOPOLOGY



Extended Service Set (ESS)

SELECTION OF THEIR ACCESS POINTS BY STATIONS

- The technique used for this purpose is known as scanning, which involves the following steps:
- **Active Scanning**: When a station joins a network or it wants to discontinue association with the existing AP.
- A station sends a probe frame.
- All APs within reach reply with a probe response frame.
- The station selects one of the access points, and sends the AP an Association Request frame.
- The AP replies with an Association Response frame.
- **Passive Scanning:** Where APs send Beacon frames periodically and station may respond with Association Request frame to join an AP.

MAC

Challenges

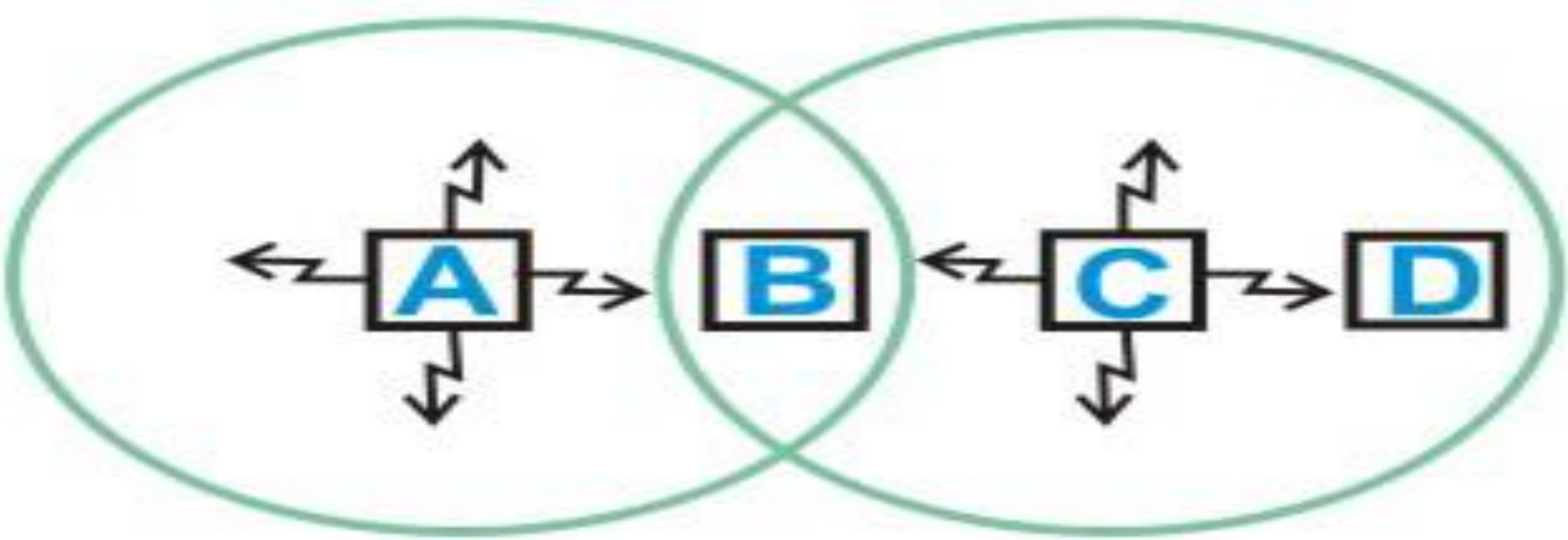
- The wireless LAN is Prone to more interference & is less reliable .

- The wireless LAN is susceptible to unwanted interception leading to security problems.

- There are so called **Exposed terminal** & **Hidden terminal problems.**

THE HIDDEN STATION PROBLEM

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



EXPOSED STATION PROBLEM

- A different situation where B is transmitting to A, and C sense the medium and detects the ongoing transmission between B and A.
- C falsely conclude that it can not transmit to D, where the fact is that such transmission would cause no problem.
- A transmission could cause a problem only when the destination is in zone between B and C, This problem is referred as Exposed station Problem.
- In this scenario as B is exposed to C, that's why C assumes it cannot transmit to D. So this problem is known as Exposed station problem (i.e. problem caused due to exposing of a station).
- The problem here is that before transmission, a station really wants to know that whether or not there is any activity around the receiver.
- CSMA merely tells whether or not there is any activity around the station sensing the carrier.

Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA)

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

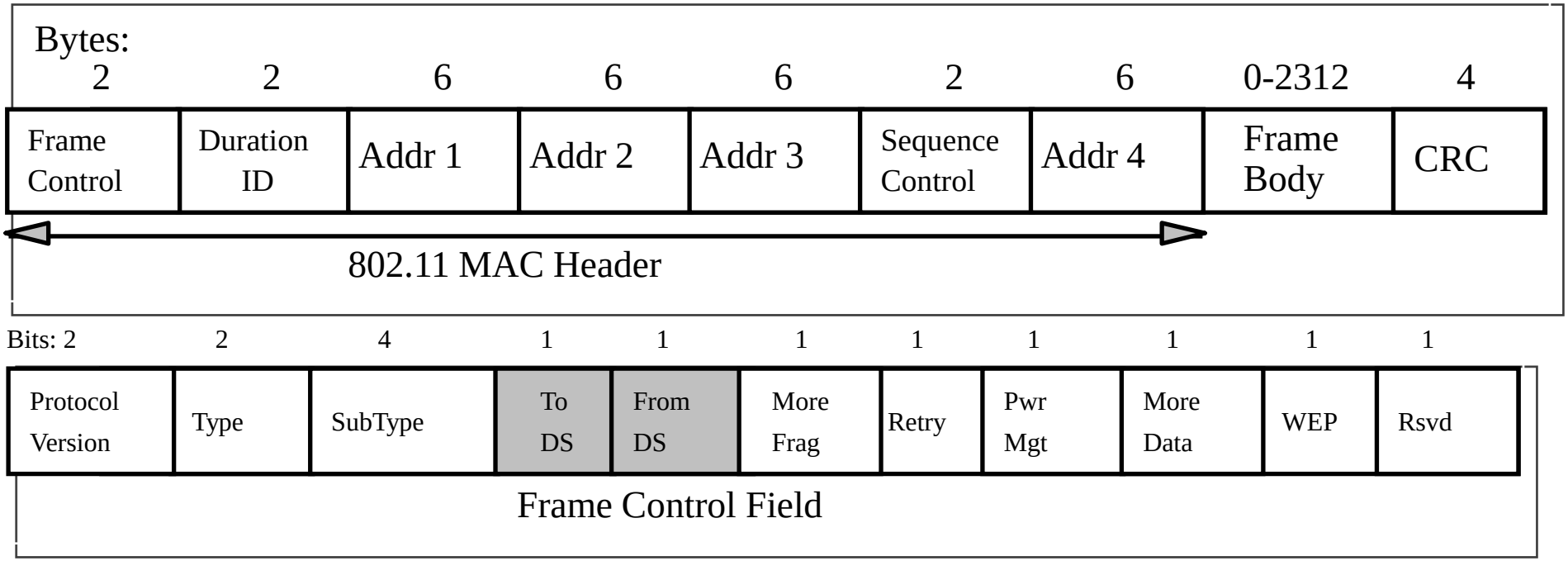
CARRIER SENSING

- In IEEE 802.11, carrier sensing is performed in two levels known as **physical carrier sensing** and **virtual carrier sensing**.
- **Physical carrier sensing** is performed at the radio interface by analyzing all detected packets and relative strength of signal from other sources.
- **Virtual carrier sensing** is used by a source station to inform all other stations in the BSS about the length of the data frame that it intends to send.

SECURITY

- Wireless LAN are subjected to possible breaches from unwanted monitoring.
- To overcome this problem ,IEEE 802.3 specifies an optional MAC layer security system known as Wired equivalent Privacy(**WEP**).
- It is done with the help of a 40 bit shared key authentication services . By default each BSS support up to 40 bit keys that are shared by all the clients in the BSS. It provides privacy ,but no integrity check.
- **Advanced Encryption Standard** (AES) 802.11 for authentication and encryption as a long term solution.

IEEE 802.11 MAC FRAME FORMAT



MAC Header format differs per Type:

- Control Frames (several fields are omitted)
- Management Frames
- Data Frames

IEEE 802.11 FRAME

The frames can be categorized into three types :

- The ***management frames*** are used for association and disassociation of stations with at the AP.
- Authentication and de-authentication,.
- Timing and Synchronization.
- ***Control frames*** are used for :
- Hand shaking.
- Positive ack during frame exchange.
- **Data frames** are used for the transmission of Data.
- MAC header provides information on frame control, duration, addressing &sequence control

MAC Frame Control Field

Frame Control Field (in MAC header)

- The **protocol version** field is 2 bits in length and will carry the version of the 802.11 standard. The initial value of 802.11 is 0; all other bit values are reserved.
- **Type and subtype** fields are 2 and 4 bits, respectively. They work together hierarchically to determine the function of the frame.
- The remaining 8 fields are all 1 bit in length.
- The **To DS** field is set to 1 if the frame is destined for the distribution system.
- **From DS** field is set to 1 when frames exit the distribution system. Note that frames which stay within their basic service set have both of these fields set to 0.
- The **More Flag** field is set to 1 if there is a following fragment of the current MSDU.

MAC FRAME CONTROL FIELD CONT….

- **Retry** is set to 1 if this frame is a retransmission.
- **Power Management** field indicates if a station is in power save mode (set to 1) or active (set to 0).
- **More data** field is set to 1 if there is any MSDUs buffered for that station.
- The **WEP** field is set to 1 if the information in the frame body was processed with the WEP algorithm.
- The **Duration/ID field** is 2 bytes long. It contains the data on the duration value for each field and for control frames .it carries the associated identity of the transmitting station.
- The **address fields** identify the basic service set, the destination address, the source address, and the receiver and transmitter addresses. Each address field is 6 bytes long.
- The **sequence control** field is 2 bytes and is split into 2 subfields, fragment number and sequence number.
- **Fragment number** is 4 bits and tells how many fragments the MSDU is broken into.
- **The sequence number** field is 12 bits that indicates the sequence number of the MSDU. The frame body is a variable length field from 0 - 2312. This is the payload

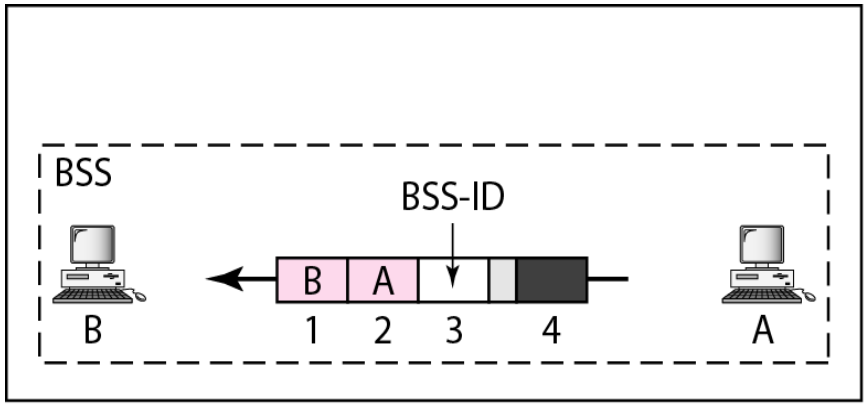
ADDRESSING MECHANISM

- The addressing mechanism in 802.11 is defined by the values of two flags in FC field, *To DS* & *From DS* .
- Each flag can either be one or zero resulting in four different situation.
- Address 1 is always address of next device.
- Address 2 is always address of previous device.
- Address 3 is always address of final destination if it is not defined by address 1.
- Address 4 is the address of original source station if it is not same as address 2.

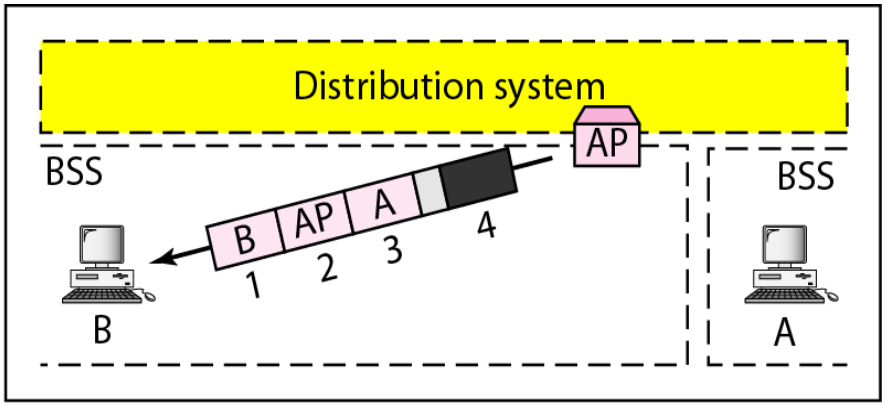
Table *Addresses*

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

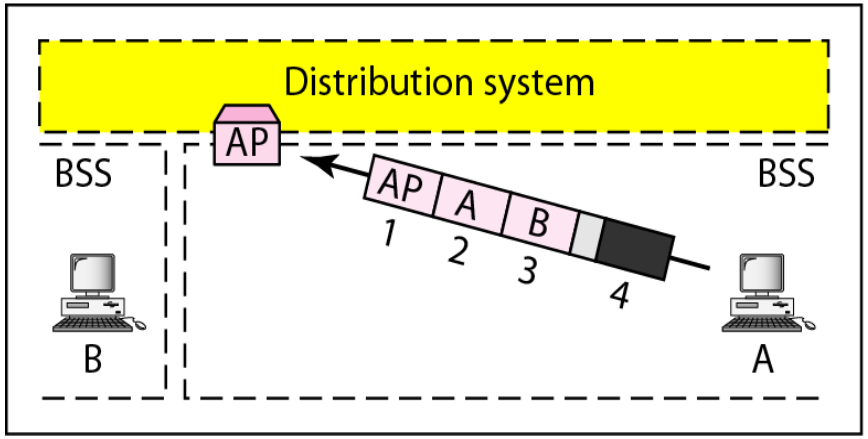
Figure Addressing mechanisms



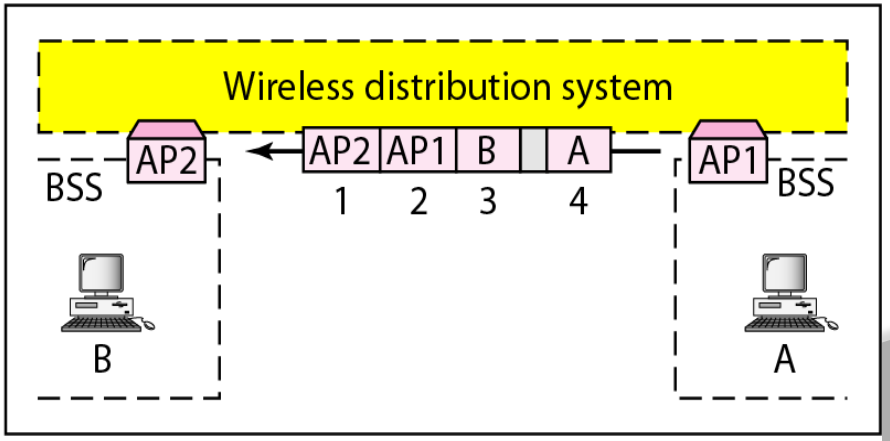
a. Case 1



b. Case 2



c. Case 3



d. Case 4

UNIT-4

INTRODUCTION

- A wireless personal area network (WPAN) is a type of personal network that uses wireless communication technologies to communicate and transfer data between the user's connected devices.
- It allows an individual to connect all or most of his or her devices together and access the Internet or a local network using any of the native/supported wireless communication techniques.
- WPAN is also known as a short wireless distance network.
- PAN works much like a standard personal area network (PAN) except that it uses a wireless communication medium instead of a wired connection.

INTRODUCTION

- Typically, the devices in WPAN include peripheral and hand-held devices such as PDAs, smart phones and tablet PCs.
- A WPAN's range depends on the wireless router's capabilities, access point or the device itself, but it is usually restricted to a house or small office.
- The IEEE 802.15 standards working group focuses on the development of standards for wireless PANs and coordinates with other standards, such as 802.11 wireless LANs.

ADVANTAGES AND DISADVANTAGES

ADVANTAGE

- They are quick and easy, WPAN devices are easy portable, usually need less technical skill

DISADVANTAGE

- Have limited range, limited to relatively low data rates, devices are not compatible with each other, devices with inbuilt WPANs are more expensive

APPLICATIONS

- In Medical and Hospital
- In Railway and Airport Stations
- In Organization and Companies
- In School and College Education
- In Military and Defence
- In Home, Office & Small Industries

BLUETOOTH

- Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers, coffee makers, and so on.
- A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously.

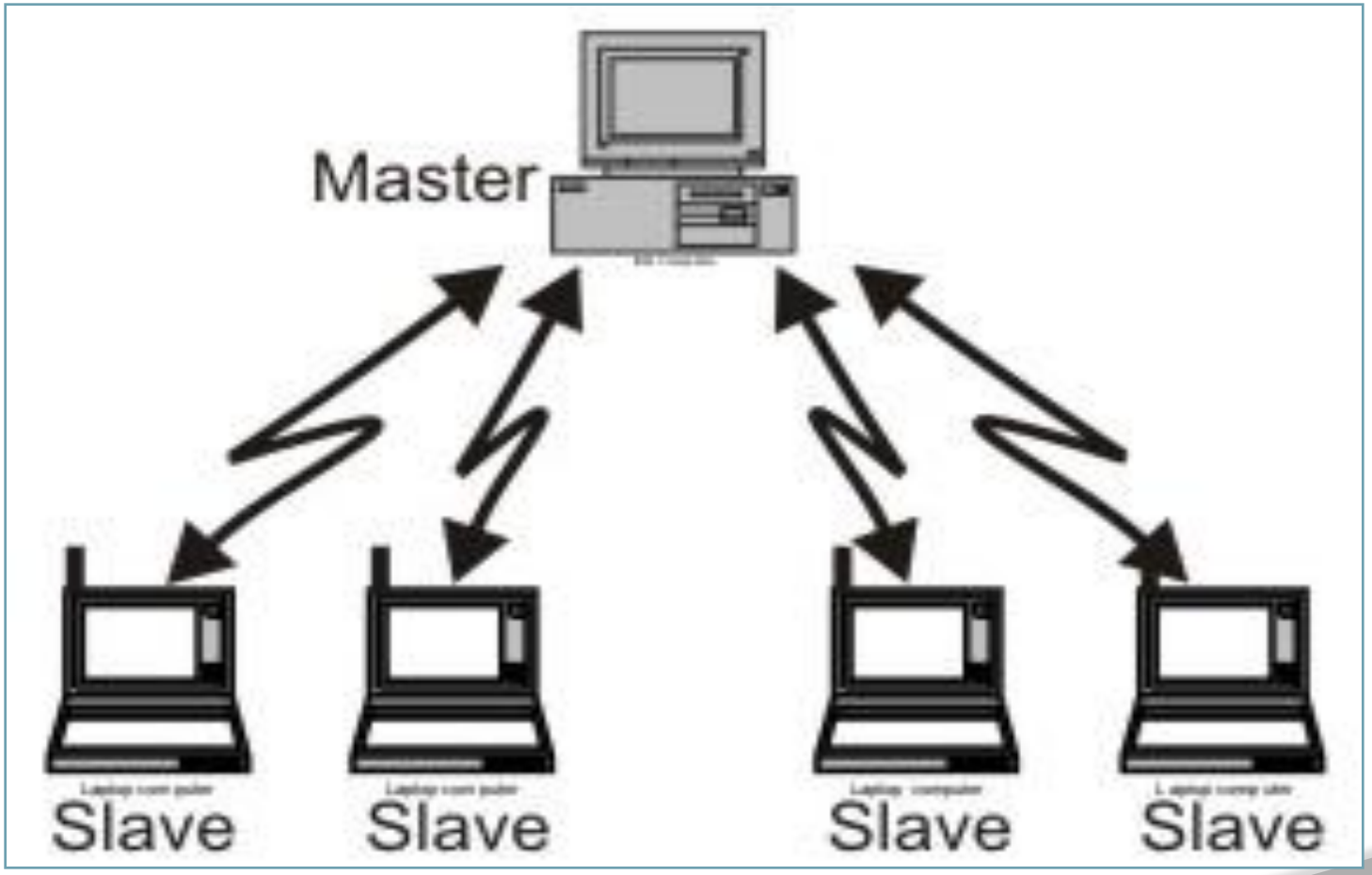
BLUETOOTH

- Bluetooth wireless technology is a short-range radio technology, which is developed for Personal Area Network (PAN).
- Bluetooth operates in the **2.4 GHz ISM band .**
- Bluetooth wireless technology makes it possible to transmit signals over short distances between telephones, computers and other devices and thereby simplify communication and synchronization between devices.
- It is an ad hoc type network operable over a small area such as a room .
- Based on **IEEE 802.15** Standard.

TOPOLOGY FOR BLUETOOTH

- There are two types of topology for Bluetooth – Piconet, Scatternet. The Piconet is a small ad hoc network of devices (normally 8 stations).
- 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 .**

TOPOLOGY FOR BLUETOOTH



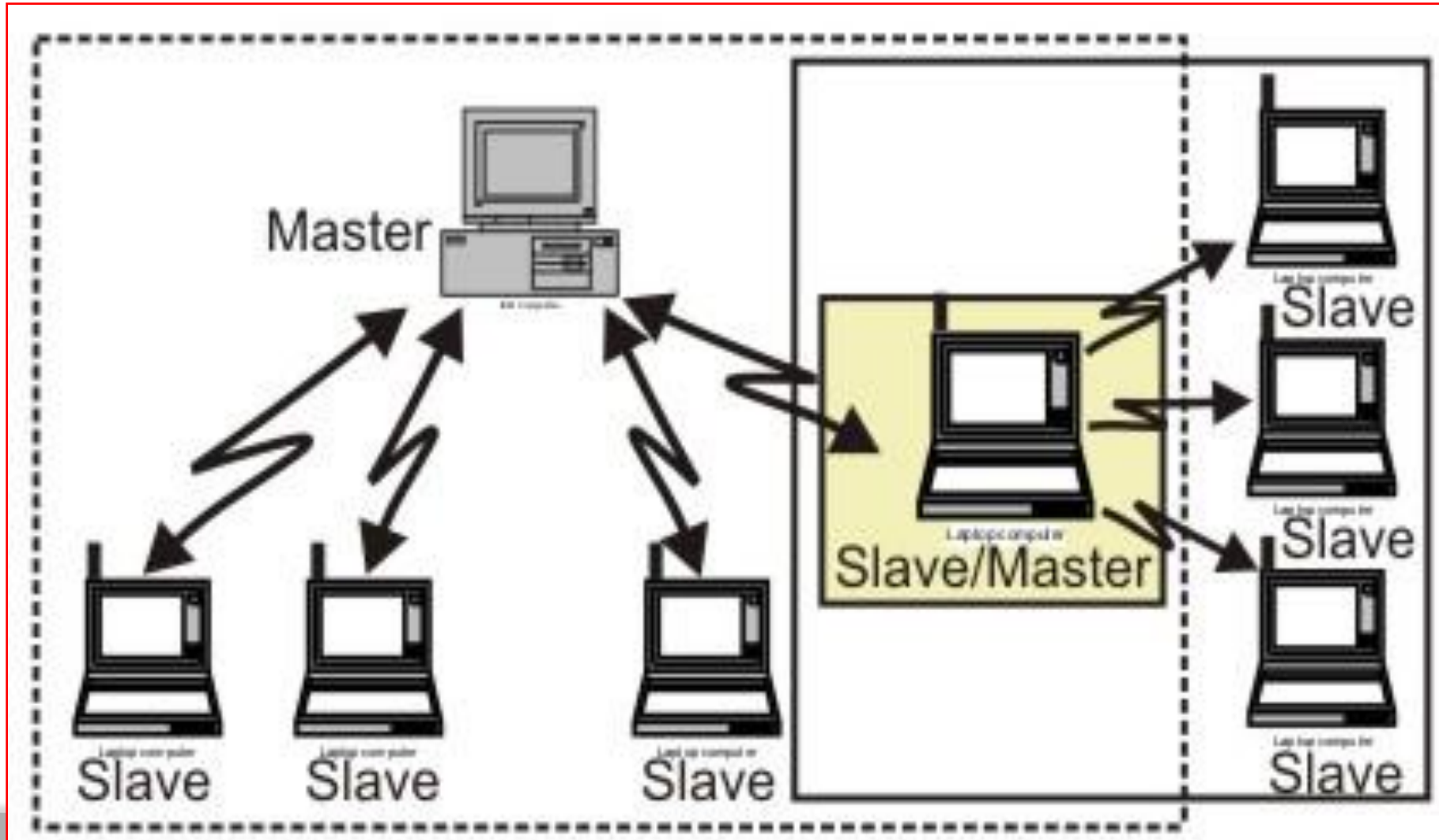
SCATTERNET

- A scatternet is a number of interconnected piconets that supports communication between more than 8 devices.
- Scatternets can be formed when a member of one piconet (either the master or one of the slaves) elects to participate as a slave in a second, separate piconet.
- The device participating in both piconets can relay data between members of both ad-hoc networks.
- Using this approach, it is possible to join together numerous piconets into a large scatternet, and to expand the physical size of the network beyond Bluetooth's limited range.

SCATTERNET TOPOLOGY

- Scatternet is formed by combining several Piconets .
- Key features of the scattering 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 TOPOLOGY



BLUETOOTH TRANSMISSION MEDIUM

- Bluetooth operates in the 2.4 GHz ISM band.
- In the US and Europe, a band of 83.5 MHz width is available; in this band, 79 RF channels spaced 1 MHz apart are defined.
- In France, a smaller band is available; in this band, 23 RF channels spaced 1 MHz part are defined .
- Uses FHSS method.
- Hops 1600 times /sec .
- Uses a sophisticated version of FSK, called GPSK for modulation.
- Carrier frequency(fc) =2402+n=0,1,2……78.

BLUETOOTH TRANSMISSION MEDIUM

•Possibility of interference with IEEE 802.11b LANs.

• Two or more Bluetooth devices using the same channel form a piconet.

• The hopping sequence is unique for the piconet and is determined by the Bluetooth device address (BD_ADDR) of the master; the phase in the hopping sequence is determined by the Bluetooth clock of the master.

• The channel is divided into time slots where each slot corresponds to an RF hop frequency.

WHAT DO YOU MEAN BY ZIGBEE?

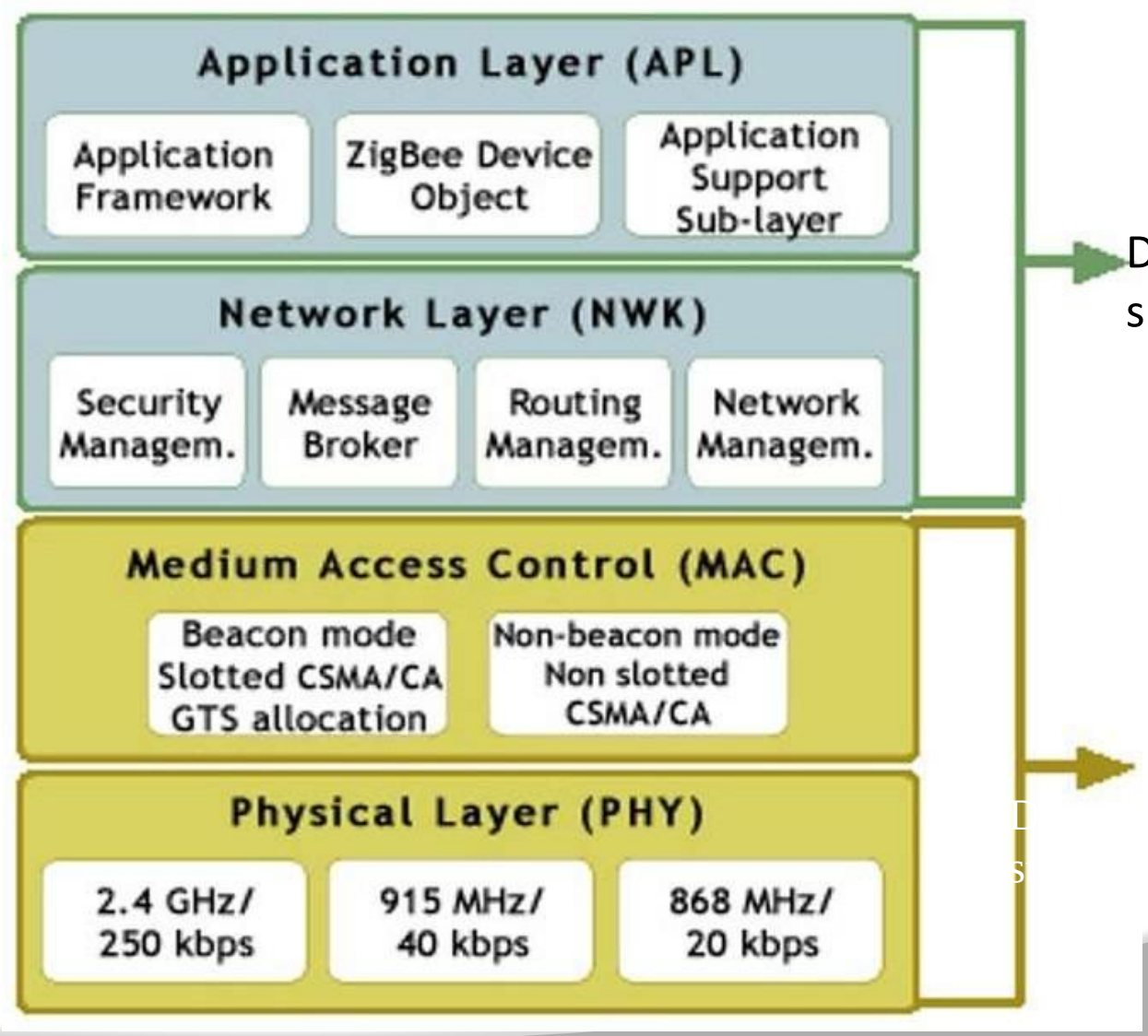
- Technological standard created for control and sensor networks
- Based on the IEEE 802.15.4 standard
- Wireless personal area networks(WPANs)
- High level communication
- Frequency band up to 2.4GHz

UNIT-5

CHARACTERISTICS OF ZIGBEE

- Data rates of 20 kbps and up to 250 kbps
- Support for Low Latency Devices
- CSMA-CA Channel Access
- Low Power Usage consumption
- 3 Frequencies bands with 27 channels
- Extremely low duty-cycle (<0.1%)
- Supports large number of nodes
- Very long battery life

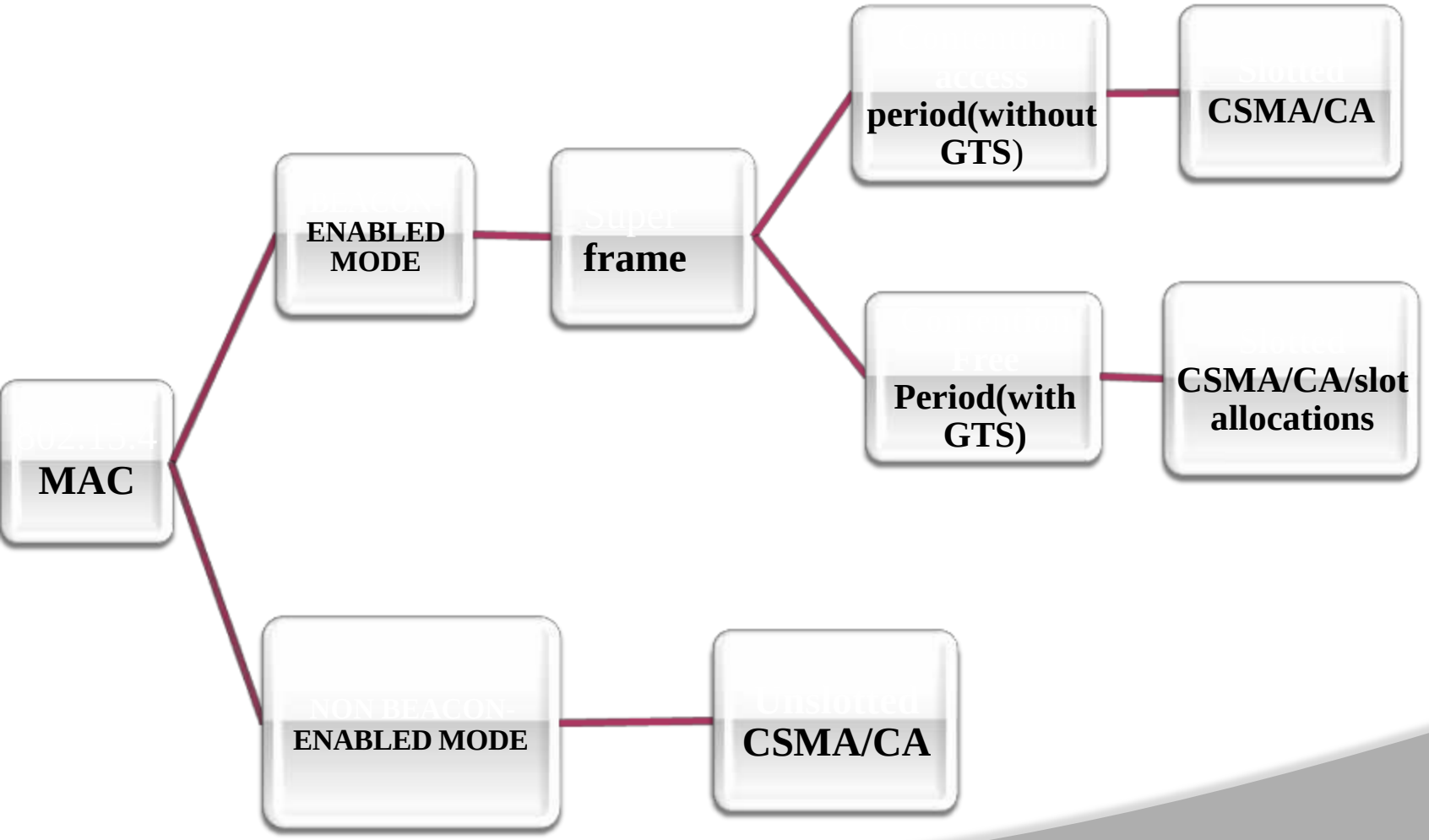
ZIGBEE PROTOCOL ARCHITECTURE



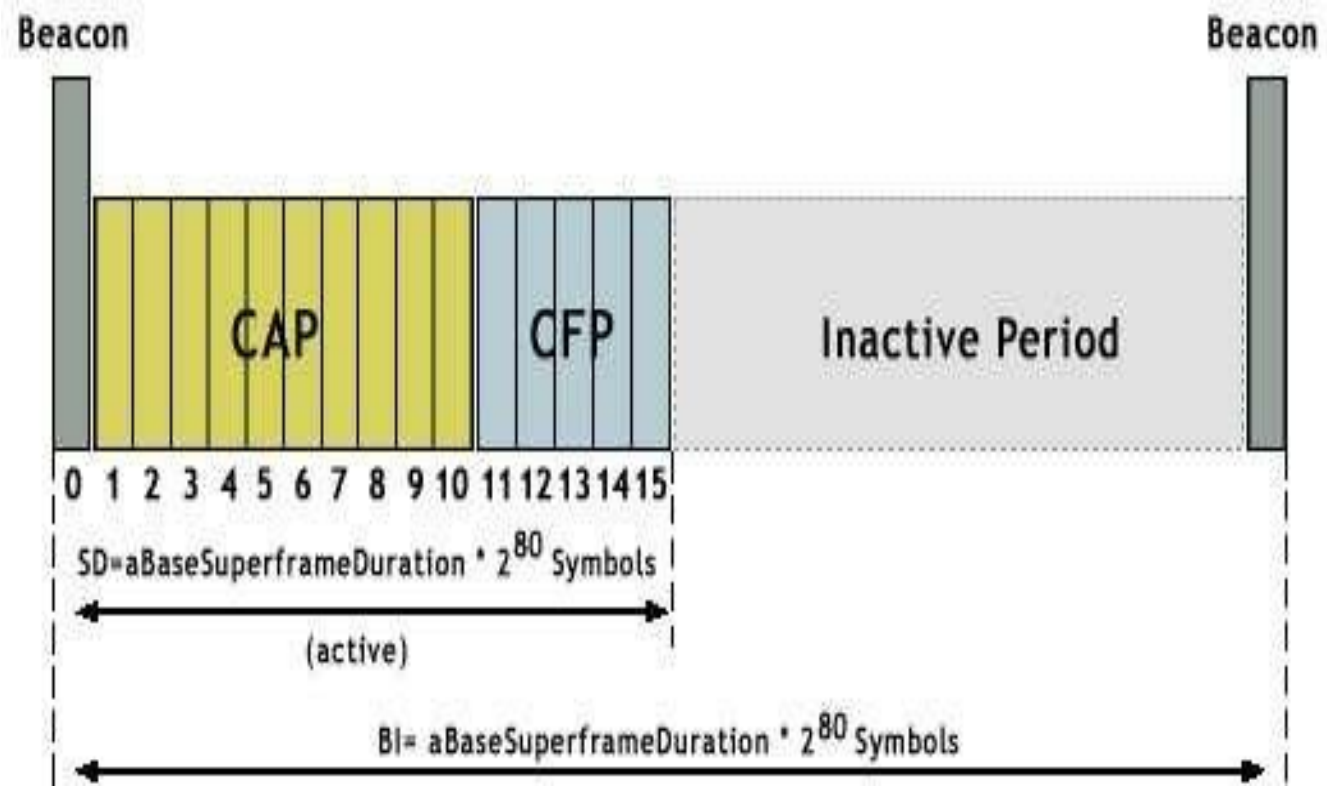
PHY LAYER TASKS

Activation and deactivation of the radio transceiver	• Transmitting • Receiving • Sleeping
Receiver Energy Detection	• Estimating received signal power
Link Quality Indication	• Quality of a received signal • Tune its transceiver in to specific channel
Clear Channel Assessment	• Energy Detection mode • Carrier Sense mode • Carrier Sense with Energy Detection mode
Channel Frequency Selection	• Tune its transceiver in to specific channel

MODES IN MAC LAYER

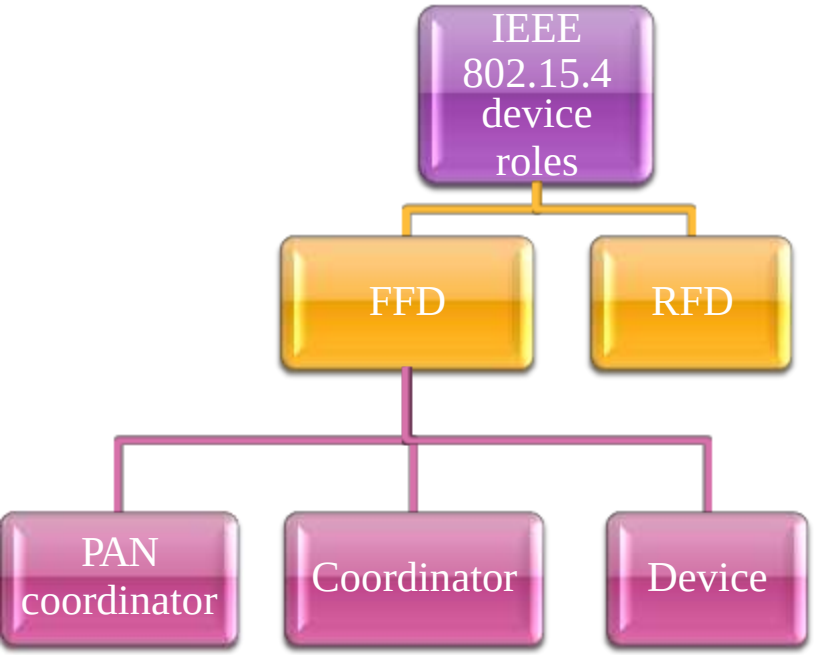


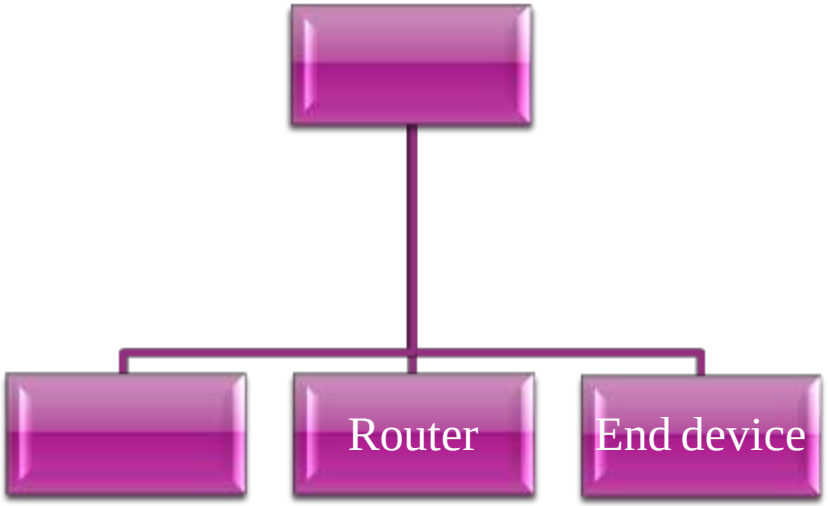
SUPER FRAME STRUCTURE



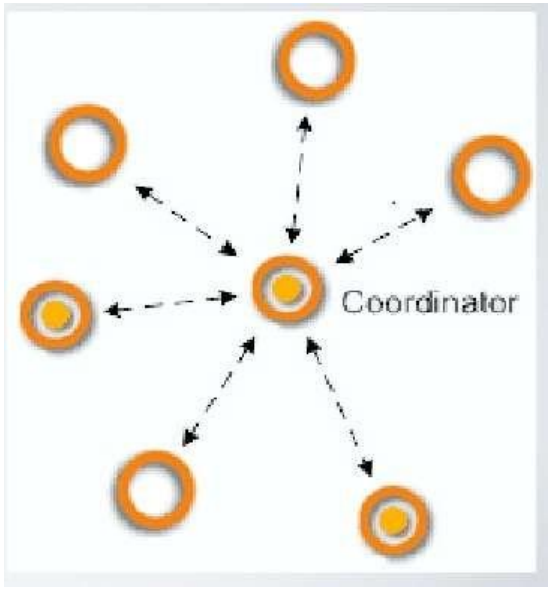
ZIGBEE DEVICE ROLES

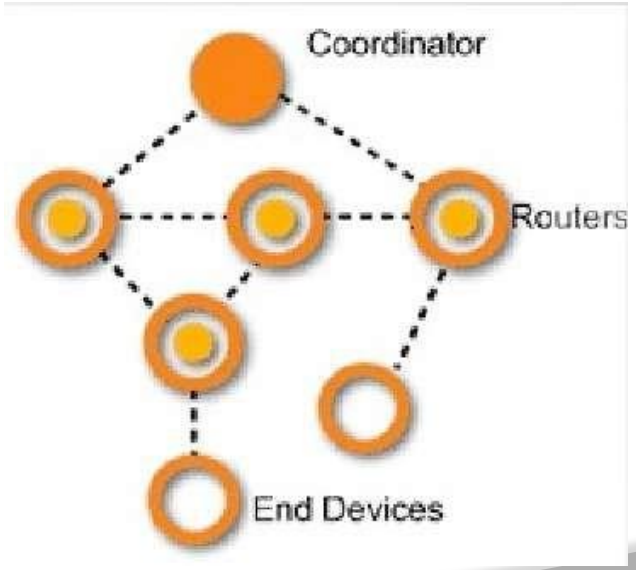
NETWORK DEVICES

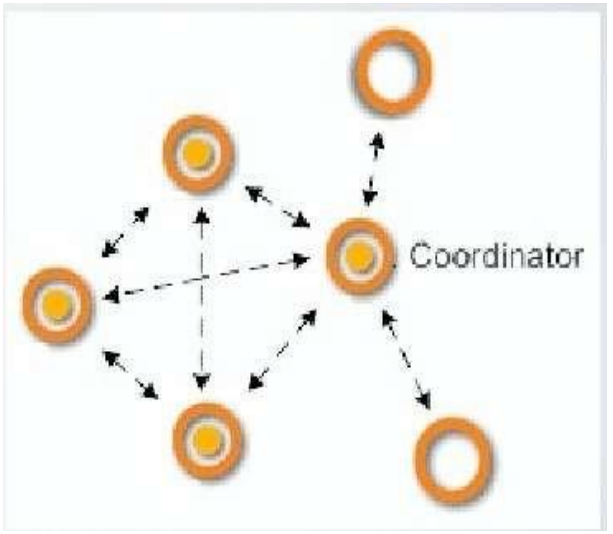




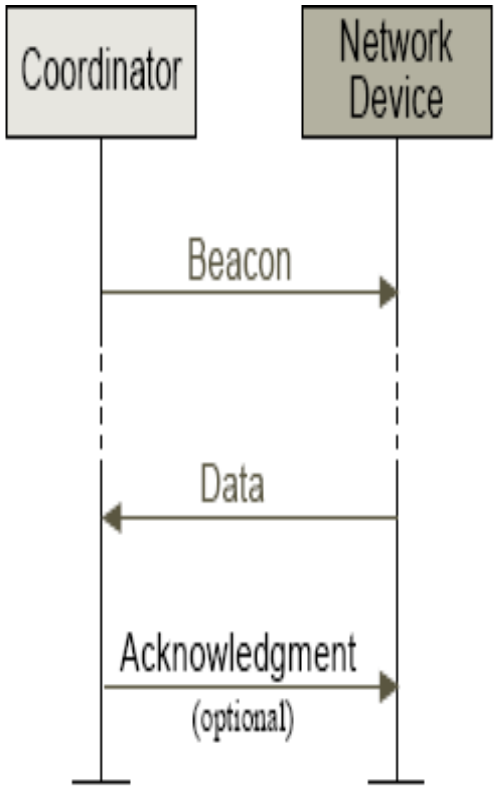
DATA TRANSFER MODELS



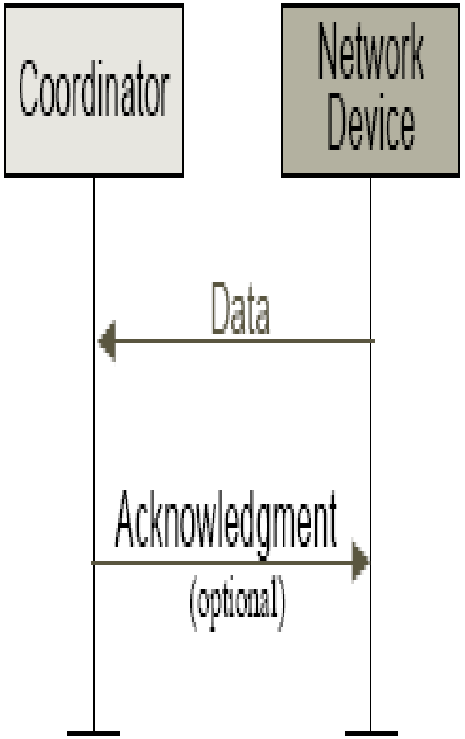




COMMUNICATION MECHANISMS -I

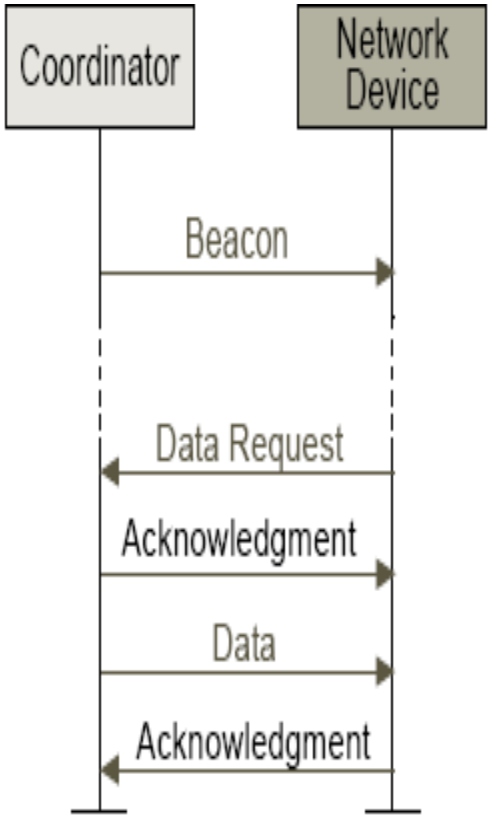


-Communication to a coordinator in a beacon-enabled network

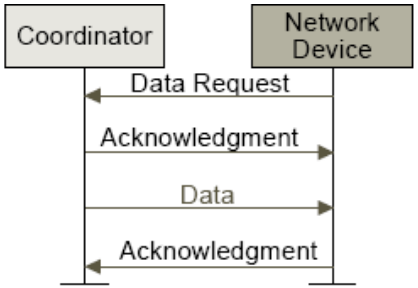


-Communication to a coordinator in a nonbeacon-enabled network

COMMUNICATION MECHANISMS -II

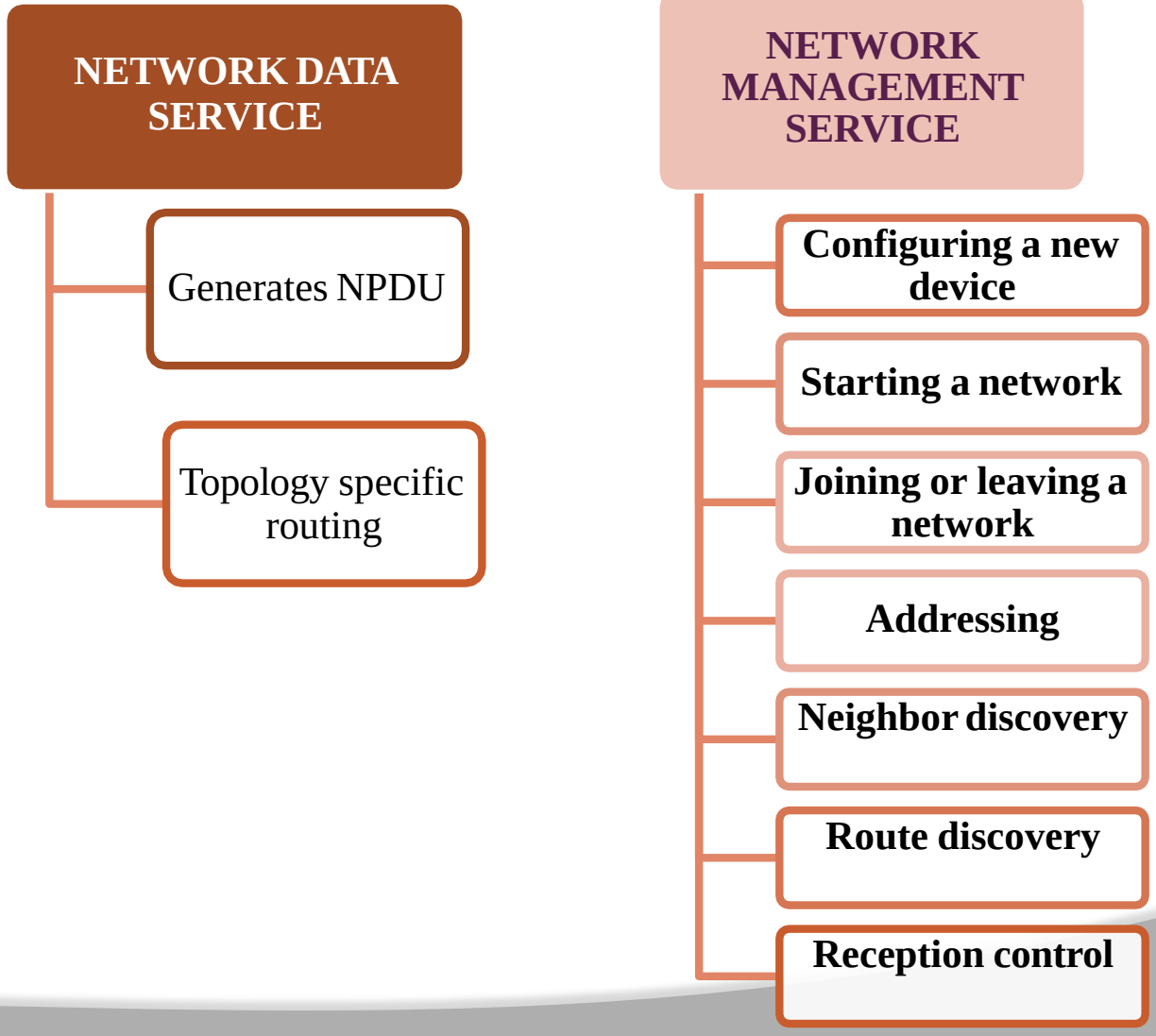


Communication from a coordinator a beacon-enabled network



Communication from a coordinator in a nonbeacon-enabled network

NETWORK LAYER



APPLICATION LAYER

APPLICATION SUPPORT SUB-LAYER

- Maintaining tables for binding
- Message forwarding between bound end devices
- Providing services

THE APPLICATION FRAMEWORK

- Key Value Pair service
- Generic Message service

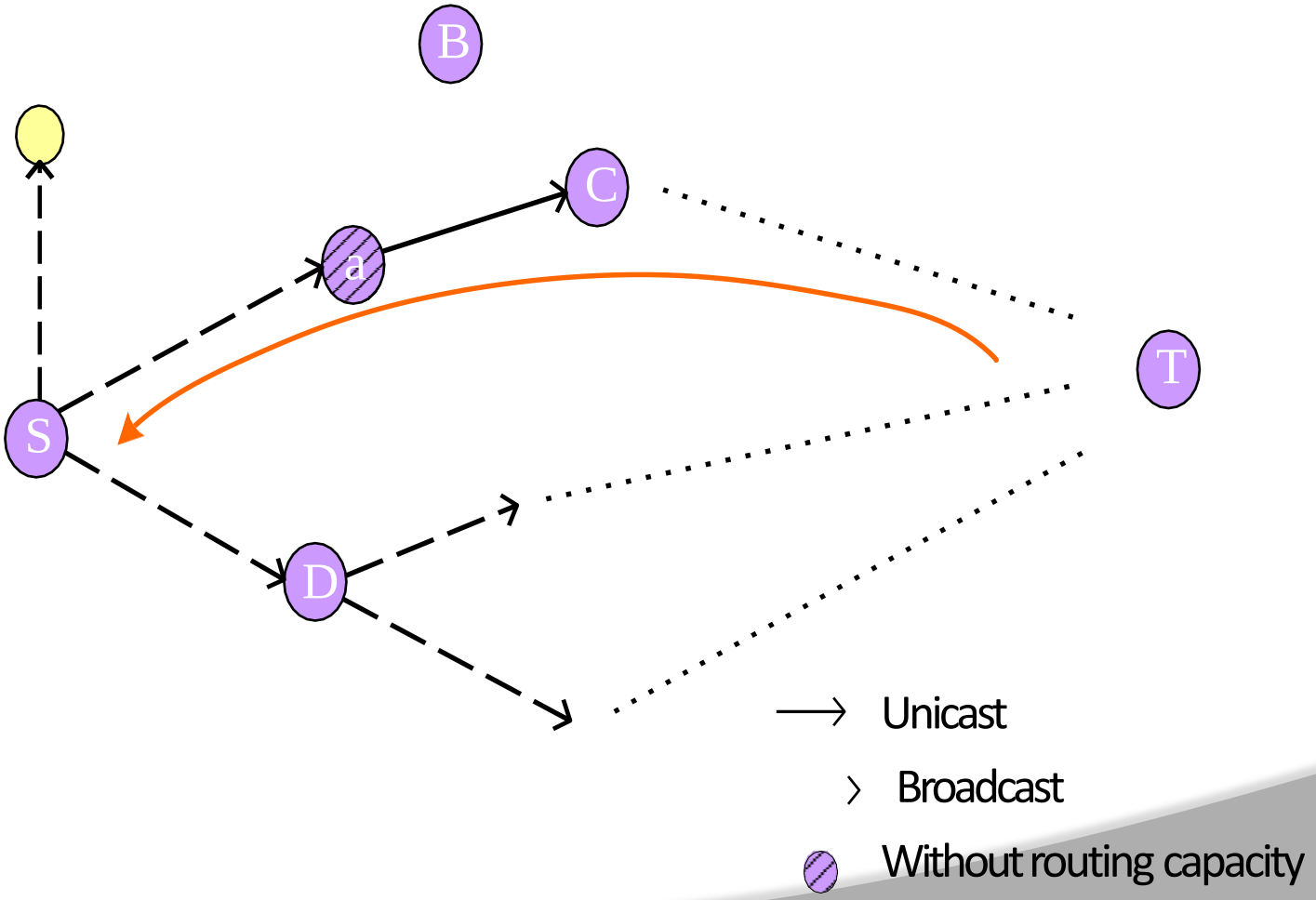
APPLICATION OBJECTS

- Manufacturer defined component
- Holds key-value attributes

ZIGBEE DEVICE OBJECT

- Role of the device
- Responsible for Discovery

ZIGBEE ROUTING IN A MESH NETWORK



IEEE 802.15.4 LR-WPAN (ZIGBEE)

- ZigBee technology is simpler (and less expensive) than Bluetooth.
- The main objectives of an LR-WPAN like ZigBee are ease of installation, reliable data transfer, short-range operation, extremely low cost, and a reasonable battery life, while maintaining a simple and flexible protocol.
- The raw data rate will be high enough (maximum of 250 kbit/s) to satisfy a set of simple needs such as interactive toys, but is also scalable down to the needs of sensor and automation needs (20 kbit/s or below) using wireless communications.

LR-WPAN DEVICE TYPES

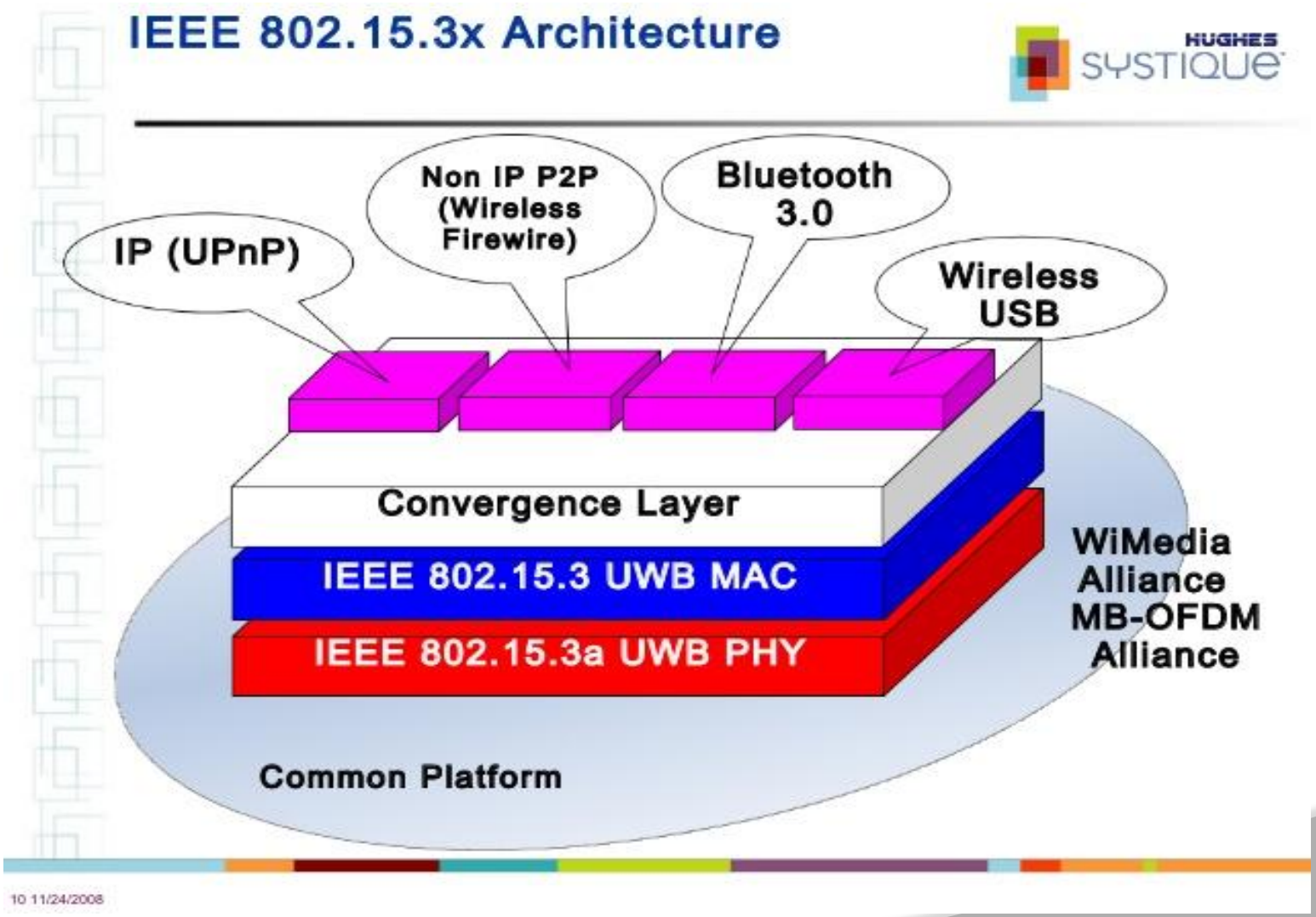
Two different device types can participate in an LR-WPAN network:

Full-function devices (FFD) can operate in three modes serving as a personal area network (PAN) coordinator, a coordinator, or a device. **Reduced-function devices (RFD)** are intended for applications that are extremely simple.

An FFD can talk to RFDs or other FFDs, while an RFD can talk only to an FFD.

- Two or more devices communicating on the same physical channel constitute a WPAN. The WPAN network must include at least one FFD that operates as the PAN coordinator.
- The PAN coordinator initiates, terminates, or routes communication around the network. The PAN coordinator is the primary controller of the PAN.
- The WPAN may operate in either of two topologies: the star topology or the peer-to-peer topology.

IEEE 802.15.3 ARCHITECTURE



IEEE 802.15.3 STANDARDS

- Direct sequence (DS-UWB)
  - Championed by Motorola/XtremeSpectrum
  - Classic UWB, simple pulses,
  - 2 frequency bands: 3.1-4.85GHz, 6.2-9.7GHz
  - CDMA has been proposed at the encoding layer
  - Spectrum dependent on the shaping filter – possible differing devices worldwide
- Multiband Orthogonal Frequency Division Multiplexing (MB-OFDM)
  - Intel/TI/many others
  - Similar in nature to 802.11a/g
  - 14 528MHz bands (simplest devices need to support 3 lowest bands, 3.1GHz – 4.7 GHz)
  - Spectrum shaping flexibility for international use