Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY | PUNE
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

CET4004B: Wireless and Mobile Device Security

SCHOOL OF COMPUTER ENGINEERING AND TECHNOLOGY

T. Y. B. TECH. COMPUTER SCIENCE AND ENGINEERING

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

CET4004B: Wireless and Mobile Device Security

Teaching Scheme
Theory: 3Hrs. / Week

Credits: 03 + 01 = 04
Practical: 2 Hrs./Week

Course Objectives:

1) Knowledge:

i. To understand wireless networks technologies and applications
ii. To study Ad-Hoc, sensor networks architecture, challenges and applications
iii. To understand basic security needs and issues in wireless networks
iv. To understand mobile device security architecture and security dynamics

2) Skills:

i. This course gives understanding of how to design and configure your own network

3) Attitude:

i. To deploy the network as well as provide various security aspects to the mobile device

Course Outcomes:

i. Compare different wired and wireless technologies
ii. Simulate and analyze wireless Ad-Hoc networks for different protocols
iii. Analyze the security threats in wireless sensor networks
iv. Configure or Program security needs in mobile devices

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Module 1
Introduction Wireless Networks

Disclaimer:

a. Information included in these slides came from multiple sources. We have tried our best to cite the sources. Please refer to the references to learn about the sources, when applicable.

b. The slides should be used only for preparing notes, academic purposes (e.g. in teaching a class), and should not be used for commercial purposes.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Points to be covered

- Introduction to Wireless Networks
- LAN, PAN, MAN, WAN- Technical issues
- Network Architecture, Advantages.
- Overview of IEEE 802.11, 802.15, 802.16- Architecture, Features and applications
- MAC protocols- CSMA-CA
- Hidden station and exposed station problems
- Mobile cellular networks - Generations overview, features and applications
- Cellular architecture system
- Handoffs and Handover
- Introduction to 4G and 5G

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

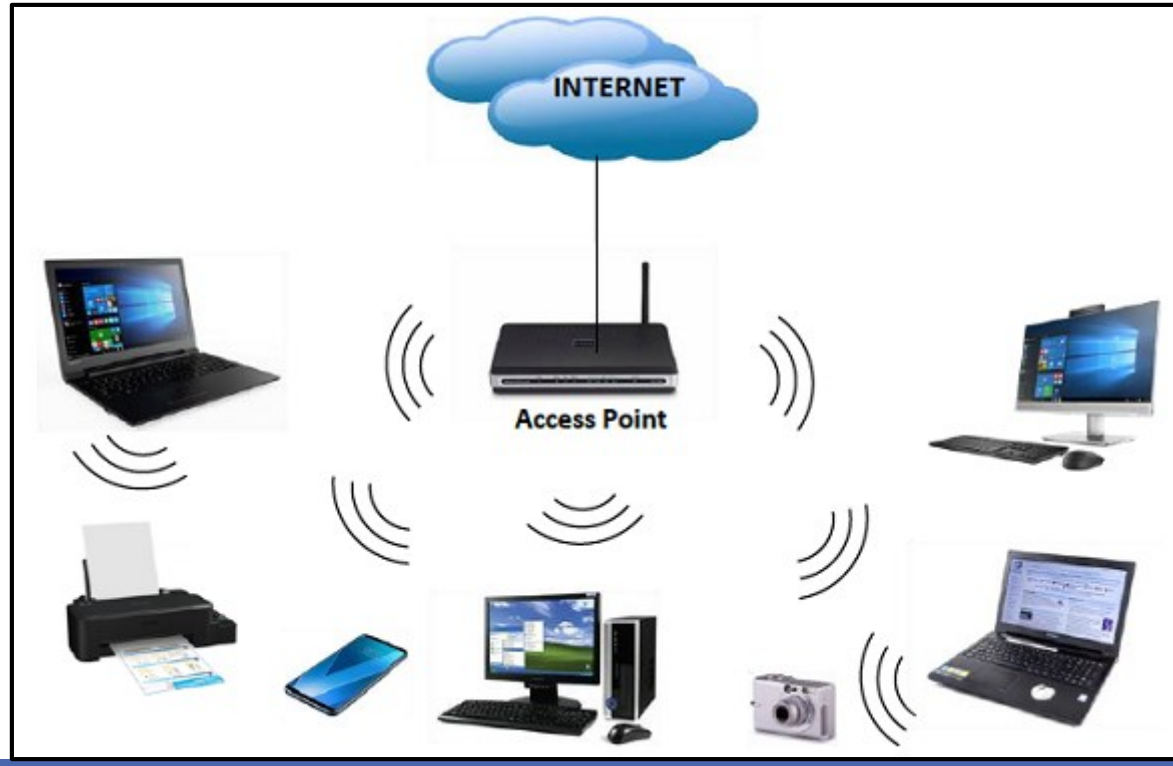
Introduction to Wireless Networks

- Computer networks that are not connected by cables
- Use radio waves for communication between the network nodes
- Allow devices to be connected to the network while roaming around within the network coverage.

Examples: Mobile phone networks, Wireless sensor networks, Satellite communication networks, Terrestrial microwave networks

Types of Wireless Networks

- Wireless LANs – Connects two or more network devices using wireless distribution techniques.
- **Wireless PANs** – connected through signals such as infrared, ZigBee, Bluetooth and ultra wideband, etc. connects electronic devices within a user's immediate area. The size of a PAN ranges from a few centimeters to a few meters.
- Wireless MANs – Connects two or more wireless LANs spreading over a metropolitan area.
- Wireless WANs – Connects large areas comprising LANs, MANs and personal networks.



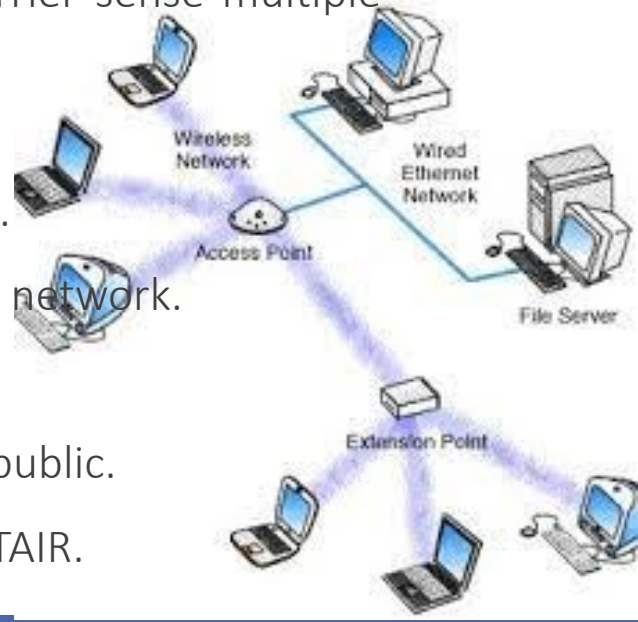
MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Characteristics of wireless communications systems

- **Mobility:** A wireless communications system allows users to access information beyond their desk and conduct business from anywhere without having a wire connectivity.
- **Reachability:** Wireless communications systems enable people to be better connected and reachable without any limitation of any location.
- **Simplicity:** Wireless communication system are easy and fast to deploy in comparison of cabled network. Initial setup cost could be a bit high but other advantages overcome that high cost.
- **Maintainability:** Being a wireless system, you do no need to spend too much to maintain a wireless network setup.
- **Roaming Services:** Using a wireless network system, you can provide service any where any time including train, buses, aeroplanes etc.
- **New Services:** Wireless communications systems provide new smart services like SMS and MMS

Fundamentals of Wireless LANs

- 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).
- Uses an encryption method i.e. wired equivalent privacy algorithm.
- Provide high speed data communication in small areas such as building or an office.
- Allow users to move around in a confined area while they are still connected to the network.
- Used to save costs and avoid laying cable,
- In some cases, it is the only option for providing high-speed internet access to the public.
- Examples of WLANs that are available today are NCR's waveLAN and Motorola's ALTAIR.



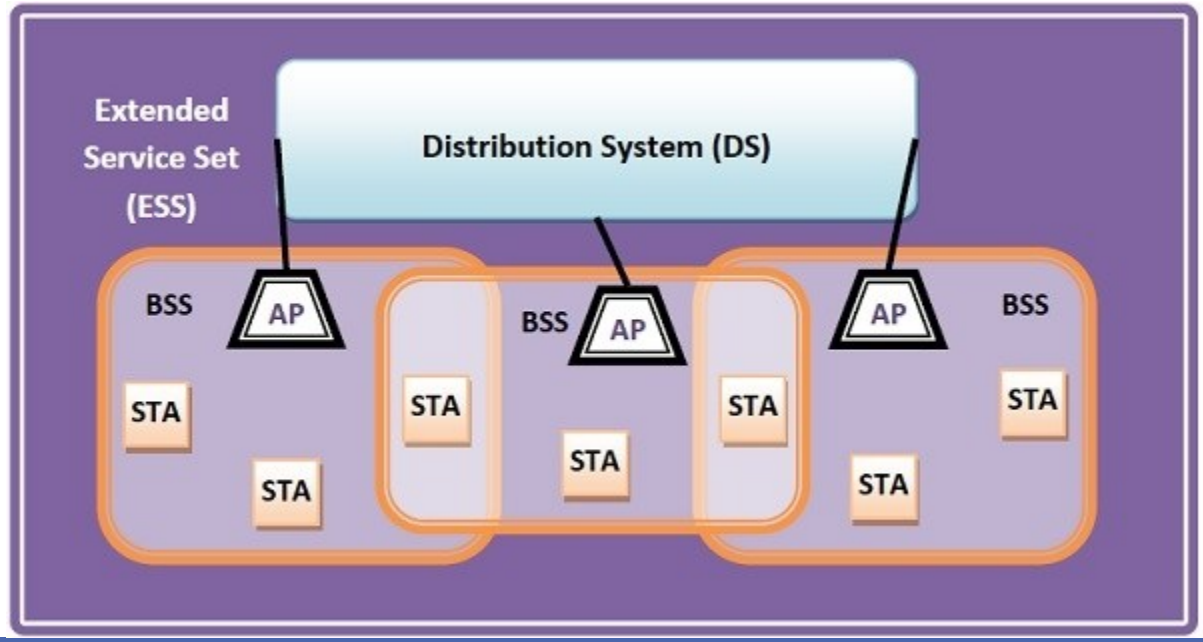
MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Fundamentals of Wireless LANs

- Use high-frequency radio waves instead of cables for connecting the devices within a limited area forming LAN (Local Area Network).
- Users connected by wireless LANs can move around within this limited area such as home, school, campus, office building, railway platform, etc.

Components of WLANs

- Stations (STA) – It comprises of all devices and equipment that are connected to the wireless LAN. Each station has a wireless network interface controller.
- A station can be of two types –
  - ✓ Wireless Access Point (WAP or AP)
  - ✓ Client
- Basic Service Set (BSS) – A basic service set is a group of stations communicating at the physical layer level. BSS can be of two categories –
  - ✓ Infrastructure BSS
  - ✓ Independent BSS
- Extended Service Set (ESS) – It is a set of all connected BSS.
- Distribution System (DS) – It connects access points in ESS.



MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

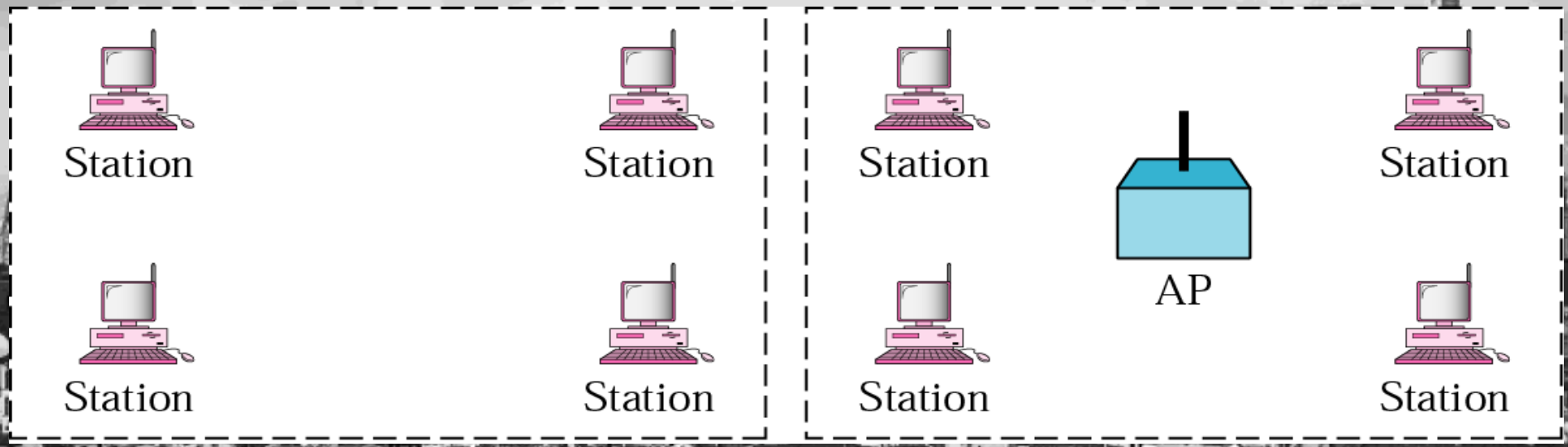
Types of WLANs

WLANs, as standardized by IEEE 802.11, operates in two basic modes, infrastructure, and ad hoc mode.

1. **Infrastructure Mode** – Mobile devices or clients connect to an access point (AP) that in turn connects via a bridge to the LAN or Internet. The client transmits frames to other clients via the AP.
2. **Ad Hoc Mode** – Clients transmit frames directly to each other in a peer-to-peer fashion.

Network Architecture

- Infrastructure Based vs. Ad Hoc LANs
  - Infrastructure: access points (APs) and mobile stations (STAs)
  - Ad hoc LANs: do not need fixed infrastructure



Ad hoc mode: BSS without an AP

Infrastructure mode: BSS with an AP

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Advantages of WLANs

1. **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.).
2. **Planning:** Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.
3. **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.
4. **Robustness:** Wireless networks can handle disasters, e.g., earthquakes, flood etc. whereas, networks requiring a wired infrastructure will usually break down completely in disasters.
5. **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. And second, wireless LAN eliminates the direct costs of cabling and the labor associated with installing and repairing it.
6. **Ease of Use:** Wireless LAN is easy to use and the users need very little new information to take advantage of WLANs.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Disadvantages of WLANs

1. **Quality of Services:** Quality of wireless LAN is typically lower than wired networks. The main reason for this is the lower bandwidth due to limitations is radio transmission, higher error rates due to interference and higher delay/delay variation due to extensive error correction and detection mechanisms.
2. **Proprietary Solutions:** Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardization functionality plus many enhanced features. Most components today adhere to the basic standards IEEE 802.11a or 802.11b.
3. **Restrictions:** Several govt. and non-govt. institutions world-wide regulate the operation and restrict frequencies to minimize interference.
4. **Global operation:** Wireless LAN products are sold in all countries so, national and international frequency regulations have to be considered.
5. **Low Power:** Devices communicating via a wireless LAN are typically power consuming, also wireless devices running on battery power. Whereas the LAN design should take this into account and implement special power saving modes and power management functions.
6. **License free operation:** LAN operators don't want to apply for a special license to be able to use the product. The equipment must operate in a license free band, such as the 2.4 GHz ISM band.
7. **Robust transmission technology:** If wireless LAN uses radio transmission, many other electrical devices can interfere with them (such as vacuum cleaner, train engines, hair dryers, etc.).Wireless LAN transceivers cannot be adjusted for perfect transmission is a standard office or production environment.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

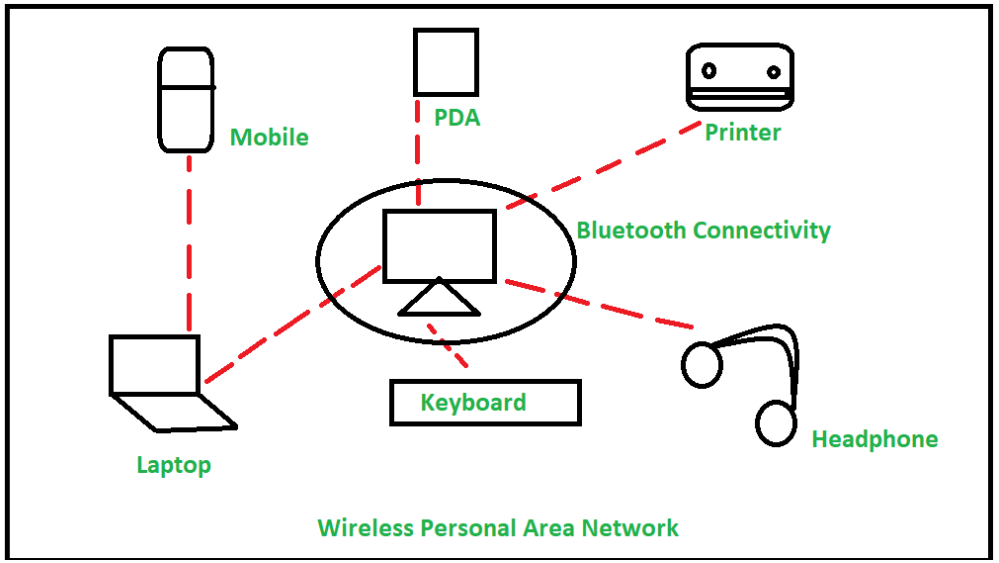
Introduction to Personal Area Network (PAN)

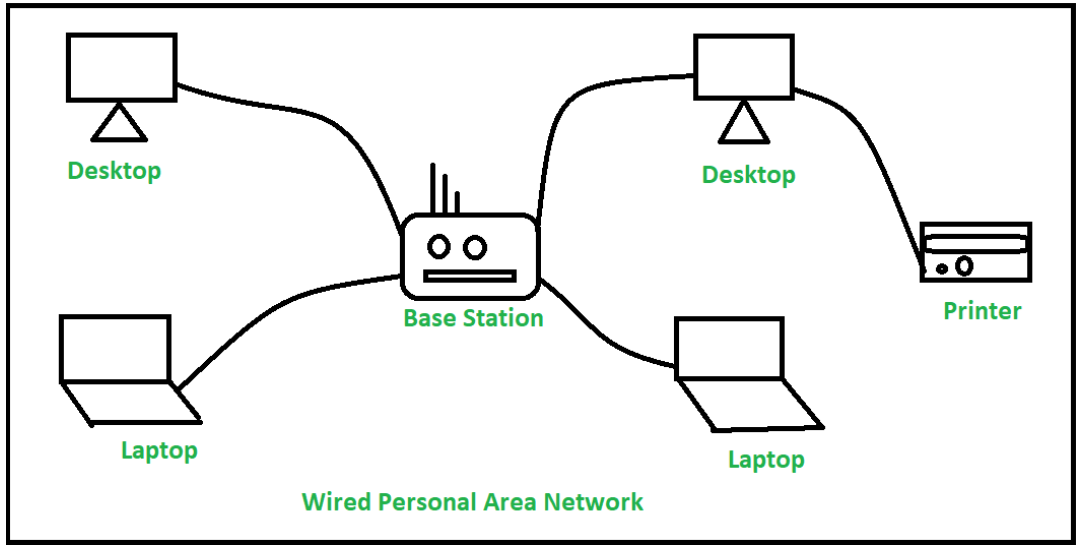
- Connects computers/devices within the range of an individual person
- Provides a network range within a person's range typically within a range of 10 meters(33 feet) it is called a Personal Area Network.
- Involves a computer, phone, tablet, printer, PDA (Personal Digital Assistant) and other and other entertainment devices like speakers, video game consoles, etc.
- Useful in the home, offices, and small network areas due to its high performance in terms of flexibility and efficiency.

Types of Personal Area Network (PAN)

Personal Area Network can be of 2 types depending upon its connection

1) **Wireless PAN:** connected through signals such as infrared, ZigBee, Bluetooth and ultra wideband, etc
2) **Wired PAN:** Wired PAN is connected through cables/wires such as Firewire or USB (Universal Serial Bus).





e.g. Body Area Network, Offline Network, Home Office, etc.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Advantages, disadvantages and Applications of PAN

Advantages

1. It needs easy setup and relatively low cost.
2. It does not require frequent installations and maintenance
3. It is easy and portable.
4. Needs fewer technical skills to use.

Disadvantages

1. Low network coverage area/range.
2. Limited to relatively low data rates.
3. Devices are not compatible with each other.
4. Inbuilt WPAN devices are a little bit costly.

Applications of PAN

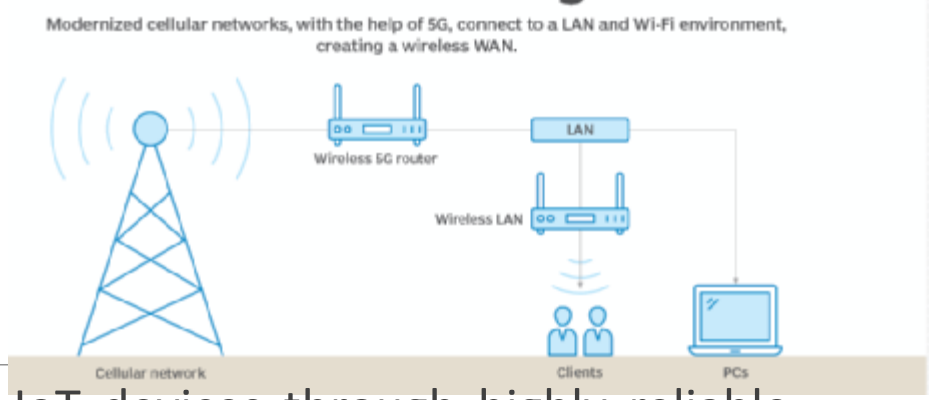
1. Home and Offices
2. Organizations and the Business sector
3. Medical and Hospital
4. School and College Education
5. Military and Defense

WMAN (Wireless Metropolitan Area Network)

- Fast communications of network within the vicinity of a metropolitan
- Put up an entire city or other related geographic area and can span up to 50km
- Designed for a larger geographical area than a LAN.
- The standard of MAN is DQDB (Distributed-Queue Dual-Bus Network) which cover up to 30 miles with the speed of 34 Mbit/s to 155 Mbit/s.
- It is more common in schools, colleges, and public services support a high-speed network backbone.
- WMAN is a certified name by the IEEE 802.16 that functioning on Broadband for its wireless metropolitan.
- It can handle thousands of user stations with prevents collisions and support legacy voice systems, voice over IP, TCP/IP.
- WMAN offer different applications with different QoS requirements.
- The technology of WMAN consist of ATM, FDDI, and SMDS (Switched Multimegabit Data Service).
- WiMAX is a term used for Wireless metropolitan area network and plinth on the IEEE 802.16.

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

WWAN (Wireless Wide Area Network)



- Connecting fixed and temporary locations, vehicles, and IoT devices through highly reliable cellular broadband
- It is a telecommunications network that connects various local area networks to each other and to headquarters, cloud servers, and elsewhere.
- Enterprise WANs allow users to share access to applications, services, and other centrally located resources.
- a Wireless WAN deploys cellular broadband — including 4G, Gigabit-Class LTE, and 5G technology — as an essential part of WAN infrastructure, connecting stores, offices, vehicles, and/or IoT devices at the network's edge.
- A Wireless WAN offers some key advantages like Highly reliable, Flexible, Scalable, Cost-effective, etc.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Comparison among types of Wireless Networks

	Wireless LAN (WLAN)	Wireless MAN (WMAN)	Wireless PAN (WPAN)	Wireless WAN (WWAN)
TYPE OF NETWORK	Local area network	Metropolitan area network	Personal area network	Wide area network
GOAL	Provide internet access within a building or limited outdoor area	Provide access outside office and home networks, typically regional	Transmit signals between devices in limited areas, typically 100 meters	Provide access outside the range of WLANs and WMANs
CONNECTIVITY	Cellular	IEEE 802.16 WiMax	Bluetooth, Zigbee and infrared	LTE

- Design Goals
  - Operational simplicity
  - Power-efficient operation
  - License-free operation
  - Global usability
  - Security
  - Safety requirements- power emission restrictions
  - Quality of service requirement
  - Compatibility with other technologies and applications

- Government regulations make specific ranges of the electromagnetic spectrum available for communication.
- A license is required to operate transmission equipment in some parts of the spectrum
  - Some parts are unlicensed

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Wireless LAN and IEEE 802.11

- Wireless LANs are those Local Area Networks that use high frequency radio waves instead of cables for connecting the devices in LAN.
- Users connected by WLANs can move around within the area of network coverage.
- Most WLANs are based upon the standard IEEE 802.11 or WiFi.
- It is a set of media access control (MAC) and physical layer (PHY) specifications for implementing WLAN computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands.
- The IEEE developed an international standard for WLANs.
- The 802.11 standard focuses on the bottom two layers of the OSI model, the physical layer (PHY) and data link layer (DLL).
- The objective is to define a medium access control (MAC) sublayer, MAC management protocols and services, and three PHYs for wireless connectivity of fixed, portable, and moving devices within a local area.
- The three physical layers are an IR base band PHY, an FHSS radio in the 2.4 GHz band, and a DSSS radio in the 2.4 GHz.

IEEE 802.11 Architecture

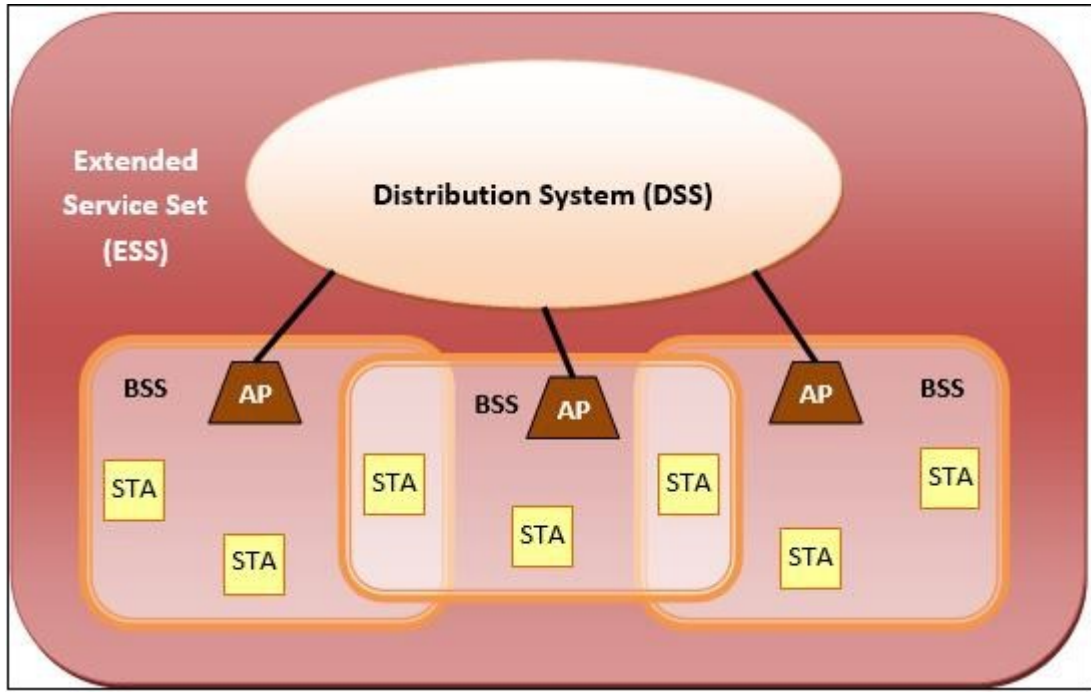
The components of an IEEE 802.11 architecture are as follows

1) Stations (STA) – Stations comprise all devices and equipments that are connected to the wireless LAN. A station can be of two types:

i. **Wireless Access Points** (WAP) – WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.

ii. **Client** – Clients are workstations, computers, laptops, printers, smartphones, etc.

- Each station has a wireless network interface controller.



IEEE 802.11 Architecture

2) Basic Service Set (BSS) –A basic service set is a group of stations communicating at physical layer level. BSS can be of two categories depending upon mode of operation:

i. **Infrastructure BSS –** Here, the devices communicate with other devices through access points.

ii. **Independent BSS –** Here, the devices communicate in peer-to-peer basis in an ad hoc manner.

3) Extended Service Set (ESS) – It is a set of all connected BSS.

4) Distribution System (DS) – It connects access points in ESS.

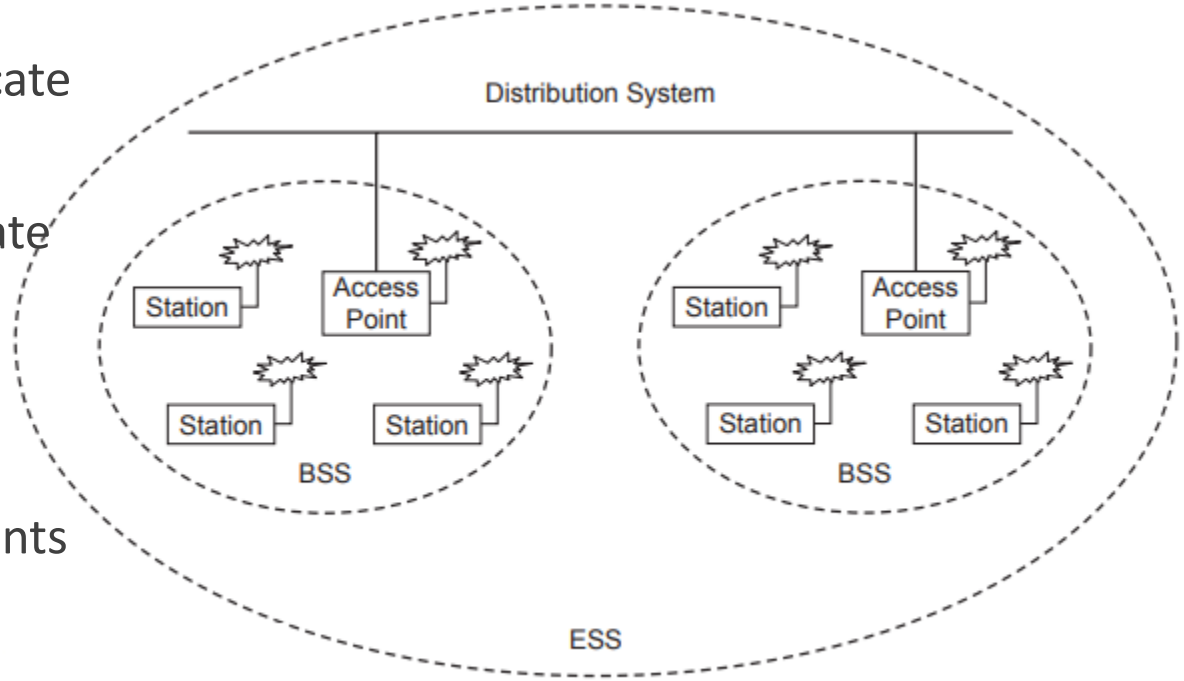
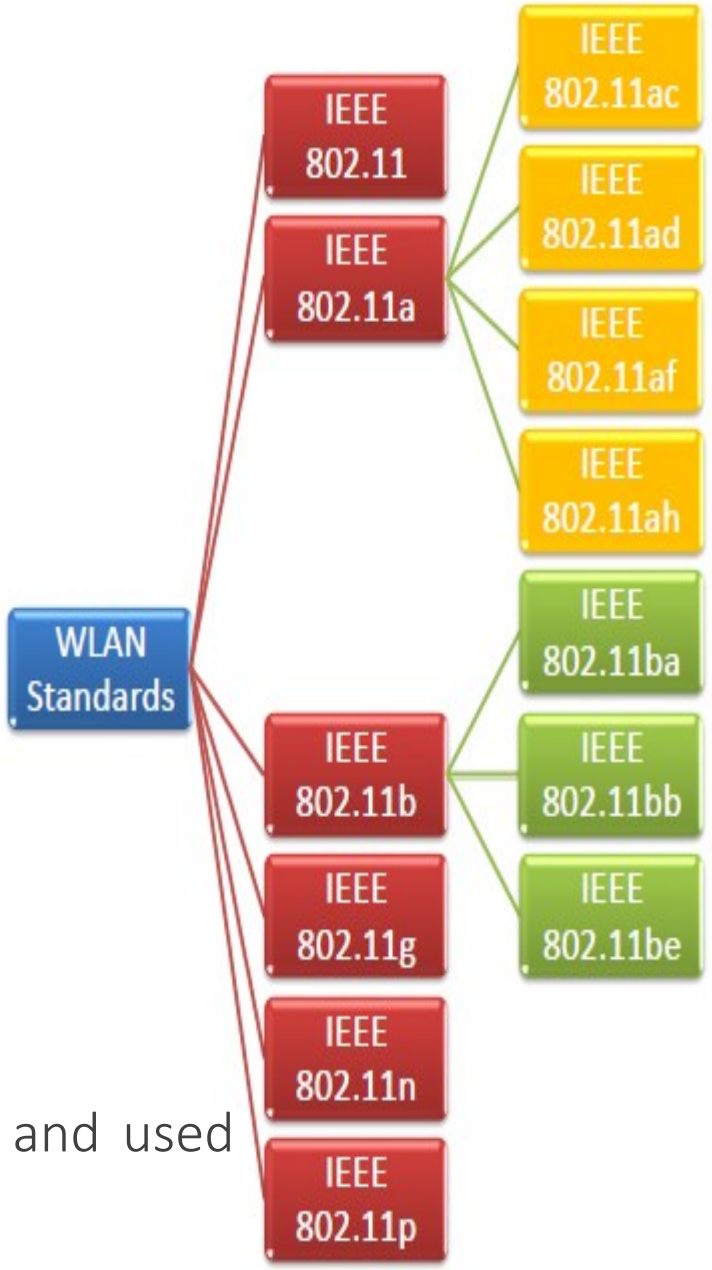


Fig : BSS and ESS configuration of IEEE 802.11 WLAN

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

IEEE 802.11 Wireless LAN Standards

- The prominent standards are 802.11, 802.11a, 802.11b, 802.11g, 802.11n and 802.11p.
- All the standards use carrier-sense multiple access with collision avoidance (CSMA/CA).
- Also, they have support for both centralized base station based as well as ad-hoc networks.



IEEE 802.11

- Original version released in 1997.
- Provided 1 Mbps or 2 Mbps data rate in the 2.4 GHz band and used either FHSS or DSSS.

IEEE 802.11 Wireless LAN Standards

IEEE 802.11a

- Was published in 1999 as a modification to 802.11, with orthogonal frequency division multiplexing (OFDM) based air interface in physical layer instead of FHSS or DSSS of 802.11.
- It provides a maximum data rate of 54 Mbps operating in the 5 GHz band.
- Besides it provides error correcting code.
- As 2.4 GHz band is crowded, relatively sparsely used 5 GHz imparts additional advantage to 802.11a.
- Further amendments to 802.11a are 802.11ac, 802.11ad, 802.11af, 802.11ah, 802.11ai, 802.11aj etc.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

IEEE 802.11 Wireless LAN Standards

IEEE 802.11b

- 802.11b is a direct extension of the original 802.11 standard that appeared in early 2000.
- It uses the same modulation technique as 802.11, i.e. DSSS and operates in the 2.4 GHz band.
- It has a higher data rate of 11 Mbps as compared to 2 Mbps of 802.11, due to which it was rapidly adopted in wireless LANs.
- However, since 2.4 GHz band is pretty crowded, 802.11b devices faces interference from other devices.
- Further amendments to 802.11b are 802.11ba, 802.11bb, 802.11bc, 802.11bd and 802.11be.

IEEE 802.11 Wireless LAN Standards

IEEE 802.11g

- 802.11g was indorsed in 2003.
- It operates in the 2.4 GHz band (as in 802.11b) and provides a average throughput of 22 Mbps.
- It uses OFDM technique (as in 802.11a).
- It is fully backward compatible with 802.11b.
- 802.11g devices also faces interference from other devices operating in 2.4 GHz band.

IEEE 802.11 Wireless LAN Standards

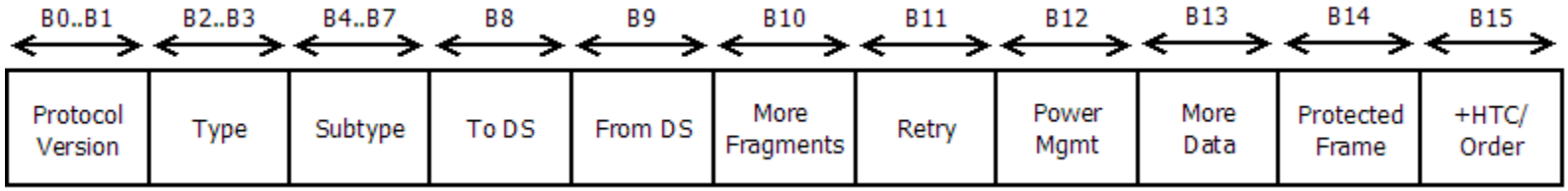
IEEE 802.11n

- 802.11n was approved and published in 2009 that operates on both the 2.4 GHz and the 5 GHz bands.
- It has variable data rate ranging from 54 Mbps to 600 Mbps.
- It provides a marked improvement over previous standards 802.11 by incorporating multiple-input multiple-output antennas (MIMO antennas).

IEEE 802.11 Wireless LAN Standards

IEEE 802.11p

- 802.11 is an amendment for including wireless access in vehicular environments (WAVE) to support Intelligent Transportation Systems (ITS).
- They include network communications between vehicles moving at high speed and the environment.
- They have a data rate of 27 Mbps and operate in 5.9 GHz band.



802.11 Frame Control

Frame Format of IEEE 802.11

The main fields of a frame of wireless LANs as laid down by IEEE 802.11 are –

Frame Control – It is a 2 bytes starting field composed of 11 subfields. It contains control information of the frame.

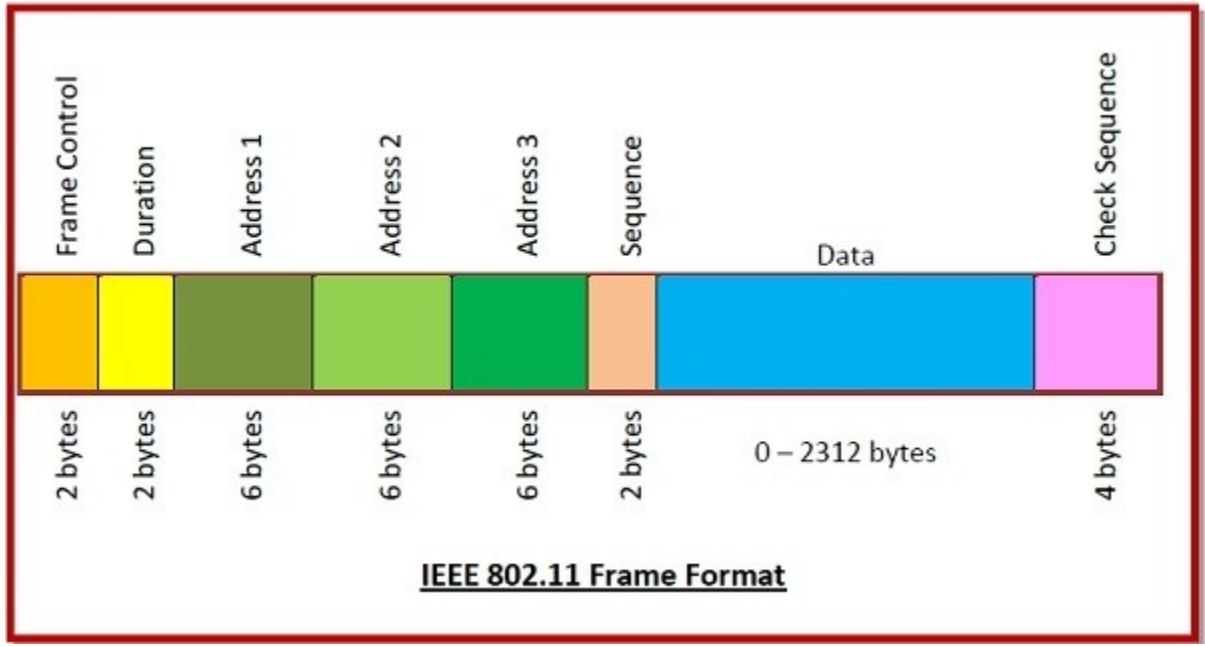
Duration – It is a 2-byte field that specifies the time period for which the frame and its acknowledgment occupy the channel.

Address fields – There are three 6-byte address fields containing addresses of source, immediate destination, and final endpoint respectively.

Sequence – It a 2 bytes field that stores the frame numbers.

Data – This is a variable-sized field that carries the data from the upper layers. The maximum size of the data field is 2312 bytes.

Check Sequence – It is a 4-byte field containing error detection information.



IEEE 802.11 Frame Format

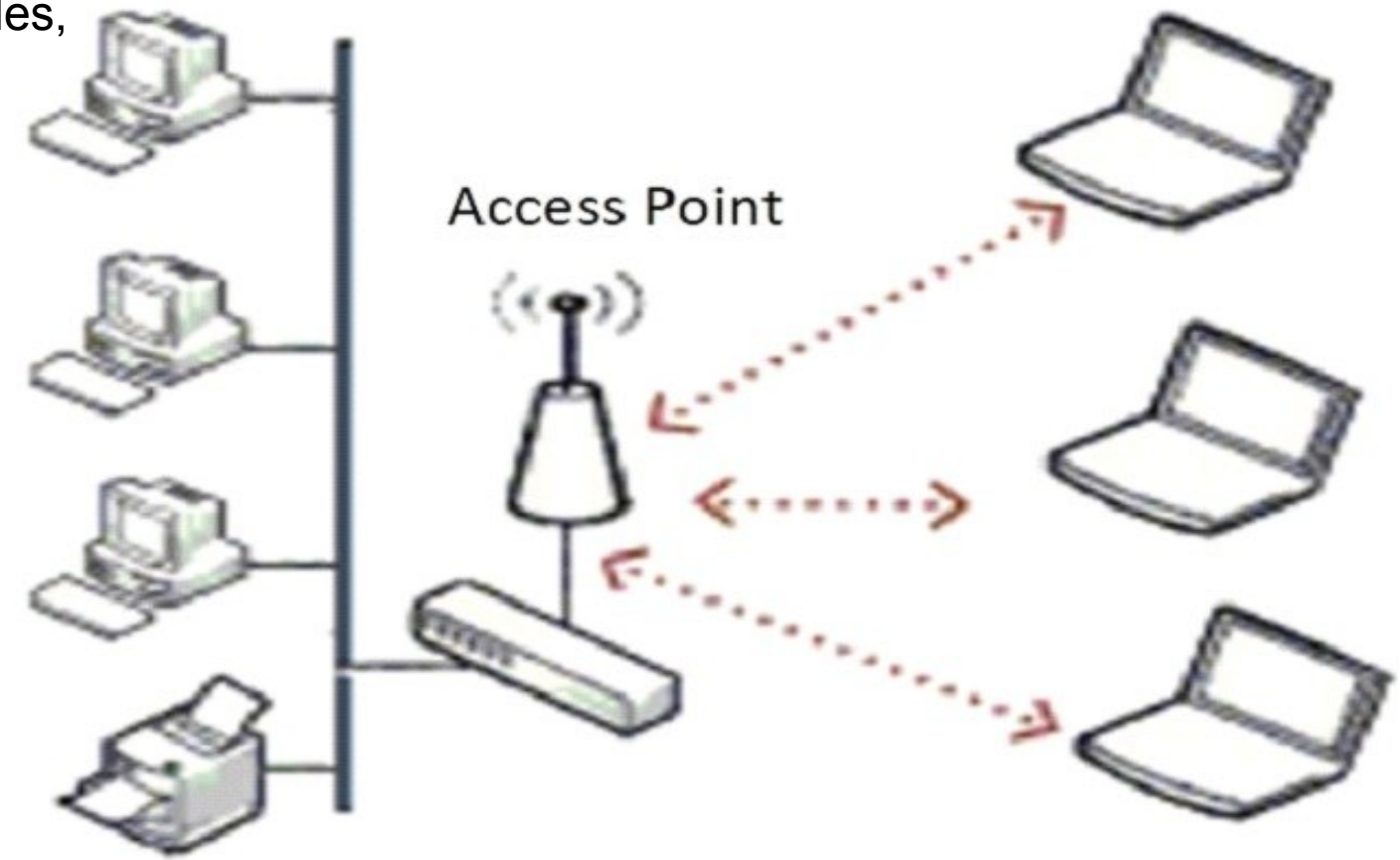
802.11 Architecture Modes

802.11 architecture uses two types of modes,

1. Infrastructure Mode
2. Ad-Hoc Mode

Infrastructure Mode

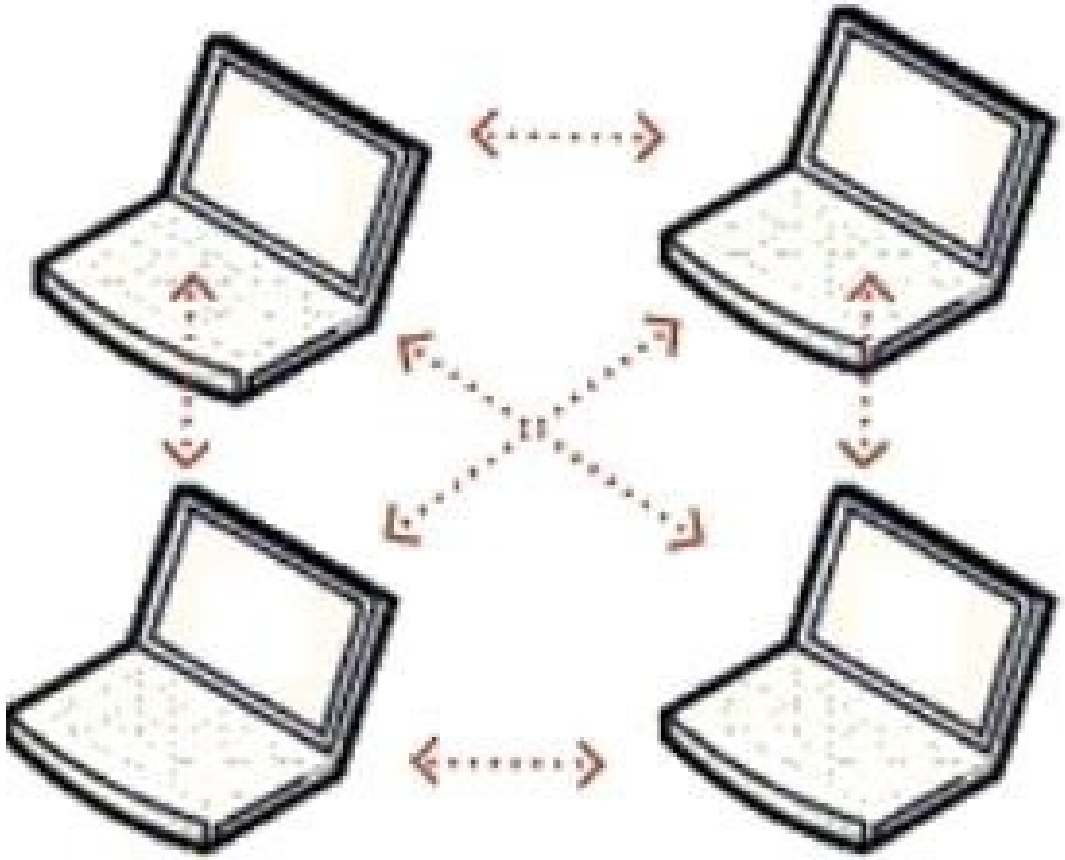
- The most popular mode used to connect clients like laptops and smartphones to another network such as company intranet or internet.
- In infrastructure mode, every client is associated with an Access point which is in turn connected to another network.
- The client sends and receives its packet via Access Point.



802.11 Architecture Modes

Ad-Hoc Mode

- Collections of computers are associated so that they can directly send frames to each other.
- There is no Access Point in Ad hoc, because Internet access is the killer application for wireless.
- Ad hoc networks are not very popular.



Parameters	Infrastructure mode	Ad-hoc mode
What is it?	In infrastructure mode, the communication occurs only between the wireless nodes and access points (AP) , but not directly between wireless nodes	In ad-hoc mode, each node communicates directly with other nodes, so no access point control is needed.
External Communication	Access points acts as a bridge to other wireless/wired network	Nodes in Ad-hoc can communicate if they are within the same range.
Physical needs	Physical infrastructure is needed	No physical infrastructure is needed.
Complexity	Designing is simple as most of the network functionality lies within AP and client is just a simple machine.	As no central co-ordination exists, we need to use decentralized MAC protocols such as CSMA/CA, with all nodes having same functionality. This shoots up the complexity and cost.
When it can't be used:	It can't be used in critical situations like disaster relief where no infrastructure is left.	It is not always fully connected as two mobile nodes may temporarily be out of range.
Applications	IEEE 802.11 & HIPERLAN2 are based on infrastructure mode.	Bluetooth is a typical ad-hoc network.
Channel Access	Most infrastructure based WLAN uses TDMA-based protocols	Most Ad-hoc based WLAN uses contention MAC protocols (e.g. CSMA)
Topology	Based on topology, one main advantage is the ability of infrastructure WLANs to provide wired network applications and services	Ad-hoc WLANs are easier to set-up and require no infrastructure

Service offered by IEEE 802.11 network

- **STA services**
  - Authentication (Open system authentication, Shared key authentication)
  - Deauthentication
  - Privacy
  - Data delivery
- **AP services/ Distribution System Services**
  - Association
  - Reassociation
  - Diassociation
  - Distribution: routing
  - Integration: if send frames through non-802.11
  - Reassociation

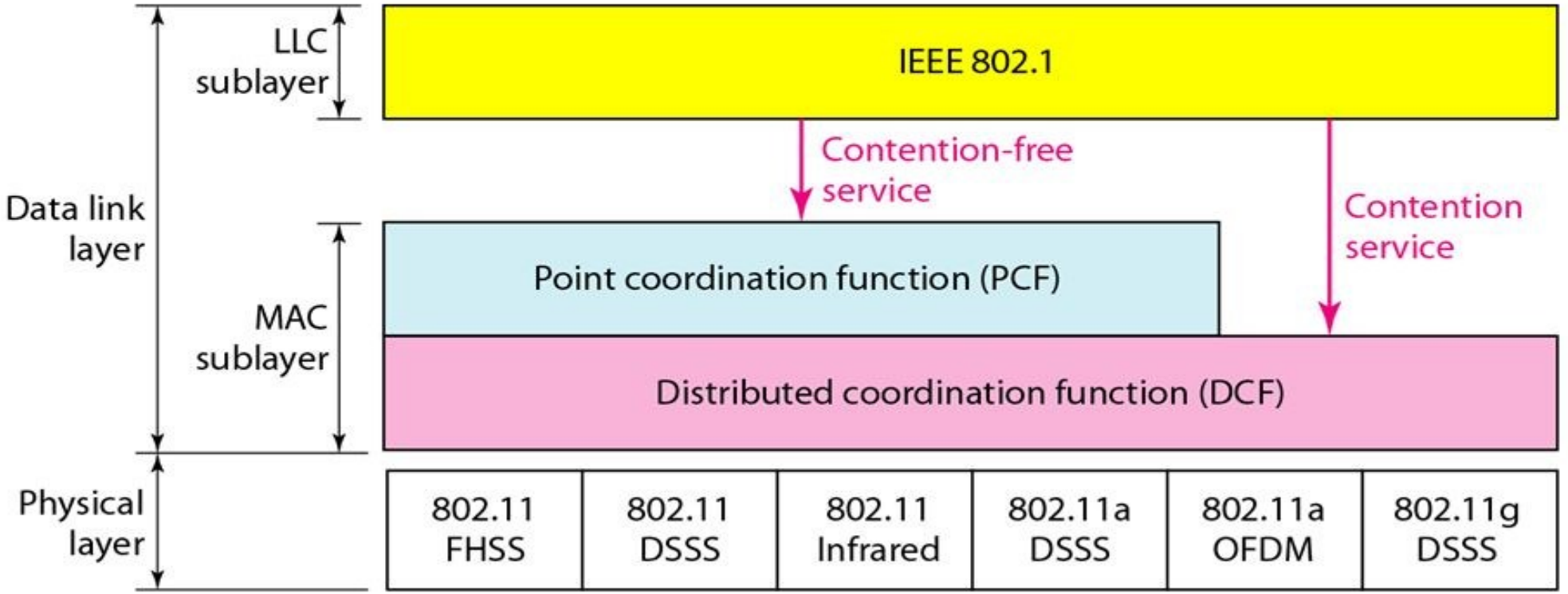
IEEE 802.11 Standard

- Commercially known as Wi-Fi (wireless fidelity)
- The 802.11 family consists of a series of half-duplex over-the-air modulation techniques that use the same basic protocol.
- 802.11 - 1997 was the first wireless networking standard in the family, but 802.11b was the first widely accepted one, followed by 802.11a, 802.11g, 802.11n and 802.11ac.
- Other standards in the family (c–f, h, j) are service amendments and extensions or corrections to the previous specifications.
- 802.11b and 802.11g use the 2.4 GHz ISM band
- Wi-Fi has a range of 46-90m

Wi-Fi Access points

Wi-Fi Router

IEEE 802.11 MAC Layer



❖ IEEE 802.11: Physical Layer

IEEE 802.11 MAC				
802.11	802.11a	802.11b	802.11g	802.11n
1-2 Mbps 2.4 GHz FHSS DSSS IR	6-54 Mbps 5 GHz OFDM	1-11 Mbps 2.4 GHz DSSS	6-54 Mbps 2.4 GHz OFDM DSSS	7.2-150 Mbps 2.4, 5 GHz OFDM

❖ **Physical Layer**

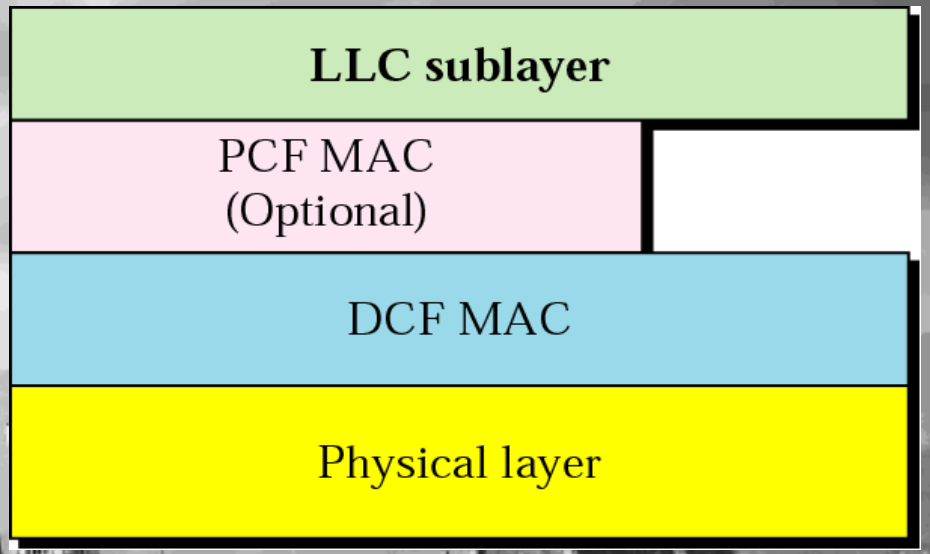
- Physical medium dependent sublayer (PMD) - encoding, decoding and modulations of signals.
- Physical layer convergence protocol (PLCP) - provides services to MAC layer, clear channel assessment signal (carrier sense) - CSMA/CA

- 3 versions: 2 radio (typ. 2.4 GHz), 1 IR
  - data rates 1 or 2 Mbit/s
- **FHSS (Frequency Hopping Spread Spectrum)** : spreading, despreading, signal strength, GFSK
- **DSSS (Direct Sequence Spread Spectrum) :** each data bit with n bits using a spreading code, DBPSK, DQPSK
- **Infrared:** 850-950nm, diffuse light, typ. 10 m range , PPM
  - carrier detection, energy detection, synchronization

❖ IEEE 802.11: MAC Layer

Traffic services:

- Asynchronous Data Service (mandatory) :
  - exchange of data packets based on “best-effort”
  - support of broadcast and multicast
- Time-Bounded Service (optional):
  - implemented using PCF (Point Coordination Function)



- **Point Coordination Function (PCF)** – (controlled access): used in infrastructure network, implemented to provide real-time services.
- When the PCF is in operation, the AP controls medium access and avoids simultaneous transmissions by the nodes.
- **Distributed Coordination Function (DCF)** – (random access): uses CSMA/CA version.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Overview of IEEE 802.15-Wireless Specialty Networks (WSN)

- Working group for **Wireless Specialty Networks** (WSN)
- Focuses on the development of consensus standards for PAN or short distance wireless networks e.g. WPANs, Bluetooth, IoT networks, mesh networks, body area networks, wearable', visible light communications and autonomous vehicles.
- Allows these devices to communicate and interoperate with one another.
- 802.15 is also the first organization to produce global standards for OWC (Optical Wireless Communications)
- The IEEE 802.15 Working Group is part of the 802 Local and Metropolitan Area Network Standards Committee of the IEEE Computer Society
- The IEEE Project 802.15.1 has derived a wireless personal area network standard based on the Bluetooth v1.1 Foundation Specifications.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

IEEE 802.15-Standards / Task groups

- **IEEE 802.15.1:** Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPAN)
- **IEEE 802.15.2:** Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Bands
- **IEEE 802.15.3:** High Data Rate Wireless Multi-Media Networks
- **IEEE 802.15.4:** Low-Rate Wireless Networks (But long battery life and very low complexity)
- **IEEE 802.15.5:** Mesh Topology Capability in Wireless Personal Area Networks (WPANs)
- **IEEE 802.15.6:** Wireless Body Area Networks (low power and short range wireless standard)
- **IEEE 802.15.7:** Visible Light Communication, Short-Range Optical Wireless Communications (wireless networking specification for home devices)
- **IEEE 802.15.8:** Peer Aware Communications
- **IEEE 802.15.9:** Key Management Protocol
- **IEEE 802.15.10:** Layer 2 Routing, Practice for Routing Packets in IEEE 802.15.4 Dynamically Changing Wireless Networks

Overview of IEEE 802.16- WiMAX

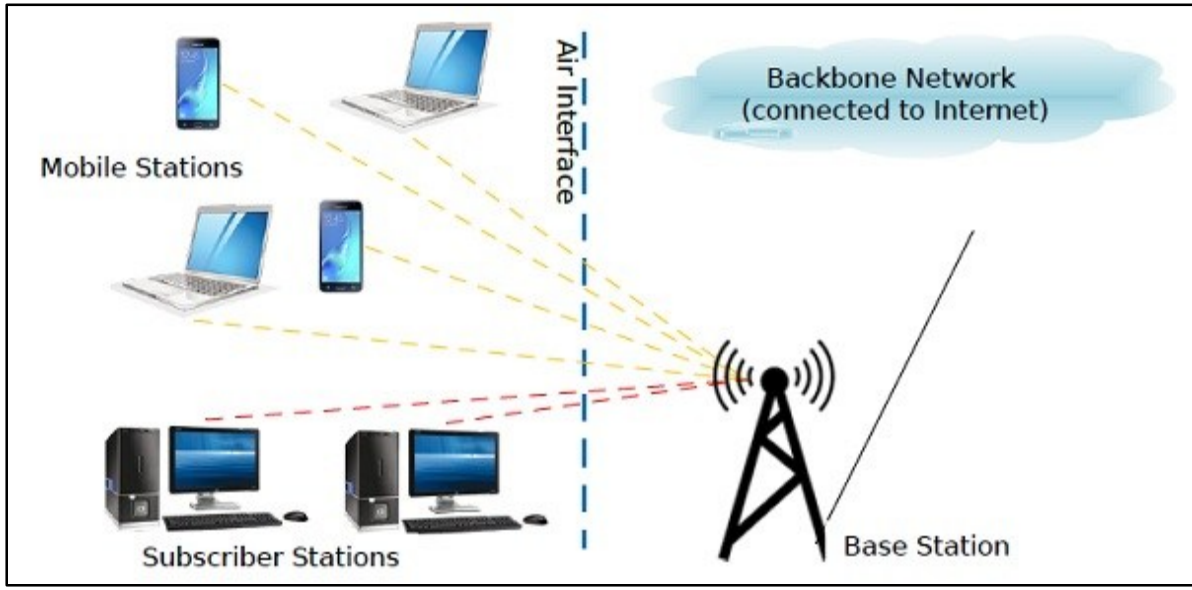
- Its a set of standards defined by IEEE that lays down the specifications for wireless broadband technology.
- Commercialized as Worldwide Interoperability for Microwave Access (WiMAX) that is responsible for delivery of last mile wireless broadband access.
- Standards for both physical layer as well as medium access control (MAC) layer for WiMAX.
- Initially provided data rates of 30 – 40 Mbps.
- The updated version (Year 2011) provides up to 1 Gbps data rates for fixed stations.
- It operates in the frequency band of 2 GHz to 11 GHz.
- The bandwidth is dynamically allocated as per user requirements.

IEEE 802.16- Architecture

Two types of user stations are there

- **Subscriber stations** – They are stationary in some fixed location. For example, broadband Internet for homes and offices.
- **Mobile stations** – They receive service while they are in motion within the range of WiMAX. For example, a WiMAX equipped vehicle.

- A user station connects wirelessly to the base station, forming the last wile of the broadband network.
- The base station is connected to the backbone network of the broadband service provider.
- The backbone network is connected to Internet.



Architecture

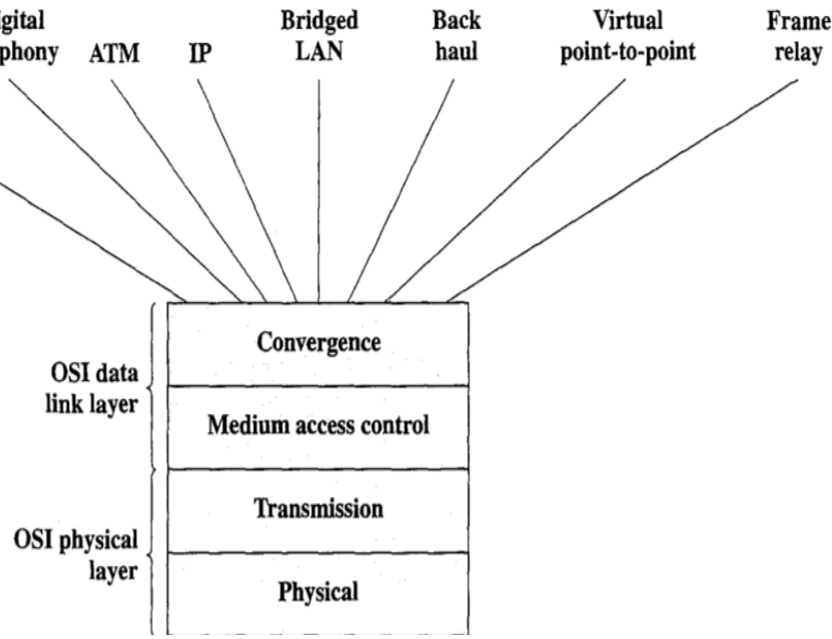
IEEE 802.16 Protocol Stack/ Architecture

Physical Layer :

- The two popular services provided as fixed WiMAX and mobile WiMAX.
- They operate in the licensed spectrum below 11 GHz.
- Fixed WiMAX was released in 2003 and uses OFDM; while mobile WiMAX was released in 2005 and uses scalable OFDM.
- Encoding/decoding of signals
- Preamble generation/removal (for synchronization)
- Bit transmission/reception

Transmission layer:

- The physical layer of the 802 model includes a specification of the transmission medium and the frequency band.
- Considered "below" the lowest layer of the OSI model.
- However, the choice of transmission medium and frequency band is critical in wireless link design, and so a specification of the medium is included.
- The 802.16 physical layer is concerned with these medium-dependent issues, and the transmission layer is concerned with the how data is to be transmitted



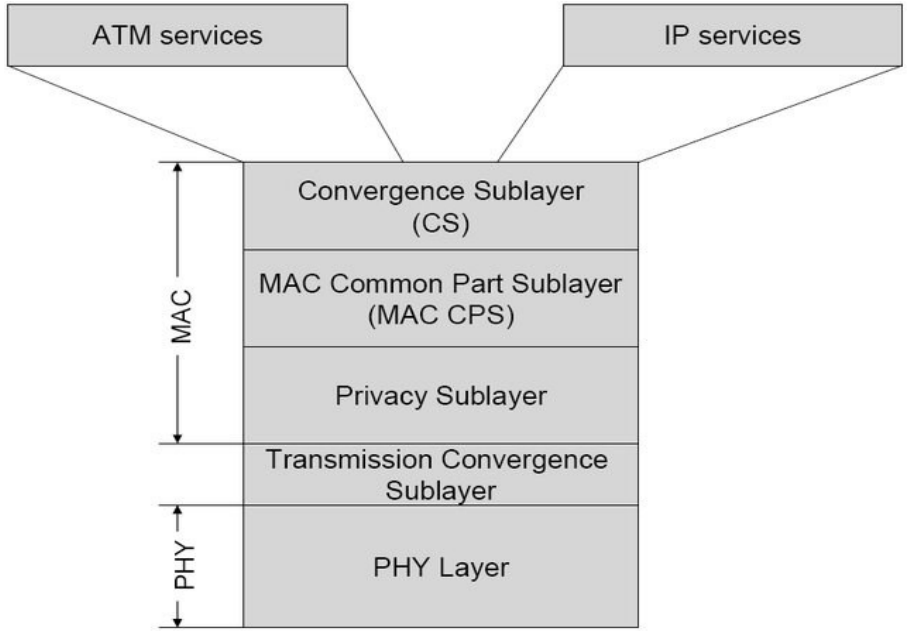
Protocol Architecture

IEEE 802.16 Protocol Stack/ Architecture

- **Data Link Layer** − The data link layer is subdivided into three sub layers as Security sublayer, MAC common sublayer, Service specific convergence sublayer
- **Security sublayer** − This is the bottommost layer and is concerned with security and privacy of the wireless network. It deals with encryption, decryption and key management.
- **Medium Access control (MAC) layer:**

Above the physical and transmission layers are the functions associated with providing service to subscribers. They include:

- On transmission, assemble data into a frame with address and error detection fields.
- On reception, disassemble frame, and perform address recognition and error detection.
- Govern access to the wireless transmission medium.
- The MAC sublayer is concerned with channel management.
- The channel management is connection oriented, a feature that plays due to which quality of service (QoS) guarantees are given to the subscriber. The base station controls the system.

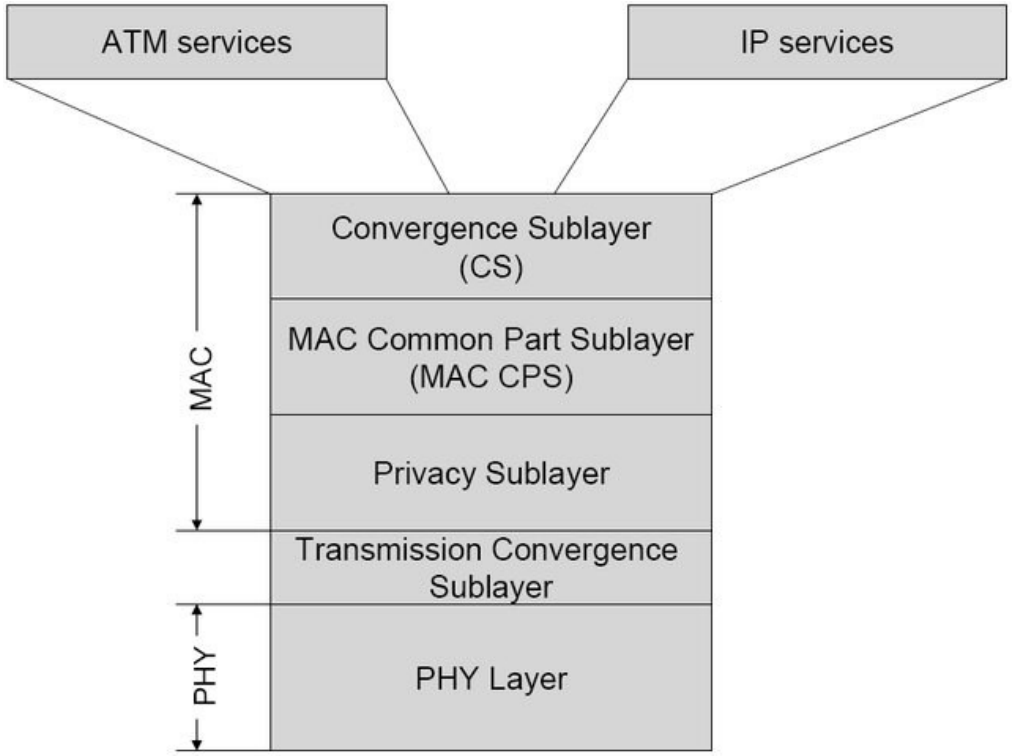


Protocol Architecture

Medium Access control (MAC) layer:

- It schedules the channels from base station to the subscriber (downlink channels) and also manages the channels from the subscriber to the base station (uplink channels).

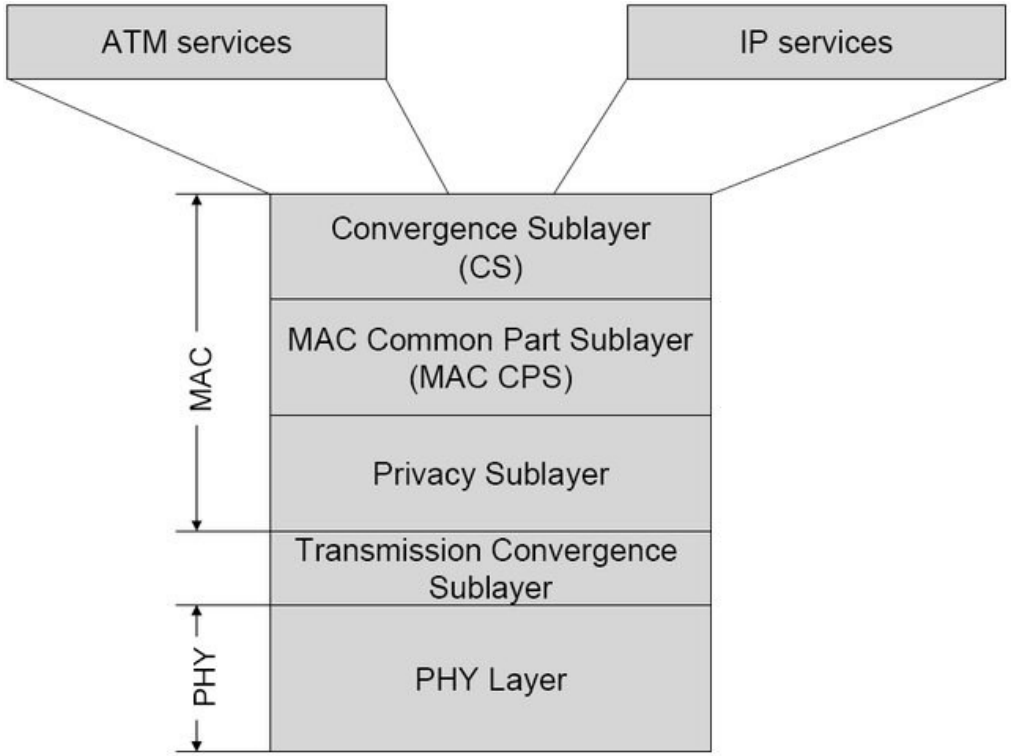
- The protocol at this layer, between the base station and the subscriber station, is responsible for sharing access to the radio channel.
- Defines how and when a base station or subscriber station may initiate transmission on the channel.
- This is because some of the layers above the MAC layer, such as ATM, require specified service levels (QoS), the MAC protocol must be able to allocate radio channel capacity so as to satisfy service demands.
- In the downstream direction (base station to subscriber stations), there is only one transmitter and the MAC protocol is relatively simple.
- In the upstream direction, mulitiple subscriber stations are competing for access, resulting in a more complex MAC protocol.



Protocol Architecture

Convergence Layer:

- This is equivalent to logical link control layer of other systems. It provides the required services and interface to network layer.
- Above the MAC layer, is a convergence layer that provides functions specific to the service being provided. A convergence layer protocol may do the following:
  - ✓ Encapsulate PDU (protocol data unit) framing of upper layers into the native 802.16 MACIPHY frames.
  - ✓ Map an upper layer's addresses into 802.16 addresses.
  - ✓ Translate upper layer QoS parameters into native 802.16 MAC format.
  - ✓ Adapt the time dependencies of the upper layer traffic into the equivalent MAC service.

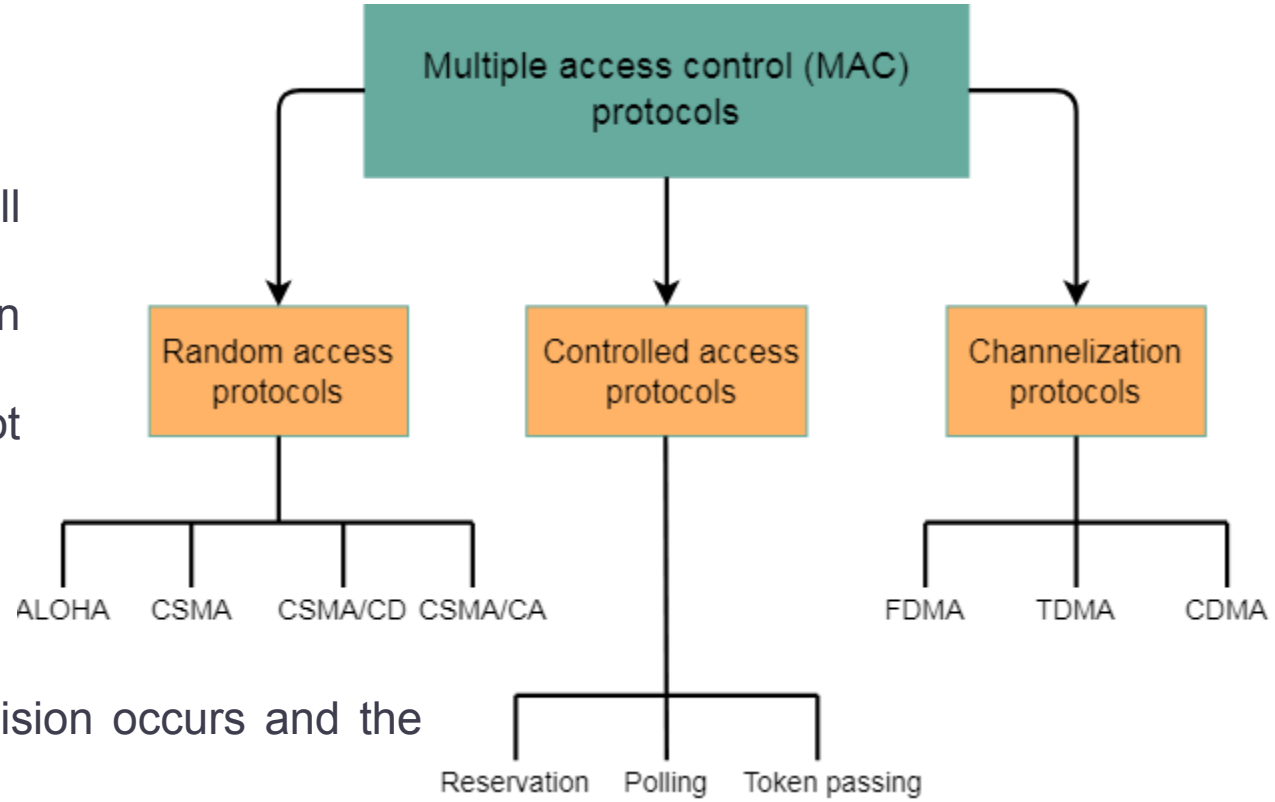


Protocol Architecture

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

MAC Protocols

MAC Protocols



Random access protocol

- No station has a higher priority than another station, all are equal.
- No predetermined time for sending data; it depends on the channel's status.
- The order of the stations transmitting data is not predefined.
- It is sub-divided into the following:

- **ALOHA:**
  - ✓ A station can transmit whenever data is available.
  - ✓ If another station broadcasts at the same time, collision occurs and the packets are lost.
  - ✓ Two versions: pure ALOHA and slotted ALOHA.

- **CSMA:** Each node must monitor the carrier for some time before attempting to deliver data packets.
  - ✓ Each node on the bus gets an equal chance to send the data across the network.

1. **CSMA/CD:** Used for carrier transmission via collision detection. Used in early Ethernet technology for LAN.
2. **CSMA/CA:** Used for carrier transmission using collision avoidance. It has wide application in wireless technology.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

MAC Protocols

Controlled access protocol

All the stations communicate with each other to determine which station has the authority to send data in order to avoid collision.

1. **Reservation:** A station reserves the transmission channel before transmitting the data packets.
2. **Polling:**
   - ✓ One device is marked as the primary station (controller) and the other as the secondary station.
   - ✓ The controller is responsible for all data transfers.
3. **Token passing:**
   - ✓ Stations are logically connected in the form of a ring.
   - ✓ To avoid collisions, this media access control technique uses token passing.
   - ✓ The only computer allowed to communicate is the one with the token.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

MAC Protocols

Channelization Protocol

Channelization is a multiple-access mechanism in which the link's available bandwidth is shared among several stations as per time, frequency, or code.

- **FDMA:** Frequency Division Multiple Access
  - ✓ The available bandwidth is split into various frequency bands.
  - ✓ To prevent crosstalk and noise, guard bands are also used to ensure that no two bands coincide.
- **TDMA:** Time Division Multiple Access
  - ✓ Bandwidth is divided across several stations.
  - ✓ Time is divided into slots and stations broadcast data in their allotted slots to prevent collisions.
- **CDMA:** Code Division Multiple Access
  - ✓ All signals are broadcast concurrently on one channel.
  - ✓ It eliminates the concept of time and bandwidth division.
  - ✓ It is a code-based communication technique.
  - ✓ CDMA codes are utilized to differentiate between various users.

The CSMA/CD algorithm does not work in wireless LANs for three reasons:

1. Wireless hosts do not have enough power to send and receive at the same time.
2. The hidden station problem prevents collision detection.
3. The distance between stations can be great.

How does CSMA/CA work?

https://www.educative.io/answers/how-does-csma-ca-work

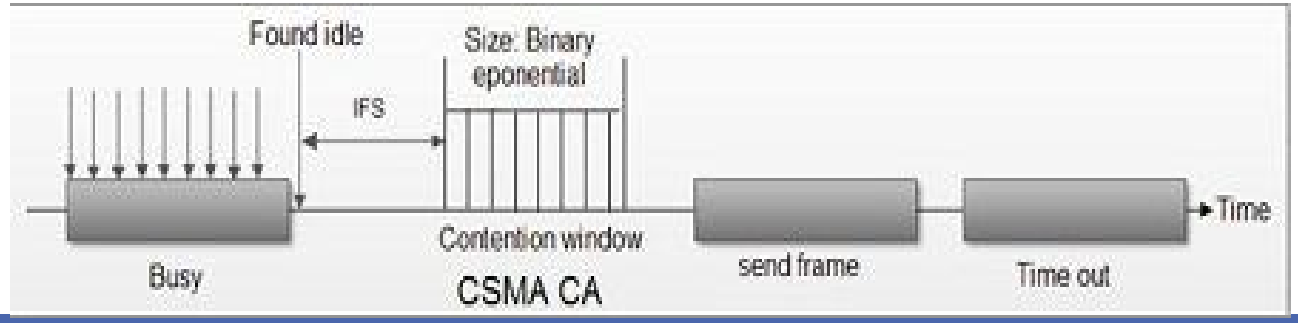
How does CSMA/CA work?

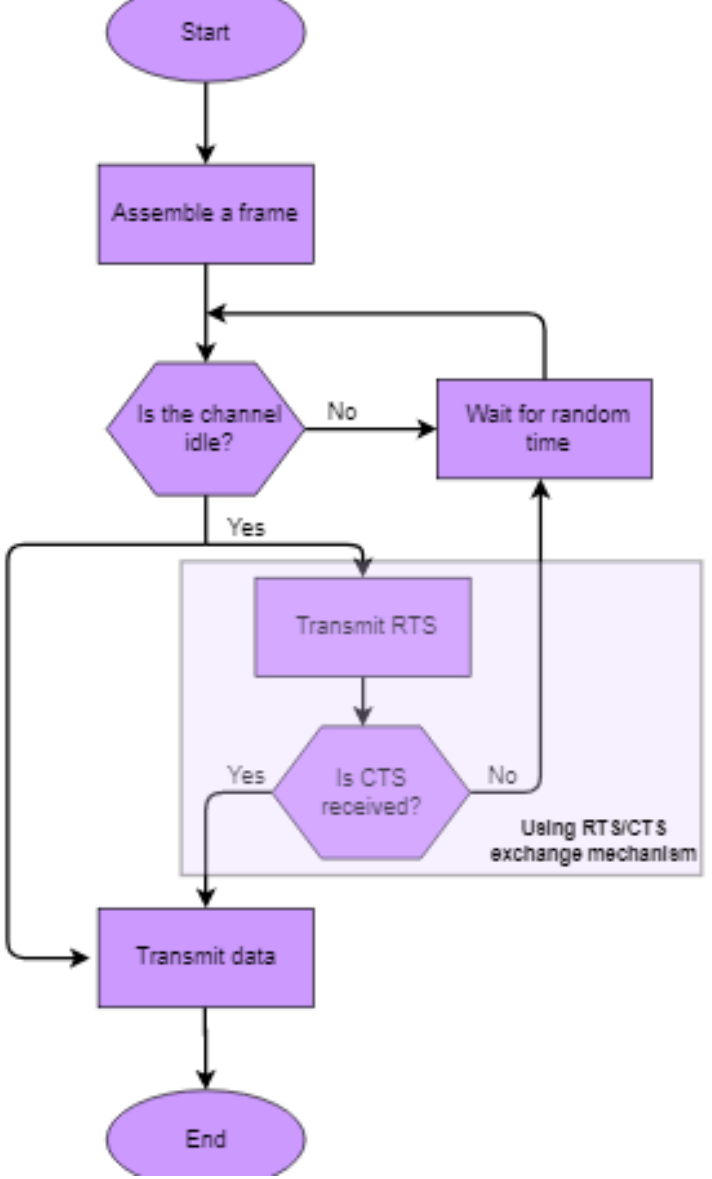
- The "**Listen Before Talk**" (LBT) principle is the foundation of CSMA/CA.
- Before the station can begin transmitting, the line must check to verify if it is free. However, this is only the first action.
- Collisions are effectively prevented with the help of additional functions that are part of the procedure.
- CSMA/CA avoids the collisions using three basic techniques.

  (i) Interframe space

  (ii) Contention window

  (iii) Acknowledgements





CSMA/CA workflow with RTS/CTS exchange mechanism

How does CSMA/CA work?

- The "**Listen Before Talk**" (LBT) principle is the foundation of CSMA/CA.
- Before the station can begin transmitting, the line must check to verify if it is free. However, this is only the first action.
- Collisions are effectively prevented with the help of additional functions that are part of the procedure.
- CSMA/CA avoids the collisions using three basic techniques.

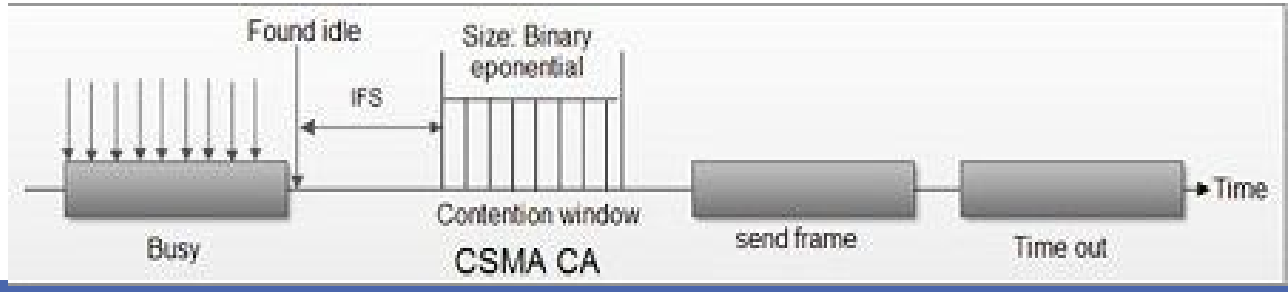
  (i) Interframe space

  (ii) Contention window

  (iii) Acknowledgements

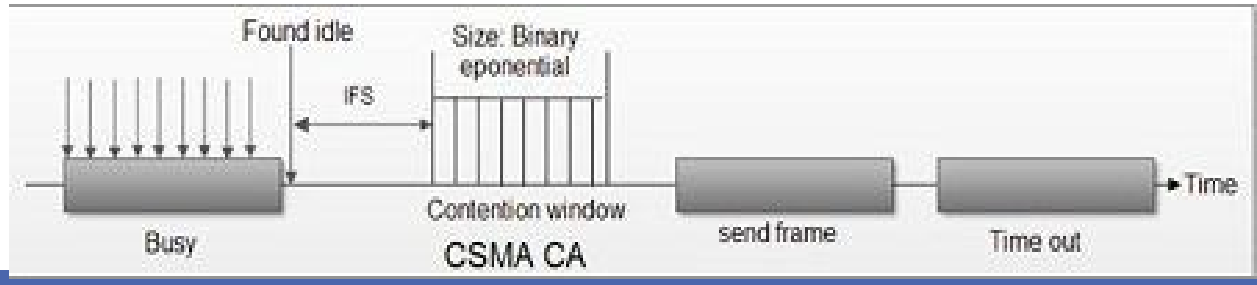
1. Interframe Space (IFS)

- Whenever the channel is found idle, the station does not transmit immediately.
- It waits for a period of time called interframe space (IFS).
- IFS is the time period between completion of the transmission of the last frame and starting transmission of the next frame apart from the variable back-off period.
- When channel is sensed to be idle, it may be possible that same distant station may have already started transmitting and the signal of that distant station has not yet reached other stations.
- The purpose of IFS time is to allow this transmitted signal to reach other stations.
- If after this IFS time, the channel is still idle, the station can send, but it still needs to wait a time equal to contention time.
- IFS variable can also be used to define the priority of a station or a frame.



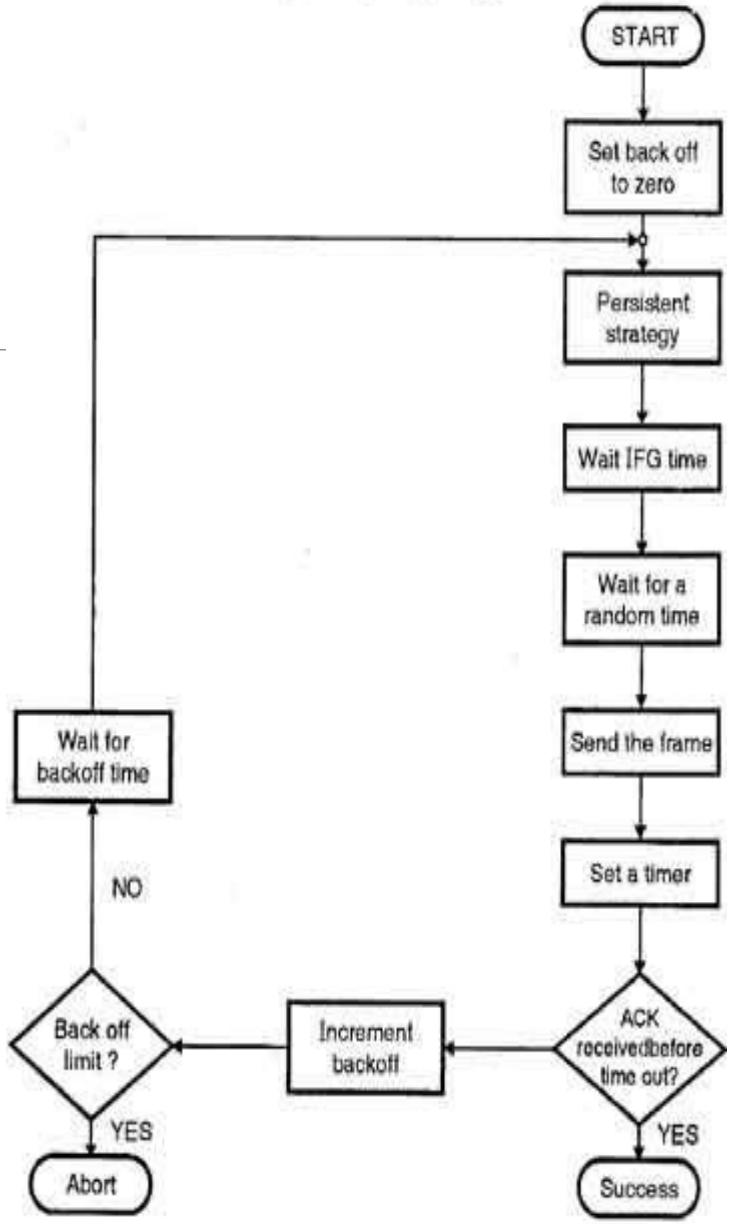
2. Contention window

- It is an amount of time divided into slots.
- A station that is ready to send, chooses a random number of slots as its wait time.
- The number of slots in the window changes according to the binary exponential back-off strategy. It means that it is set of one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.
- In contention window the station needs to sense the channel after each time slot.
- If the station finds the channel busy, it does not restart the process. It just stops the timer & restarts it when the channel is sensed as idle.



3. Acknowledgement

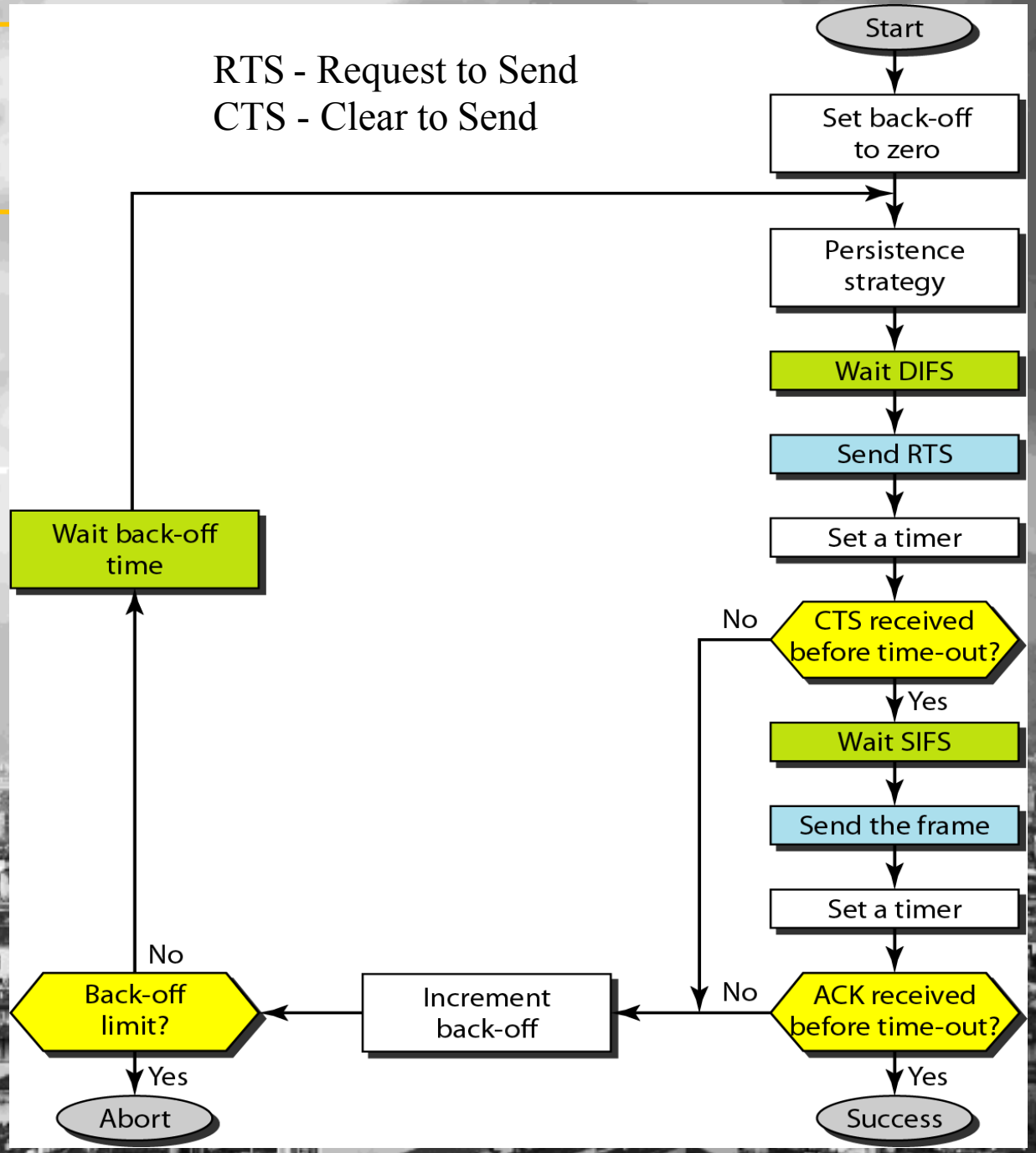
- Despite all the precautions, collisions may occur and destroy the data.
- The positive acknowledgment and the time-out timer can help guarantee that receiver has received the frame.



CSMA/CA Procedure

CSMA/CA Operation

- Inter-frame spacing refers to the time interval between the transmission of two successive frames by any station.
- There are four types of IFS: SIFS, PIFS, DIFS, and EIFS.
- **Short inter-frame spacing (SIFS)**: the shortest of all the IFSs and denotes highest priority to access the medium. It is defined for short control messages such as acknowledgments for data packets and polling responses.
- **PCF** (Point coordination function) **inter-frame spacing (PIFS):** is the waiting time whose value lies between SIFS and DIFS. This is used for real-time services.
- **DCF inter-frame spacing (DIFS)** is used by stations that are operating under the Distributed coordination function (DCF) mode to transmit packets. This is for asynchronous data transfer within the contention period.
- **Extended inter-frame spacing (EIFS)** is the longest of all the IFSs and denotes the least priority to access the medium.

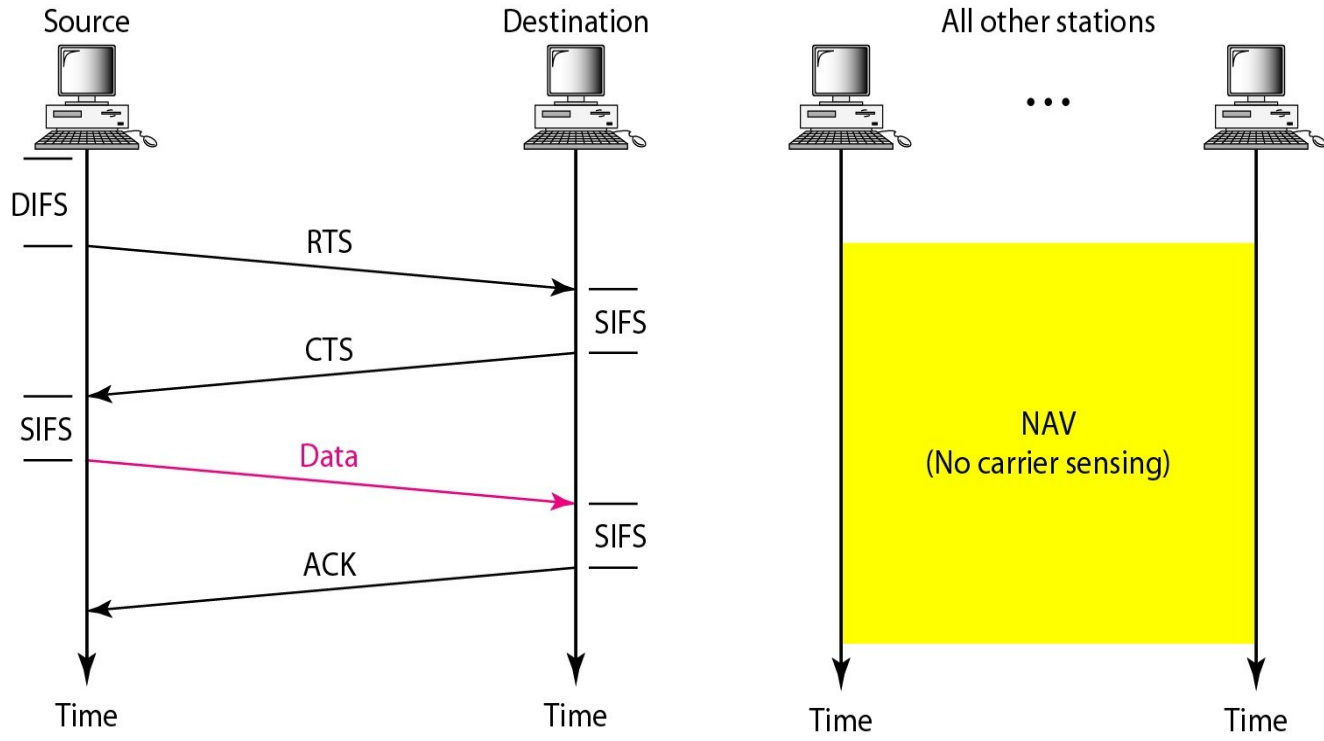


Network Allocation Vector (NAV)

How do other station defer sending their data if one station acquires access?

- NAV is a virtual carrier sensing mechanism that forms an important part of CSMA/CA

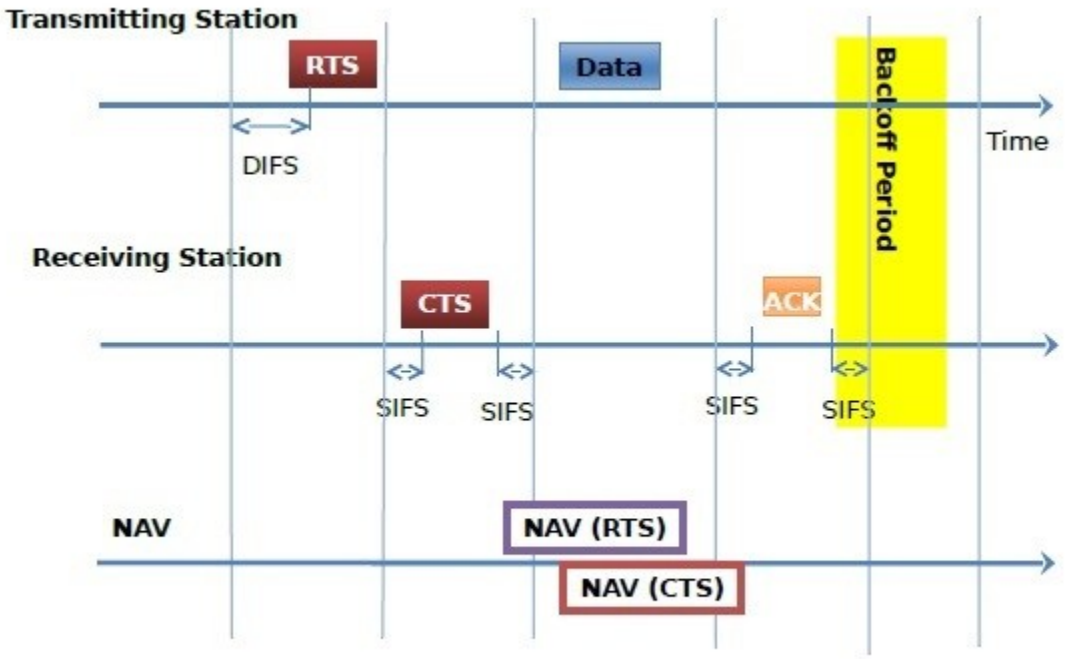
- The network allocation vector can be considered as a counter that counts down to zero.
- The maximum NAV duration is the transmission time required by frame, which is the time for which the channel will be busy.
- At the start of transmission of a frame, the NAV value is set to its maximum.
- A non-zero value indicates that the channel is busy, and so no station contends for it.
- When the NAV value decrements to 0, it indicates that the channel is free and the other stations can contend for it.



NAV in wireless data communication

The steps in transmission as

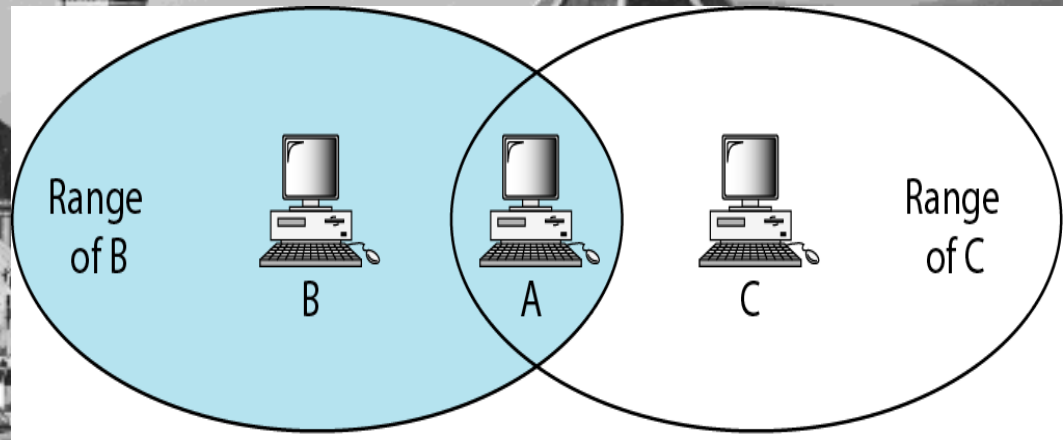
- The transmitting station waits for a time equal to distributed inter – frame space (DIFS) and issues a request to send (RTS) if the channel is clear.
- After sending RTS, a NAV (RTS) is initialized, so that no other station attempts to transmit.
- The receiving station waits for a short inter – frame space (SIFS) and issues a clear to send (CTS).
- With the CTS, a NAV (CTS) is initialized.
- The sender waits for a SIFS and transmits its data frame.
- On receiving the data frame, the receiver waits for a SIFS and sends an acknowledgement frame (ACK).
- Both the NAV values decrements to 0 during this time period.
- The stations wait for a SIFS and a backoff period before contending for the channel.



NAV in wireless communication

Hidden Station Problem

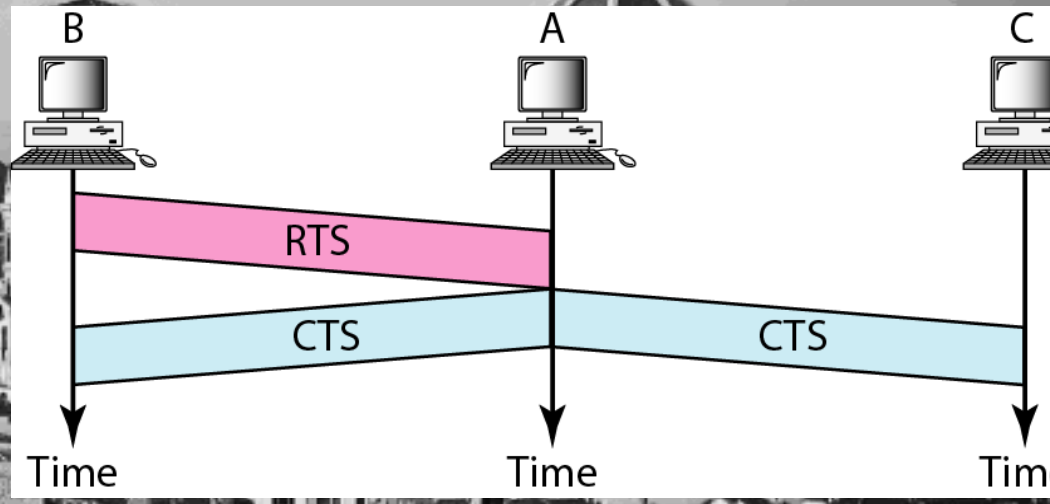
- The transmission range of B reaches A but not C. Similarly, the range of C reaches A but not B. Also the range of A reaches both B and C.
- Now, the node B starts to send something to A and C doesn't receive this transmission.
- Now C also wants to send data to A and senses the carrier. As it senses it to be free, it also starts sending to A.
- **Hidden station problem occurs when two nodes that are outside each other's range performs simultaneous transmission to a node that is within the range of each of them resulting in a collision.**
- That means the data from both parties B and C will be lost during the collision.
- Hidden nodes mean increased probability of collision at receiver end.
- One solution to avoid this is to have the channel sensing range much greater than the receiving range.
- Another solution is to use the Multiple Access with Collision Avoidance (MACA).



B and C are hidden from each other with respect to A.

Hidden Station Problem_Solution

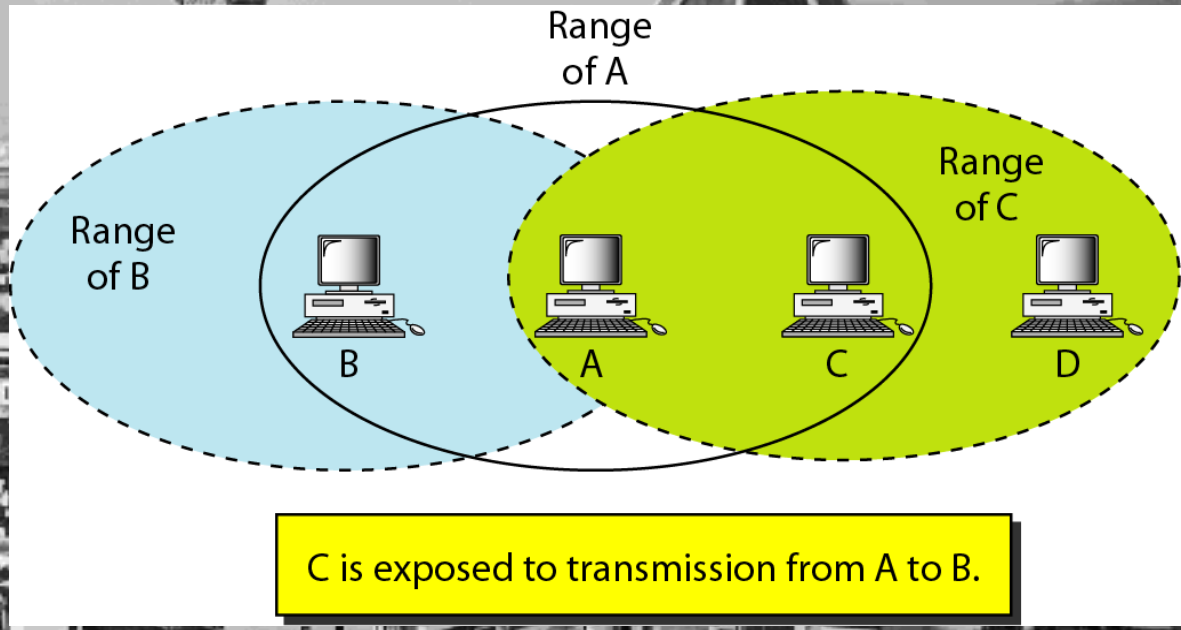
- Hidden Station Problem (HSP) can be prevented by using handshake frames.
- In the below shown diagram, RTS message from B reaches A but not C.
- However, both B and C are within range of A.
- CTS message containing duration of data transmission from B to A, reaches C.
- Thus C knows some hidden station is using channel and does not transmit until that duration is over.



- The CTS frame in CSMA/CA handshake can prevent collision from a hidden station.

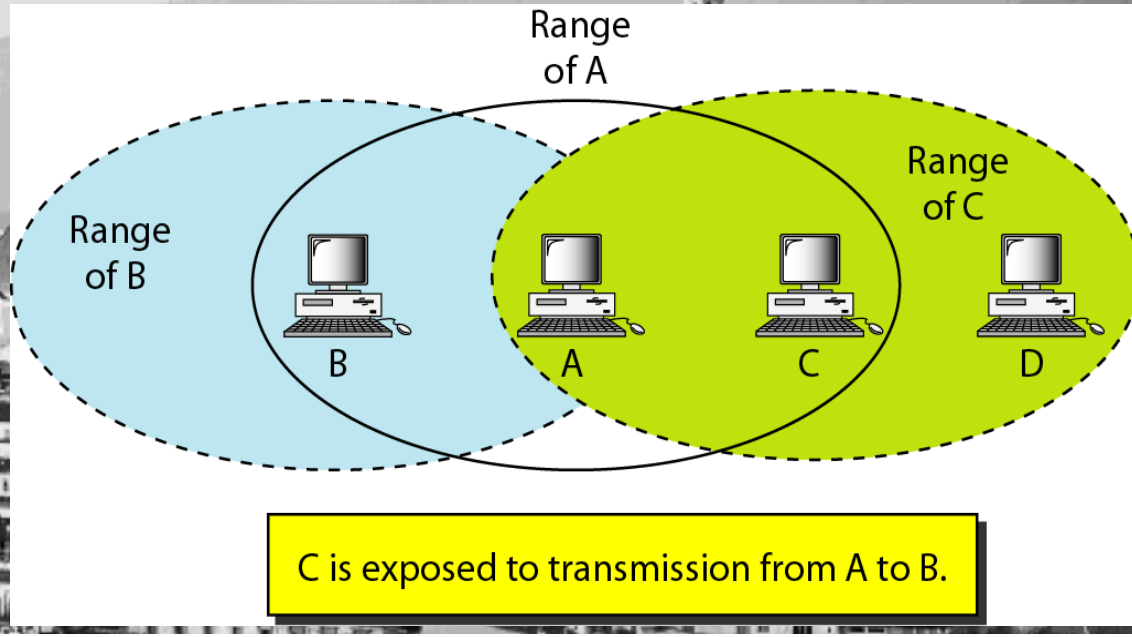
Exposed Station Problem

- The exposed terminal problem is a frequent difficulty.
- It happens when a wireless node cannot transfer data because another node that is outside its communication range is sending data to another node that is inside it.
- Throughput and network performance may suffer as a consequence.
- This happens when a station can be seen by a wireless access point but not by other stations that are connected to the access point.



Exposed Station Problem

- Lets Assume, there are four stations with the names A, B, C, and D, where A and C are transmitters and B and D are receivers.
- The stations are set up so that the two emitters A and C can hear each other but the two receivers B and D cannot hear each other over radio waves.
- Imagine a situation wherein the A node is currently sending some data to node B, transmission from A to B is happening.
- Now the other node C which is right now free want to send data to some node D, which is outside the range of A and B.
- Now before starting transmission it senses the carrier and realizes that the carrier is busy (due to interference of A's signal).
- As a result, C ceases attempting to transmit to D after mistakenly assuming that the above transmission will cause interference.
- Hence, the C node postpones the transmission to D until it detects the medium to be idle.
- However, since the communication from C to D is outside of A's range, interference would not have happened. Known as the exposed terminal issue.
- Exposed node means denied channel access unnecessarily which ultimately results in under utilization of bandwidth resources.
- It also results in wastage of time resource.

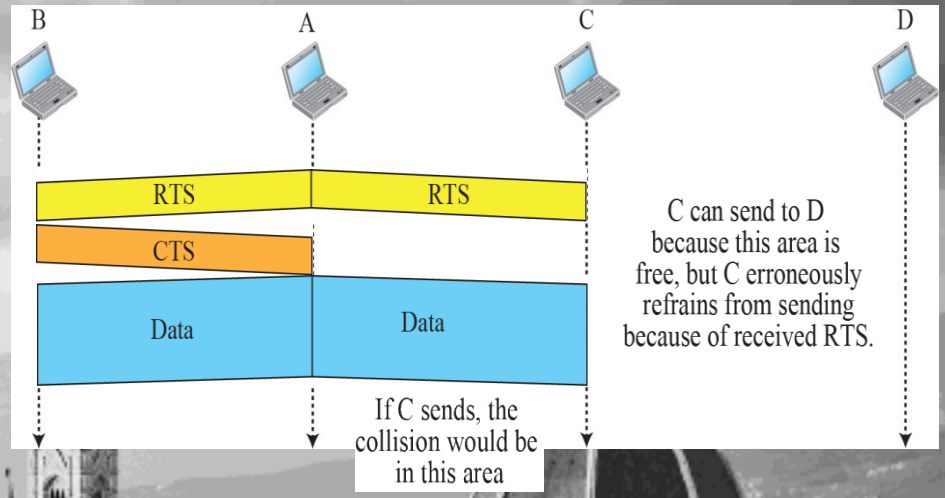


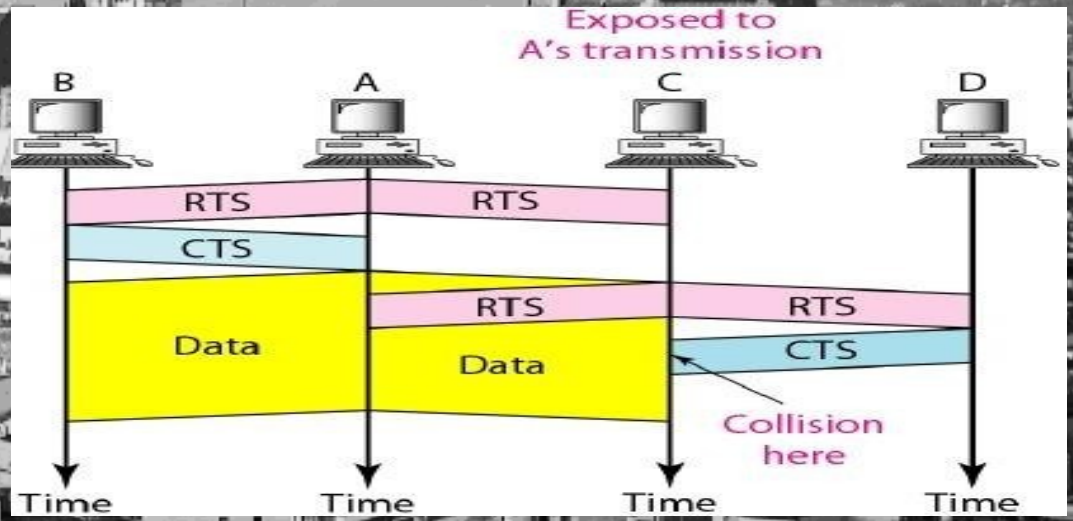
- It remains exposed until A finishes sending its data

Exposed Station Problem_Solution

- The use of RTS/CTS mechanisms, which can stop two or more nodes from transmitting data at the same time, is the solution to the exposed terminal issue.
- An RTS message is the first thing a node sends to the intended recipient when it wishes to send data.
- The sender knows it has a clear route to transmit data unhindered by other nodes if the intended recipient replies with a CTS message.
- Any station that hears the RTS is near the transmitter and stays silent long enough for the CTS to arrive.
- During the data transmission, any station that hears the CTS is near to the receiving station and stays silent.
- In this case, station C receives RTS from station A but not CTS from station B. To station D, it is therefore open to transmit.
- In this way the Exposed terminal problem can be solved by using MAC (medium access control) layer protocol.

Exposed Station Problem



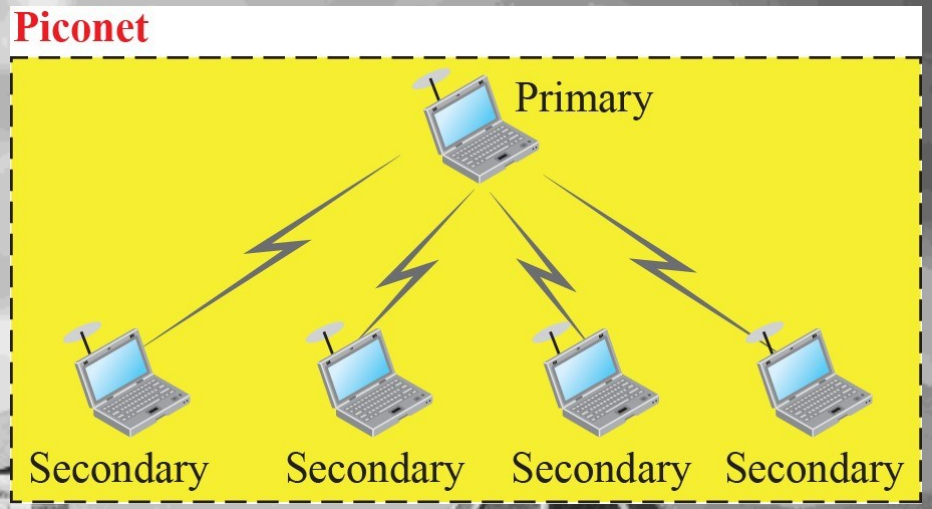


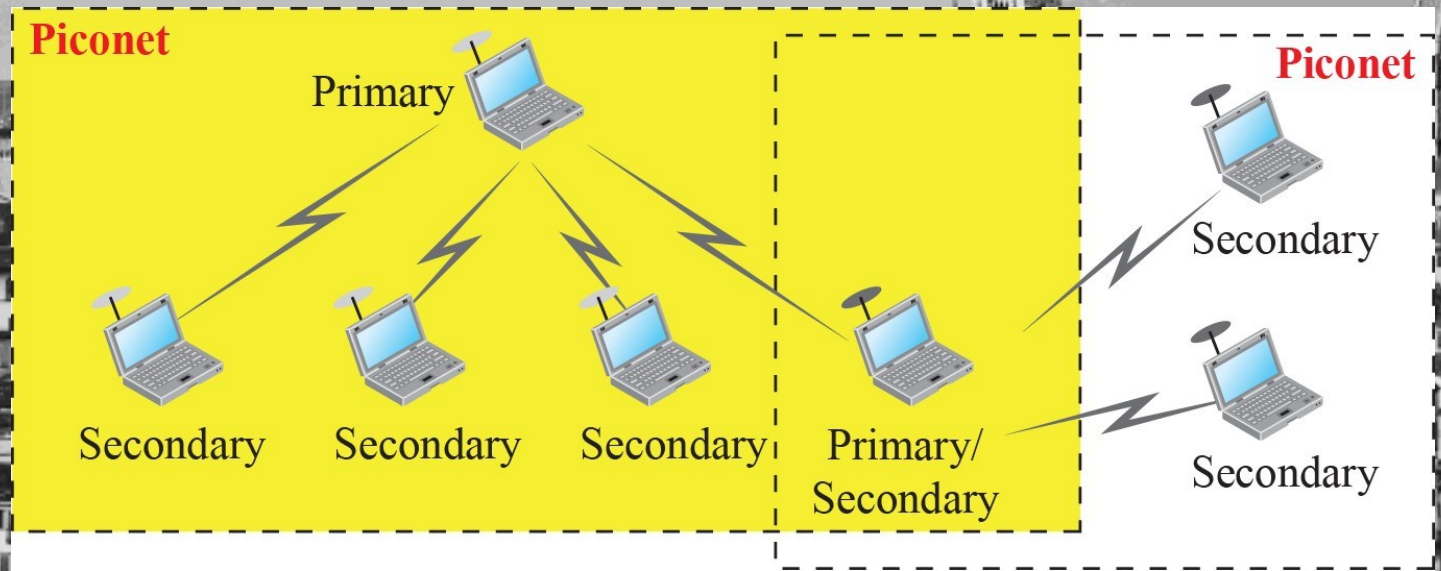
Bluetooth (IEEE 802.15 :WPAN)

❖Bluetooth is a low-cost, low power, short range wireless communication technology.

❖This uses the globally available unlicensed ISM radio band of 2.4GHz.

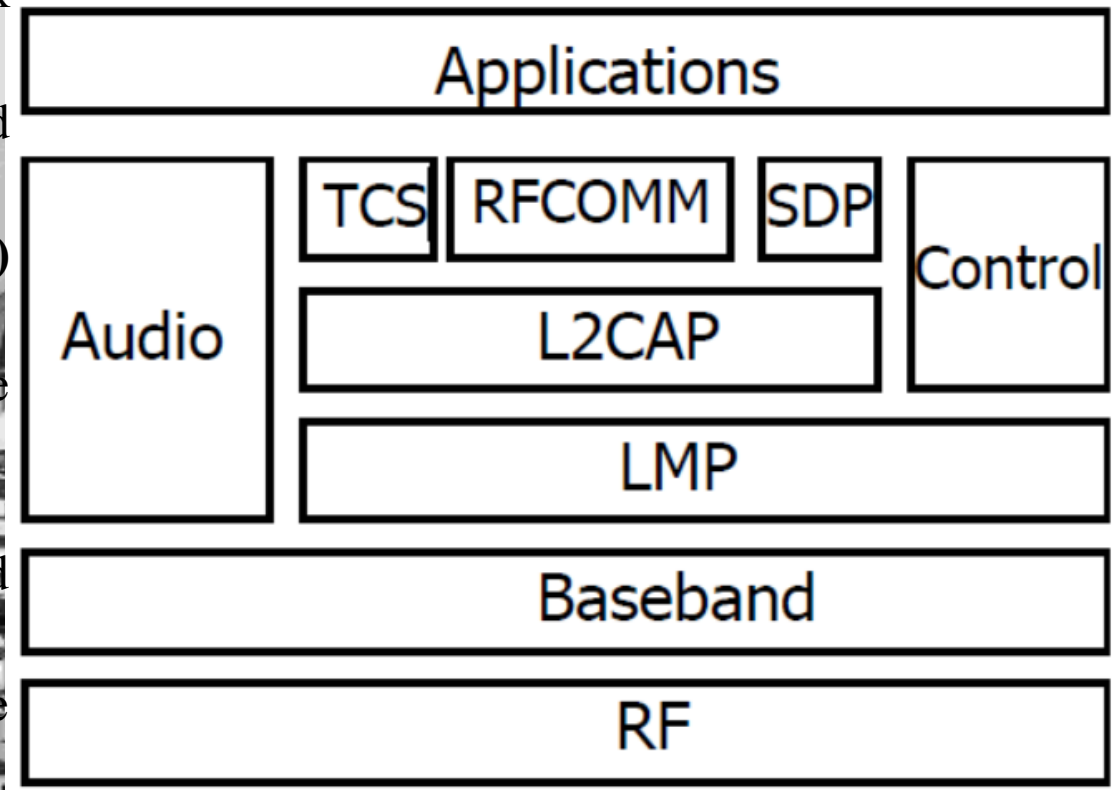
❖ Two types of Networks: **piconet and scatternet**





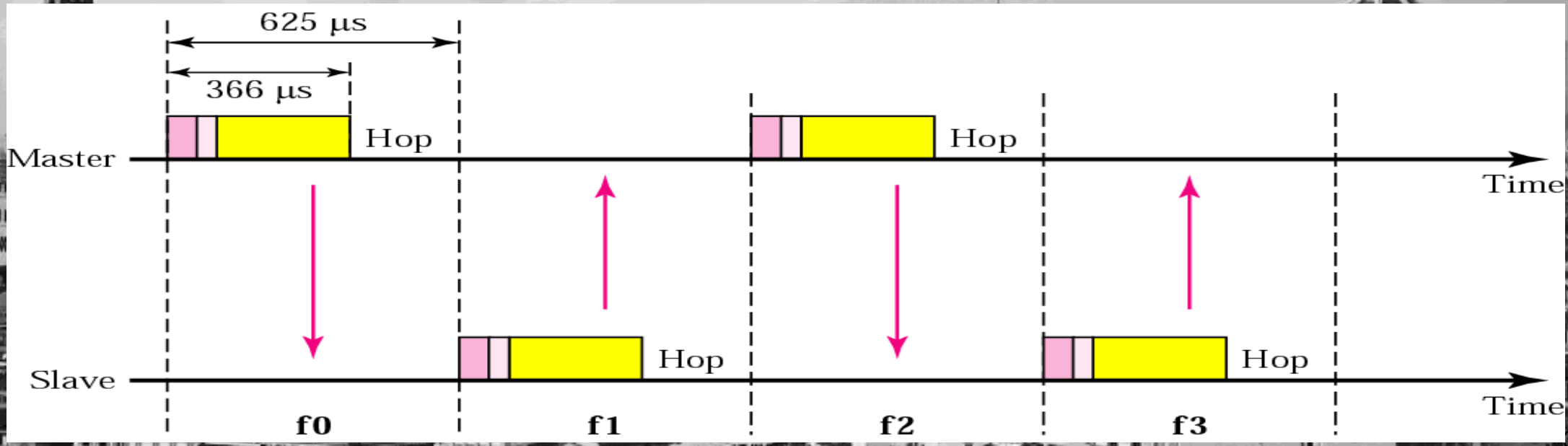
Bluetooth Layer (Bluetooth Protocol Architecture)

- Every Bluetooth device consists of a built in short range **radio transmitter**.
- The current data rate is 1Mbps and bandwidth is 2.4 GHz.
- **RF layer** specifies the radio modem used for transmission and reception
- The **Baseband Layer** controls the radio, and specifies the link control at the bit and packet level
- The **Link Management Protocol (LMP)** handles configuration and control of the Bluetooth baseband links
- The **Logical Link Control and Adaptation Protocol (L2CAP)** provides multiplexing and demultiplexing
- **Service Discovery Protocol (SDP)** finds the characteristics of the services and connects two devices to support a service
- **Telephony Control Protocol Specification (TCS)** defines the call control signaling and mobility management for the establishment of speech
- **RFCOMM** is a cable replacement protocol that emulates the standard RS-232 control and data signals over Bluetooth baseband

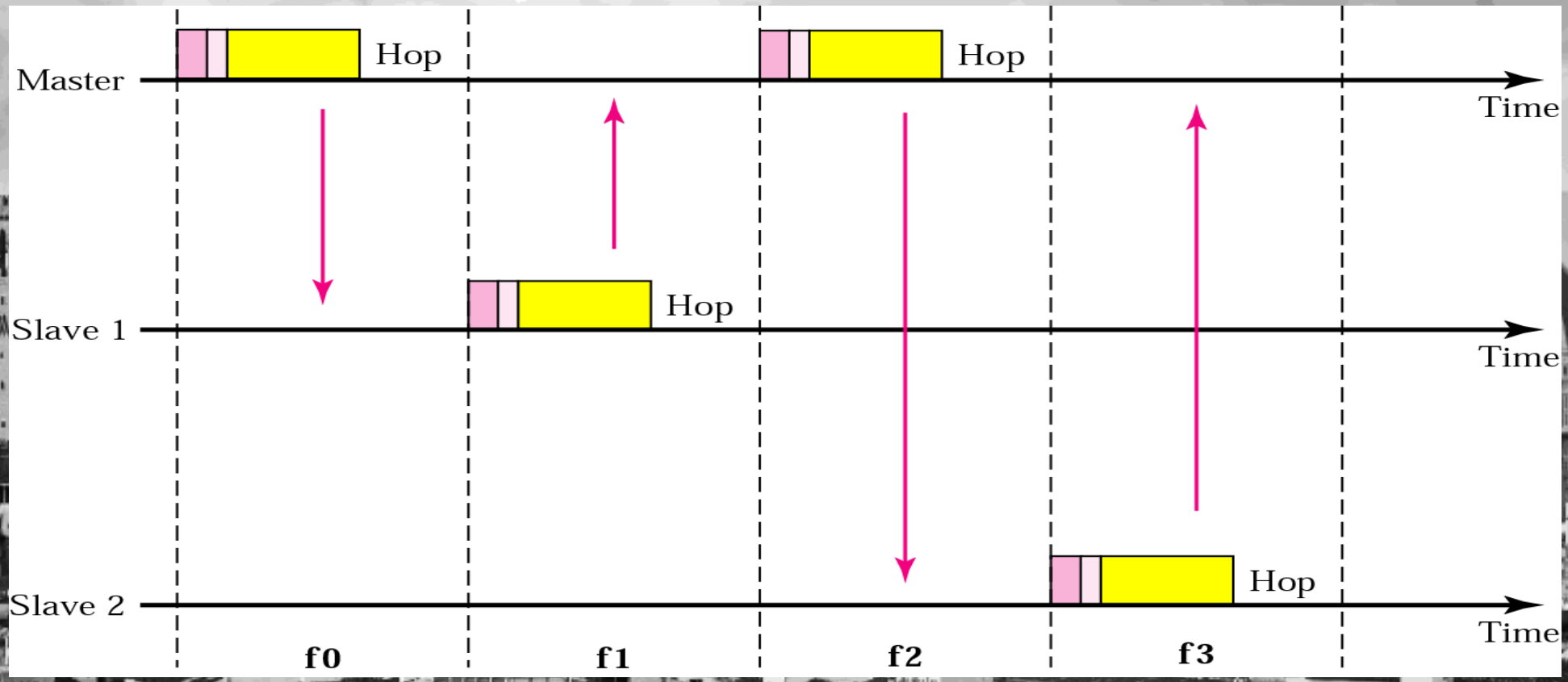


- **Radio Layer :** Each device changes its modulation frequency 600 times per second. A device uses a frequency for only 625µs(1/1600s) before it hops to another frequency.
- Band divided into 79 channels of 1 MHz each

- **Baseband Layer :** The access method is TDMA. The primary & secondary communicate with each other using time-slots. The length of time slot is **625µs**
- In one slot frame, 259µs is needed for hopping and control mechanisms.



Multiple-secondary communication



Two kind of link exists:

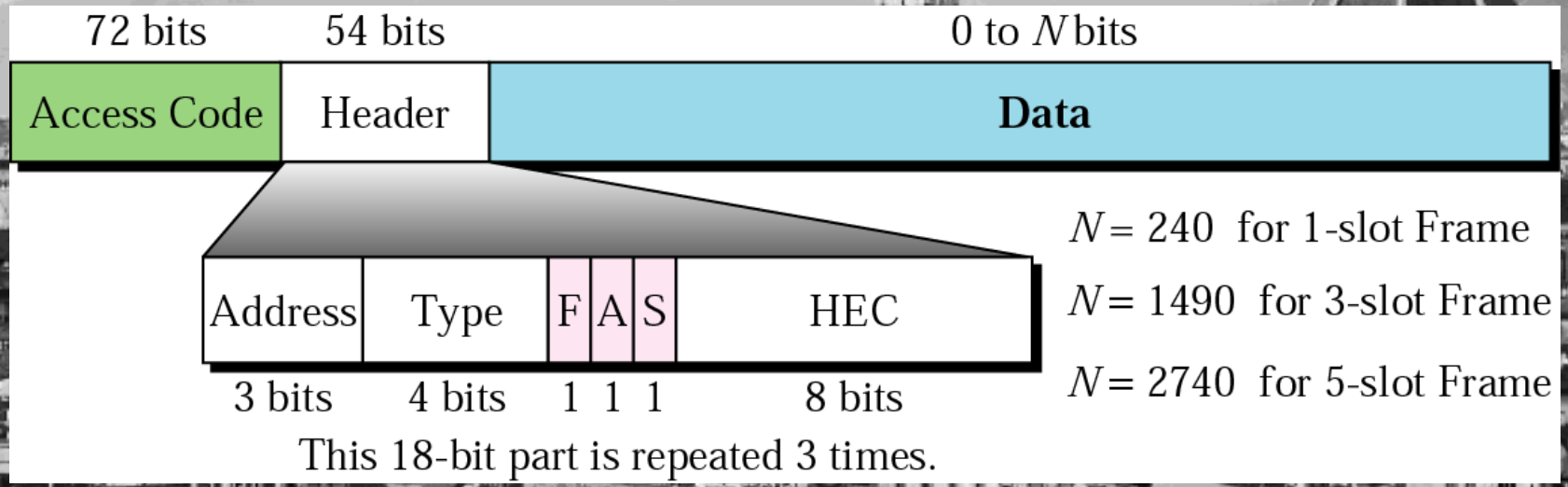
Synchronous connection oriented (SCO): This link is used when avoid latency is more important than integrity.

Asynchronous connectionless link (ACL): This link is used when data integrity is more important than avoiding latency

❖ **Logical Link Control and Adaptation Protocol (L2CAP):**

- It accepts packets of up to 64Kb
- It handles multiplexing and demultiplexing
- It handles the quality of service requirements both when links are established and during normal operation

Frame Format: frame types: one-slot, three-slot, or five-slot



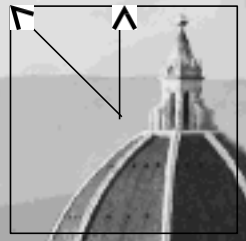
MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Mobile Cellular Networks

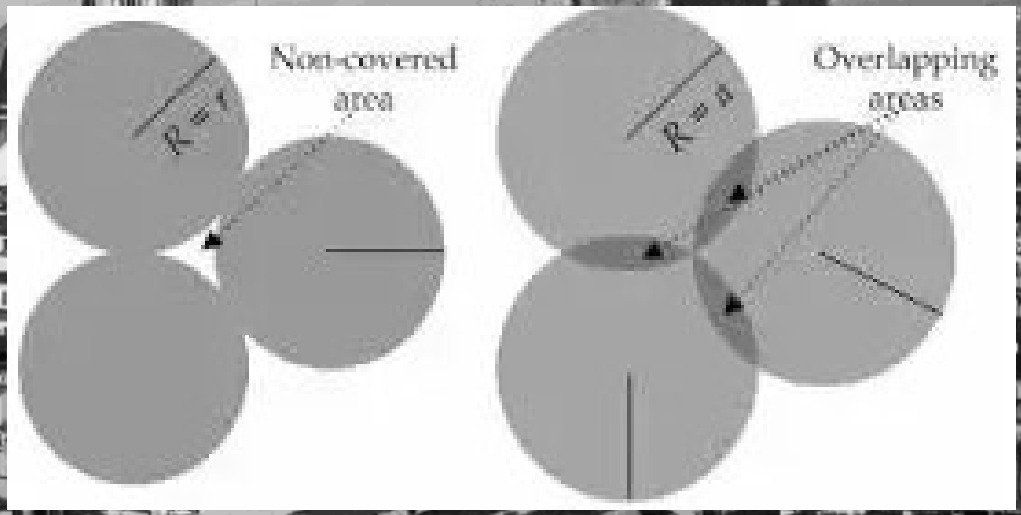
Wireless WANs and MANs

The Cellular Concept

- To ensure efficient utilization of the available radio spectrum.
- A large geographical area is divided into a number of contiguous smaller geographical coverage areas called **cells.**
- Cells are hexagonal.

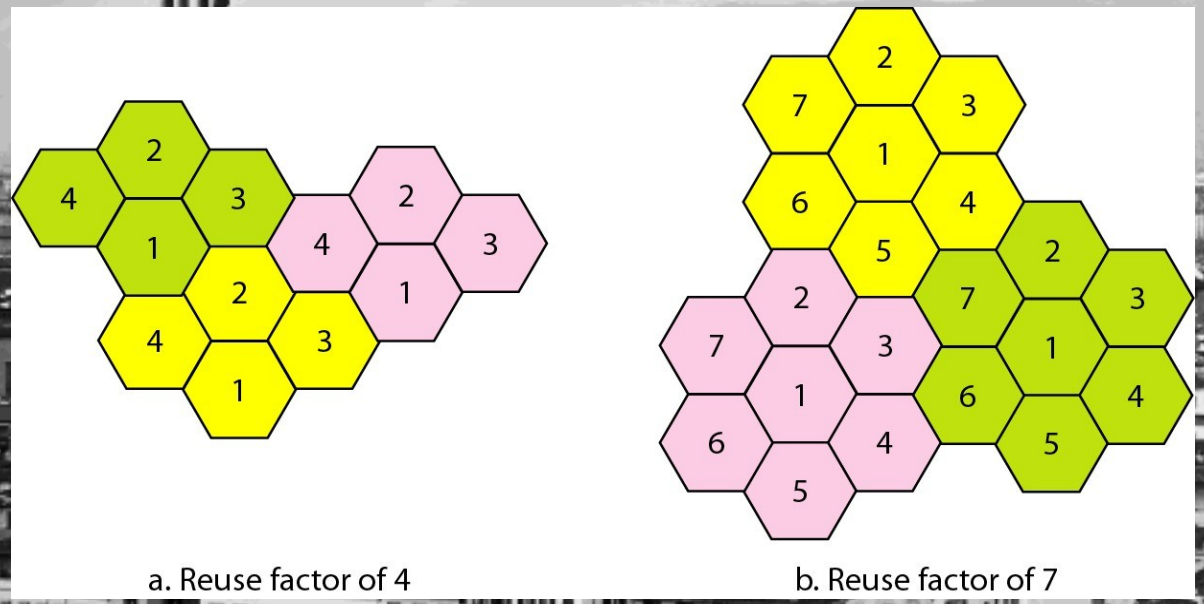


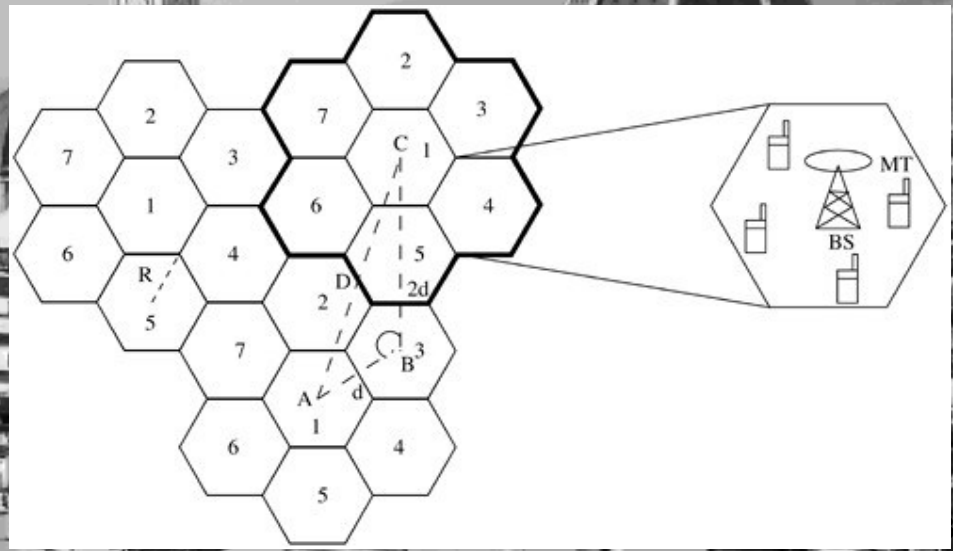
Why hexagonal cell shape is perfect over square or triangular cell shapes in cellular architecture?



While designing a network, 2 things are kept in mind:
1) A tower in a cell should provide equal signal in that cell
2)No blackspots. Blackspots are those areas where you won't get any signals

- Neighboring cells do not use same set of frequencies to prevent interference.
- Frequency reuse concept is used.
- Usage of the same frequency by different users separated by a distance, without interfering with each other
- The cluster size N is the number of cells in each cluster.
- No two cells within a cluster use channels of the same frequency.

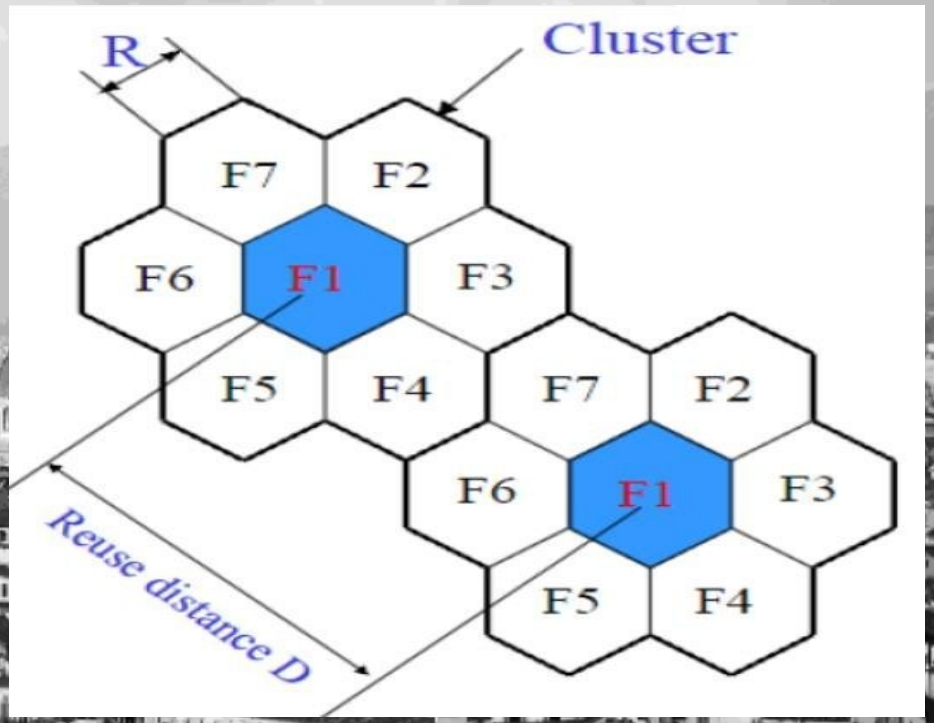




- If the radius of a cell is R, then the distance between two adjacent cells is $\sqrt{3}$ R. i. e. **d = $\sqrt{3}$ R**
- For a hexagonal cellular structure, the permissible values of the cluster size N are of the form $N = i^2 + j^2 + ij$ where i and j are any non-negative integers.

- For hexagonal cells, reuse distance $D = \sqrt{3N} \times R$

- The frequency reuse factor, determined from the cluster size N as $\frac{D}{R} = \sqrt{3 \times N}$



Two types of interference:

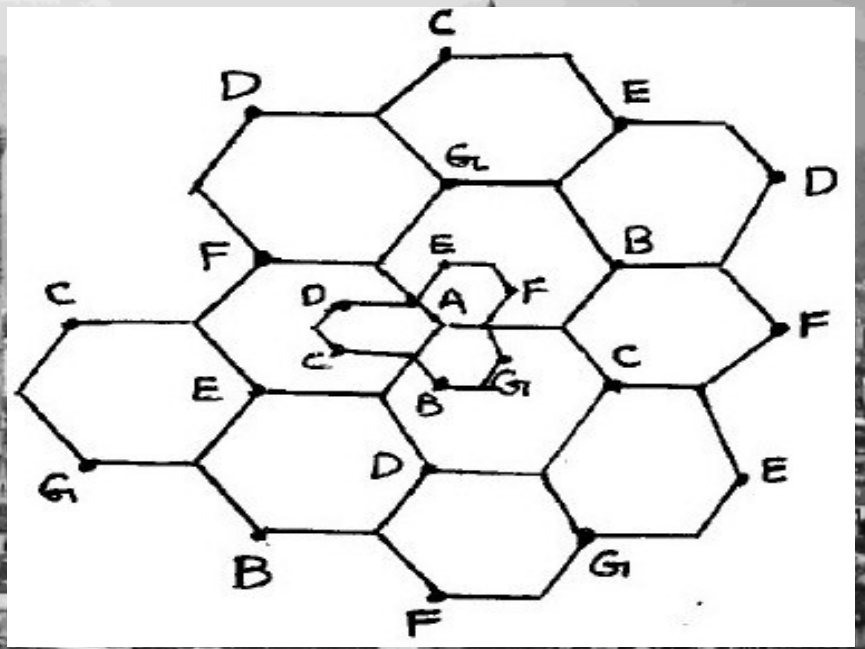
- **Co-channel interference** which results from the use of same frequencies in cells of different clusters.---- The reuse distance..
- **Disadvantage:** If the system is not properly designed, co-channel interference may occur due to the simultaneous use of the same channel.
- Co-channel Interference is the major concern in the concept of frequency reuse.
- Cells, which use the same set of frequencies, are referred to as co-channel cells.
- **Adjacent channel interference** results due to usage of adjacent frequencies within a cluster.

Why cell splitting and sectoring?

- As users increases channel capacity decreases.
- Techniques are needed to provide extra channels.
- Cell splitting and sectoring increases capacity.

- The process of subdividing a congested cell into smaller cell.
- Each with its own base station and a corresponding reduction in antenna height.
- leads to increase in capacity

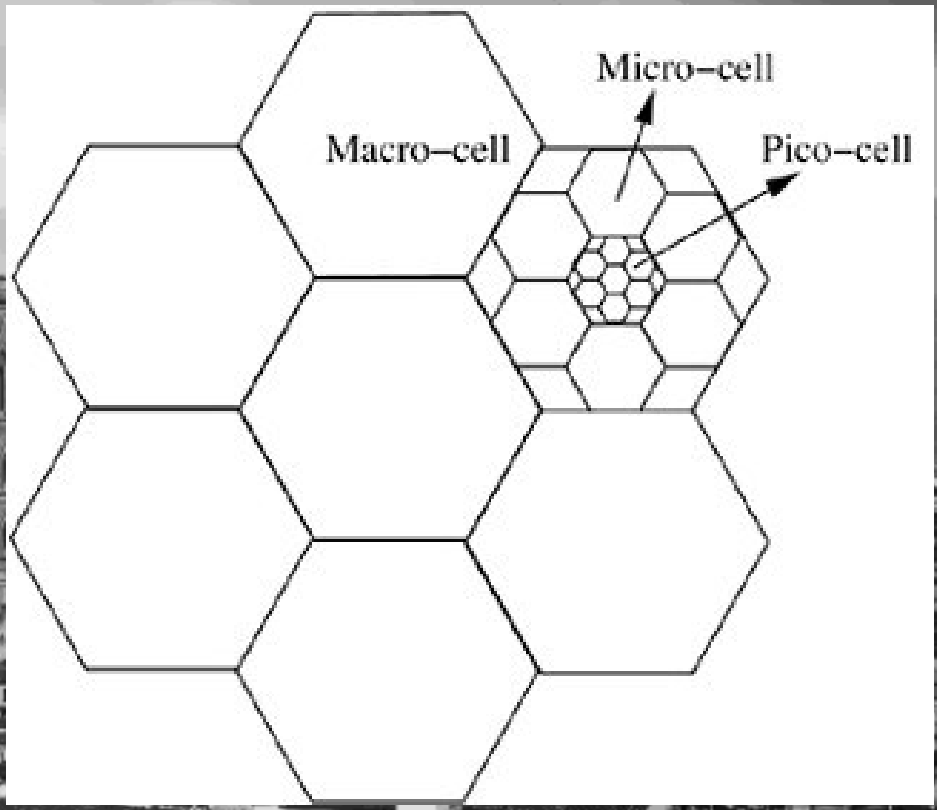
- The nearest BS is not always the best for a mobile station, due to shadowing, reflections, and other propagation-based features.



Cell Splitting:

- Cell splitting is the process of splitting a mobile cell into several smaller cells. This is usually done to make more voice channels available to accommodate traffic growth in the area covered by the original cell.
- If the radius of a cell is reduced from R to R/2, the area of the cell is reduced from Area to Area/4. The number of available channels is also increased.
- Cell splitting is usually done on demand; when in a certain cell there is too much traffic which causes too much blocking of calls. The cell is split into smaller microcells.

- Macro-cells ---- 10 kilometers
- Micro-cells ---- less than 1Km
- Pico-cells ---- few meters



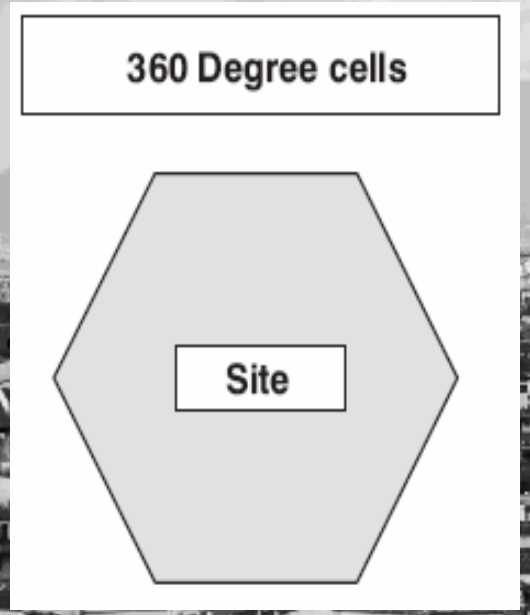
Cell Splitting Drawbacks:

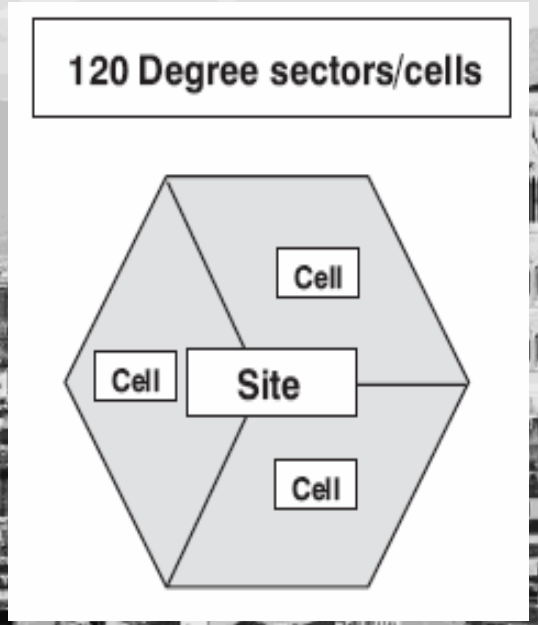
- In practice not all cells are split simultaneously, therefore we may have cells of different sizes.
- Also the handoff between the cells and microcells has to be taken care off so that high speed and low speed mobiles are equally served.
- Decreasing cell size results in more handoffs per call and higher processing load per subscriber. Thus, the handoff rate will increase exponentially.

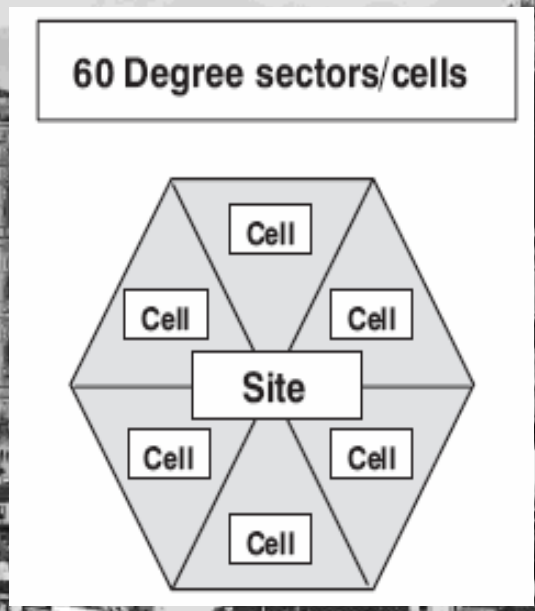
Cell sectoring:

To provide more channels per unit coverage

- To overcome some limitations like co-channel interference[a],cell sectoring is done.
- Involves replacing an omni- directional antenna at the base station by several directional antennas







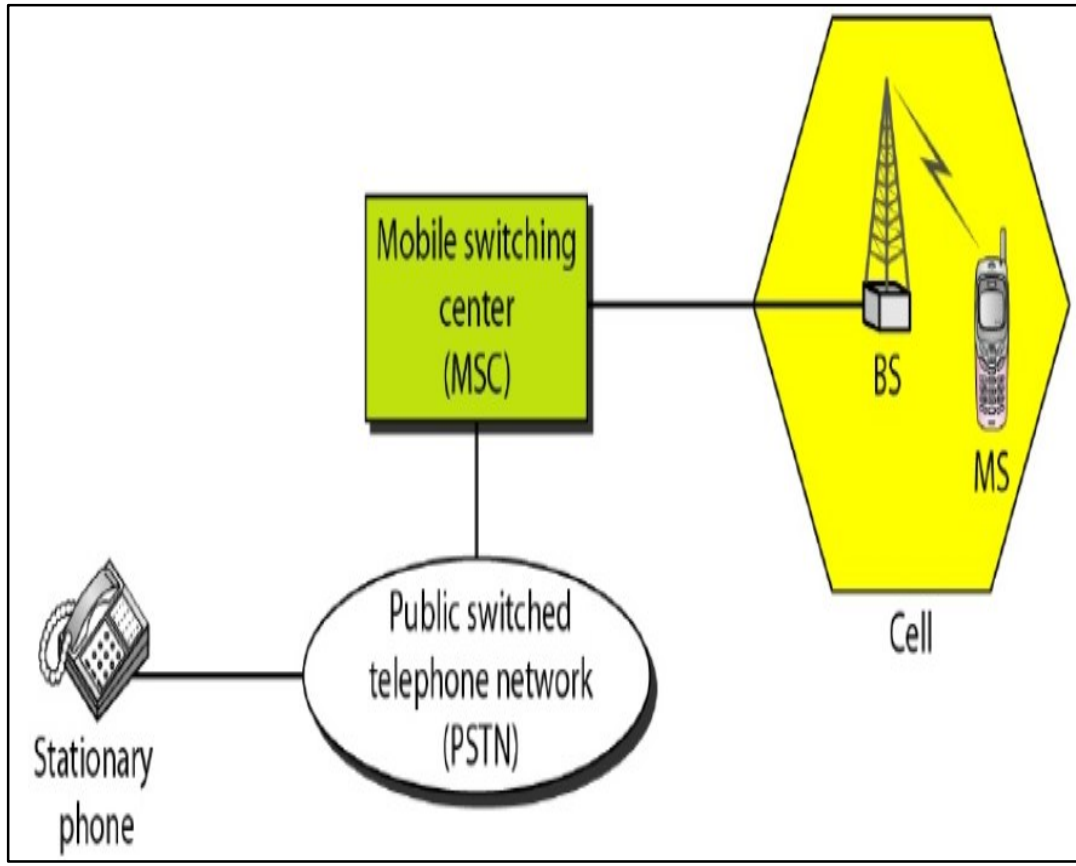
- The sectoring is done by replacing a single omni-directional antenna with 3 directional antennas (120^O sectoring) or with 6 directional antennas (60^O sectoring).
- In this scheme, each cell is divided into 3 or 6 sectors. Each sector uses a directional antenna at the BS and is assigned a set of channels.
- The number of channels in each sector is the number of channels in a cell divided by the number of sectors. The amount of co-channel interferer is also reduced by the number of sectors.

Drawbacks:

- Increase the number of antennas at each BS.
- The number of handoffs increases when the mobile moves from one sector to another.

Cellular Telephony System

- Communications between 2 moving units (Mobile stations (MS)), or between a mobile unit and a stationary unit
- Service provider
  - Locate and track a caller
  - Assign a channel to the call
  - Transfer the channel from BS to BS as the caller moves out of range
- Cellular service area divided into cells
- Each cell contains an antenna and controlled by a BS
- Each BS in turn is controlled by a switching office called a Mobile Switching Center (MSC)



Cellular Telephony System

- Cellular systems implements Space Division Multiplexing Technique (SDM).
- Each transmitter is called a base station and can cover a fixed area called a cell.
- This area can vary from few meters to few kilometers.
- Mobile network providers install several thousands of base stations each with a smaller cell instead of using power full transmitters with large cells following advantages:

  Higher capacity, Less transmission power, Local interference only, Robustness

- Disadvantages of Cellular Systems

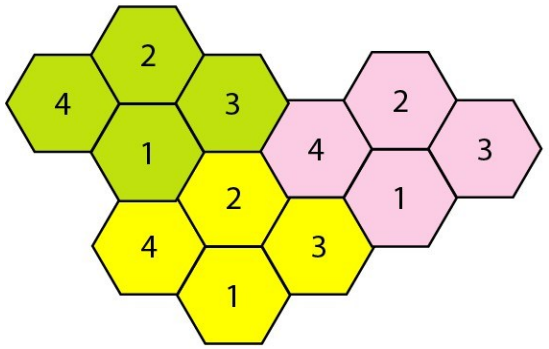
  Infrastructure needed, Handover needed, Frequency planning

Frequency Reuse Principle

- If one transmitter is far away from another, i.e., outside the interference range, it can reuse the same frequencies.
- Cell size is not fixed and can be increased or decreased depending on population
- Typical radius of a cell is 1 to 12 miles
- Neighboring cells cannot use the same set of frequencies for communication because it may create interference for the users located near the cell boundaries
- Set of frequencies available are limited → frequency reuse
  - A frequency reuse pattern is a configuration of N cells, (N is the reuse factor) in which each cell uses a unique set of frequencies
  - When pattern repeated, frequencies can be reused

Frequency Reuse Pattern

- Neighboring cells do not use same set of frequencies to prevent interference.
- Frequency reuse concept is used.
- Usage of the same frequency by different users separated by a distance, without interfering with each other
- The cluster size N is the number of cells in each cluster.
- No two cells within a cluster use channels of the same frequency.



a. Reuse factor of 4

b. Reuse factor of 7

Transmitting System

- Caller enters a phone number and presses the send button
- MS scans the band, seeking a setup channel with a strong signal, sending the phone number to the closest BS using that channel
- The BS relays the data to MSC
- The MSC sends the data to the central telephone office
- If the called party is available, a connection is made and the result is relayed back to MSC
- MSC assigns an unused voice channel to the call, and a connection is established
- MS automatically adjusts its tuning to the new channel

Receiving System

- Telephone central office sends the number to MSC
- MSC searches for location of MS by using paging (query signals to each cell)
- Once found, MSC transmits a ringing signal
- When MS answers, a voice channel is assigned to the call

Hand-off (Handover)

- During a conversation, if the mobile station moves from one cell to another, the signal may become weak
- To solve this, MSC monitors the level of the signal every few seconds.
- If the signal strength is low, MSC then changes the channel carrying the call (Handoff)
- As soon as a user changes a cell due to changes in signal strength, interference, or load balancing, the system has to redirect all connections or forward all data
- It is a process of handover of a connection between two or more base stations using the same wireless technology

Types of Hand-off (Handover)

- **Hard handoff:**
  - A mobile station only communicates with one base station
  - When MS moves from one cell to another, communication is broken with the previous base station before communication can be established with the new one.

- **Soft handoff:**
  - A mobile station can communicate with two base stations at the same time.
  - During handoff, a mobile station may continue with the new base station before breaking off from the old one.

Handoffs

❖When a user moves from the coverage area of one BS to the adjacent one, a handoff has to be executed to continue the call.

❖There are two main parts to the handoff procedure: the first is to find an uplink-downlink channel pair from the new cell to carry on the call, and the second is to drop the link from the first BS.

Two types:

Hard Handoff: Characterized by an actual break in the connection while switching from one cell or base station to another. ...

Soft Handoff: Entails two connections to the cell phone from two different base stations.

Issues Involved in Handoffs:

- Optimal BS selection
- Ping-pong effect
- Data loss
- Detection of handoff requirement

Handoff Quality:

- Handoff delay
- Duration of interruption
- Handoff success
- Probability of unnecessary handoff

Roaming

- A user can have access to communication or can be reached where there is coverage
- A service provider usually has limited coverage
- Neighboring service providers can provide extended coverage through a roaming contract
- Similar to snail mail between countries

GSM (Global System for Mobile Communications)

GSM (Global System for Mobile Communications)

- GSM stands for **Global System for Mobile Communication.**
- GSM is an open and digital cellular technology used for mobile communication.
- It uses 4 different frequency bands of 850 MHz, 900 MHz, 1800 MHz and 1900 MHz .
- It uses the combination of FDMA and TDMA.

GSM is having 4 different sizes of cells are used in GSM :

1. Macro : In this size of cell, Base Station antenna is installed.
2. Micro : In this size of cell, antenna height is less than the average roof level.
3. Pico : Small cells' diameter of few meters.
4. Umbrella : It covers the shadowed (Fill the gaps between cells) regions.

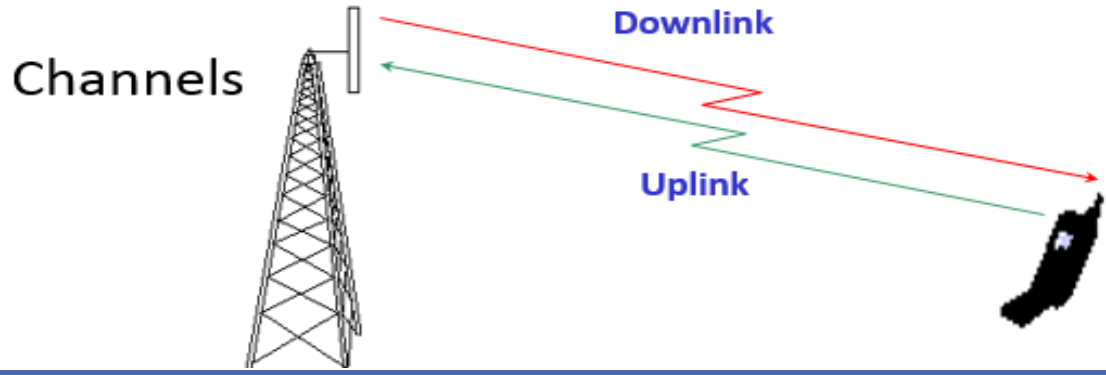
MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Features of GSM

- Supports international roaming
- Clear voice clarity
- Ability to support multiple handheld devices
- Spectral / frequency efficiency
- Low powered handheld devices
- Ease of accessing network
- International ISDN compatibility
- Low service cost
- New features and services

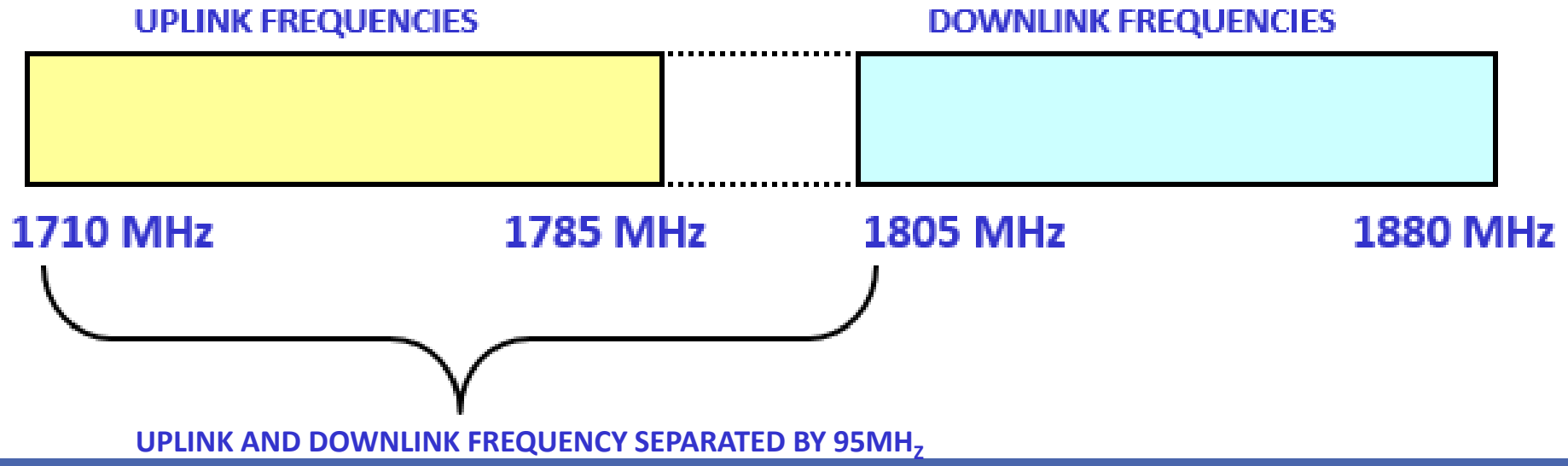
GSM (Global System for Mobile Communications) Channels

- Physical Channel:
  - It is specified by specific time slot/ carrier frequency.
  - Each time slot on a carrier is referred to as a physical channel.
- Logical Channel:
  - Logical channel run over physical channel i.e. logical channels are time multiplexed on physical channels
  - Variety of information is transmitted between the MS and BTS
- Different types of logical channels:
  - ✓ Traffic channel: Used to carry digitally encoded user speech or user data.
  - ✓ Control Channel: Carry signaling and synchronizing commands between the BS and MS

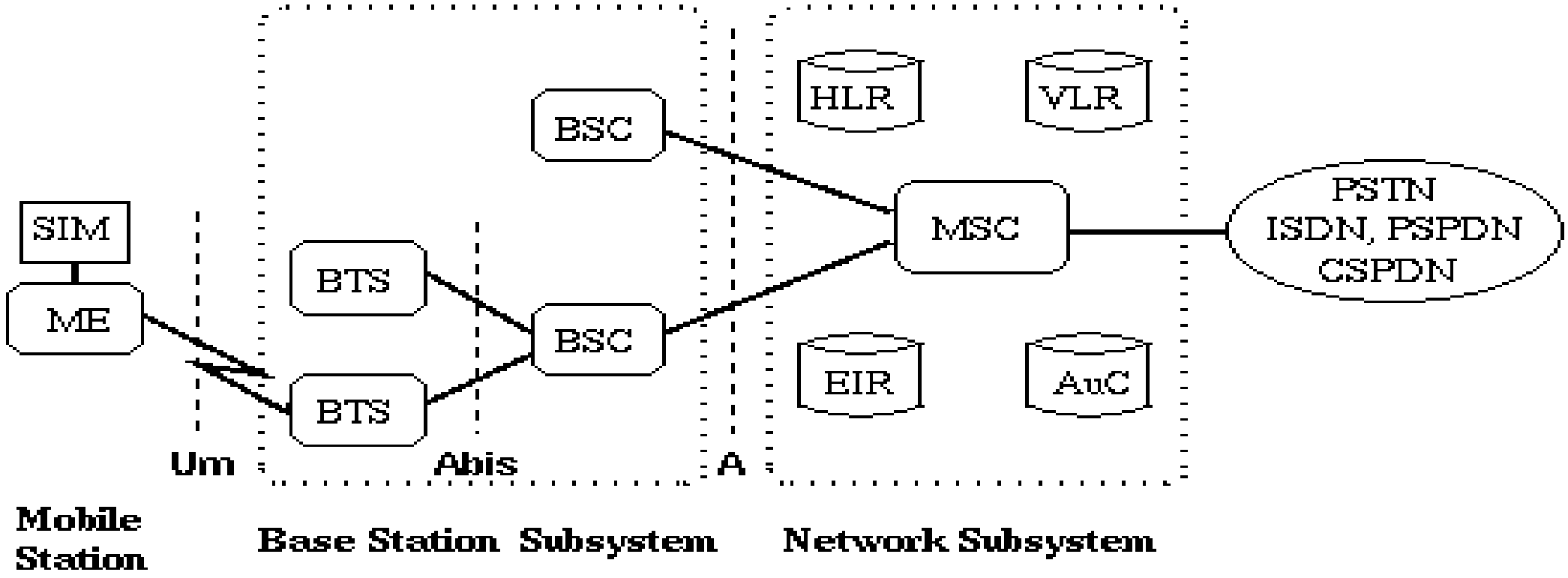


GSM Frequencies

- Originally designed on 900 MHz range, now also available on 800 MHz, 1800 MHz and 1900 MHz ranges
- Separate Uplink and Downlink frequencies
  - One example channel on the 1800 MHz frequency band, where RF carriers are space every 200 MHz



GSM Architecture



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

Cellular Architecture

Mobile Switching Center (MSC):

- Location update, call delivery and user authentication

Authentication Center (AUC):

1) mainly used for security
2) data storage location and functional part of the network

Equipment Identity Register (EIR):

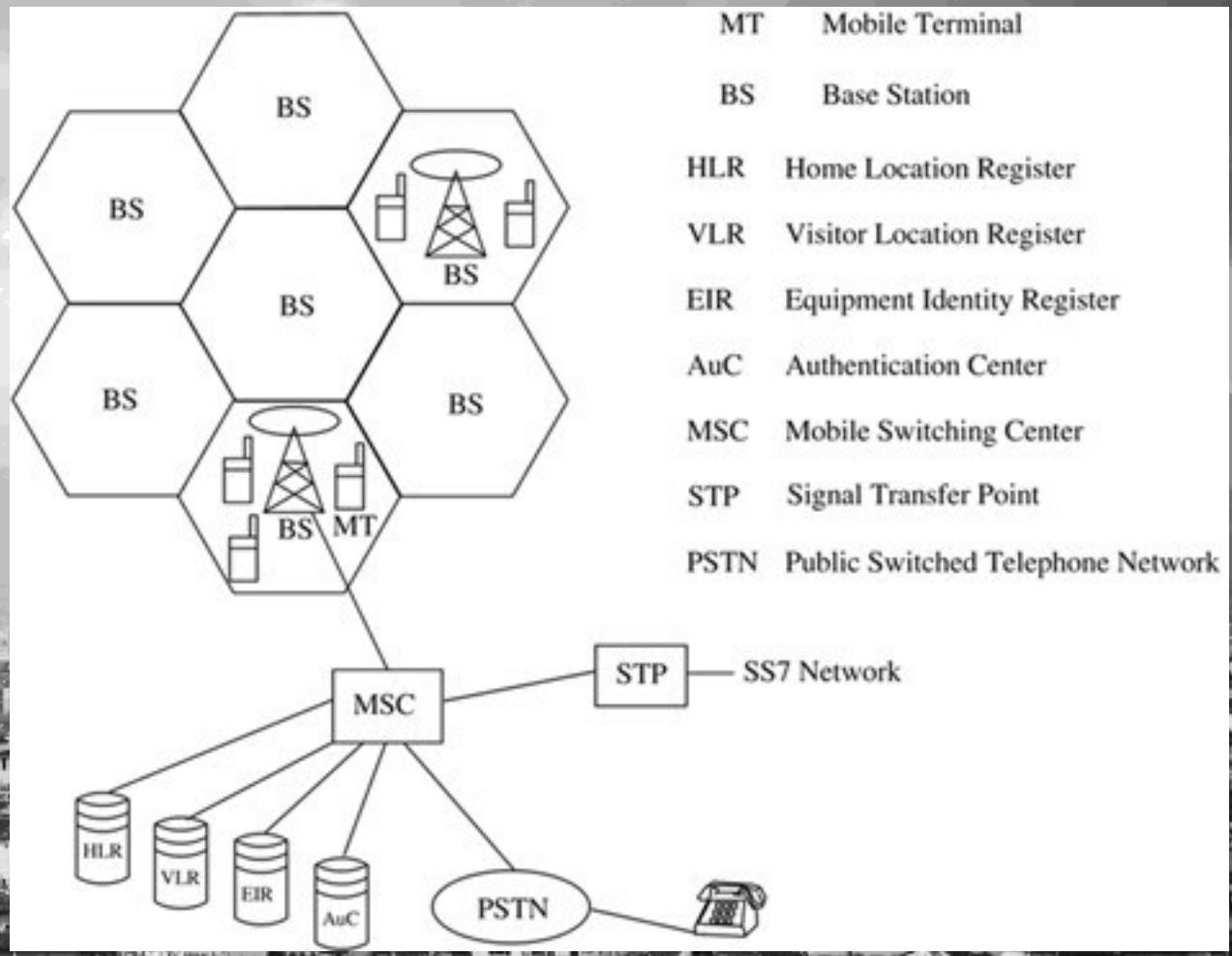
1) Database that is used to track handsets using the IMEI
2) Made up of three sub-classes: White List, Black List and Gray List

Home Location Registers (HLR):

1) contains administrative information of each MT
2) current location of the mobile

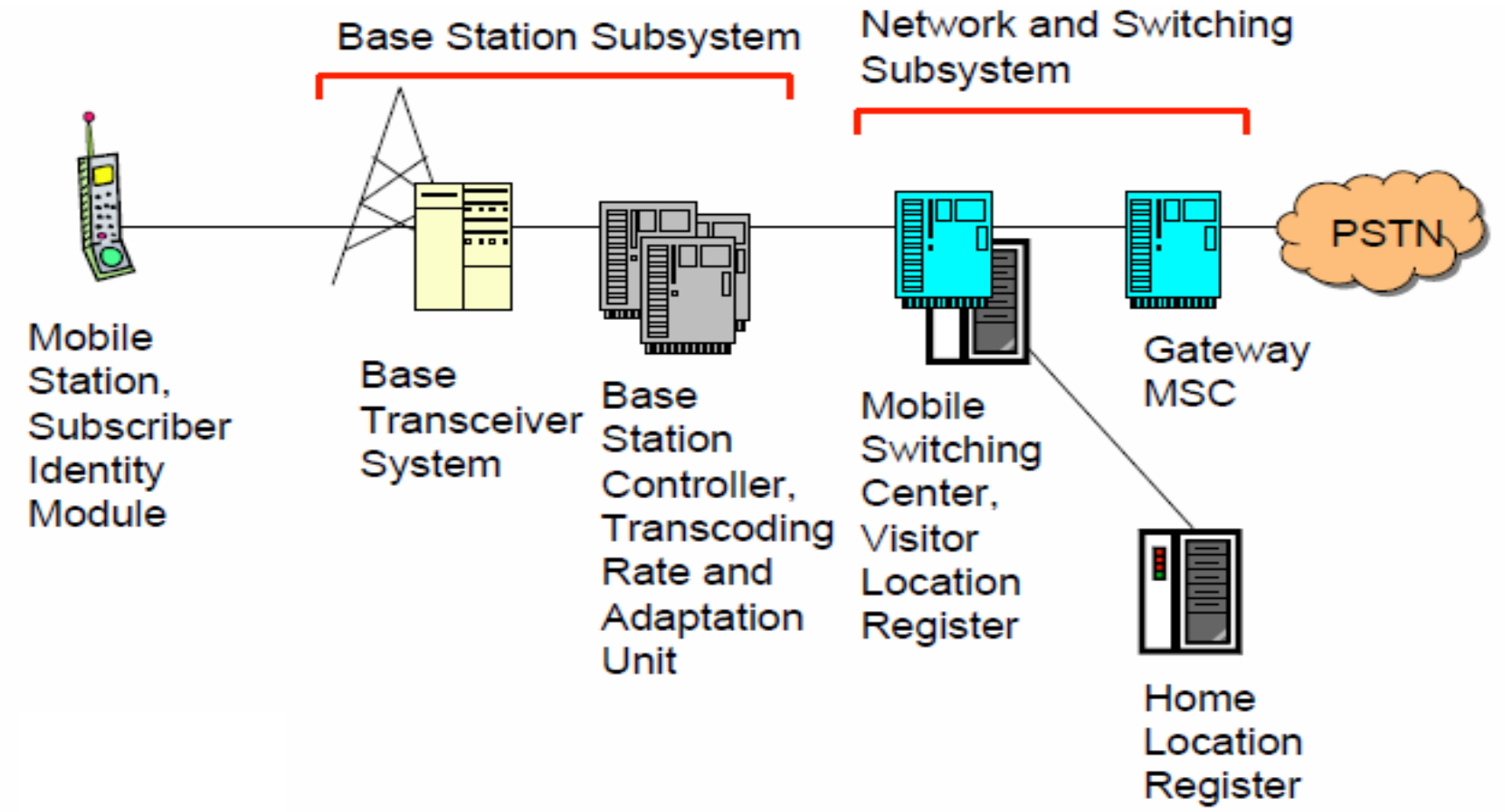
Visitor Location Registers (VLR):

1) Roaming user in a cell
2) tracks which customers have the phone on and ready to receive a call
3) periodically updates the database on which phones are turned on and ready to receive calls



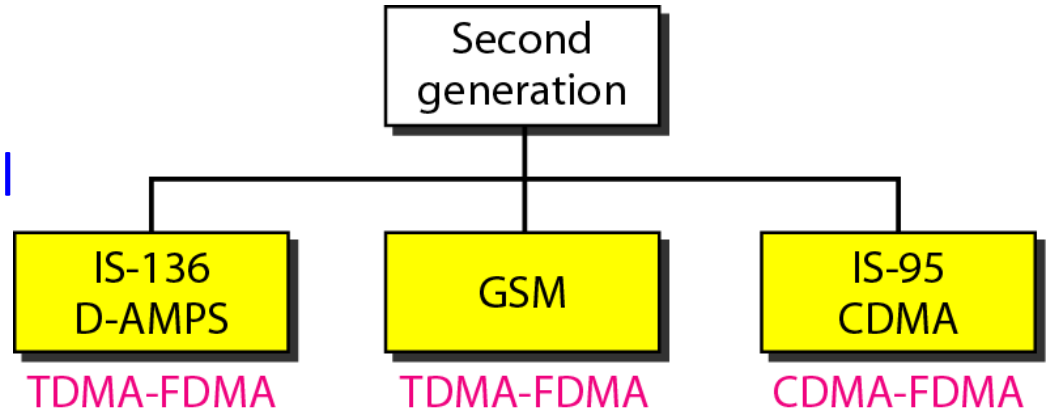
1) The MSCs are linked through **a signaling system 7 (SS7) network**, which controls the setting up, managing, and releasing of telephone calls.
2) The SS7 protocol introduces certain nodes called signaling transfer points (STPs) which help in call routing.

GSM Architecture



Mobile Generations

- **First Generation:**
  - Voice communication using analog signals
  - e.g. Advanced Mobile Phone System (AMPS) is an analog cellular phone system using FDMA.
- **Second Generation:**
  - Voice communication using digital signal
- **Third Generation:**
  - High-speed digital cellular telephony (including video telephony)



- **Fourth Generation:**
  - IP-based “anytime, anywhere” voice, data, and multimedia telephony at faster data rates than 3G

Evolution of Mobile Communication System

Advanced Mobile Phone System (AMPS): Analog cellular systems in North America using FDMA. 1980s, 2Kbps

Global System for Mobile Communication (GSM) is a European standard, 2000, 64Kbps

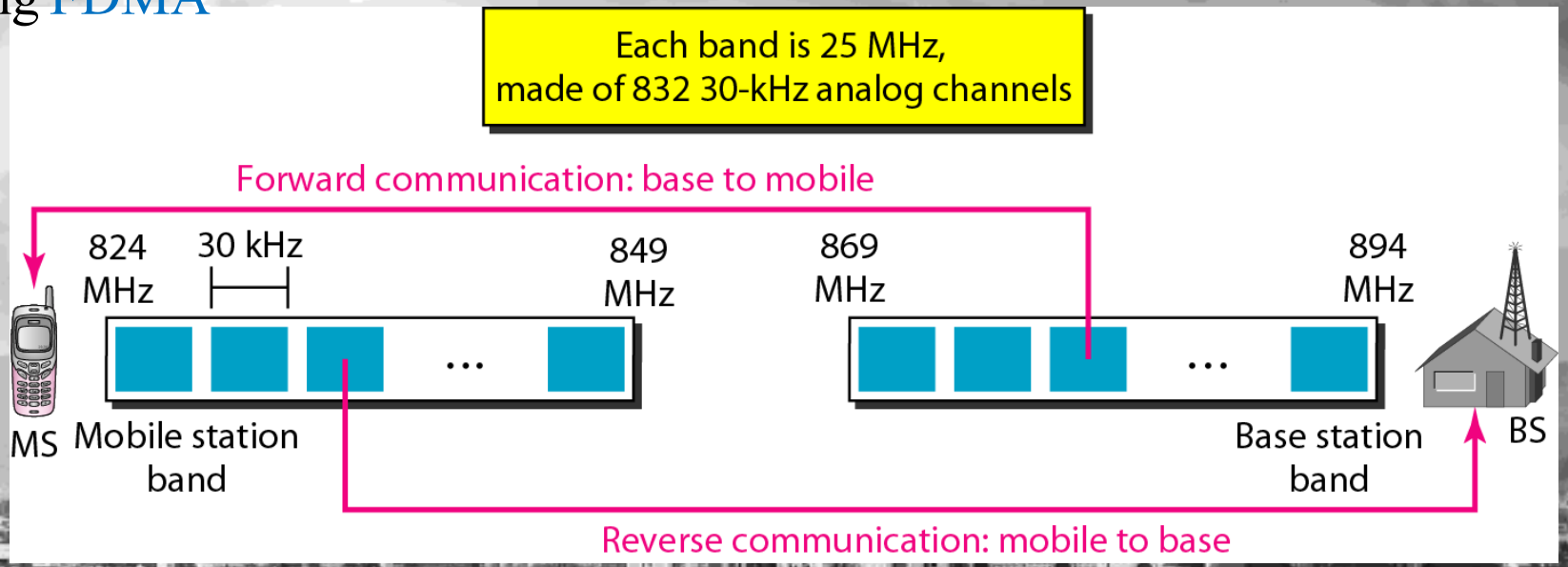
2001-2004, 144Kbps, sms and mms

Wideband-CDMA, 2005-2010, 12Mbps, high quality audio-video data

2011, 1Gbps, Wimax, LTE, Wi-Fi, IP based

First Generation Cellular System

❖**Advanced Mobile Phone System (AMPS)** is one of the leading analog cellular systems in North America using FDMA

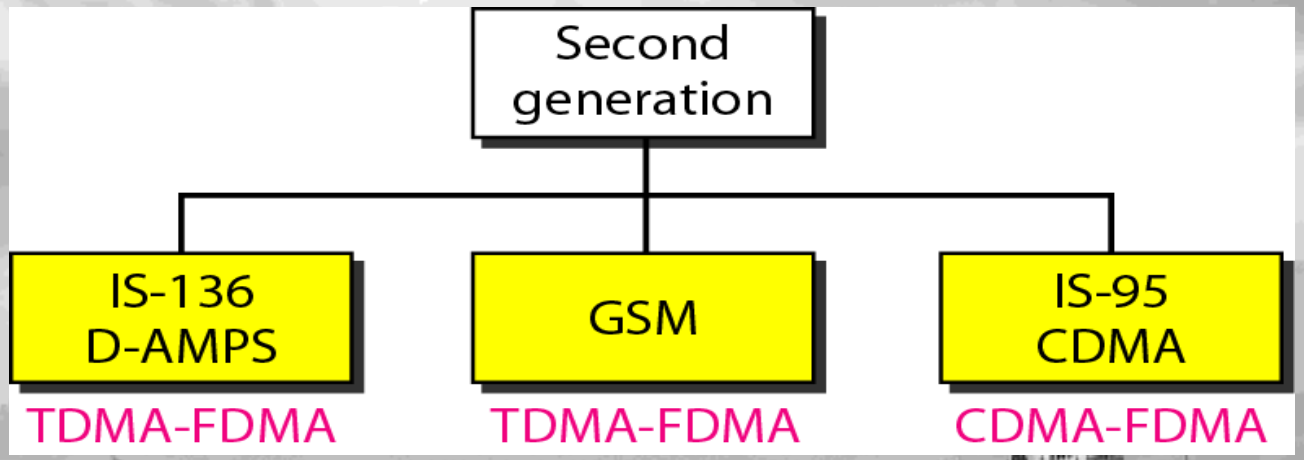


❖Two providers can share an area, which means **416 channels** in each cell for each provider. Out of these 416, **21 channels** are used for **control**, which leaves 395 channel

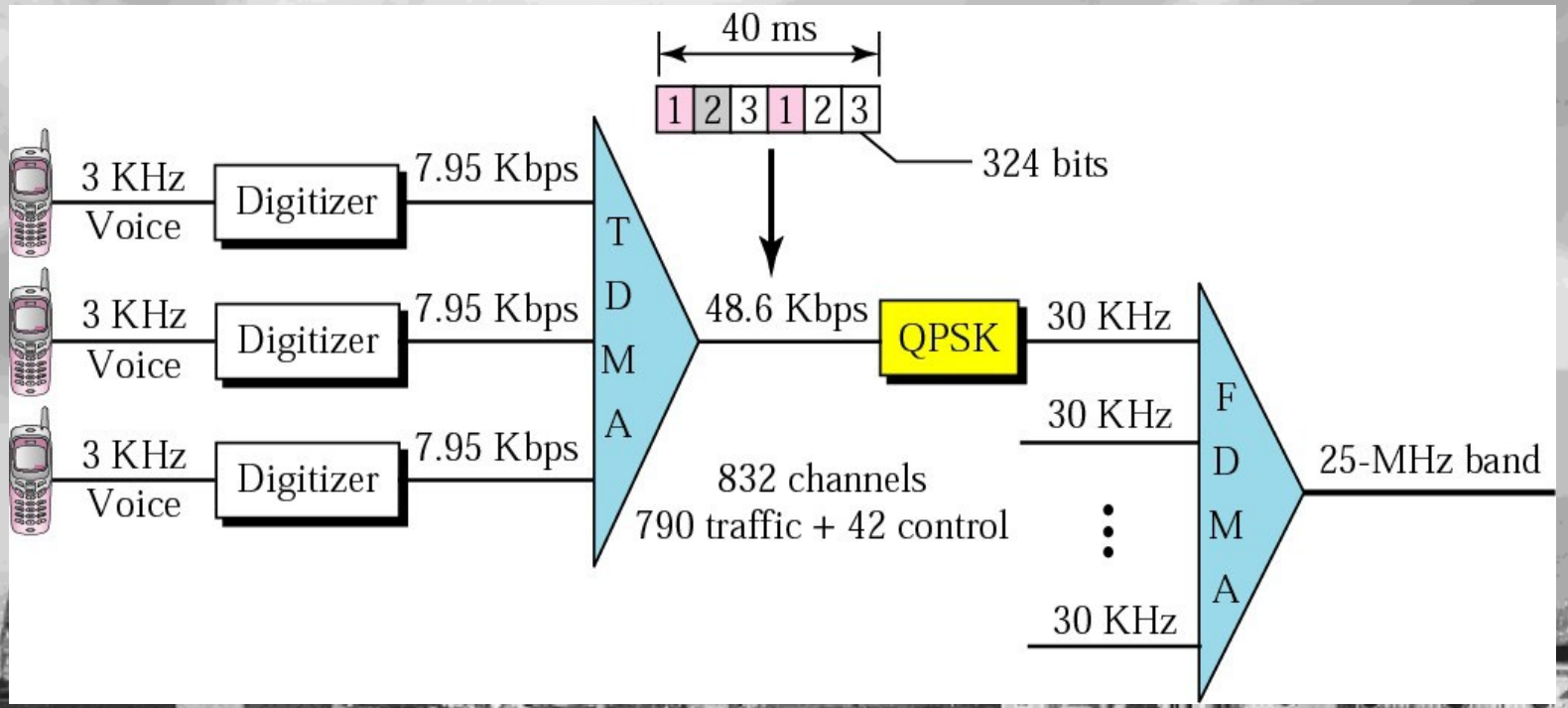
❖ AMPS has a frequency reuse factor of 7; this means only ***one-seventh of these 395 traffic channels are actually available in a cell.***

Second Generation Cellular System

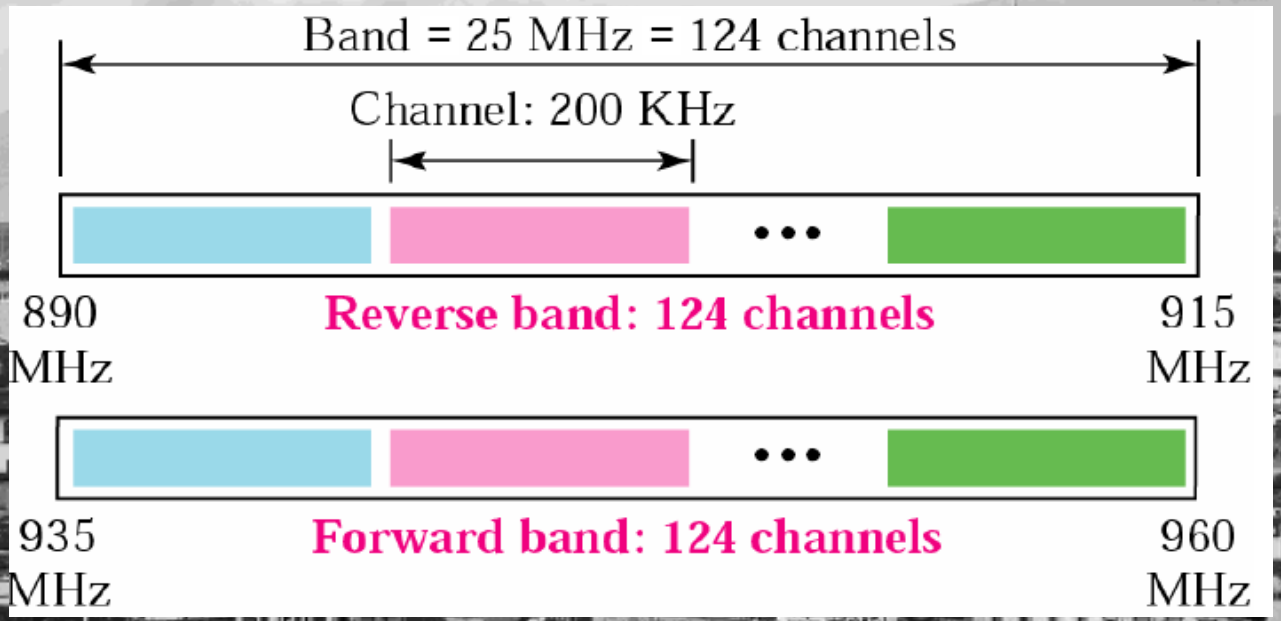
- The second generation was mainly designed for digitized voice.

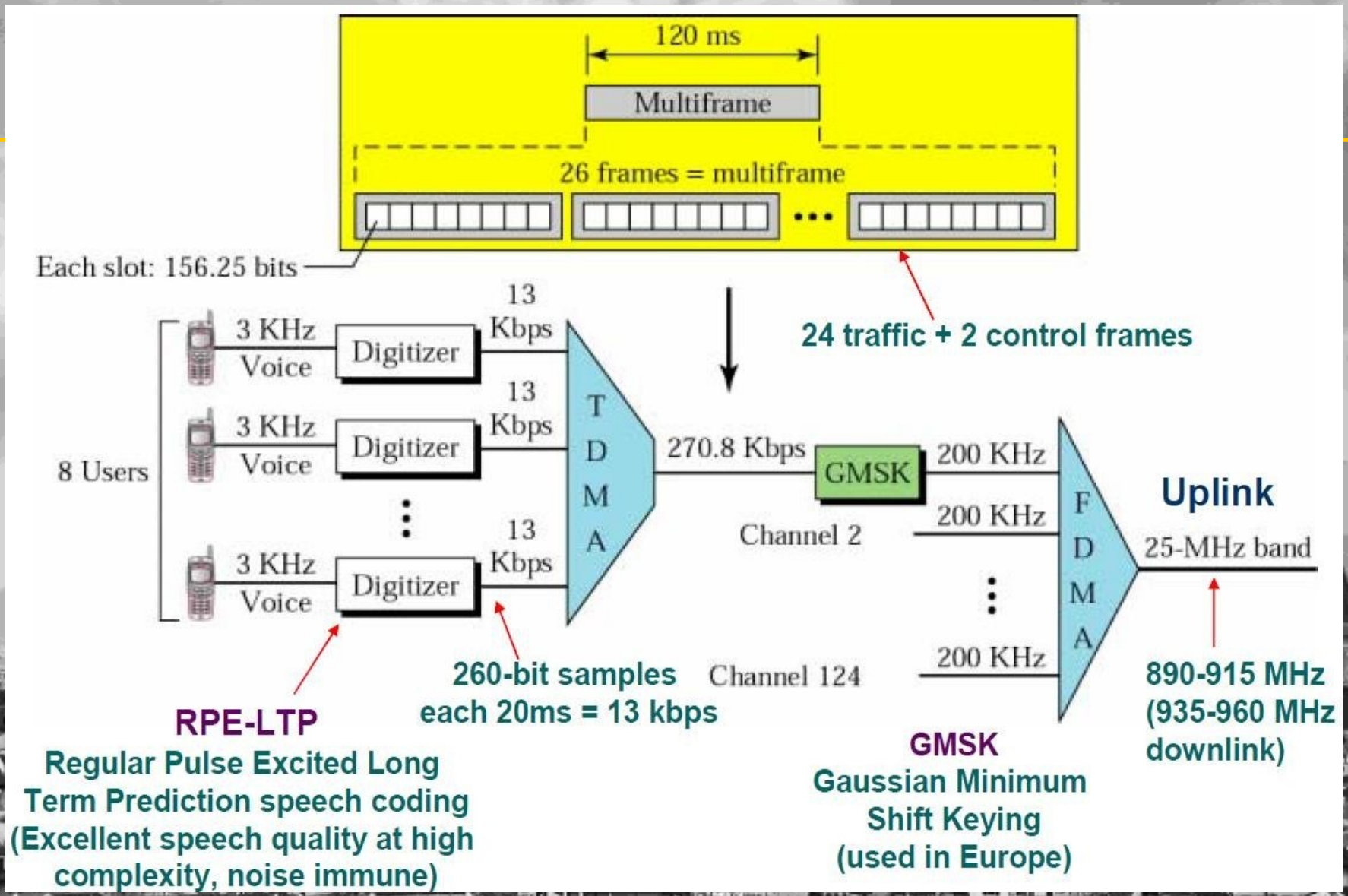


- D-AMPS was designed to be **backward-compatible** with AMPS. This means that in **a cell, one** telephone can use **AMPS** and **another D-AMPS**
- D-AMPS uses the same bands and channels as AMPS.


40 ms
1 2 3 1 2 3
324 bits
3 KHz Voice
Digitizer
7.95 Kbps
3 KHz Voice
Digitizer
7.95 Kbps
3 KHz Voice
Digitizer
7.95 Kbps
TDMA
48.6 Kbps
QPSK
30 KHz
30 KHz
30 KHz
832 channels
790 traffic + 42 control
FDMA
25-MHz band

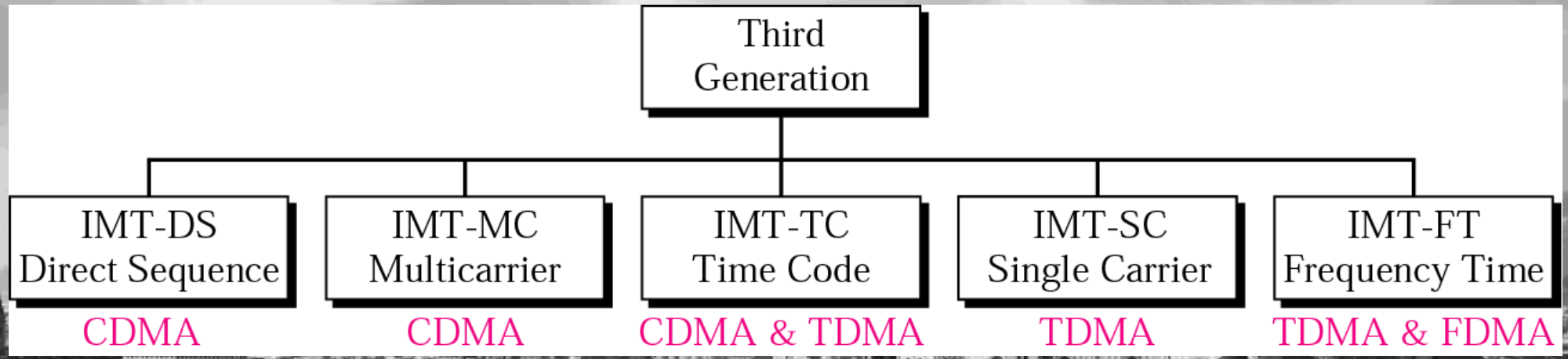
- **Global System for Mobile Communication (GSM)** is a European standard.
- GSM uses two bands for duplex communication.
- Each band is 25 MHz in width, shifted toward 900 MHz.
- Each band is divided into 124 channels of 200 kHz separated by guard bands.




120 ms
Multiframe
26 frames = multiframe
Each slot: 156.25 bits
24 traffic + 2 control frames
8 Users
3 KHz Voice
Digitizer
13 Kbps
TDMA
270.8 Kbps
GMSK
200 KHz
Channel 2
Channel 124
FDMA
Uplink
25-MHz band
890-915 MHz (935-960 MHz downlink)
260-bit samples each 20ms = 13 kbps
RPE-LTP
Regular Pulse Excited Long Term Prediction speech coding (Excellent speech quality at high complexity, noise immune)
GMSK
Gaussian Minimum Shift Keying (used in Europe)

Third Generation Cellular System

❖The main goal of third-generation cellular telephony is to provide **universal personal communication.**



Generations in Telecommunication (1G, 2G, 3G, 4G)

Parameters	1G	2G	3G	4G
Image				
Name	1st Generation Mobile Network	2nd Generation Mobile Network	3rd Generation Mobile Network	4th Generation Mobile Network
Introduced in year	1980s	1993	2001	2009
Location of first commercialization	USA	Finland	Japan	South Korea
Technology	AMPS (Advanced Mobile Phone System), NMT, TACS	IS-95, GSM	IMT2000, WCDMA	LTE, WiMAX
Multiple Address/Access system	FDMA	TDMA, CDMA	CDMA	CDMA
Switching type	Circuit switching	Circuit switching for Voice and Packet switching for Data	Packet switching except for Air Interface	Packet switching
Speed (data rates)	2.4 Kbps to 14.4 kbps	14.4 Kbps	3.1 Mbps	100 Mbps
Special Characteristic	First wireless communication	Digital version of 1G technology	Digital broadband, speed increments	Very high speeds, All IP
Features	Voice only	Multiple users on single channel	Multimedia features, Video Call	High Speed, real time streaming
Supports	Voice only	Voice and Data	Voice and Data	Voice and Data
Internet service	No Internet	Narrowband	Broadband	Ultra Broadband
Bandwidth	Analog	25 MHz	25 MHz	100 MHz
Operating frequencies	800 MHz	GSM: 900MHZ, 1800MHz CDMA: 800MHz	2100 MHz	850 MHz, 1800 MHz
Band (Frequency) type	Narrow band	Narrow band	Wide band	Ultra Wide Band
Carrier frequency	30 KHZ	200 KHz	5 MHz	15 MHz
Advantage	Simpler (less complex) network elements	Multimedia features (SMS, MMS), Internet access and SIM introduced	High security, international roaming	Speed, High speed handoffs, MIMO technology, Global mobility
Disadvantages	Limited capacity, not secure, poor battery life, large phone size, background interference	Low network range, slow data rates	High power consumption, Low network coverage, High cost of spectrum licence	Hard to implement, complicated hardware required
Applications	Voice Calls	Voice calls, Short messages, browsing (partial)	Video conferencing, mobile TV, GPS	High speed applications, mobile TV, Wearable devices

Generation	1G	2G	2.5G	3G	3.5G	4G	5G
Start	1970-1980	1990-2000	2001-2004	2004-2005	2006-2010	2011-Now	Soon (2020)
Data Bandwidth	2 Kbps	64 Kbps	144 Kbps	2 Mbps	More than 2 Mbps	1 Gbps	more than 1 Gbps
Technology	Analog Cellular	Digital Cellular	GPRS, EDGE, CDMA	CDMA 2000 (1xRT, EVDO) UMTS, EDGE	EDGE. Wi-Fi	WiMax LTE Wi-Fi	wwww
Service	Voice	Digital Voice, SMS,Higher Capacity Packet Size Data	SMS, MMS	Integrated High Quality Audio, Video & Data	Integrated High Quality Audio, Video & Data	Dynamic Information access, Wearable Devices	Dynamic Information access, Wearable Devices with AI Capabilities
Multiplexing	FDMA	TDMA, CDMA	CDMA	CDMA	CDMA	CDMA	CDMA
Switching	Circuit	Circuit, Packet	Packet	Packet	All Packet	All Packet	All Packet
Core Network	PSTN	PSTN	PSTN	Packet N/W	Internet	Internet	Internet
Handoff	Horizontal	Horizontal	Horizontal	Horizontal	Horizontal	Horizontal & Vertical	Horizontal & Vertical

Differences Between IEEE802.11 and IEEE802.16

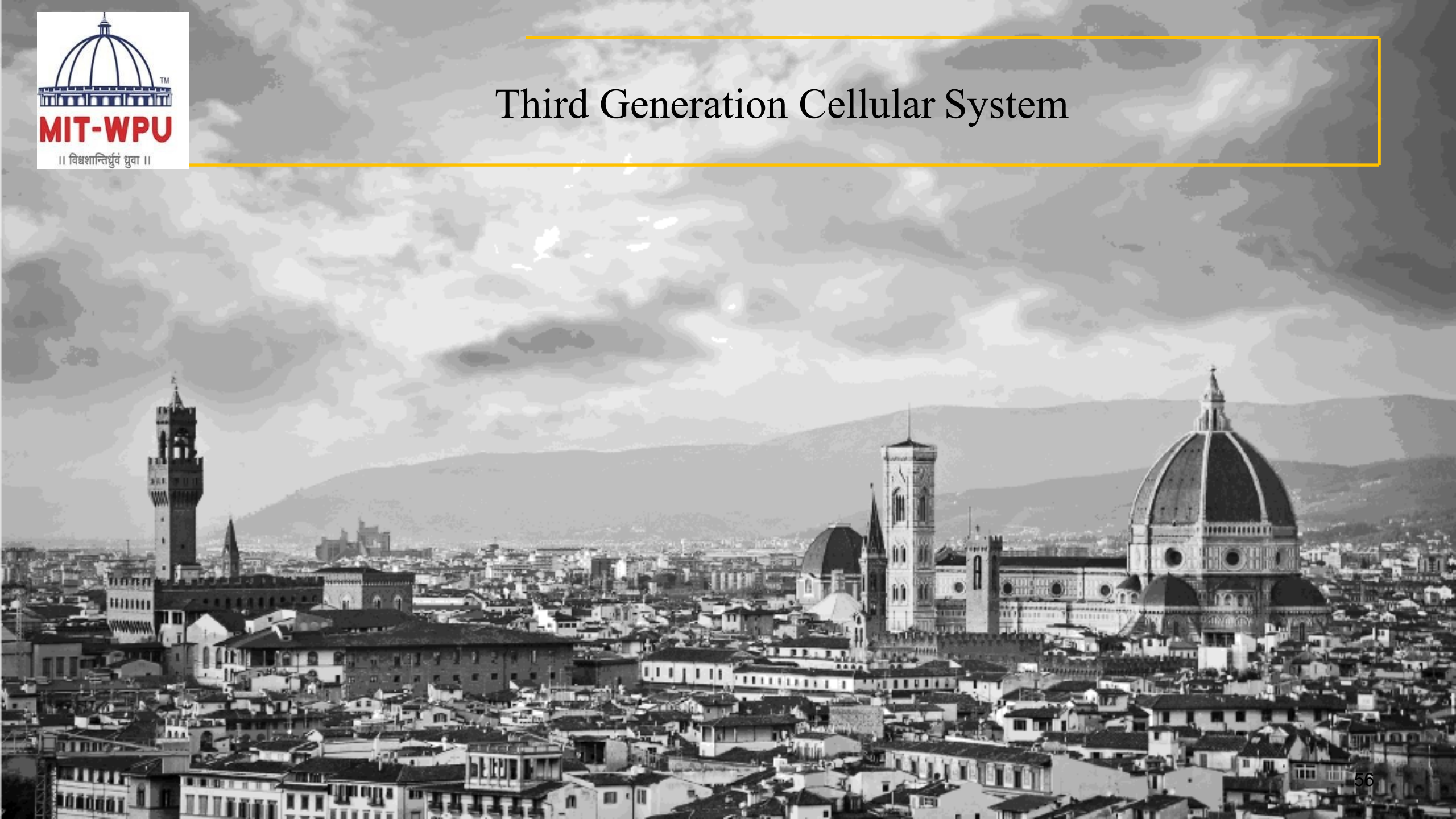
❖IEEE 802.11 has been designed for mobile terminals, which is irrelevant in the context of MANs. IEEE 802.16 has been designed for broadband data such as digital video and telephony.

❖The number of users and bandwidth usage per user is much higher in a typical IEEE 802.16 network when compared to a typical IEEE 802.11 basic service set. This calls for usage of a larger frequency spectrum in IEEE 802.16 as against the ISM bands used by IEEE 802.11. BWA typically uses millimeter wave bands and microwave bands (above 1 GHz frequencies).

❖IEEE 802.16 is completely connection-oriented and QoS guarantees are made for all transmissions. Though IEEE 802.11 provides some QoS support for real-time data (in the PCF mode), it has not been designed for QoS support for broadband usage.

Characters	Bluetooth	Wi-Fi	WiMax
Start date	1998	1990	
Transfer rate of data	800Kbps	11Mbps	1Gbps
Operating Frequency	2.4GHz	2.4GHz	2.3-3.5GHz
Range	10m	100m	50km
IEEE standard	IEEE 802.15	IEEE 802.11	IEEE 802.16
Power consumption	5mW	10mW	~5mW
Authorize	Bluetooth SIG	IEEE WECA	WiMax
Primary device	Industrial automation devices, PDAs,	Desktop, computers, notebook	Home devices, mobile phones,

Third Generation Cellular System



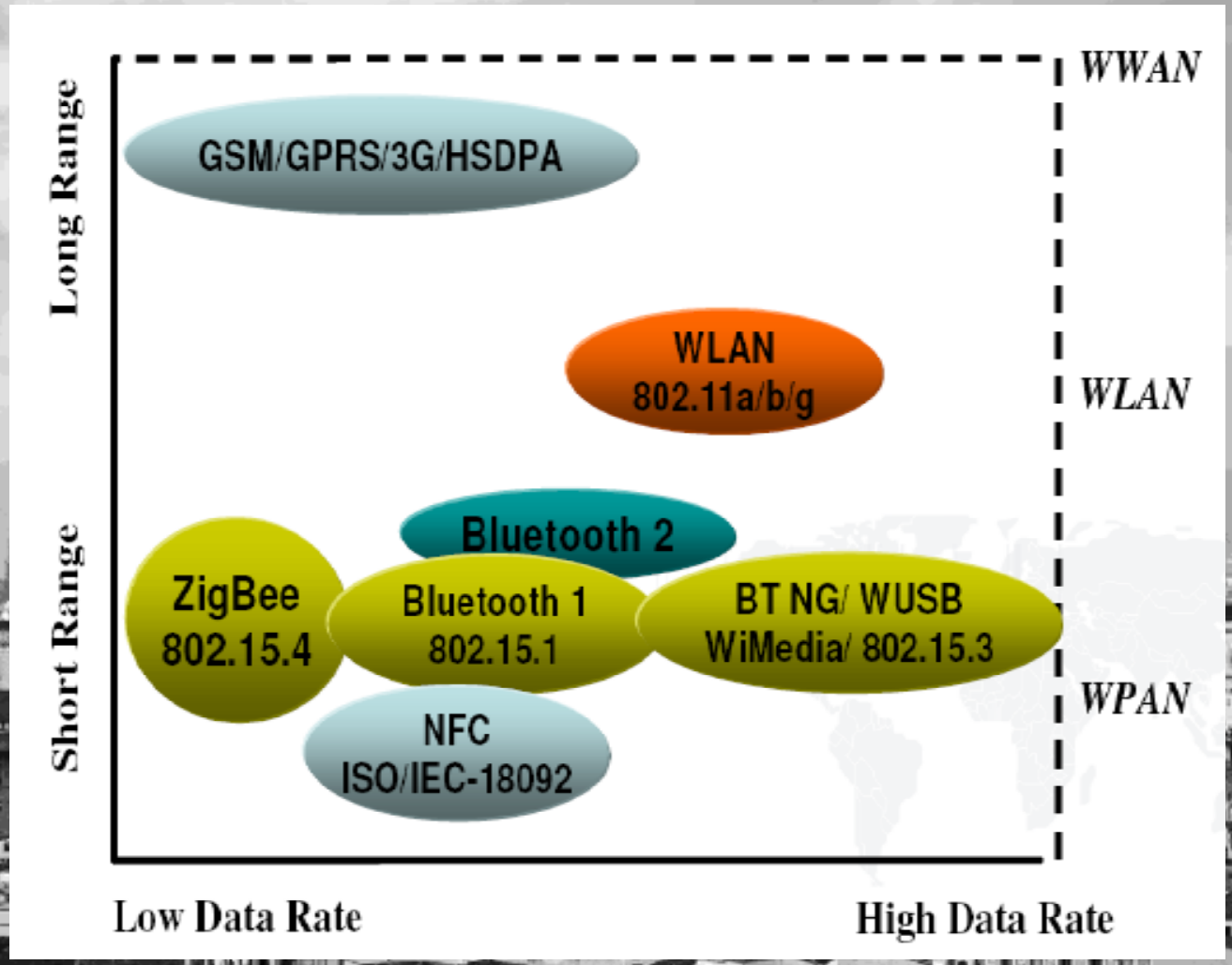
Near Field Communication

NFC = **Near Field Communication**

A short-range wireless connectivity technology

- Operates at 13.56 Mhz
- Based on RFID technology
- Data transfer rate: up to 424 kbits/second
- Reader & Tag communicate
- Promoted by the NFC-Forum

Comparison with other Wireless Networks



Near Field Communication

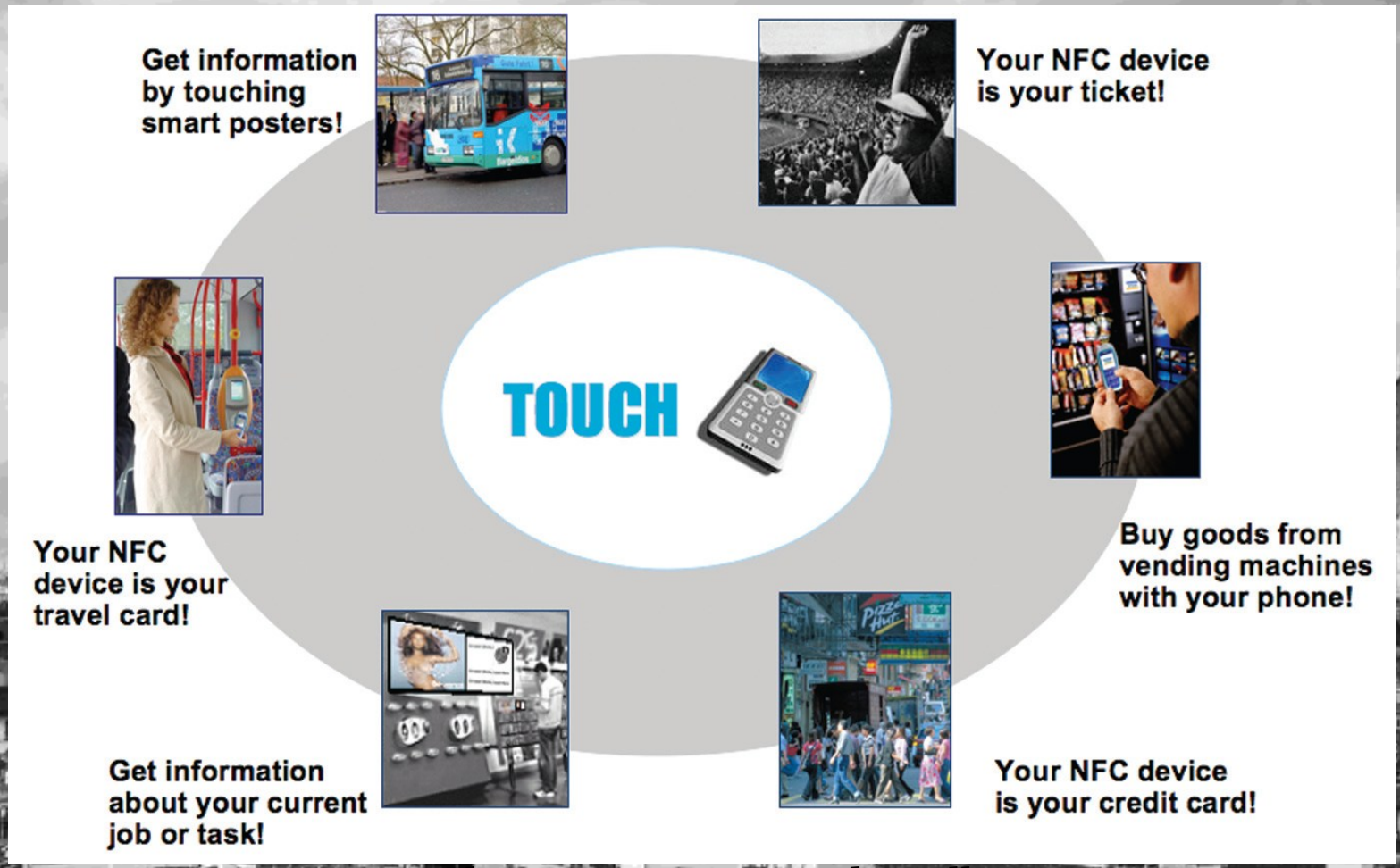
Advantages:

- Quick setup time (<0.1ms)
- Short range distance (up to 10cm)
- Does not require line of site
- Backward compatibility
- Consumer experience

NFC Use cases

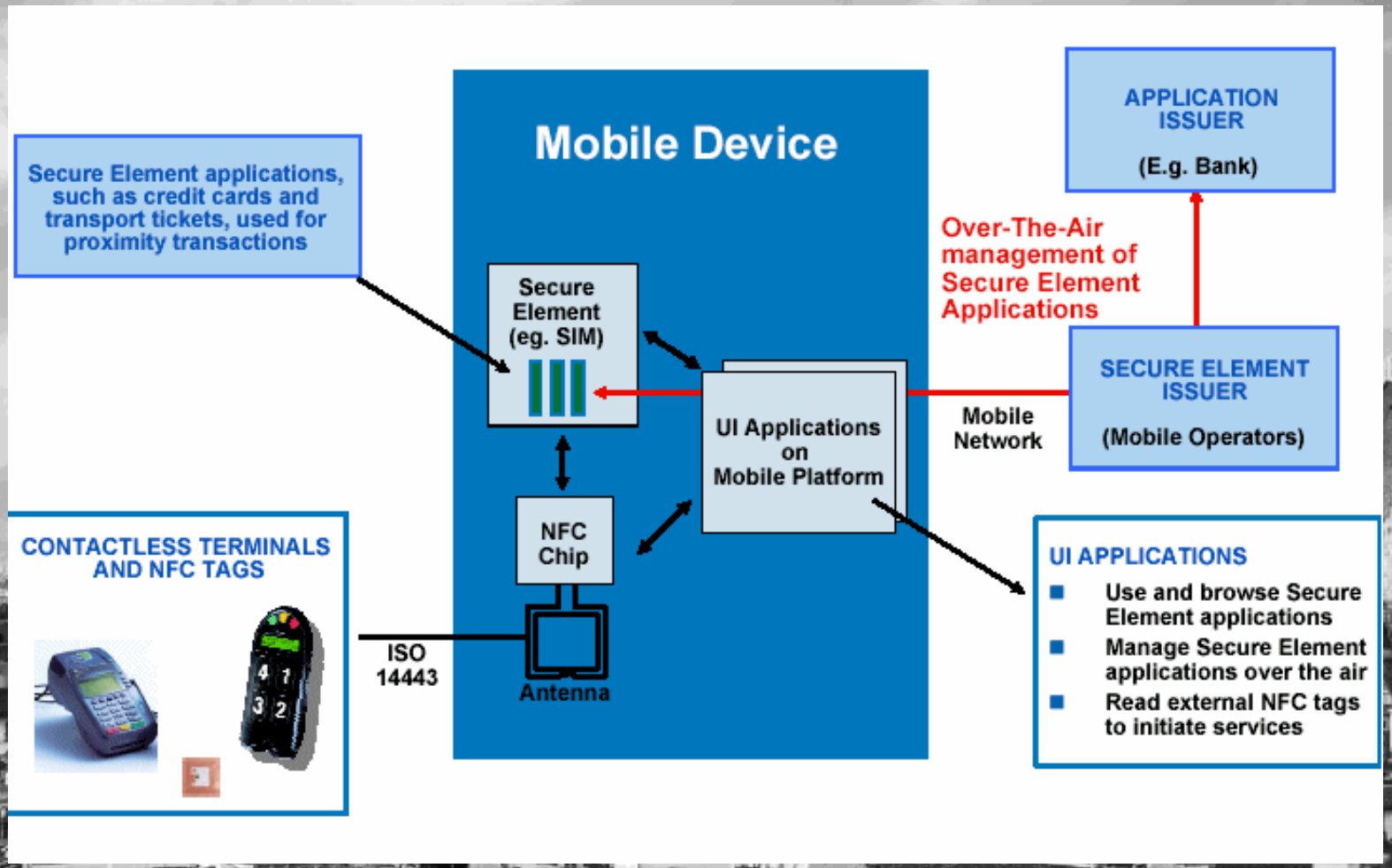
- Connect Electronic Devices
  - Exchange data
  - Simple, secure pairing e.g. Bluetooth
- Access Information
  - Advertisements
  - Identification Cards
- Mobile transactions
  - Contactless payment
  - Mobile ticketing

NFC use cases



Phone = Keys, ID card, Wallet

Mobile payment Architecture



NFC Challenges

- Security
  - Eavesdropping, Data corruption
  - Solution: Establish secure channel
- NFC ecosystem
  - Technology already in-place
  - Monetization issues
  - Operators, Handset Manufacturers, Banks
  - Solution: Market push, agreement

NFC future work

- Mobile Payment infrastructure
  - Goals: Security, Openness, Interoperability
- New NFC use cases
  - Location sensing
  - Supply Chains
  - Multiple Tags

NFC on Mobile Phones: Issues, Lessons and Future Research Vassilis Kostakos, Eamonn O'Neill
March 2007 **PERCOMW '07:** Proceedings of the Fifth IEEE International Conference on Pervasive Computing and Communications Workshops

An Assessment of NFC for Future Mobile Payment Systems Jan Madrus, Yves Pigneur
July 2007 **ICMB '07:** Proceedings of the International Conference on the Management of Mobile Business

Publisher: IEEE Computer Society

Managing an NFC Ecosystem Gerald Madlmayr, Josef Langer, Josef Scharinger
July 2008 **ICMB '08: Proceedings of the 2008 7th International Conference on Mobile Business - Volume 00** , Volume 00

Introduction to Ultra-Wide Band Communication

- Extremely short bursts of radio frequency.
- One bursts last from few tens of picoseconds to few nanoseconds
- The bursts are spread across a very, very broadband of frequencies.
- Frequency range of 3.1GHz to 10.6GHz
- This is sometimes called “carrier-free”
- Very low interference with existing RF communications

UWB vs Current Technology

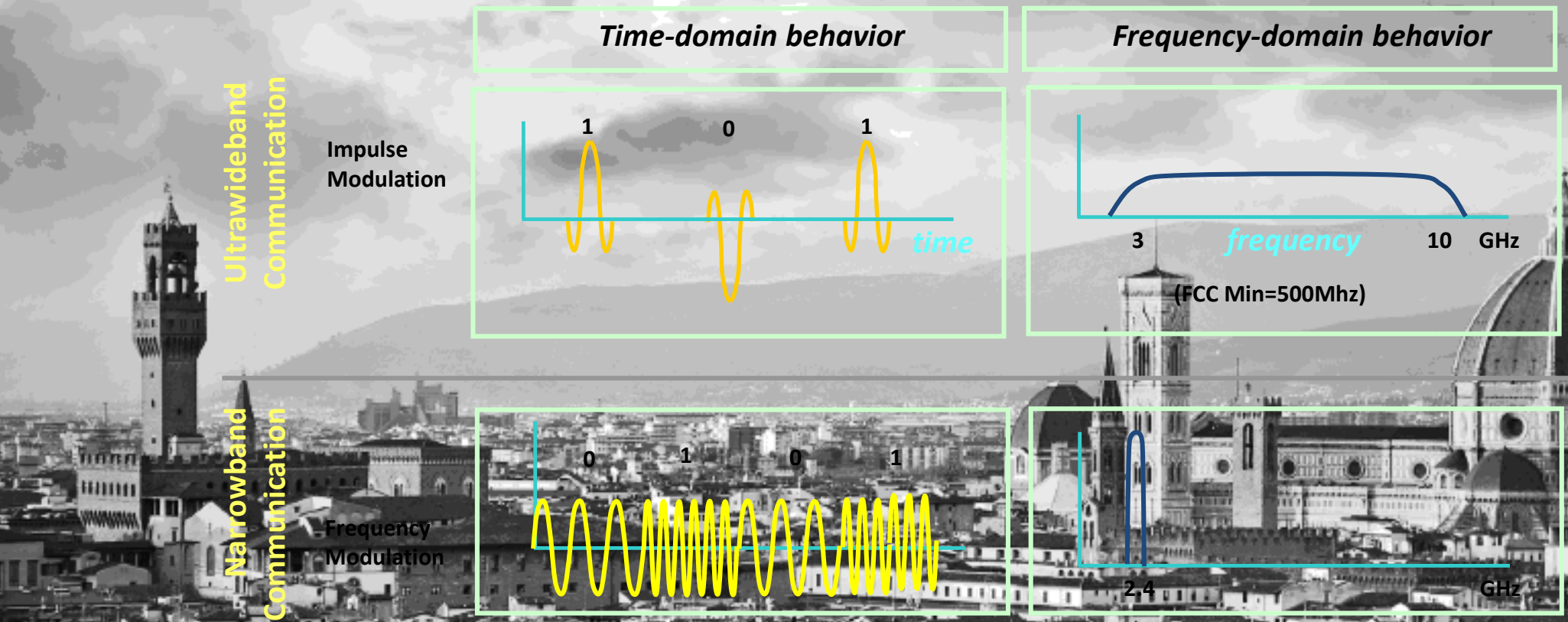
UWB: 110Mbps, 220Mbps by year's end
802.11g: 54Mbps

UWB: Has no IEEE standard
802.11: An IEEE standard

UWB: ~ 10 meter range
802.11b: 100+ meter range

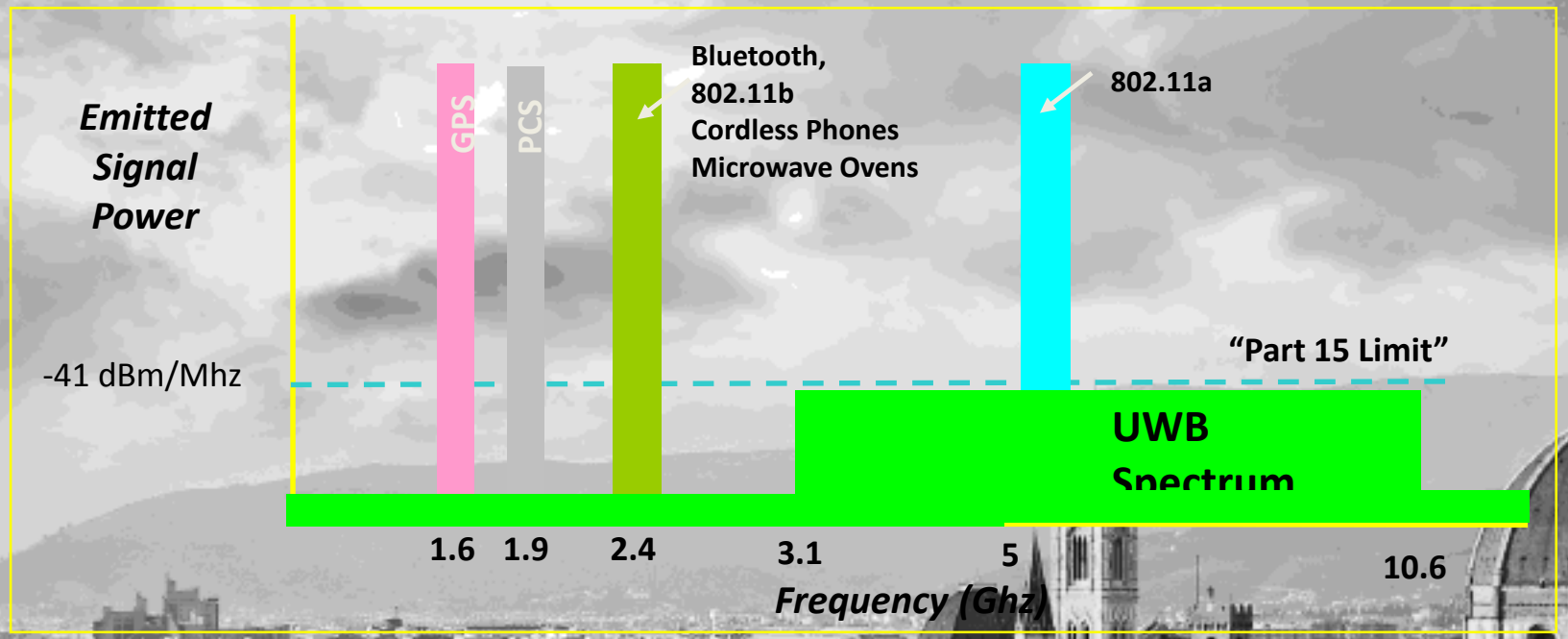
What is Ultra Wideband?

Radio technology that modulates impulse based waveforms instead of continuous carrier waves



UWB Spectrum

FCC ruling permits UWB spectrum overlay



- FCC ruling issued 2/14/2002 after ~4 years of study & public debate
- FCC believes current ruling is conservative

So why is UWB so Interesting?

7.5 Ghz of "free spectrum" in the U.S.
- FCC recently legalized UWB for commercial use
- Spectrum allocation overlays existing users, but its allowed power level is very low to minimize interference

Very high data rates possible
- 500 Mbps can be achieved at distances of 10 feet under current regulations

"Moore's Law Radio"
- Data rate scales with the shorter pulse widths made possible with ever faster CMOS circuits

Simple CMOS transmitters at very low power
- Suitable for battery-operated devices
- Low power is CMOS friendly

Ultra Wideband Characteristics

Extremely low transmission energy (less than 1mW)
Very high bandwidth within short range (200Mbps within 10m)
Extremely difficult to intercept
- Short pulse excitation generates wideband spectra – low energy densities
- Low energy density also minimizes interference to other services

Multipath immunity
Commonality of signal generation and processing architectures
Radar
- Inherent high precision – sub-centimeter ranging
- Wideband excitation for detection of complex, low RCS targets

Geolocation/Positioning
- Sub-centimeter resolution using pulse leading edge detection
- passes through building blocks, walls, etc. (LOS not required)

Low Cost
- Nearly "all-digital" architecture
- ideal for microminiaturization into a chipset

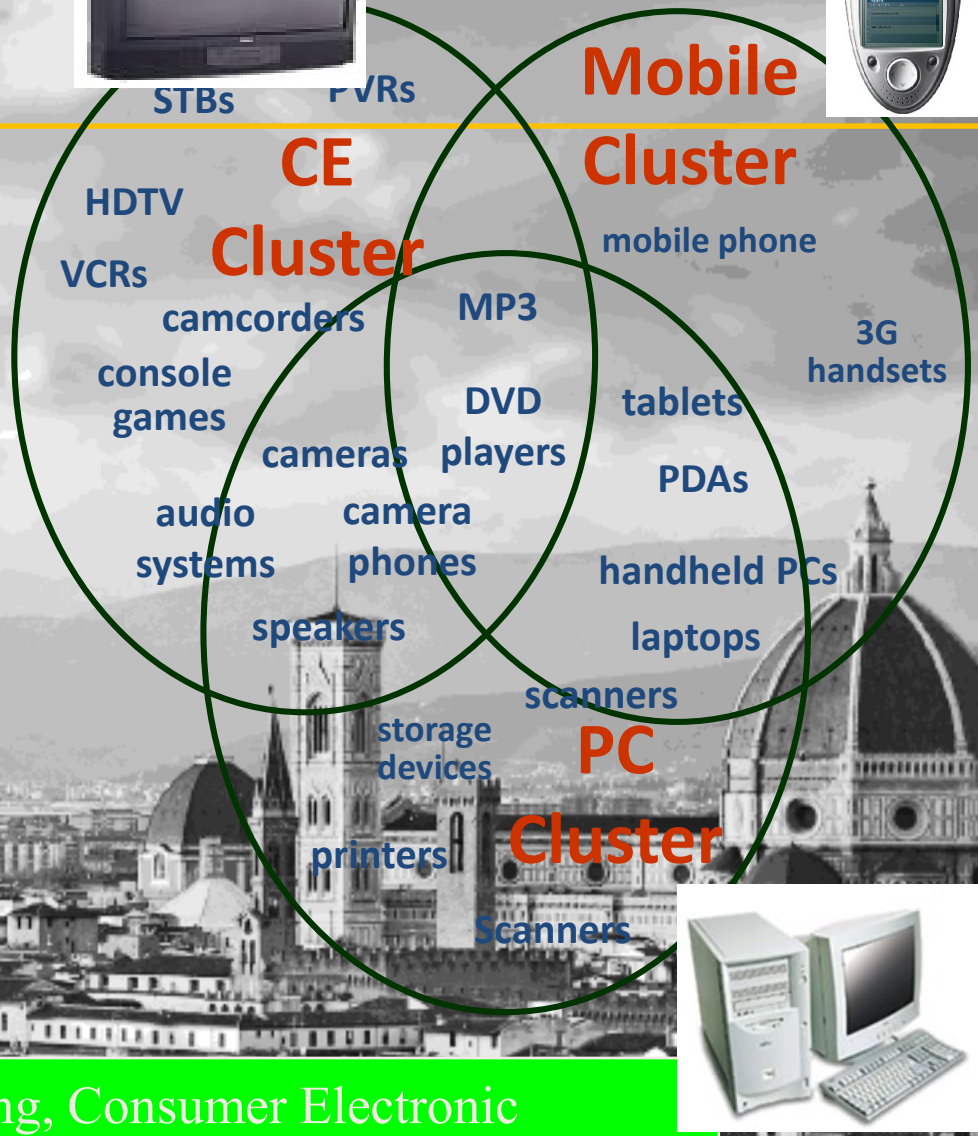
Frequency diversity with minimal hardware modifications

UWB Advantages

- Capacity
  - possibility of achieving high throughput
- Low power & Low cost
  - Can directly modulate a baseband pulse
  - Can be made nearly all digital
  - High capacity with lower Tx power levels
- Fading robustness
  - Wideband nature of the signal reduces time varying amplitude fluctuations (?)
  - Relatively immune to multipath cancellation effects
    - Path delay ~ 1ns > pulse duration
    - But don't we build RAKE just to rebuild the multipath thing ?
    - What about ISI ?
- Position location capability
  - Developed first as radar technology (!)
- Flexibility
  - Can dynamically trade-off throughput for distance

UWB Application 1 : WPAN

- Desktop and Laptop PCs
  - High res. printers, scanners, storage devices, etc
  - Connectivity to mobile and CE devices
- Mobile Devices
  - Multimedia files, MP3, games, video
  - Personal connectivity CE Devices
  - Cameras, DVD, PVR, HDTV
  - Personal connectivity



One PHY for Personal Computing, Consumer Electronic and Mobile, Wireless Personal Area Connectivity

UWB Application 2

Positioning, Geolocation, Localization

- High Multipath Environments
- Obscured Environments

Communications

- High Multipath Environments
- Short Range High Data Rate
- Low Probability of Intercept/ Interference

Radar/Sensor : MIR (motion detector, range-finder, etc.)

- Military and Commercial: Asset Protection
- Anti-Terrorist/Law Enforcement
- Rescue Applications

Related Standards

IEEE 802.15 : Wireless Personal Area Network (WPAN)
IEEE 802.15.1 : Bluetooth, 1Mbps
IEEE 802.15.3 : WPAN/high rate, 50Mbps
IEEE 802.15.3a: WPAN/Higher rate, 200Mbps, UWB
IEEE 802.15.4 : WPAN/low-rate, low-power, mW level, 200kbps

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Learning Resources

Text books

1. C. Siva Ram Murthy, B.S. Manoj, “Adhoc Wireless Networks Architectures and Protocols”, PHI, ISBN - 9788131706885, 2007.
2. Nekoley Elenkov, “Android Security internals”, No Starch Press, ISBN-10: 1-59327-581-1 ISBN-13: 978-1-59327-581

Reference Books

1. KiaMakki, Peter Reiher, “Mobile and Wireless Network Security and Privacy “, Springer, ISBN 978-0-387-71057-0, 2007.
2. Hakima Chaouchi, Maryline Laurent-Maknavicius , “Wiress and Mobile Networks Security”, Wiley publication, ISBN 978-1-84821-117-9
3. Noureddine Boudriga, “Security of Mobile Communications”, ISBN 9780849379413, 2010.
4. Kitsos, Paris; Zhang, Yan, “RFID Security Techniques, Protocols and System-On-Chip Design”, ISBN 978-0-387-76481-8, 2008.
5. Johny Cache, Joshua Wright and Vincent Liu,” Hacking Wireless Exposed: Wireless Security Secrets & Solutions “, second edition, McGraw Hill, ISBN: 978-0-07-166662-6, 2010
6. Tim Speed, Darla Nykamp,Mari Heiser,Joseph Anderson,Jaya Nampalli, "Mobile Security: How to Secure, Privatize, and Recover Your Devices", Copyright © 2013 Packt Publishing, ISBN 978-1-84969-360-8

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Learning Resources

Web Resources:

i. http://whatis.techtarget.com/definition/mobile-security

ii. http://techgenix.com/security/mobile-wireless-security/

Weblinks

i. https://en.wikipedia.org/wiki/Mobile_security

MOOCs:

i. https://www.ntnu.edu/studies/courses/TTM4137#tab=omEmnet
ii. http://nptel.ac.in/courses/106105160/37
iii. https://www.eccouncil.org/
iv. https://www.csoonline.com/article/2122635/mobile-security/wireless-security--the-basics.html

THANK YOU FOR LISTENING ANY QUESTION?