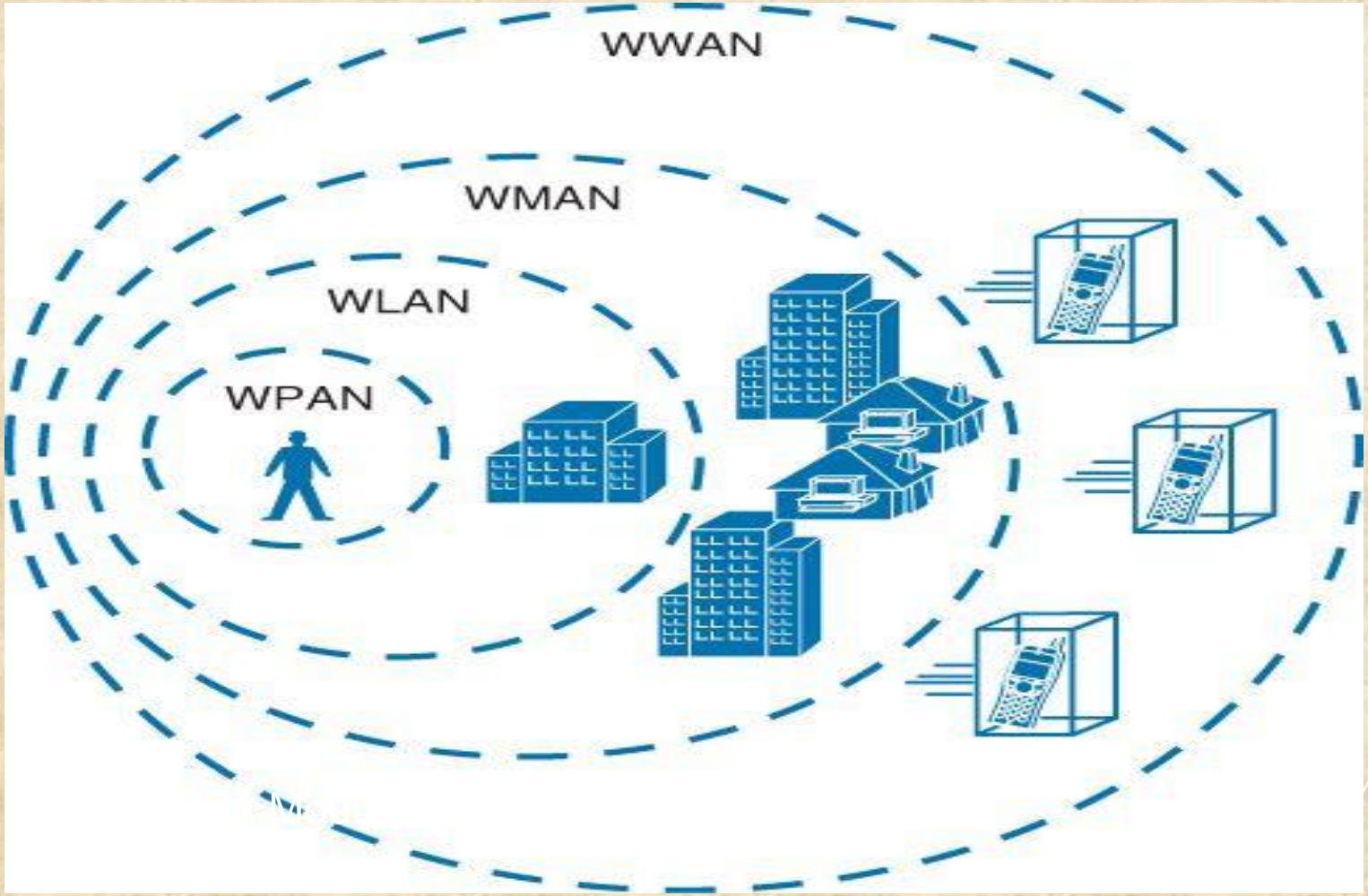
MODULE 3

WIRELESS METROPOLITAN AND LOCAL AREA NETWORKS

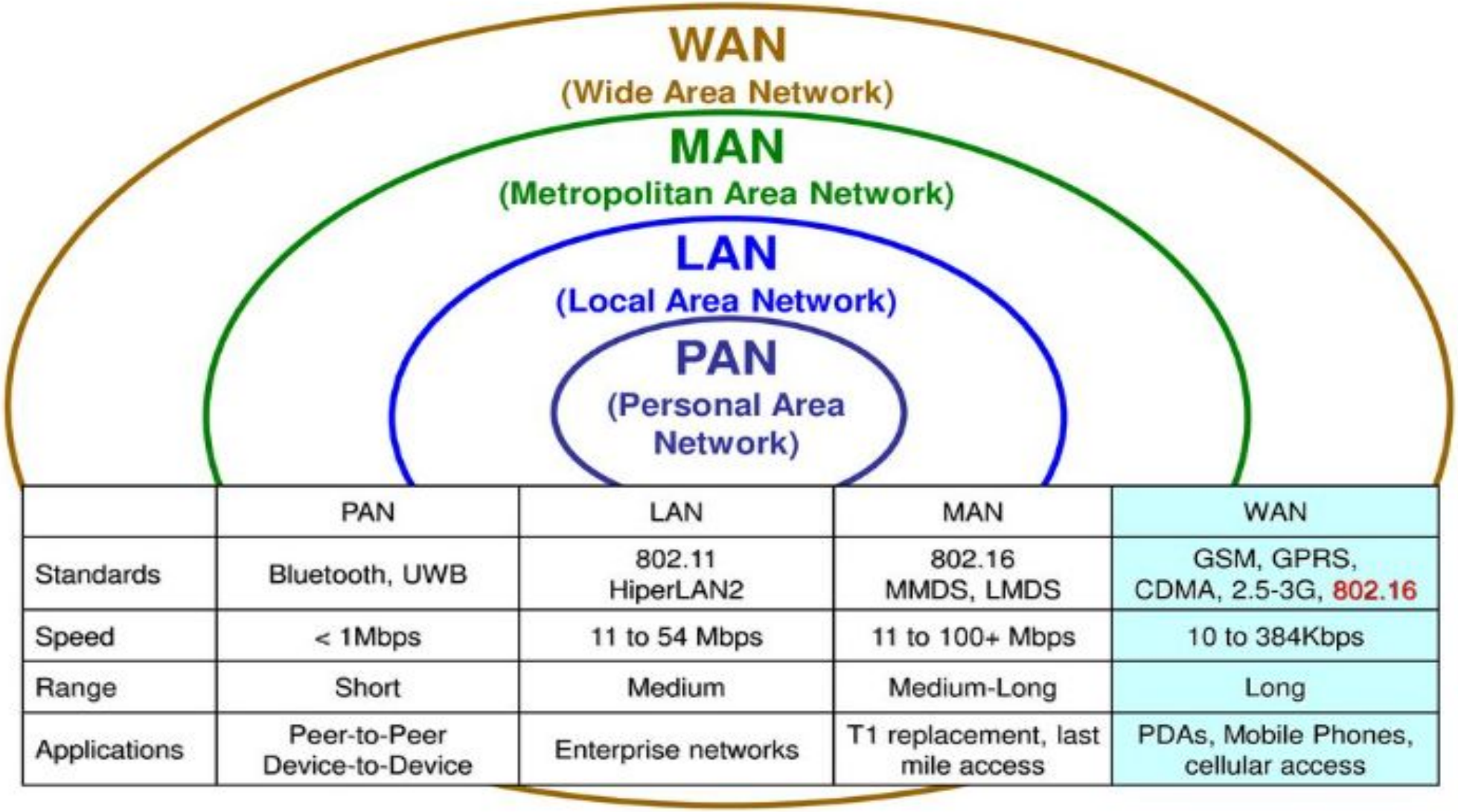
IEEE 802.16 (WIMAX) – MESH MODE, PHYSICAL AND MAC LAYER; IEEE 802.11(WI-FI) – ARCHITECTURE, PROTOCOL STACK, ENHANCEMENTS AND APPLICATIONS.

SELF-LEARNING TOPICS:- WLL(WIRELESS LOCAL LOOP)

Wireless Metropolitan Area Networks(WMAN)



Background: Wireless Technologies



	PAN	LAN	MAN	WAN
Standards	Bluetooth, UWB	802.11 HiperLAN2	802.16 MMDS, LMDS	GSM, GPRS, CDMA, 2.5-3G, 802.16
Speed	< 1Mbps	11 to 54 Mbps	11 to 100+ Mbps	10 to 384Kbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise networks	T1 replacement, last mile access	PDAs, Mobile Phones, cellular access

Wireless Metropolitan Area Networks

- Metropolitan area networks (MANs) are large computer networks usually spanning a city.
- They typically use wireless infrastructure or optical fiber connections to link their sites.
- A MAN is optimized for a larger geographical area compared to local area network (LAN),ranging from several blocks of buildings to the entire city.
- They often provide means for internetworking of local networks. MANs can span up to 50 km.
- The wireless MAN (WMAN) is a promising broadband wireless access (BWA) technology that provides high-speed, high-bandwidth efficiency, and high-capacity multimedia services for both residential and enterprise applications

WiMAX: WiMAX is defined as worldwide interoperability for microwave access by the WiMAX Forum, promises to deliver last mile wireless broadband Internet access capable of carrying data intensive applications

-June 2001 to promote conformance and interoperability of the IEEE 802.16 standard, officially known as Wireless MAN.

- Some members of WiMAX(IEEE 802.16a) Forum are Airspan Networks, Alvarion, Aperto Networks, Ensemble Communication, Fujitsu of America, Intel, Nokia, Proxim, and Wi-LAN.
- The Forum describes WiMAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and digital subscriber line(DSL).'

Last mile: the final leg of the telecommunications networks that deliver services to retail end-users

- WiMAX operates over licensed and non-licensed frequencies using non-line-of-sight (NLOS) and line-of-sight (LOS) technologies, extending broadband coverage to cities and towns wirelessly via a MAN.
- In NLOS, a small antenna on the mobile unit is connected to the WiMAX tower.
- In this mode, WiMAX uses a lower frequency range of 2–11 GHz (similar to Wi-Fi).
- In LOS, a fixed dish antenna points straight at the WiMAX tower from a rooftop or a pole.
- The LOS connection is stronger and more stable, so it is able to send a lot of data with fewer errors.

- LOS transmissions use higher frequencies, with ranges reaching approximately 66 GHz.
- the average cell ranges for most WiMAX networks have 4–5 mile range (in NLOS capable frequencies) even through tree cover and building walls.
- Service ranges up to 10 miles (16 km) are very likely LOS applications.
- Ranges beyond 10 miles are possible but may not be desirable for heavily loaded networks.

IEEE 802.16 Goal

To provide high-speed Internet access to home and business subscribers without wires.

- It supports services such as voice over IP (VoIP), transmission control protocol/Internet protocol (TCP/IP) applications with different quality of service (QoS) requirements, etc.

Properties of IEEE 802.16

Some of the important properties of IEEE 802.16 are as follows:

1. It has broad bandwidth that supports up to 134 Mbps in 28 MHz channel (in 10–66 GHz air interface).

2. It supports multiple services and efficiently transports IPv4, IPv6, asynchronous transfer mode (ATM), Ethernet, etc.

3. It has media access control (MAC) designed for efficient use of spectrum which has comprehensive, modern, and extensible security.

4. It has point-to-multipoint topology (P2MP) with mesh extensions.

5. It supports adaptive antennas and space–time coding.

IEEE 802.16 Standards-(802.16a, 802.16c, 802.16d, 802.16e, and 802.16m)

Parameters	*IEEE 802.16*	*IEEE 802.16a*	*IEEE 802.16e*
Spectrum	10–66 GHz	2–11 GHz	<6 GHz
Configuration	Line-of-sight	Non-line-of-sight	Non-line-of-sight
Bit rate	32–134 Mbps (28 MHz channel)	≤70 or 100 Mbps (20 MHz channel)	Up to 15 Mbps
Modulation	QPSK, 16-QAM, 64-QAM	256 subcarrier OFDM using QPSK, 16-QAM, 64-QAM, 256-QAM	Same as 802.16a
Mobility	Fixed	Fixed	≤75 Mph
Channel bandwidth	20, 25, 28 MHz	Selectable 1.25–20 MHz	5 MHz (planned)
Typical cell radius	1–3 miles	3–5 miles	1–3 miles

IEEE 802.16 vs. IEEE 802.11

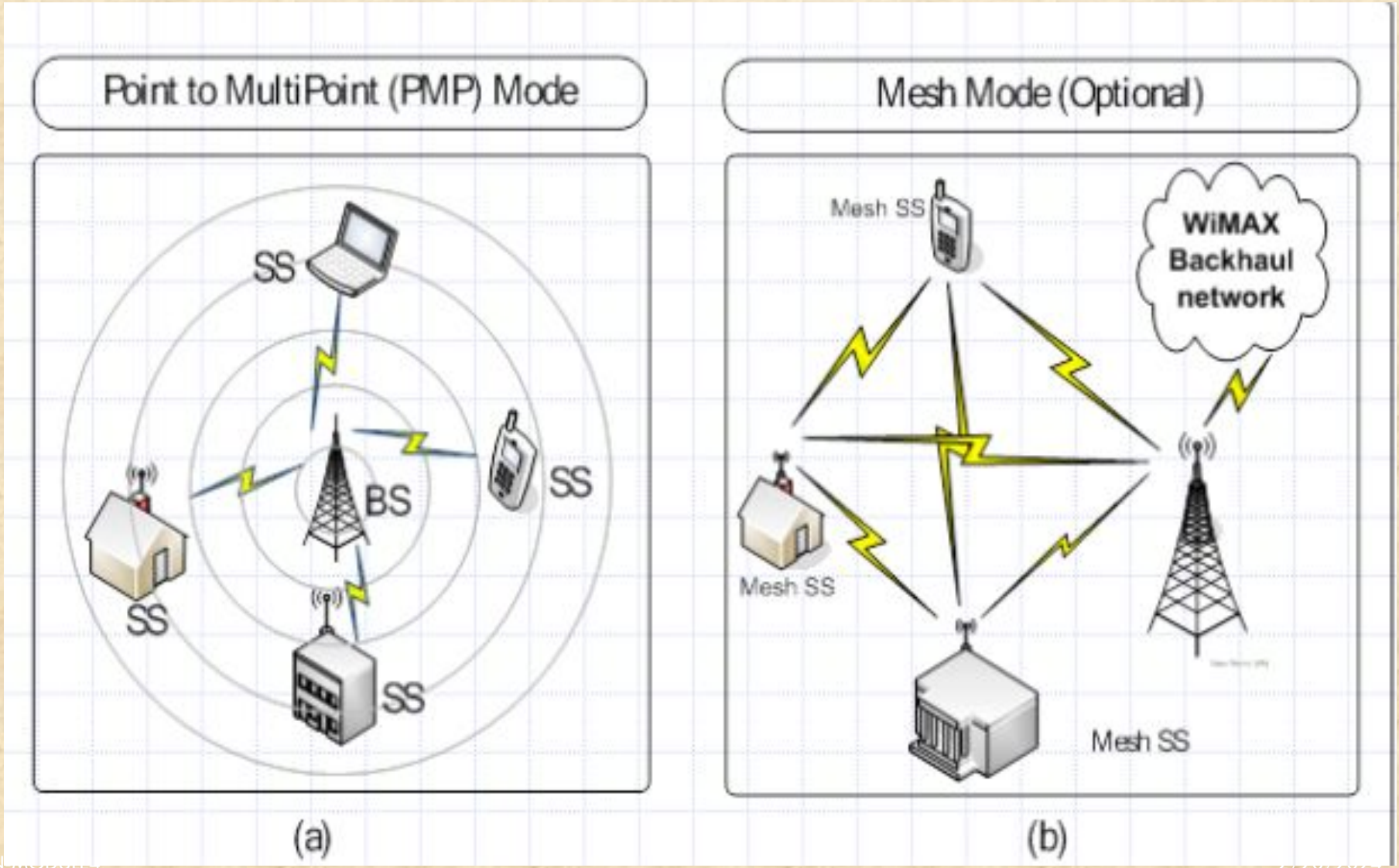
Parameter	*IEEE 802.11*	*IEEE 802.16*	*Explanation*
Range	**30–100 m**	**Typical cell size: 7–10 km; up to 50 km; no hidden stations.**	**802.16 handles multipath propagation much better. Good signal quality in larger Distances**
Target usage	**Indoor**	**Outdoor; support of mesh topologies**	**802.16 is used outdoor.**
Scalability	**Bandwidth of 20 MHz is fixed**	**Bandwidth between 1.5 and 28 MHz allows an adaptation to the users.**	**802.16 has no problem with overlapping cells; usage of demand assignment multiple access (DAMA)–time division multiple access (TDMA) instead of CSMA/CA; adaptive modulation possible.**

Contd…

Parameter	*IEEE 802.11*	*IEEE 802.16*	*Explanation*
Data rate	**Up to 54 Mbps**	**Up to 134 Mbps, depending on assigned bandwidth**	**OFDM with higher modulation ratio; net data rate also is higher (due to DAMA)**
QoS	**Only with 802.11e**	**Differentiated services**	**Reservation of capacity allows several service classes.**
Costs	**License-free**	**License-free as well as licensed bands.**	**Costs are accepted in 802.16 – alternative to xDSL**

Architecture

- P2MP (Point to Multi point)
  - Wireless MAN
  - BS connected to Public Networks
  - BS serves Subscriber Stations (SS)
  - Provides SS with first mile access to Public Networks
- Mesh Architecture
  - Optional architecture for WiMAX


Point to MultiPoint (PMP) Mode
SS
BS
SS
SS
SS
(a)
Mesh Mode (Optional)
Mesh SS
WiMAX
Backhaul
network
Mesh SS
Mesh SS
(b)

WMAN Network Architecture

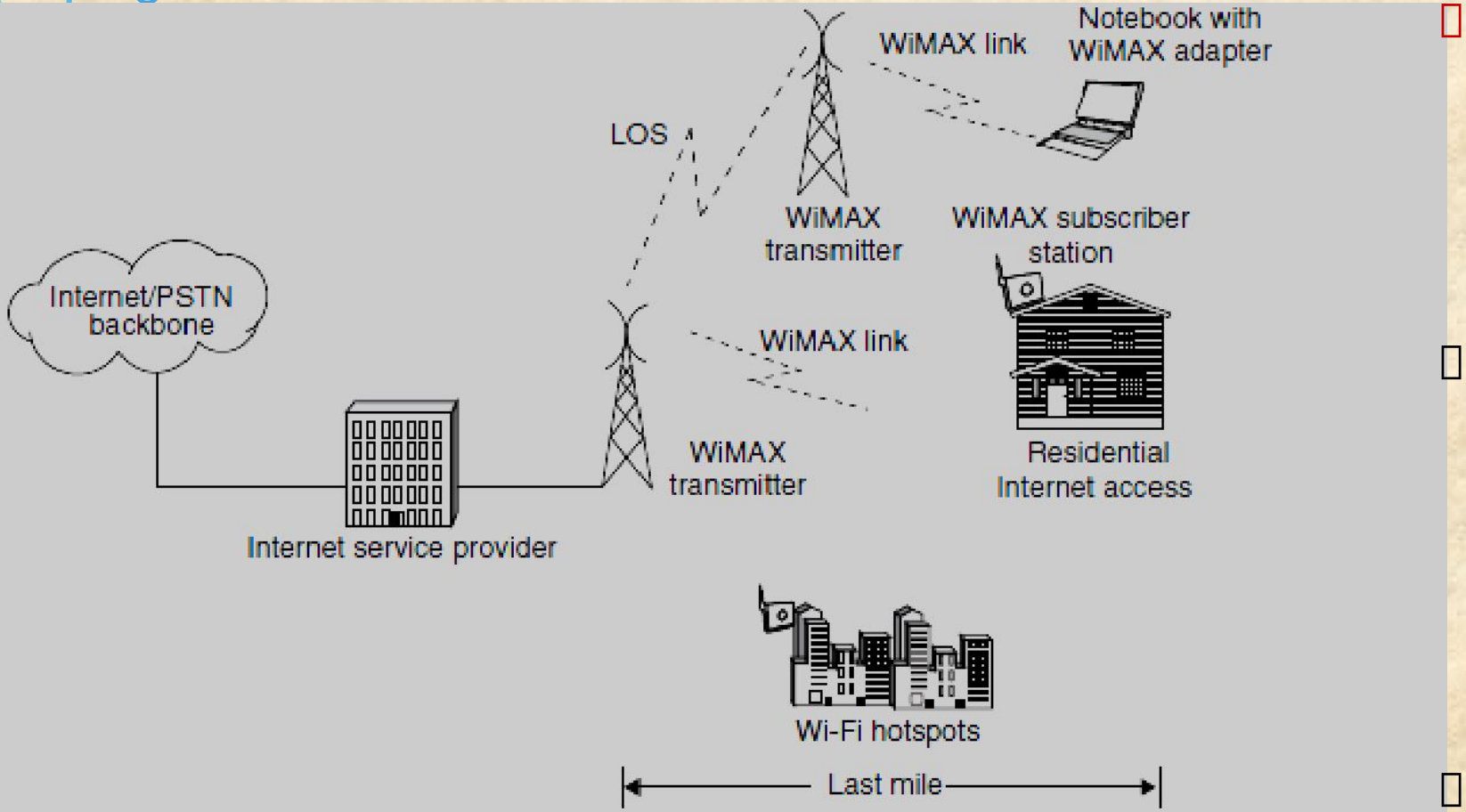


Figure 6.1 | WMAN network architecture.

A TYPICAL DISTRIBUTED WIMAX NETWORK ARCHITECTURE.

- Extension of the Internet or public switched telephone network (PSTN) to the mobile user
- The cell equipment in the WiMAX BS comprises the basic BS equipment, radio equipment, and a BS link to the backbone network.
- The BS provides the interface between the mobile users and the WiMAX network

- The coverage radius of a typical BS in urban areas is around 500–900 m.

Network Components

- The main components of the WiMAX system are the BS, WiMAX receiver, and the backhaul

1. **WiMAX base station:** A WiMAX BS consists of indoor electronics and a WiMAX tower.

coverage to a very large area up to a radius of 6 miles.

- The WiMAX BSs would use the MAC layer defined in the standard.
- A common interface makes the networks interoperable

and would allocate uplink (UL) and downlink (DL) bandwidth to subscribers according to their needs, on an essentially real-time basis.

- Each BS provides wireless coverage over an area called a *cell*.

- Theoretically, the maximum, radius of a cell is 50 km or 30 miles; however, practical considerations limit it to about 10 km or 6 miles.
- A BS and one or more subscriber stations (SSs) can form a cell with a P2MP structure.
- On air, the BS controls activity within the cell, including access to the medium by SSs, allocations to achieve QoS, and admission to the network based on network security mechanisms.

2.WiMAX receiver: A WiMAX receiver may have a separate antenna or could be a standalone box or an interface card sitting on the laptop or computer or any other device.

- This is also referred to as customer premise equipment (CPE)
- An 802.16-based system often uses fixed antenna at the SS site is mounted on the roof
- A BS typically uses either sectored/directional or omnidirectional antennas.
- A fixed SS typically uses directional antenna whereas a mobile or portable SS usually uses an omnidirectional antenna.

3. Backhaul:

- Backhaul refers to the connection from the access point to the BS and from the BS to the core network.
- It is possible to connect several BSs to one another using high-speed backhaul microwave links.

A WiMAX tower station can connect directly to the Internet using a high-bandwidth wired connection.

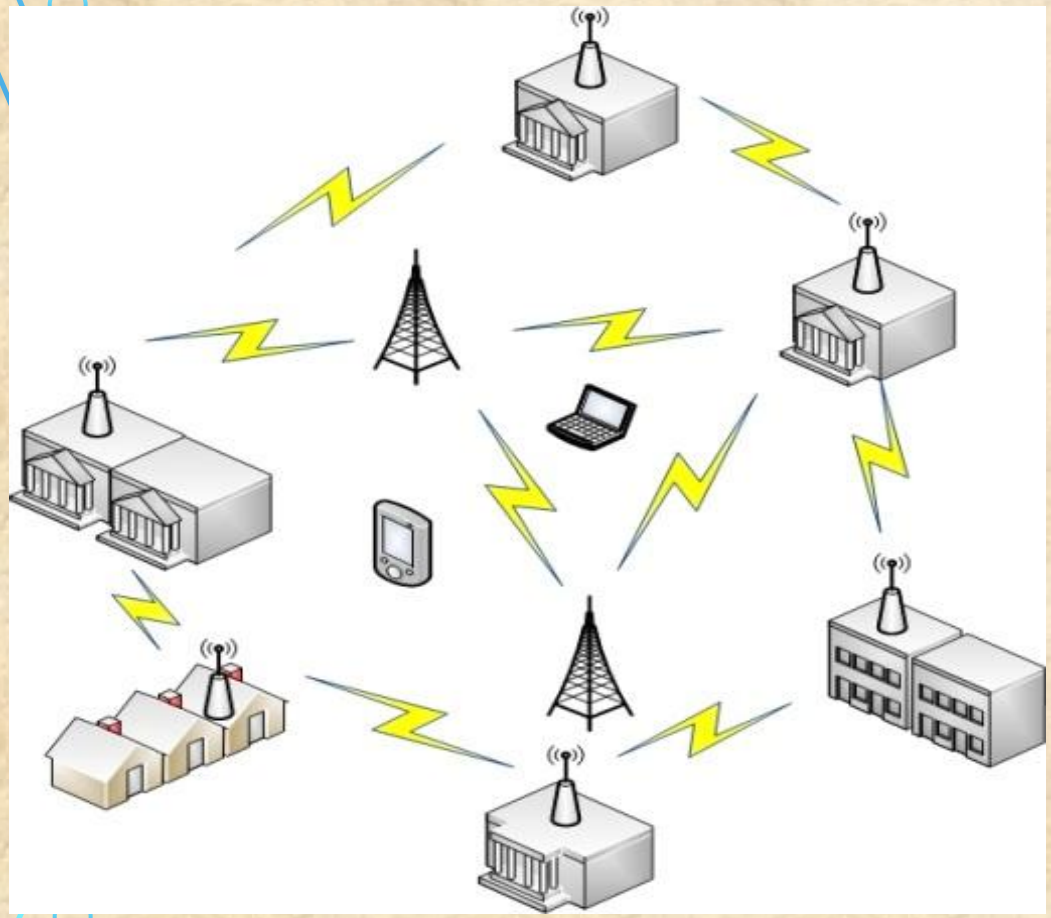
- It can also connect to another WiMAX tower using a LOS, microwave link.
- This allows for roaming by a WiMAX subscriber from one BS coverage area to another, similar to the roaming enabled by cell phones

- Each WiMAX service provider uses one or more licensed operating frequencies somewhere between 2 and 11 GHz.

- WiMAX link can transfer data (including handshaking and other overhead) at up to 70 Mbps, but most commercial WiMAX services are significantly slower than that.

- as more and more users share a single WiMAX tower and BS, there is a signal quality deterioration

WiMAX mesh network architecture-interconnect multiple mobile clients together with many WiMAX base stations (nodes).



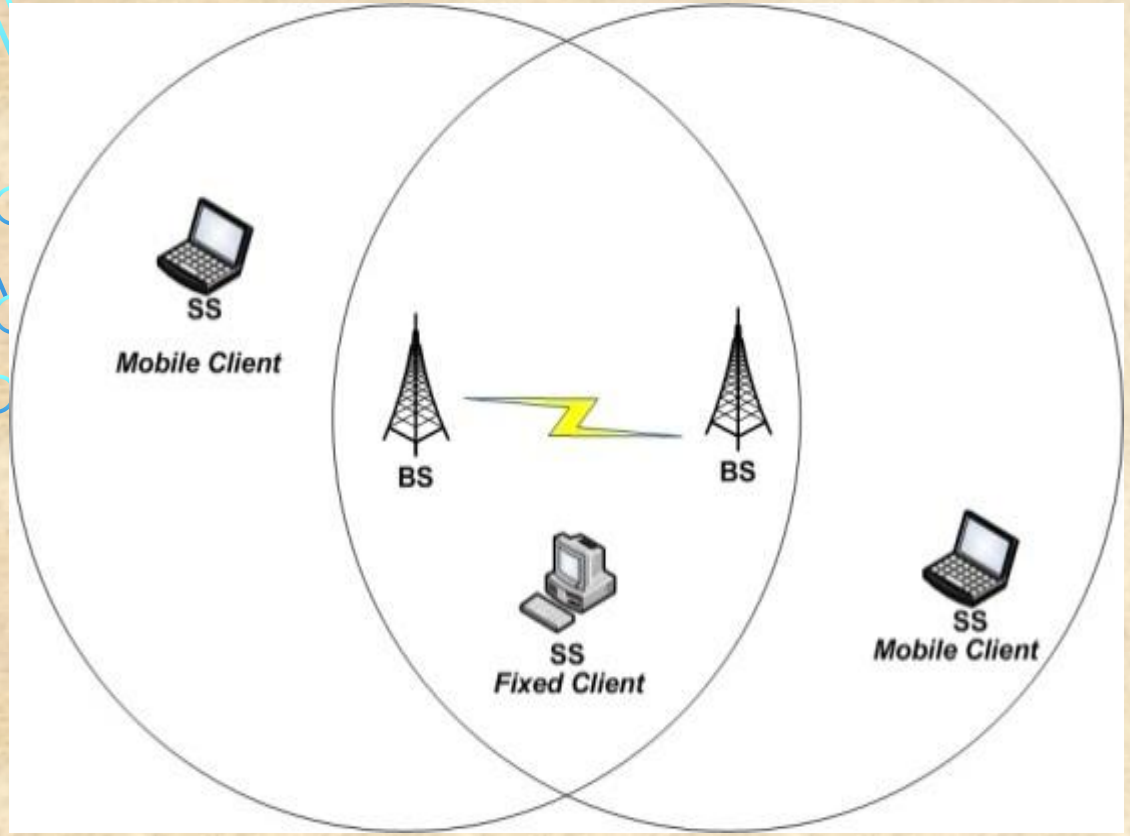
WIDE COVERAGE AREA FOR MOBILE CLIENTS.

Mesh networks --a dynamic topology that show a variable and constant change with growth or decline, and consist of nodes whose communication at the physical level occurs through variants of the IEEE 802.11 and IEEE 802.16 standard, and whose routing is dynamic.

In mesh networks, the access point / base stations area is usually fixed.

All the clients can communicate with each other and there is no need for an intermediate node to act as the mediator of the network.

The basic topology of an IEEE 802.16 mesh network consists of two participating entities, called Base Station (BS) and Subscriber Station (SS),



The BS is the central node, responsible for coordinating all the communication and providing connectivity to the client stations (fixed or mobile).

Operation

The most effective way to discover the operation of the mesh network is the routing protocol,

which scans the different possible routes / paths of data flow, on the basis of a pivot table where devices such as BS select the most efficient route to follow to reach a goal, while taking into account that the greater the speed, the packet loss, or the faster the access to the Internet (and others).

This scan is carried out several times per second and is transparent to the user, even when it occurs at re-routing access gateways, which are the nodes that have direct access to the internet

An important feature -concept of roaming, also known as a- transparent handoff mobility scheme offering fast handoff in wireless networks.

This makes it feasible for users to become mobile clients who can move around between network nodes without losing the connection at the time of exchange.

The practical consequence is that the system allows geographical mobility.
In a WiMAX mesh network, a “Mesh BS” (MBS – mesh base station) provides the external backhaul link.

The backhaul links connect the WiMAX network to other communication networks.
There may be multiple Mesh BSs in a network; other nodes are known as “Mesh SSs” (MSS – mesh subscriber stations).

In point-to-multipoint mode, the SSs are under the direct control of the BS.

In Mesh mode, the uplink and downlink is not clearly separated and SSs can communicate with each other without communicating with the BS.

Features of WiMAX(List features of IEEE802.16)

1. **Flexible architecture:** WiMAX supports several system architectures, including P2P, P2MP, and ubiquitous coverage.

- The WiMAX MAC supports P2MP and ubiquitous service by scheduling a time slot for each SS.
- If there is only one SS in the network, the WiMAX BS will communicate with the SS on a P2P basis.
- A BS in a P2P configuration may use a narrower beam antenna to cover longer distances

2.High security: WiMAX supports Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES).

- By encrypting the links between the BS and the SS, WiMAX provides subscribers with privacy (against eavesdropping) and security across the broadband wireless interface.
- Security also provides operators with strong protection against theft of service.
- WiMAX also provides protection for data that are being transmitted by different users on the same BS.

3.WiMAX QoS: WiMAX can be dynamically optimized for the mix of traffic that is being carried.

Five types of services are supported:

- unsolicited grant service (UGS),- fixed allocation is made by BS
- real-time polling service (rtPS),- BS regularly polls MS to findout allocation need. Hence bandwidth is allocated on need basis and is adaptive in nature
- extended real-time polling service (ertPS),- There will be no traffic transmission during silence time.
- non-real-time polling service (nrtPS),
- best effort (BE) service- BW is granted to mobile subscriber if and only there will be left over bandwidth from other QoS classes

4. Quick deployment: Compared with the deployment of wired solutions, WiMAX requires little or no external plant construction. Once the antenna and equipment are installed and powered, WiMAX is ready for service.

5. OFDM-based Physical Layer

The WiMAX physical layer (PHY) is based on orthogonal frequency division multiplexing, a scheme that offers good resistance to multipath, and allows WiMAX to operate in NLOS conditions.

6. **Very High Peak Data Rates**

WiMAX is capable of supporting very high peak data rates. In fact, the peak PHY data rate can be as high as 74Mbps when operating using a 20MHz wide spectrum.

More typically, using a 10MHz spectrum operating using TDD scheme with a 3:1 downlink-to-uplink ratio, the peak PHY data rate is about 25Mbps and 6.7Mbps for the downlink and the uplink, respectively.

7.Support for Advanced Antenna Techniques

The WiMAX solution has a number of hooks built into the physical-layer design, which allows for the use of multiple-antenna techniques, such as beamforming, space-time coding, and spatial multiplexing.

7. Flexible and Dynamic per User Resource Allocation

Both uplink and downlink resource allocation are controlled by a scheduler in the base station. Capacity is shared among multiple users on a demand basis, using a burst TDM scheme.

8. Mobility: The IEEE 802.16e amendment has added key features in support of mobility.

- The mobile WiMAX variant of the system has mechanisms to support secure seamless handovers for delay-tolerant full-mobility applications, such as VoIP.
- These improvements, which include scalable OFDMA,MIMO, and support for idle/sleep mode and handoff, will allow full mobility at speeds up to 160 km/h.

9. Cost-effective: WiMAX is based on an open, international standard. Mass adoption of the standard, and the use of low-cost mass-produced chipsets, will bring costs down

10. Wider coverage: WiMAX dynamically supports multiple modulation levels, including binary phase-shift keying (BPSK), quadrature phase-shift keying (QPSK), 16 QAM, and 64 QAM.

- When equipped with a high-power amplifier and operating with a low-level modulation (BPSK or QPSK, for example), WiMAX systems are able to cover a large geographic area when the path between the BS and the SS is unobstructed.

11. NLOS operation: WiMAX is based on OFDM technology, which has the inherent capability of handling NLOS environments.

- This capability helps WiMAX products deliver broad bandwidth in an NLOS environment, which other wireless products cannot do.

12. High capacity: Using higher modulation (64 QAM) and channel bandwidth, WiMAX systems can provide significant bandwidth to end-users.

Network Protocols

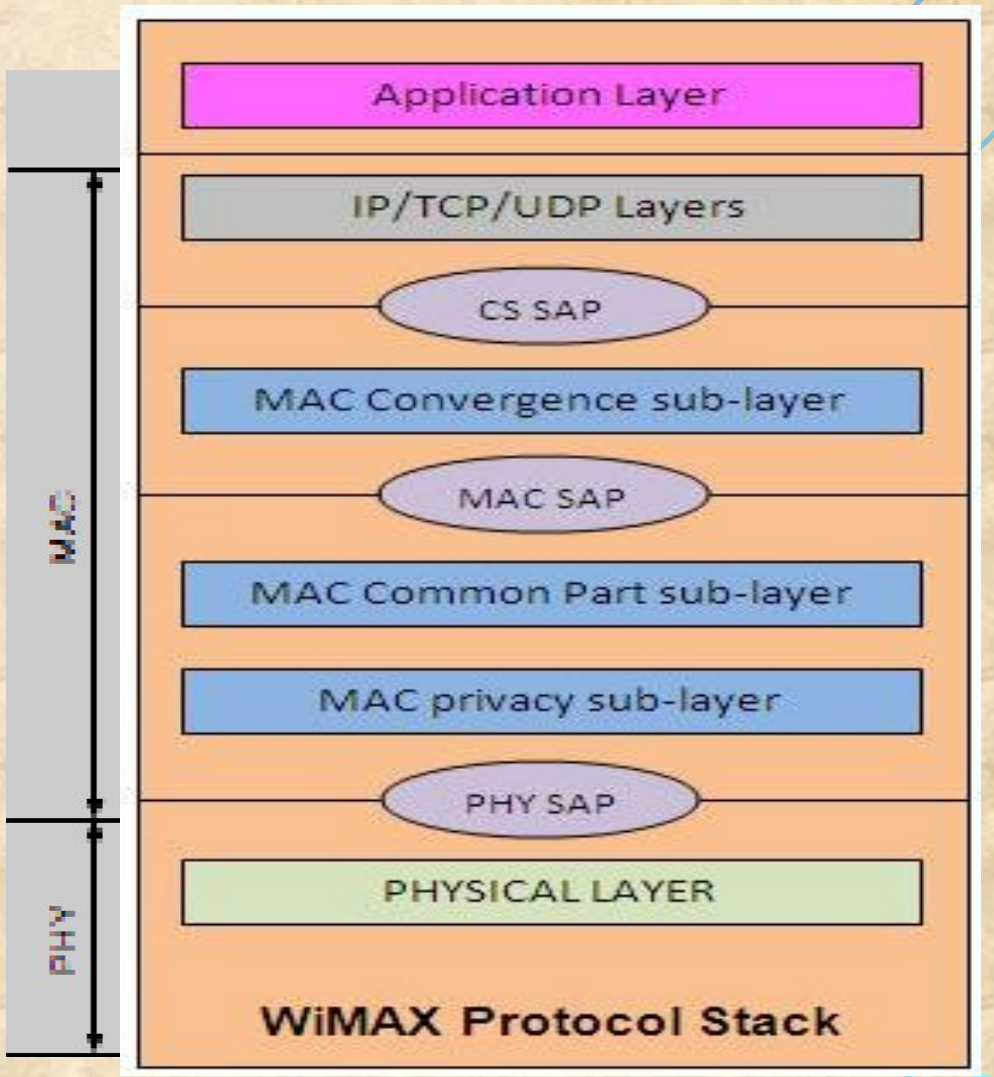
The 802.16 protocol stack is shown in Fig..

- The MAC layer is formed with three sublayers:

✔ Service-specific convergence sublayer (CS),

✔ MAC common part sublayer (CPS),

✔ privacy sublayer.

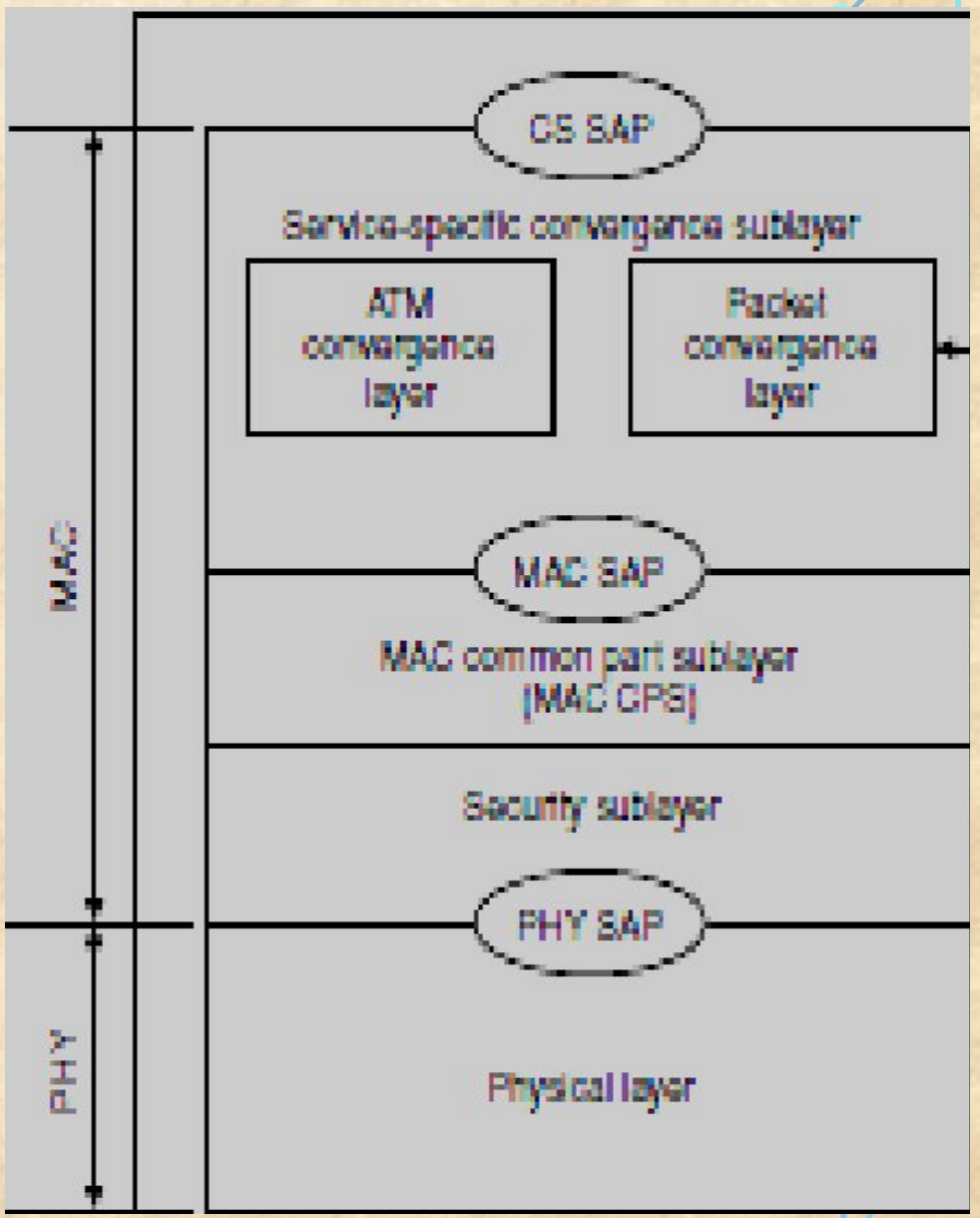


The 802.16 protocol stack is shown in Fig.. Draw and explain Wimax protocol stack.

- The MAC CS receives higher level data through CS service access point (SAP) and provides transformation and mapping into MAC service data unit (SDU).
- MAC SDUs are then received by MAC CPS through MAC SAP.
- The specification targeted two types of traffic transported through IEEE 802.16 networks:

✔ Asynchronous transfer mode (ATM)

✔ Packets.



- **MAC common part sublayer (CPS)**
- It is core part of the MAC layer, defining medium access method.
- The CPS provides functions related to duplexing and channelization, channel access, packet data unit (PDU) framing, network entry, and initialization.
- This provides the rules and mechanism for system access, bandwidth allocation, and connection maintenance.
- QoS decisions for transmission scheduling are also performed within the MAC CPS.

✔ Privacy Sublayer

- The privacy layer lies between the MAC CPS and the PHY layer.
- Security is a major issue for public networks.
- This sublayer provides the mechanism for encryption and decryption of data transferring to and from PHY layer, and is also used for authentication and secure key exchange.
- Data, PHY control, and statistics are transferred between the MAC CPS and the PHY layer through the PHY SAP.

Physical Layer

The PHY layer includes multiple specifications which make the standard adaptable to different frequency ranges

- Different variants of the IEEE 802.16 PHY layer with their capabilities and conditions of operation.
- The original version of the standard on which WiMAX is based (IEEE 802.16) specified a PHY layer operating in the 10–66 GHz range.
- 802.16a, updated to 802.16-2004 in 2004, added specifications for the 2–11 GHz range.
- 802.16-2004 was updated by 802.16e-2005 in 2005 and uses scalable orthogonal frequency division multiple access (SOFDMA) as opposed to the orthogonal frequency division multiplexing version with 256 subcarriers.

Scalable Orthogonal Frequency Division Multiple Access (SOFDMA) The concept of scalability was introduced as part of the OFDMA PHY layer mode of the IEEE 802.16 WMAN standard.

- A scalable PHY layer allows standard-based solutions to deliver optimal performance in channel bandwidths ranging from 1.25 to 20 MHz, with fixed subcarrier spacing for both fixed and portable/mobile usage models while keeping product costs low.
- A subchannel structure, with variable fast Fourier transform (FFT) sizes per channel bandwidth, enables scalability.

- 802.16e, has multiple antenna support through MIMO.
- Its benefits –

✔ Terms of coverage,

✔ Self-installation,

✔ Power consumption,

✔ Frequency reuse

✔ Bandwidth efficiency,

✔ Full mobility support.

- IEEE 802.16 standard has been standardized -European Telecommunications Standards Institute (ETSI),High-Performance Metropolitan Area Network (HIPERMAN).

Supported band of frequency. The IEEE 802.16 -licensed and unlicensed bands of frequency:

1. **10–66 GHz licensed band:**

✔ In this frequency band, due to shorter wavelength, LOS operation is required and as a result the effect of multipath propagation is neglected.

✔ It promises to provide data rates up to 120 Mbps in this frequency band.

2. **2–11 GHz licensed and licensed exempt:**

✔ It operates in near LOS and NLOS environment and to mitigate the effect of multipath propagation.

IEEE 802.16 physical layer interface variants. The standard has assigned a unique name to each physical interface

1.WMAN-SC: - operate in 10–66 GHz frequency band.

- single-carrier modulation with adaptive burst profiling, in which transmission parameters, including the modulation and coding schemes, may be tuned individually to each SS on a frame-by-frame basis.
- supports both FDD and TDD to separate UL and DL.
- supports half-duplex FDD,
- Access in UL direction is done by a combination of TDMA and demand assignment multiple access (DAMA);

- UL channel is divided into several time slots.
- Communication on the DL in ATM architecture is using TDM.
- It also specifies the randomization, forward error correction (FEC), modulation, and coding schemes.

2.WMAN-SCa:

- This is based on single-carrier modulation targeted for 2–11 GHz
- Access is done by TDMA technique both in UL and DL; additionally, TDM is also supported in DL.

3. WMAN-OFDM:

- It is based on OFDM with a 256-point transform to support multiple SSs in 2–11 GHz
- Access is done by TDMA.
- The WiMAX forum has adopted this PHY layer specification for broadband wireless access.
- Due to employing OFDM and other features like multiple FEC method, this is the most suitable candidate to provide fixed support in NLOS environment.

4. WMAN-OFDMA:

- It uses OFDMA with at least a single support of specified multipoint transform (2048, 1024, 512, or 128) to provide combined fixed and mobile broadband wireless access.
- Operation is limited to below 11 GHz licensed band.
- multiple access is provided by addressing a subset of the multiple carriers to individual receivers.

5. WHUMAN: This wireless high-speed unlicensed metropolitan access network (WHUMAN) is targeted for license-exempt band below 11 GHz.

- Any of the air interfaces specified for 2–11 GHz can be used for this.
- This supports only TDD for duplexing.

- WiMAX is intended as a solution for metropolitan broadband access applications; however, multipath effects from buildings and other obstructions must be overcome.
- So, the OFDM versions of WiMAX were developed.
- In a single-carrier system, a single carrier is digitally modulated with a relatively fast symbol rate.
- In an operating environment with severe multipath conditions, the use of a fast symbol rate can result in loss of data and poor signal performance.

- An OFDM signal actually consists of many orthogonal carriers, and each signal is digitally modulated with a relatively slow symbol rate.
- Because of the slower symbol rates, such signals are less affected by multipath interference, which creates delayed and reflected versions of transmitted signals.
- By transmitting one symbol on multiple carriers, it is possible to use FEC to reconstruct the contents of faulty carriers.
- commercial interest is in the 802.16d and 802.16e standards, as the lower frequencies used in these variants suffer less from inherent signal attenuation and therefore give improved range and in-building penetration

Table 6.3 | IEEE 802.16 PHY layer

Parameter	*Function*	*LOS/ NLOS*	*Frequency band*	*Carrier*	*Duplexing*
WMAN-SC	Point-to-multipoint	LOS	10–66 GHz	Single	TDD, FDD
WMAN-SCa	Point-to-multipoint	LOS	2–11 GHz; licensed	Single	TDD, FDD
WMAN-OFDM	Point-to-multipoint	NLOS	2–11 GHz; licensed	256	TDD, FDD
WMAN-OFDM (16e)	Point-to-multipoint	NLOS	2–11 GHz; licensed	2048	TDD, FDD
WHUMAN (HU – high speed unlicensed)	Point-to-multipoint	NLOS	2–11 GHz license-exempt	1/256/2048	TDD, dynamic frequency selection

- WMAN-OFDM PHY layer is the version of the 256-point OFDM-based air interface specification. Of these 256 subcarriers, 192 are used for user data, 56 are nulled for guard band, and 8 are used as pilot subcarriers for various estimation purposes.

- Benefits of this mechanism are:

✔ Lower peak to average ratio,

✔ Faster FFT calculation,

✔ Less stringent requirements for frequency synchronization compared to 2048-point WMAN-OFDMA.

Some of the other mechanisms of the PHY layer are as follows:

1. Robust error control mechanism,
2. Adaptive modulation and coding,
3. Space time block codes (STBC),
4. Adaptive antenna

Table 6.5 | IEEE 802.16 physical layer features

Feature	*Benefit*
256-point FFT OFDM waveform	Built-in support for addressing multipath in outdoor LOS and NLOS environments.
Adaptive modulation and variable error correction encoding per RF burst	Ensures a robust RF link while maximizing the number of bps for each subscriber unit.
TDD and FDD duplexing support	Addresses varying worldwide regulations where one or both may be allowed.
Flexible channel sizes	Provides the flexibility necessary to operate in many different frequency bands with varying channel requirements around the world.
Designed to support smart antenna systems	Smart antennas are fast becoming more affordable; as these costs come down, their ability to suppress interference and increase system gain will become important to broadband wireless deployments.

MAC Layer

- The primary task of the WiMAX MAC layer is to provide an interface between the higher transport layers and the PHY layer.
- the IEEE 802.16 MAC describes a number of CSs that describe how wireline technologies such as Ethernet, ATM, and IP are encapsulated on the air interface, how data are classified, etc.
- Secure communications are delivered by using secure key exchange during authentication and encryption using Advanced Encryption Standard (AES) or Data Encryption Standard (DES) (as the encryption mechanism) during data transfer.

- Features of the MAC layer: 1. Power-saving mechanisms (using sleep mode and idle mode), 2.Handover mechanisms

Sub channelization

- A single user in an OFDM WiMAX system can use all subcarriers at any given time.
- In OFDMA, subsets of subcarriers are assigned to multiple users, allowing a number of subscribers to be served simultaneously.
- Using a technique known as *sub channelization*, specific carrier groups are used for each subscriber.
- These subcarrier assignments change dynamically to overcome the effects of multipath interference

- Sub channelization is a key concept for effective WiMAX network operation.
- The technique makes it possible to group a number of OFDM carriers into blocks, and then assign each block to a different WiMAX BS sector.
- The blocks, which contain a number of adjacent carriers, can be spread over the full operating frequency range.
- By using adjacent BS sections, the effects of interference can be minimized.
- A WiMAX network's sub-channel index controls the use of different blocks over its operating frequency spectrum

- WiMAX systems can be used in TDD, FDD, or half-duplex FDD configurations.
- In a TDD approach, the BS and the SS each transmit on the same frequency, although separated in time.
- The BS transmits a DL subframe, followed by a short gap called a *transmit/receive transition gap* (TTG), and then individual subscribers transmit the UL subframes.
- Subscribers are accurately synchronized so that their transmissions do not overlap with each other when they arrive at the BS.
- Following all UL subframes, another short gap called a receive/transmit transition gap (RTG) is allocated before the BS can start transmitting again.

- In WiMAX, the whole-time axis is divided into frames .
- A frame consists of an UL subframe and a DL subframe.
- A frame is a structured sequence of data of fixed duration comprising a DL burst and an UL burst.
- These bursts or subframes contain different data for different users.

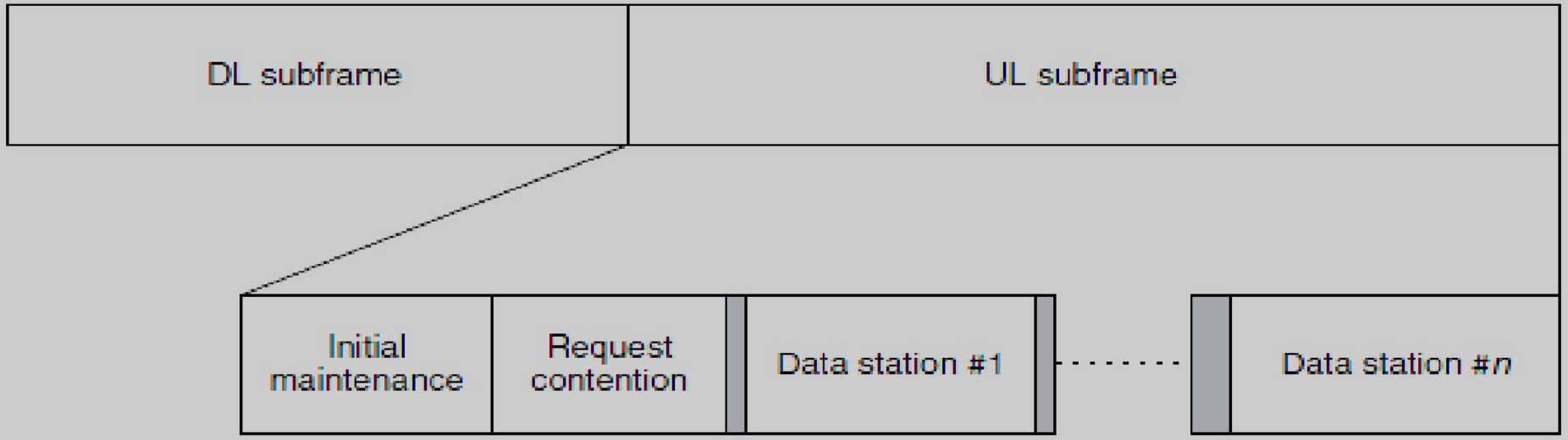


Figure 6.7 | UL/DL subframe.

- The frame structure makes use of the following power levels for efficiency and robustness

1. Initial maintenance: First access by stations to detect round-trip-time to the BS as well as necessary transmission power (random choice of a time slot in that field by backoff mechanism); collisions are possible.

2. Request contention: Demands reservations in coming UL maps (again by backoff mechanism); collisions are possible.

- The MAC includes service-specific CSs that interface to higher layers. The sublayer below the common part sublayer is the privacy sublayer.

1. **Service-specific CS:** IEEE Standard 802.16 defines two general service-specific CSs for mapping services to and from 802.16 MAC connections.

- The ATM CS is defined for ATM services, and the packet CS is defined for mapping packet services such as IPv4, IPv6, Ethernet, and virtual local area network (VLAN).
- The primary task of the sublayer is to classify SDUs to the proper MAC connection, preserve or enable QoS, and enable bandwidth allocation.
- The mapping takes various forms depending on the type of service

2. Common part sublayer: The 802.16 MAC is designed to support a P2MP architecture with a central BS handling multiple independent sectors simultaneously.

- On the DL, data to SSs are multiplexed in TDM. The UL is shared between SSs in TDMA fashion. The 802.16 MAC is connection-oriented.
- All services, including inherently connectionless services, are mapped to a connection.
- This provides a mechanism for requesting bandwidth associating QoS and traffic parameters, transporting and routing data to the appropriate CS, and all other actions associated with the contractual terms of the service.
- Connections are referenced with 16-bit connection identifiers (CIDs) and may require continuously granted bandwidth or bandwidth on demand

- Each SS has a standard 48-bit MAC address, but this serves mainly as an equipment identifier, because the primary addresses used during operation are the CIDs.
- Upon entering the network, the SS is assigned three management connections in each direction

1. The first is used for the transfer of short, time-critical MAC and radio link control (RLC) messages.

- The *primary management connection* is used to transfer longer, more delay tolerant messages such as those used for authentication and connection setup.

2. The *secondary management connection* is used for the transfer of standard-based management messages such as dynamic host configuration protocol (DHCP), trivial file transfer protocol (TFTP), and simple network management protocol (SNMP).

3. In addition to these management connections, SSs are allocated *transport connections* for the contracted services.

- Transport connections are unidirectional to facilitate different UL and DL QoS and traffic parameters; they are typically assigned to services in pairs

MAC PDU Formats

- The MAC PDU is the data unit exchanged between the MAC layers of the BS and its SSs.
- MAC PDUs contain either MAC management messages or CS data. MAC PDU consists of a fixed-length generic MAC header, a variable-length payload, and an optional cyclic redundancy check (CRC) code.

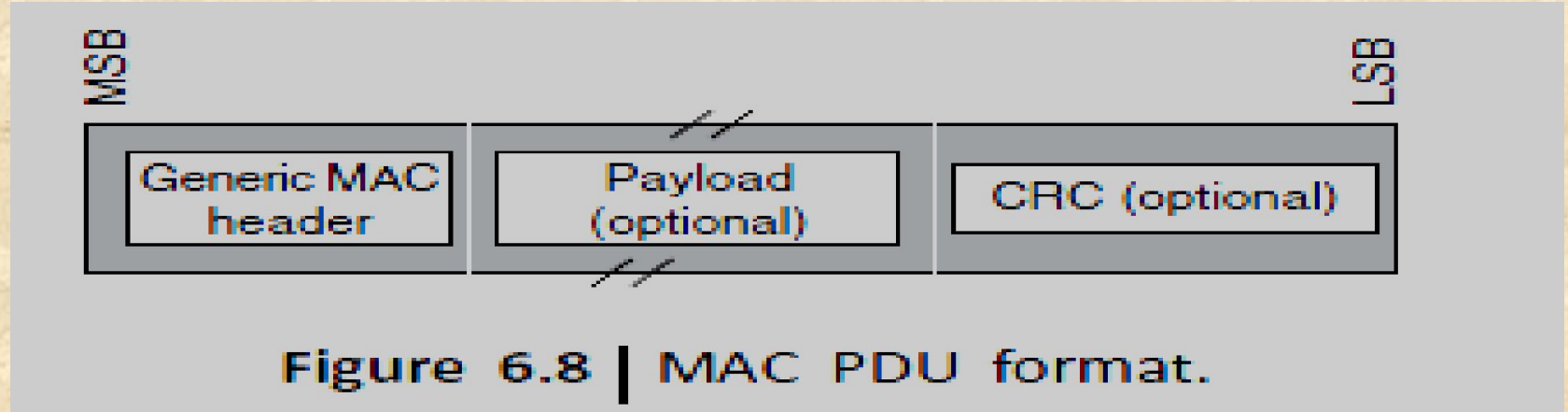


Figure 6.8 | MAC PDU format.

Three types of MAC subheader may be present.

- The *grant management subheader* is used by an SS to convey bandwidth management needs to its BS.
- The *fragmentation subheader* contains information that indicates the presence and orientation in the payload of any fragments of SDUs.
- The *packing subheader* is used to indicate the packing of multiple SDUs into a single PDU.

Transmission of MAC PDUs. The IEEE 802.16 MAC supports various higher layer protocols such as ATM or IP.

- Incoming MAC messages or SDUs from corresponding CSs are formatted according to the MAC PDU format (here the SDUs 1 and 2 are formatted to PDU4)
- FEC can be done to minimize the errors.

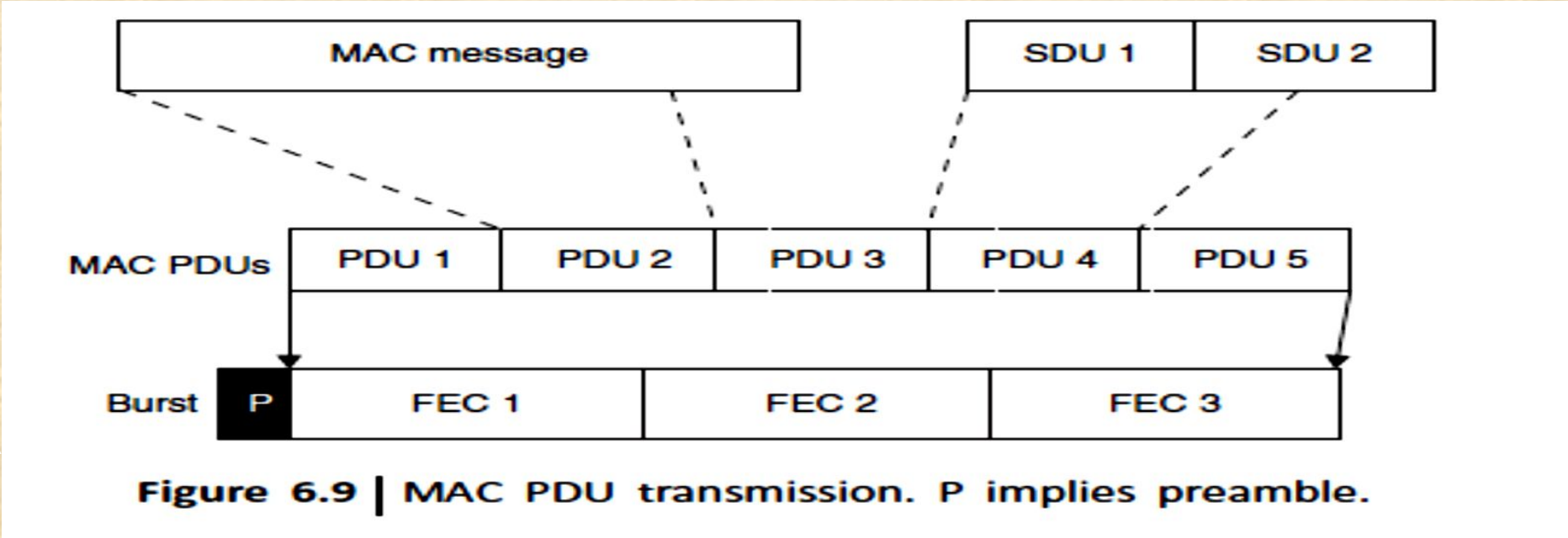


Figure 6.9 | MAC PDU transmission. P implies preamble.

- IEEE 802.16 takes advantage of incorporating the packing and fragmentation processes with the bandwidth allocation process to maximize the flexibility, efficiency, and effectiveness of both
- *Fragmentation* is the process in which a MAC SDU is divided into one or more MAC SDU fragments.
- *Packing* is the process in which multiple MAC SDUs are packed into a single MAC PDU payload.
- Both processes may be initiated by either a BS for a DL connection or an SS for a UL connection.

- Bandwidth allocation in IEEE 802.16 can be made in two ways:

✔ By grant per connection (GPC) or By grant per service station (GPSS).

- In the first case, each grant is associated with a specific connection.
- The disadvantage of this approach is that it creates additional overhead.
- In the other approach, GPSS, the SS is given a single grant for all its connections.
- Then the local scheduler in the SS decides how to allocate the transmission opportunities to each connection.

MAC Quality of Service (QoS)

- A key feature of 802.16 is that it is a *connection-oriented technology*.
- The SS cannot transmit data until it has been allocated a channel by the BS.
- This allows 802.16e to provide strong support for QoS.
- In WiMAX, QoS is supported by allocating each connection between the SS and the BS to a specific QoS class.

The IEEE 802.16 MAC layer defines five service classes:

- UGS, rtPS, ertPS, nrtPS, and BE service.

- The *scheduling* algorithms needed for implementing the first three types of services are implemented in the BS (while allocating UL bandwidth to each SS). Each SS negotiates its service policies with the BS at the connection setup time.
- These five service classes are explained as follows:

1. **Unsolicited Grant service (UGS):** It offers fixed size grants on a real-time periodic basis, which eliminates the overhead and latency of SS request and assures that grants are available to meet the flow's real-time needs.

- Typical UGS applications are delay-sensitive speech signal communications, VoIP (without silence suppression), etc.

2. Real Time Polling Service (rtPS): It is designed to support real-time service flows that generate variable size data packets on a periodic basis for streaming video.

- This service requires more request overhead than UGS but supports variable grant sizes for optimum data transport efficiency.

3. Extended Real Time Polling Service (ertPS): It was added in 802.16e-2005 (or mobile-WiMAX) and supports real-time applications where the applications require guaranteed data rate and delay

- The ertPS is designed to support real-time service flows that generate variable-sized data packets on a periodic basis such as VoIP (with silence suppression).

4. Non Real Time Polling Service (nrtPS): It is designed to support non-real-time service flows that require variable size bursts in the UL on a regular (but not strictly periodic) basis.

5. Best Effort (BE) service: It is intended to be used for BE traffic where no throughput or delay guarantees are provided

WMAN Applications

- Two broad categories: **private and public networks applications**.
- Private networks, used exclusively by a single organization, institution, or business, offer dedicated communication links for the secure and reliable transfer of voice, data, and video.
- Quick and easy deployment is generally a high priority, and configurations are typically P2P or P2MP.
- In public network, resources are accessed and shared by different users, including both businesses and private individuals.
- Public networks generally require a cost-effective means of providing ubiquitous coverage, as the location of the users is neither predictable nor fixed.

- The main applications of public networks are voice and data communication, although video communication is becoming increasingly popular

WMAN Applications:

- *Wireless Service Provider Backhaul*
- *Banking Networks*
- *Education Networks*
- *Public Safety*

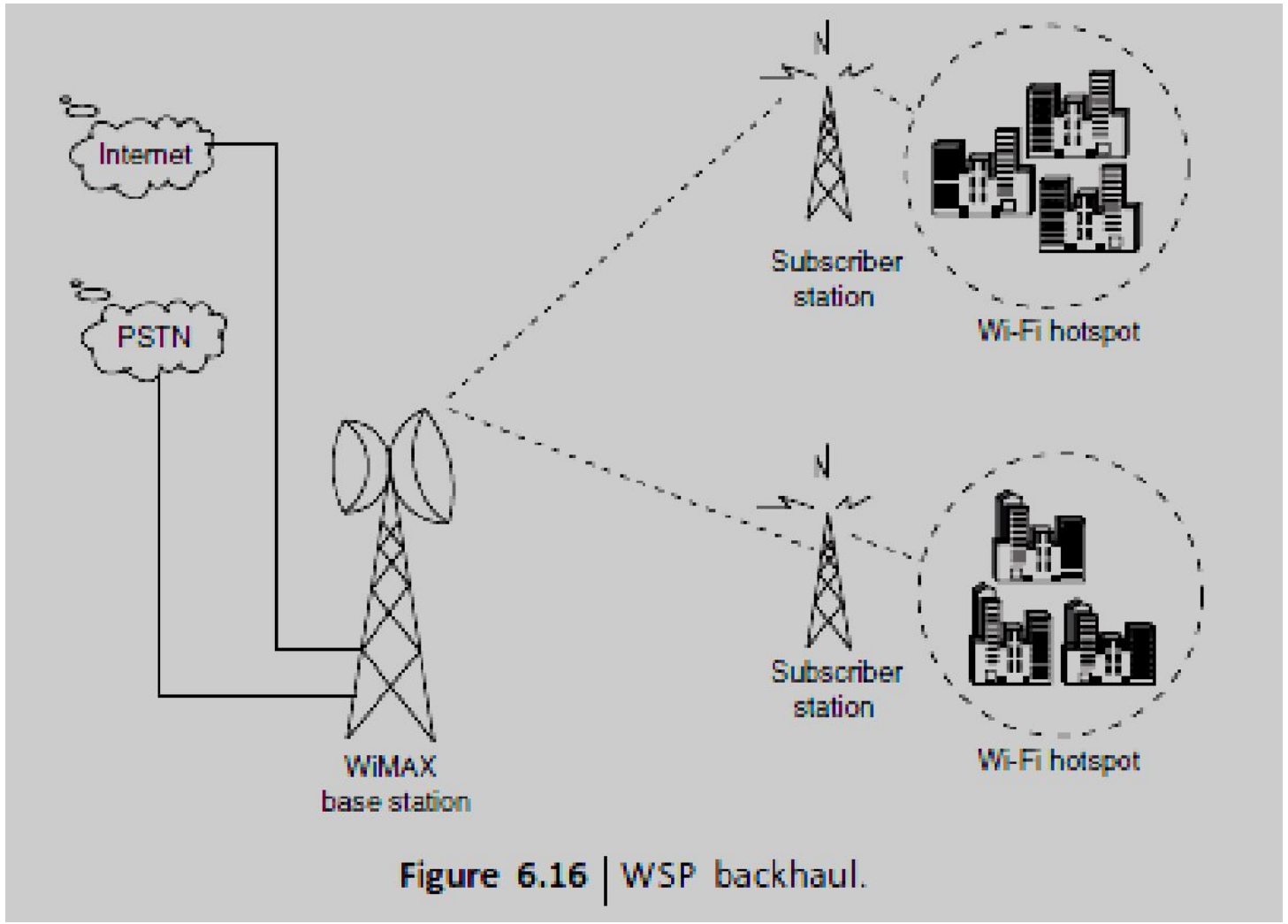


Figure 6.16 | WSP backhaul.

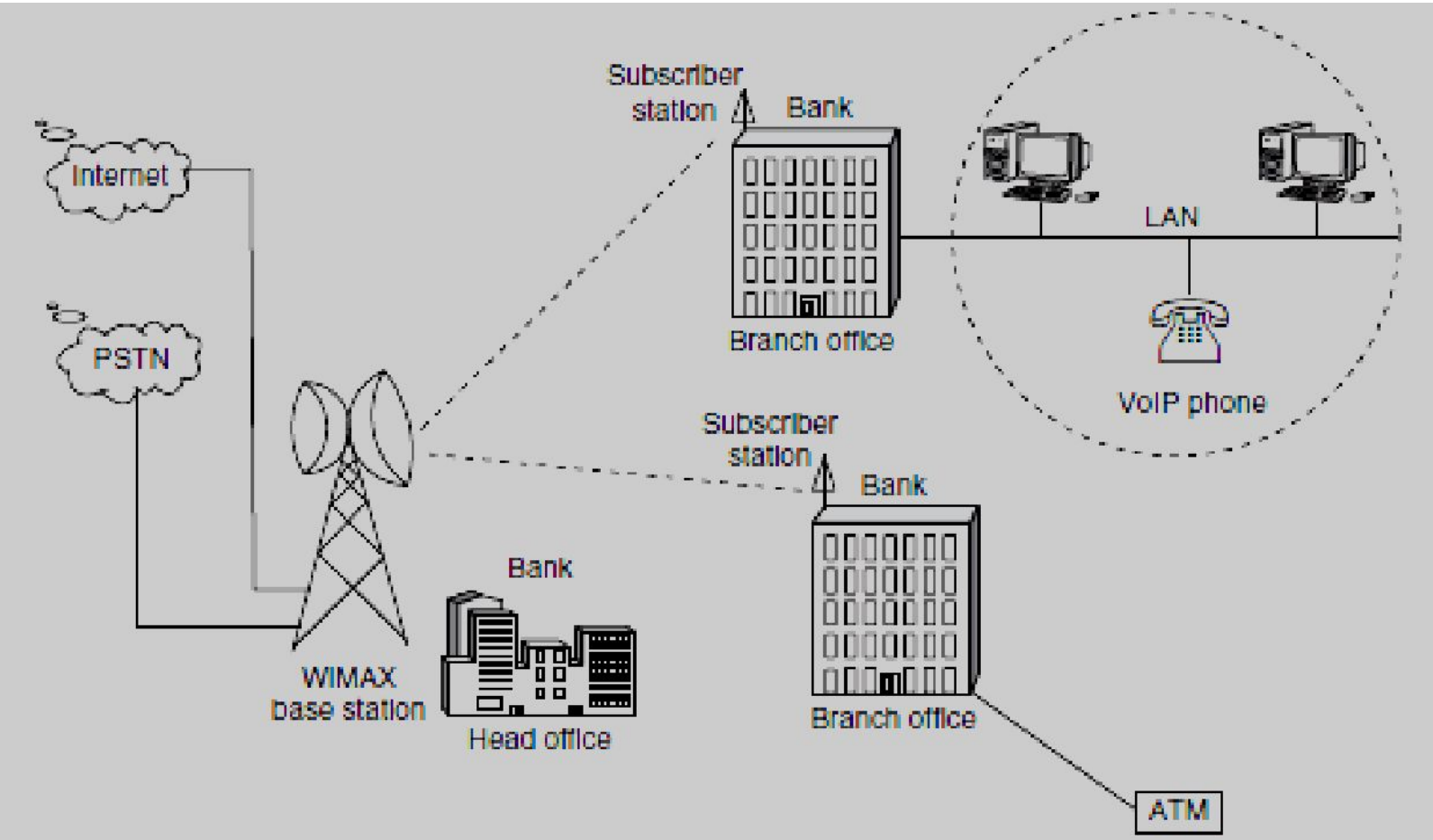


Figure 6.17 | WiMAX network for banking.

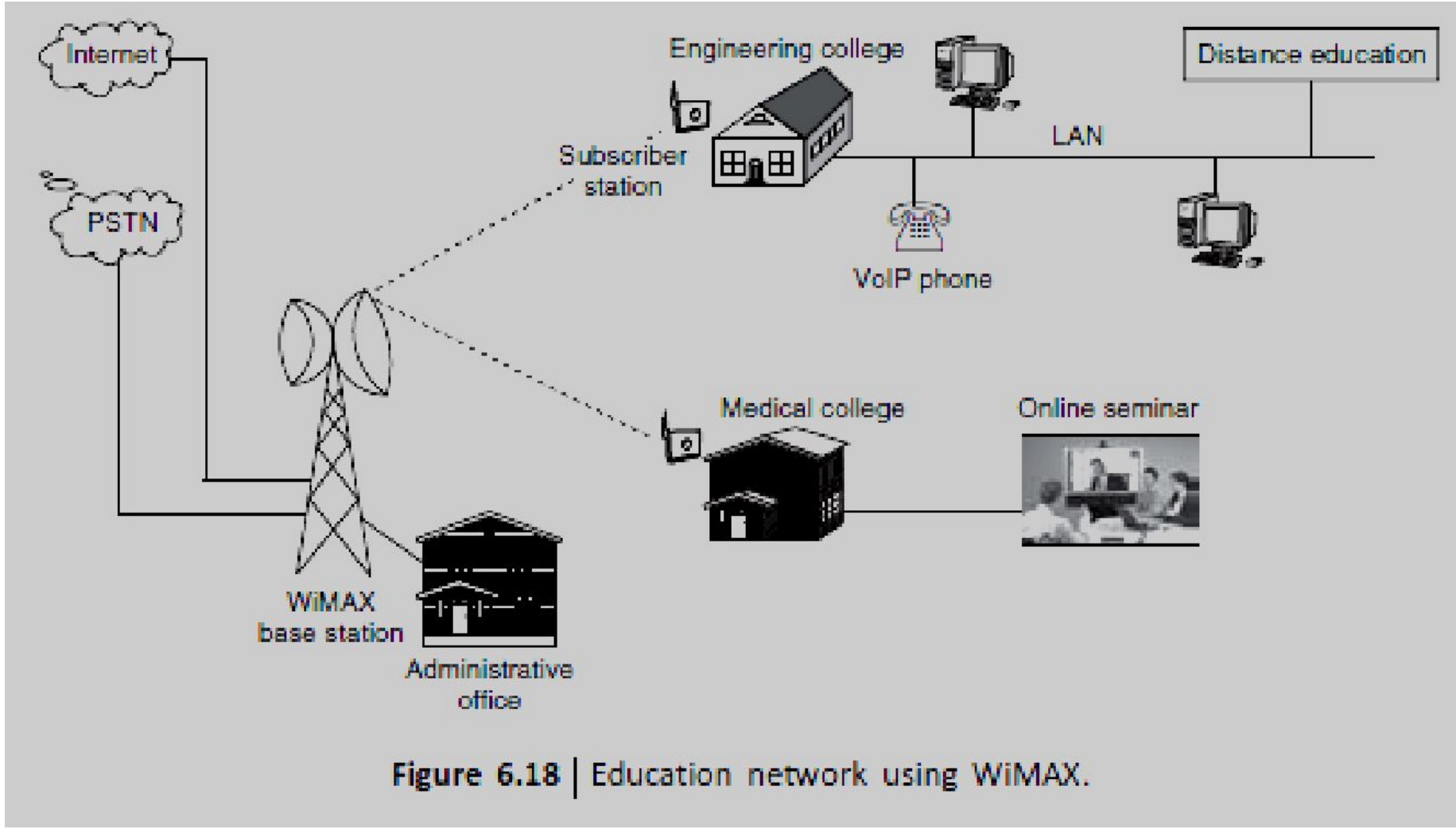


Figure 6.18 | Education network using WiMAX.

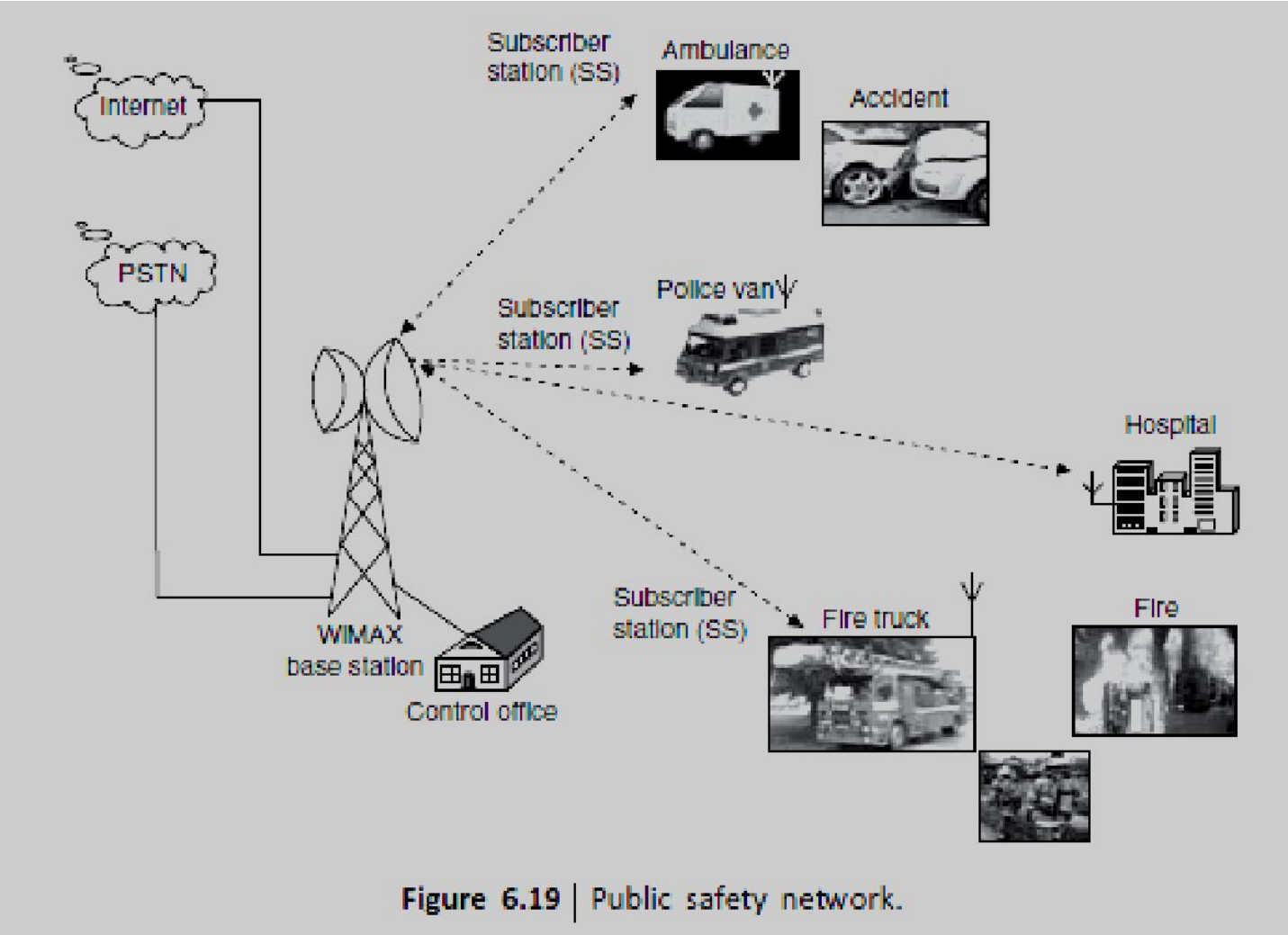


Figure 6.19 | Public safety network.

WIRELESS LOCAL AREA NETWORKS

Reference :Wireless Communication by Vijay Garg

WLAN Introduction

- WLANs are flexible data communication systems that can be used for applications in which mobility is required.
- In the indoor business environment, although mobility is not an absolute requirement, WLANs provide more flexibility than that achieved by the wired LAN.
- Currently, WLANs can provide data rates up to 11 Mbps, but the industry is making a move toward high-speed WLANs.
- Manufacturers are developing WLANs to provide data rates up to 54 Mbps or higher.
- High speed makes WLANs a promising technology for the future data communications market.

- WLANs are flexible data communications systems implemented as an extension or as an alternative for wired LANs.
- Using radio frequency (RF) technology, WLANs transmit and receive data over the air, minimizing the need for wired connections. Thus, WLANs combine data connectivity with user mobility

Table 21.1 Industrial, scientific, and medical (ISM) bands.

No.	Band (GHz)	Bandwidth (MHz)	Power level	Spread spectrum
1	0.902–0.928	26	1W	FHSS, DSSS
2	2.4–2.4835	83.5	1W	FHSS, DSSS
3	5.725–5.850	125	1W	FHSS, DSSS
4	24.0–24.5	250	50 mW/m @ 3 m	Not Applicable

The IEEE 802.11 committee is responsible for WLAN standards. WLANs include IEEE 802.11a (WiFi 5), IEEE 802.11b (WiFi), IEEE 802.11g and IEEE 802.11n

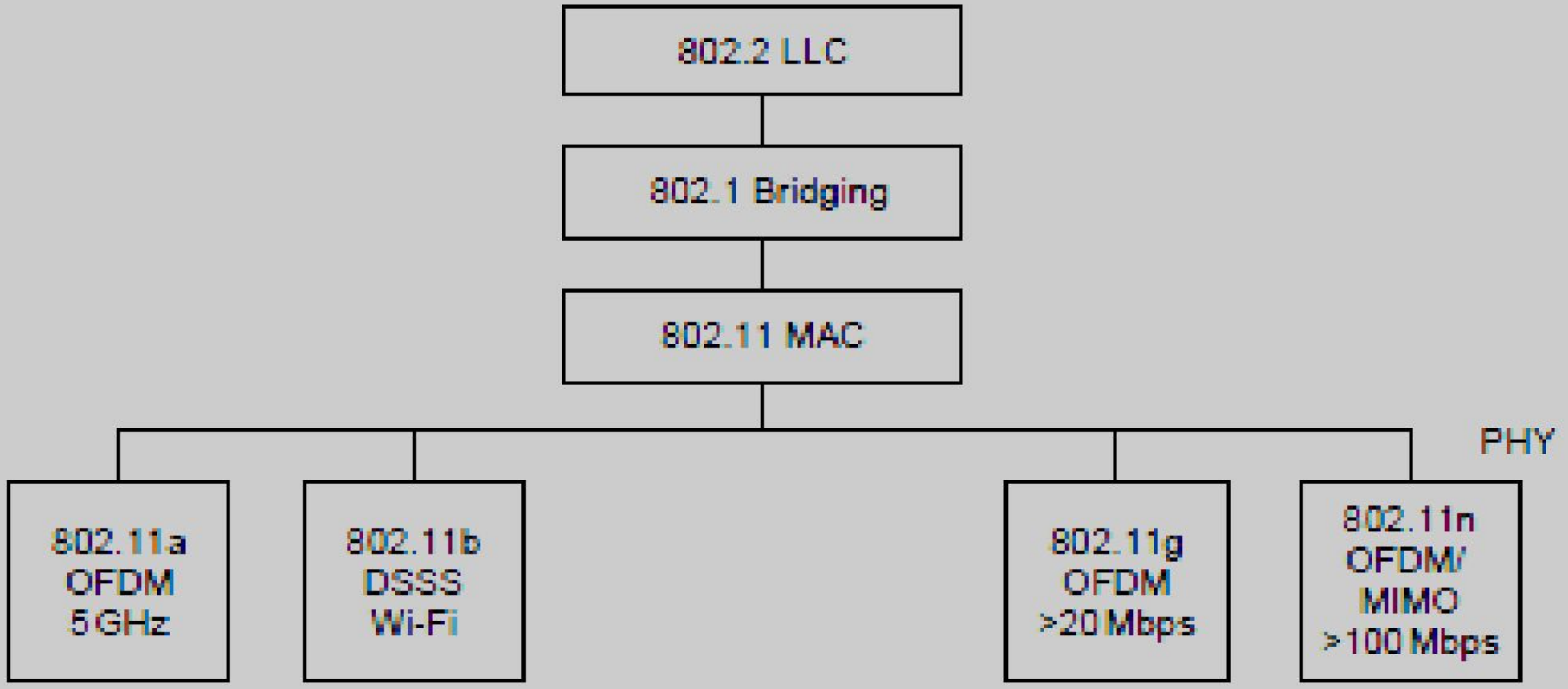


Figure 21.1 IEEE 802.11 WLAN standards.

- Recently, manufacturers have deployed WLANs for process and control applications. Retail applications have expanded to include wireless point of sale (WPOS).
- The health-care and education industry are also fast-growing markets for WLANs.
- WLANs provide high-speed, reliable data communications in a building or campus environment as well as coverage in rural areas. WLANs are simple to install.

Table 21.2 IEEE 802.11 subgroups.

802.11a	High speed physical layer in 5 GHz band
802.11b	Higher speed physical layer extension of wireless in 2.4 GHz band
802.11d	Local and metropolitan area wireless
802.11g	Broadband wireless
802.11i	Security
802.11n	Wideband service

WLAN Equipment

There are three main links that form the basis of the wireless network. These are:

LAN adapter: Wireless adapters are made in the same basic form as their wired counterparts: **Personal Computer Memory Card International Association** (PCMCIA) ,Card bus, PCI, and USB. They also serve the same function, enabling end-users to access the network. In a WLAN, they provide the interface between the network operating system and an antenna to create a transparent connection to the network.

Access point (AP): The AP is the wireless equivalent of an LAN hub. It receives, buffers, and transmits data between the WLAN and the wired network, supporting a group of wireless user devices.

- An AP is typically connected with the backbone network through a standard Ethernet cable, and communicates with wireless devices by means of an antenna. The AP or antenna connected to it is generally mounted on a high wall or on the ceiling.
- APs have a range from 20 to 500 meters. A single AP can support between 15 to 250 users, depending on technology, configuration, and use. It is relatively easy to scale a WLAN by adding more APs to reduce network congestion and enlarge the coverage area.
- Large networks requiring multiple APs deploy them to create overlapping cells for constant connectivity to the network. A wireless AP can monitor movement of a client across its domain and permit or deny specific traffic or clients from communicating through it.

Outdoor LAN bridges:

- ✔ Outdoor LAN bridges are used to connect LANs in different buildings. When the cost of buying a fiber optic cable between buildings is considered, particularly if there are barriers such as highways or bodies of water in the way, a WLAN can be an economical alternative.
- ✔ **An outdoor bridge can provide a less expensive alternative to recurring leased line charges**.
- ✔ WLAN bridge products support fairly high data rates and ranges of several miles with the use of line-of-sight directional antennas. Some APs can also be used as a bridge between buildings of relatively close proximity.

WLAN Topologies

WLANs can be built with either of the following topologies:

- ✔ Peer-to-peer (ad hoc) topology
- ✔ Access point-based topology
- ✔ Point-to-multipoint bridge topology

 In peer-to-peer topology, client devices within a cell communicate directly to each other.

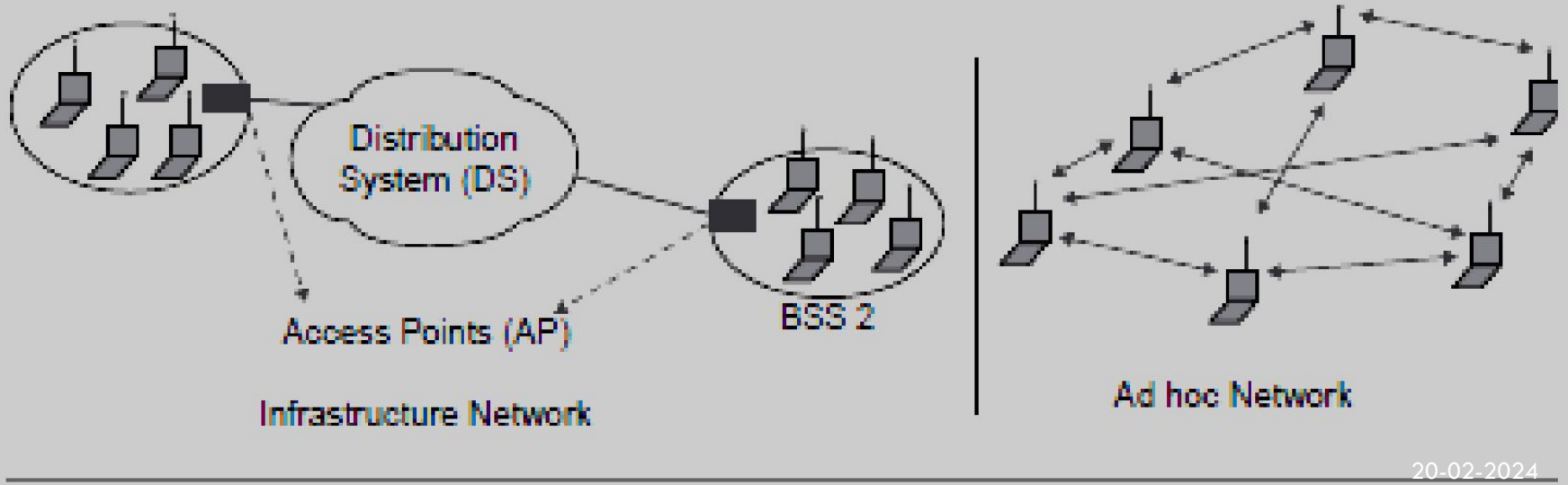


Figure 21.3 Peer-to-peer topology (Ad hoc Network).

- AP-based technology uses access points to bridge traffic onto a wired (Ethernet or Token Ring) or a wireless backbone.
- AP enables a wireless client device to communicate with any other wired or wireless device on the network.
- AP-based topology is more commonly used and demonstrates that the WLAN does not replace the wired LAN, it extends connectivity to mobile devices.

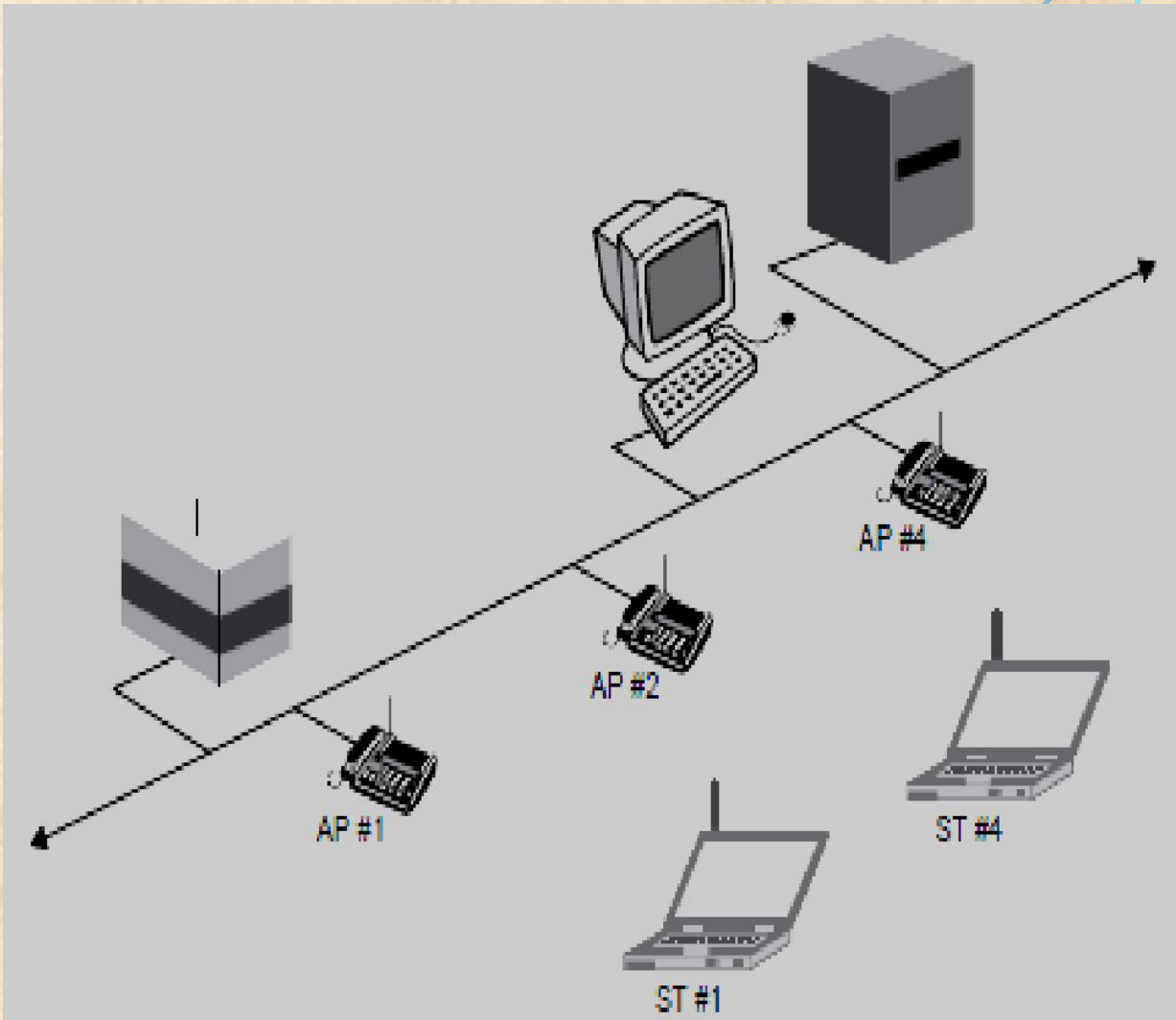
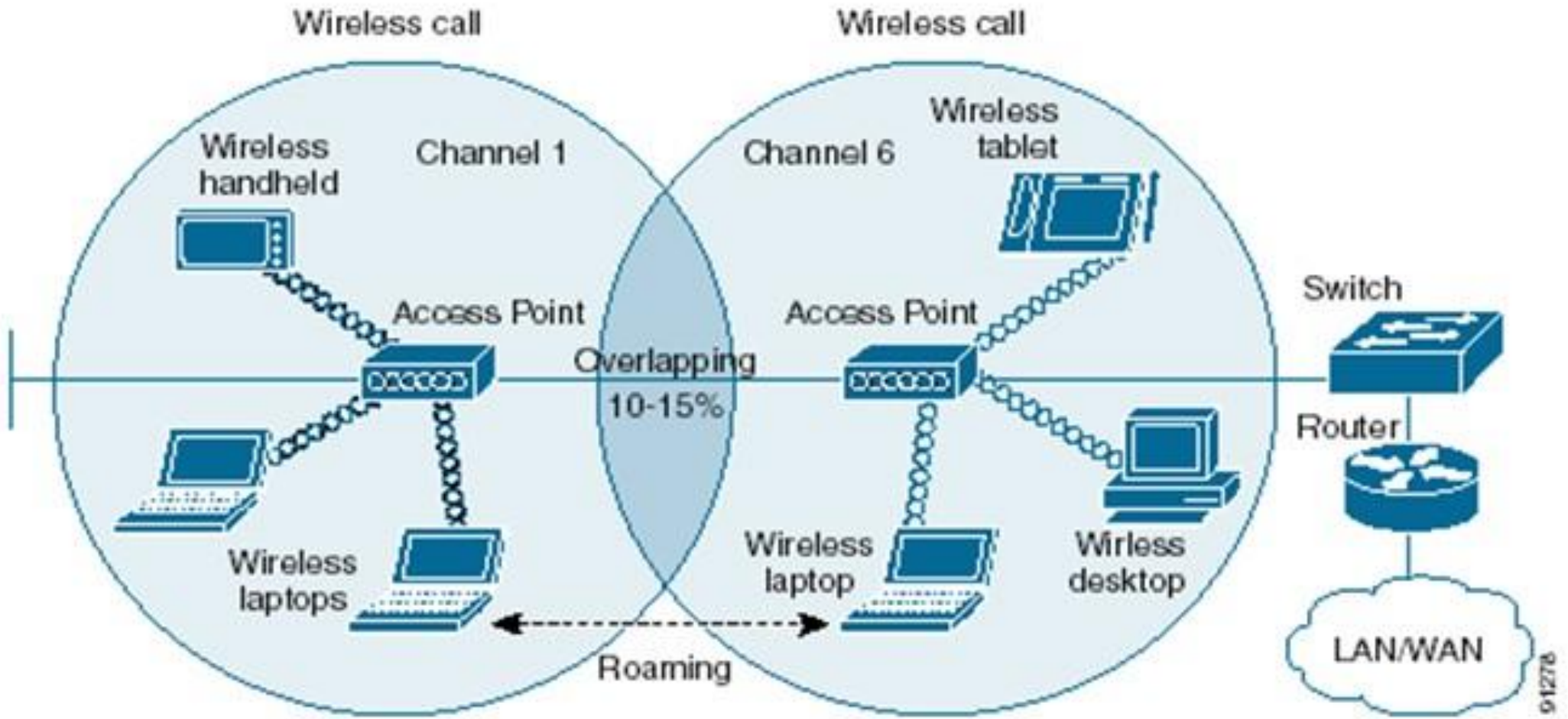


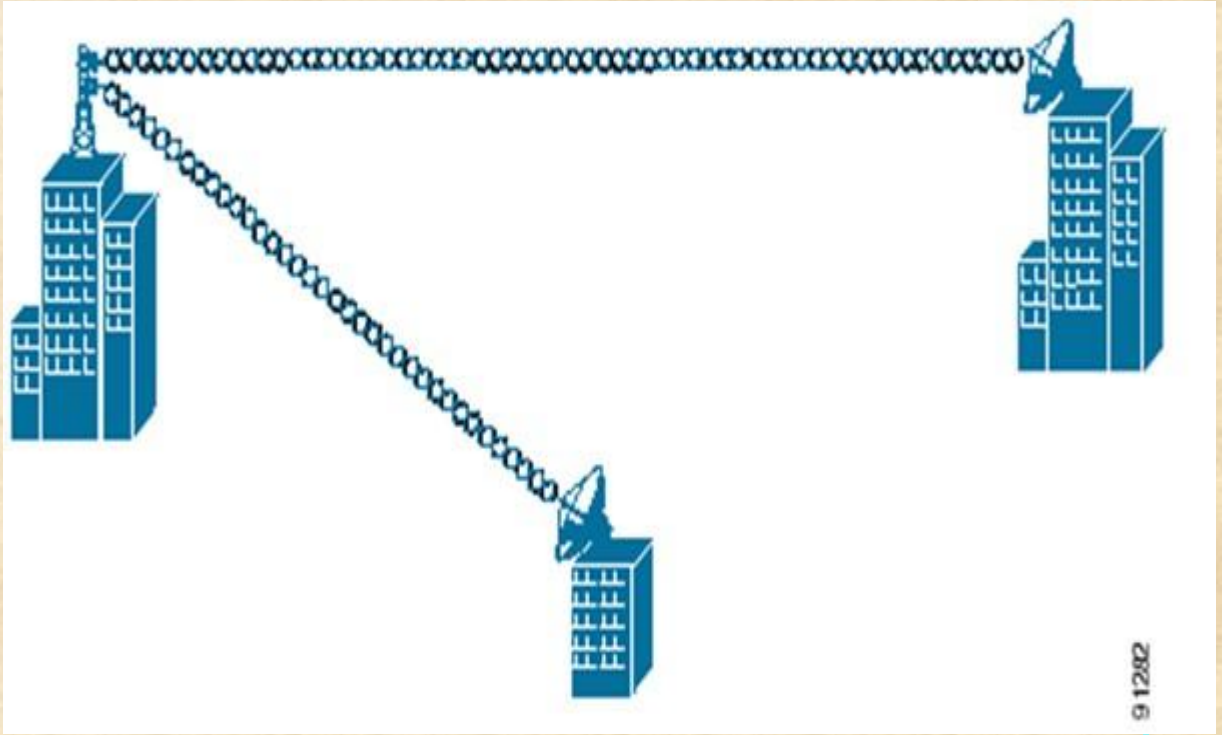
Figure 21.4 Access point-based topology.

Figure 1-3 Typical WLAN



Point-to-multipoint bridge:

- ✔ Wireless bridges connect LANs in one building to LANs in another building even if the buildings are miles apart.
- ✔ These conditions receive a clear line-of-sight between buildings.
- ✔ The line-of-sight range varies based on the type of wireless bridge and antenna used as well as environmental conditions.



IEEE 802.11 Architecture

- The architecture of the IEEE 802.11 WLAN is designed to support a network where most decision making is distributed to mobile stations.
- This type of architecture has several advantages:

✔ It is tolerant of faults in all of the WLAN equipment and eliminates possible bottlenecks a centralized architecture would introduce.

✔ The architecture is flexible and can easily support both small, transient networks and large, semi permanent or permanent networks.

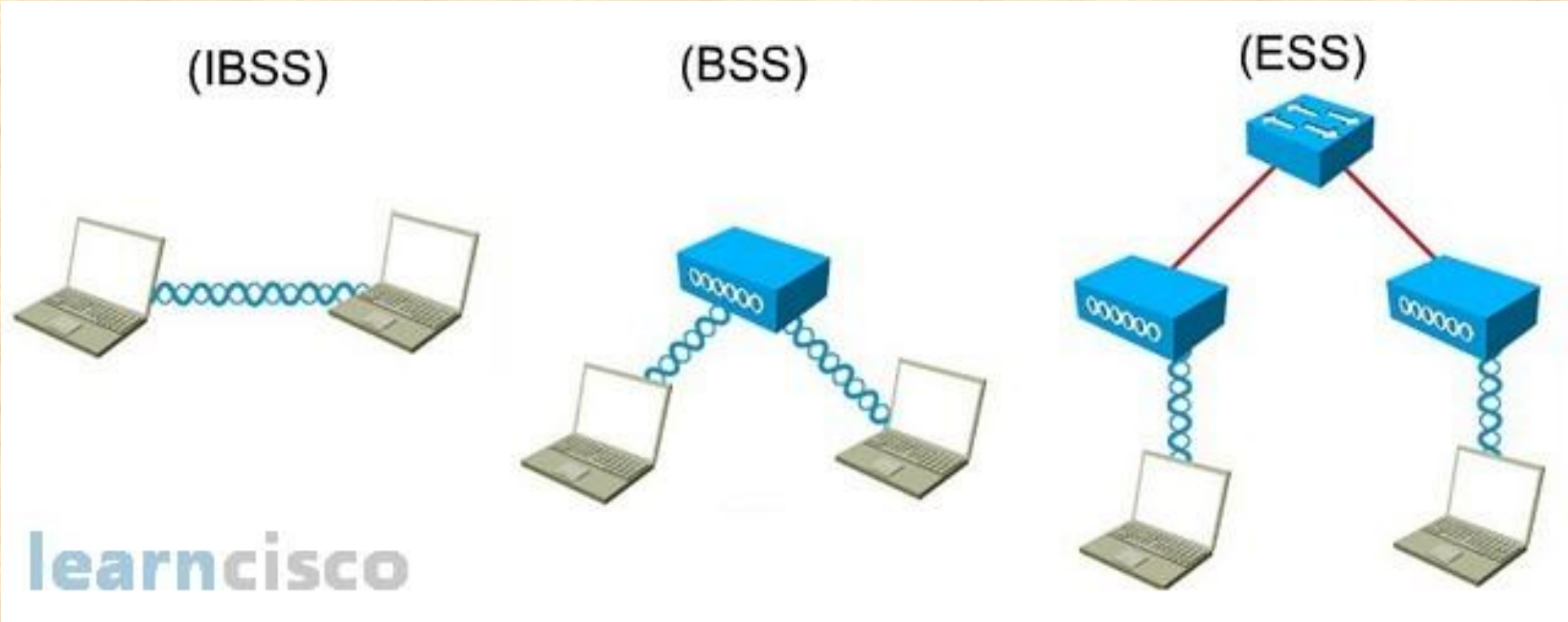
✔ In addition, the architecture and protocols offer significant power saving and prolong the battery life of mobile equipment without losing network connectivity.

Two network architectures are defined in the IEEE 802.11 standard:

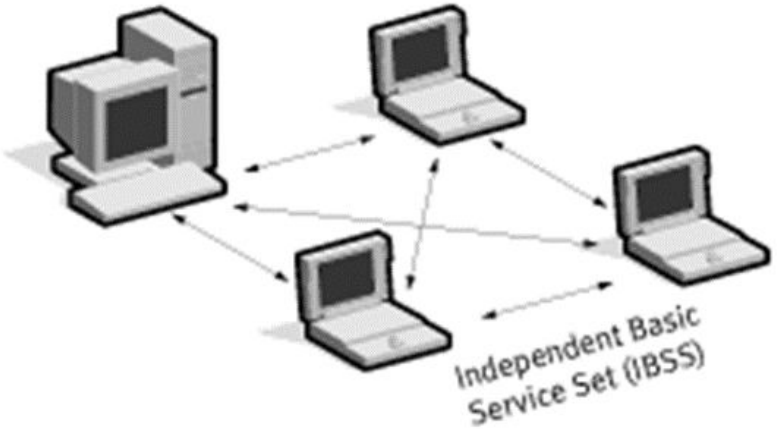
- ***Infrastructure network:*** An infrastructure network is the network architecture for providing communication between wireless clients and wired network resources. The transition of data from the wireless to wired medium occurs via an AP. An AP and its associated wireless clients define the coverage area. Together all the devices form a *basic service set*.
- ***Point-to-point (ad hoc) network:*** An ad hoc network is the architecture that is used to support mutual communication between wireless clients. Typically, an ad hoc network is created spontaneously and does not support access to wired networks. An ad hoc network does not require an AP.

IEEE 802.11 supports three basic topologies for WLANs:

- ✔ Independent basic service set (IBSS),
- ✔ Basic service set,
- ✔ Extended service set (ESS).



Define BSS and ESS and explain their role in the architecture



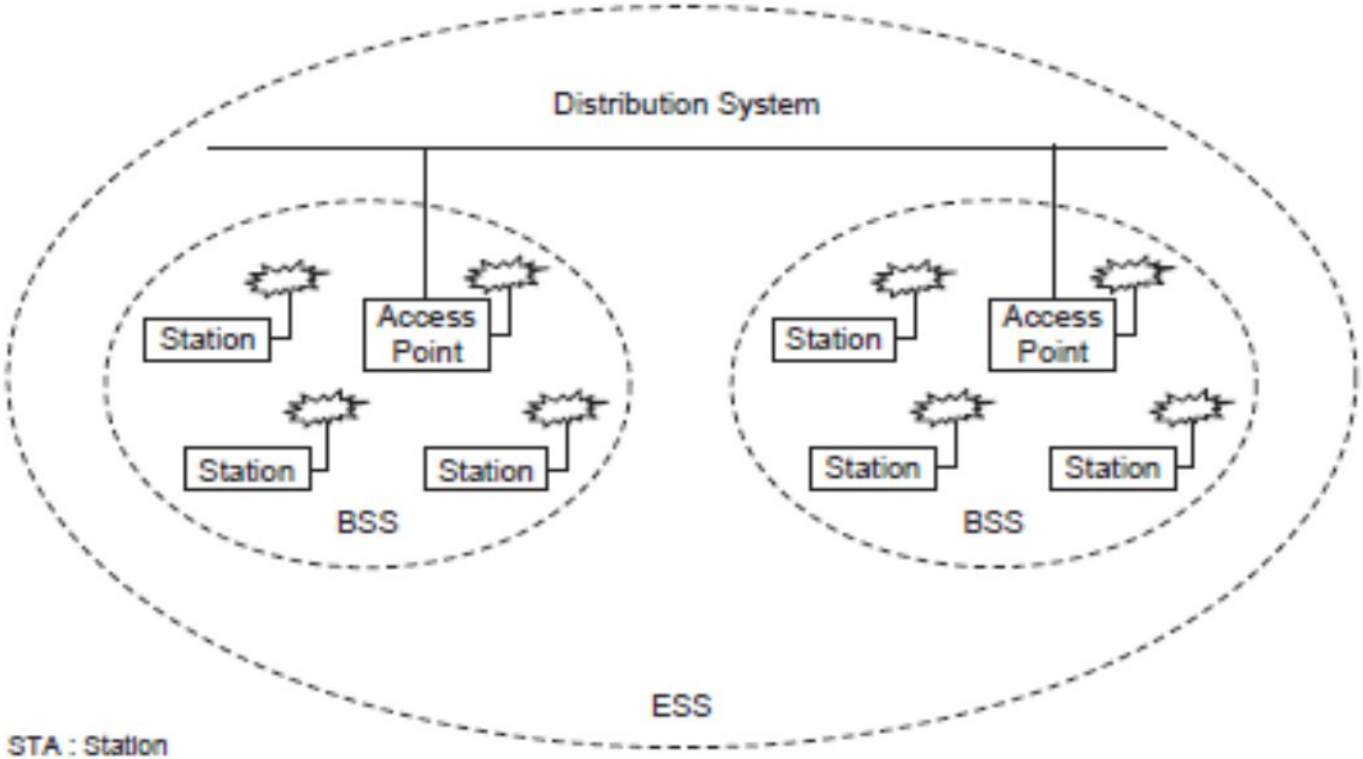


Figure 21.5 BSS and ESS configuration of IEEE 802.11 WLAN.

The MAC layer supports implementations of IBSS, basic service set, and ESS configurations.

IBSS configuration:

- ✔ It is referred to as an independent configuration or ad hoc network.
- ✔ An IBSS configuration is analogous to a peer-to-peer office network in which no single node is required to act as a server.
- ✔ IBSS WLANs include a number of nodes or wireless stations that communicate directly with one another on an ad hoc, peer-to-peer basis. Generally, IBSS implementations cover a limited area and are not connected to any large network.
- ✔ An IBSS is typically a short-lived network, with a small number of stations, that is created for a particular purpose.

Basic service set configuration

- ✔ It relies on an AP that acts as the logical server for a single WLAN cell or channel.
- ✔ Communications between station 1 and station 4 actually flow from station 1 to AP1 and then from AP1 to AP2 and then from AP2 to AP4 and finally AP4 to station 4 (refer to Figure 21.4).
- ✔ An AP performs a bridging function and connects multiple WLAN cells or channels and connects WLAN cells to a wired enterprise LAN.

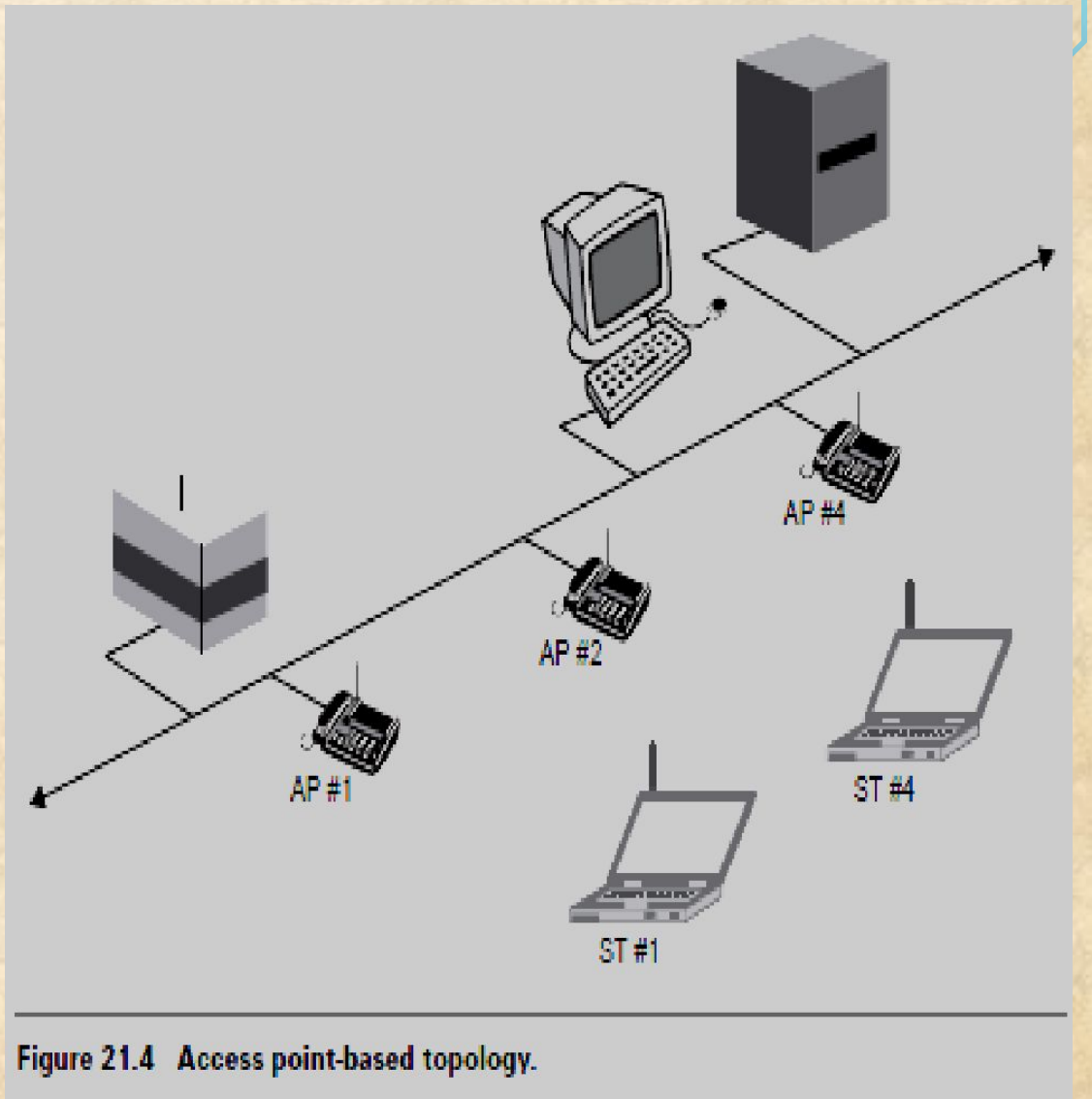


Figure 21.4 Access point-based topology.

ESS configuration

- ✔ It consists of multiple basic service set cells that can be linked by either wired or wireless backbones called a distributed system.
- ✔ IEEE 802.11 supports ESS configurations in which multiple cells use the same channel, and configurations in which multiple cells use different channels to boost aggregate throughput.
- ✔ To network the equipment outside of the ESS, the ESS and all of its mobile stations appear to be a single MAC layer network where all stations are physically stationary.
- ✔ Thus, the ESS hides the mobility of the mobile stations from everything outside the ESS.

802.11 Physical Layer (PHY)

- At the physical layer, IEEE 802.11 defines three physical characteristics for WLANs: Diffused infrared (baseband), DSSS, and FHSS.
- All three support a 1 to 2 Mbps data rate. Both DSSS and FHSS use the 2.4 GHz ISM band (2.4–2.4835 GHz).

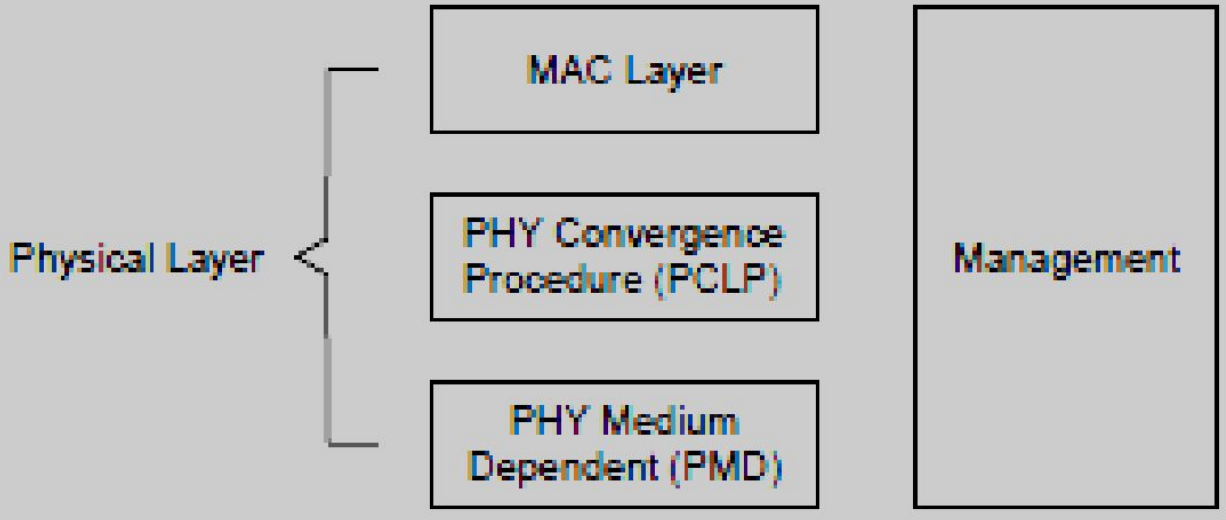


Figure 21.6 OSI model for IEEE 802.11 WLAN.

- The physical layer provides three levels of functionality:

(1) Frame exchange between the MAC and PHY under the control of the physical layer convergence procedure (PLCP) sublayer;

(2) Use of signal carrier and spread spectrum (SS) modulation to transmit data frames over the media under the control of the physical medium dependent (PMD) sublayer; and

(3) Providing a carrier sense indication back to the MAC to verify activity on the media

- Each of the physical layers is unique in terms of the modulation type, designed to coexist with each other and operate with the MAC.

DSSS PHY

In the DSSS PHY, data transmission over the media is controlled by the physical medium dependent (PMD) sublayer as directed by the physical layer convergence procedure (PLCP) sublayer. The PMD sublayer takes the binary information bits from the PLCP protocol data unit (PPDU) and converts them into RF signals by using modulation and DSSS techniques.

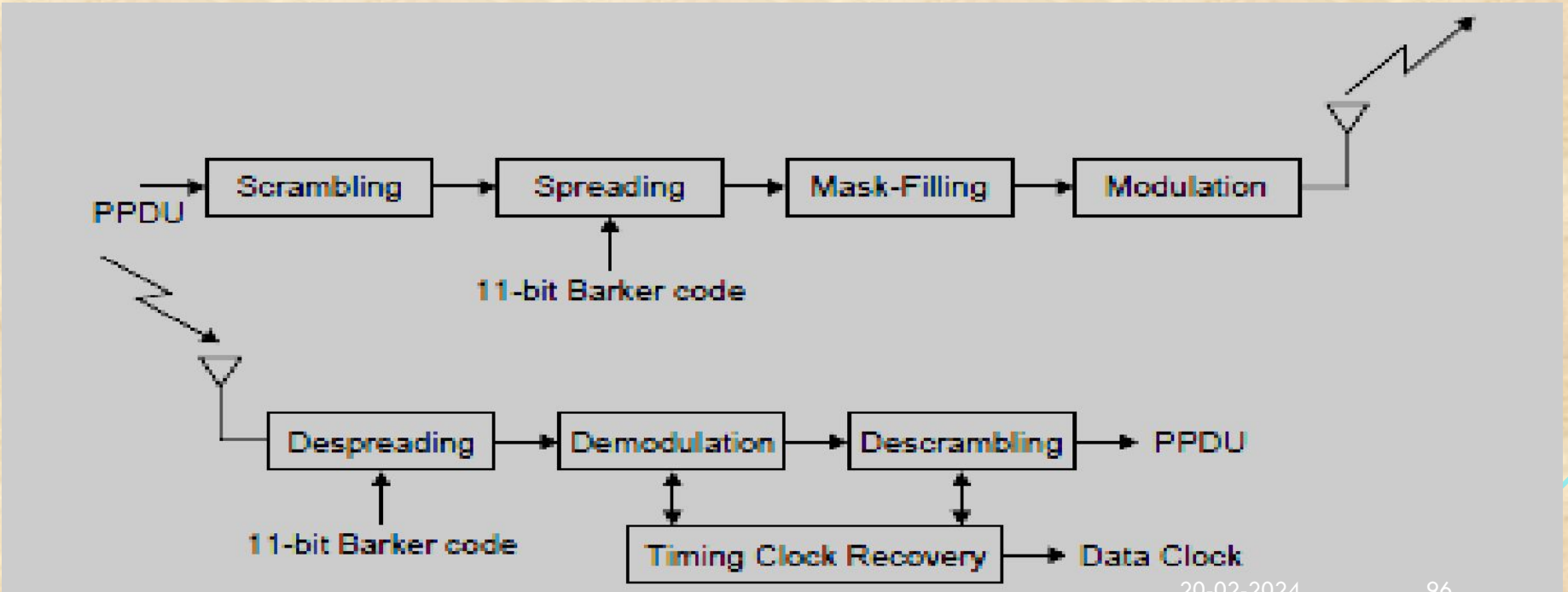


Figure 21.7 Transmit and receive DSSS PPDU.

- ✔ Figure shows the PPDU frame, which consists of a PLCP preamble, PLCP header, and MAC protocol data unit (MPDU).
- ✔ The PLCP preamble and PLCP header are always transmitted at 1 Mbps, and the MPDU can be sent at 1 or 2 Mbps.
- ✔ The **start of frame delimiter (SFD)** contains information that marks the start of the PPDU frame. The ***signal field*** indicates which modulation scheme should be used to receive the incoming MPDU. The binary value in this field is equal to the data rate multiplied by 100 kbps.

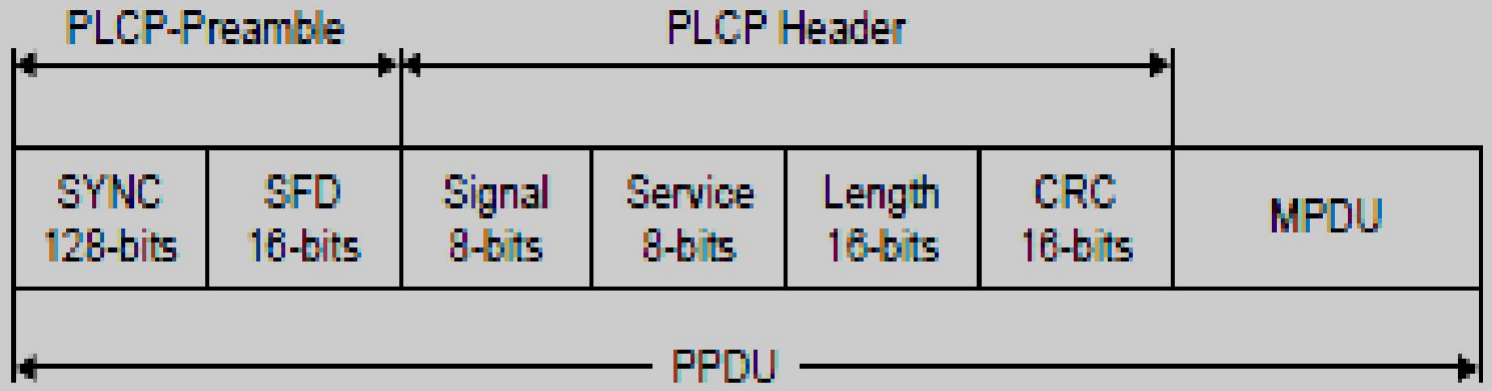


Figure 21.8 DSSS PHY PPDU frame.

FHSS PHY

- In FHSS PHY, data transmission over media is controlled by the FHSS physical medium dependent (PMD) sublayer as directed by the FHSS PLCP sublayer.
- The FHSS PMD takes the binary information bits from the whitened PSDU and converts them into RF signals by using carrier modulation and FHSS techniques (see Figure 21.10).

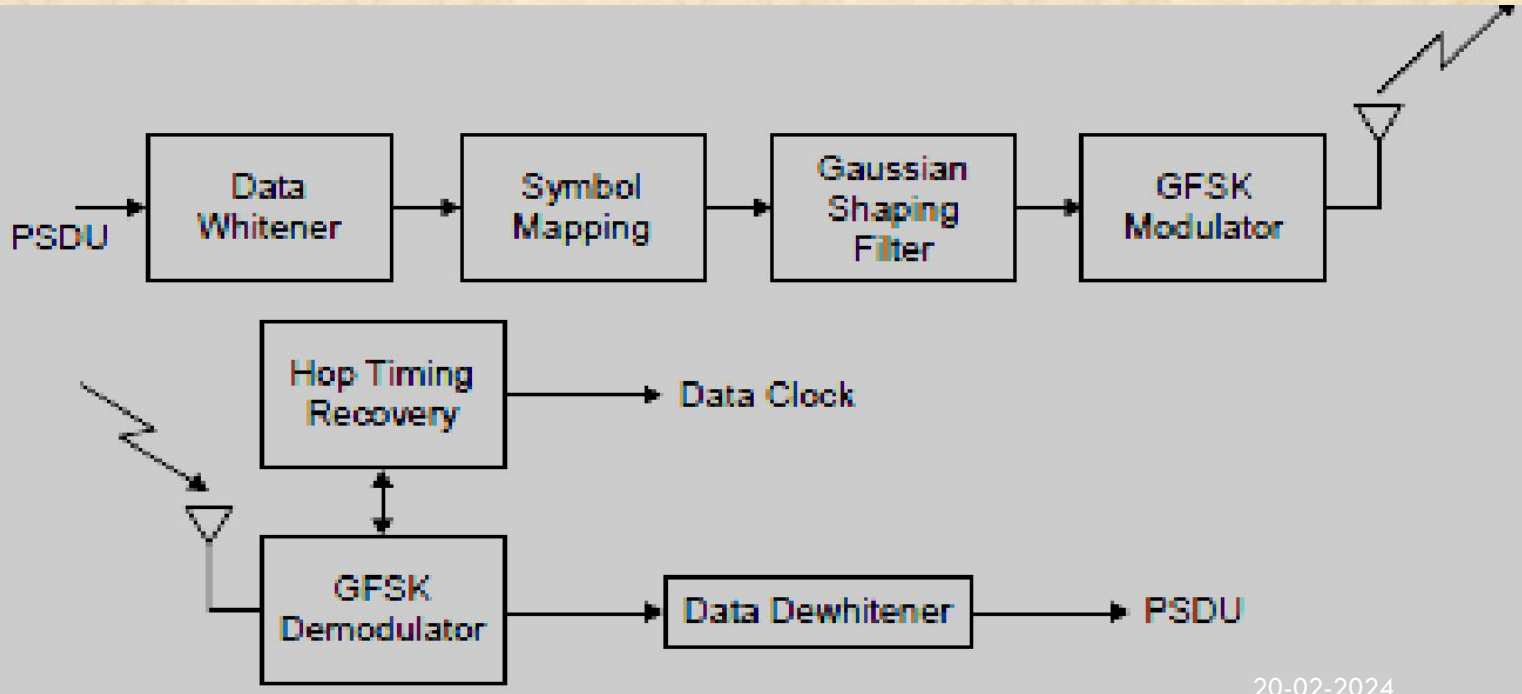


Figure 21.10 FHSS PHY transmitter and receiver.

- PPDU consists of: PLCP preamble, PLCP header, PLCP service data unit (PSDU).
- The PLCP preamble is used to acquire the incoming signal and synchronize the receiver's demodulator.
- The PLCP header contains information about PSDU from the sending physical layer. The PLCP preamble and header are transmitted at 1 Mbps.
- The *sync field* contains a string of alternating 0s and 1s pattern and is used by the receiver to synchronize the receiver's packet timing and correct for frequency offsets.

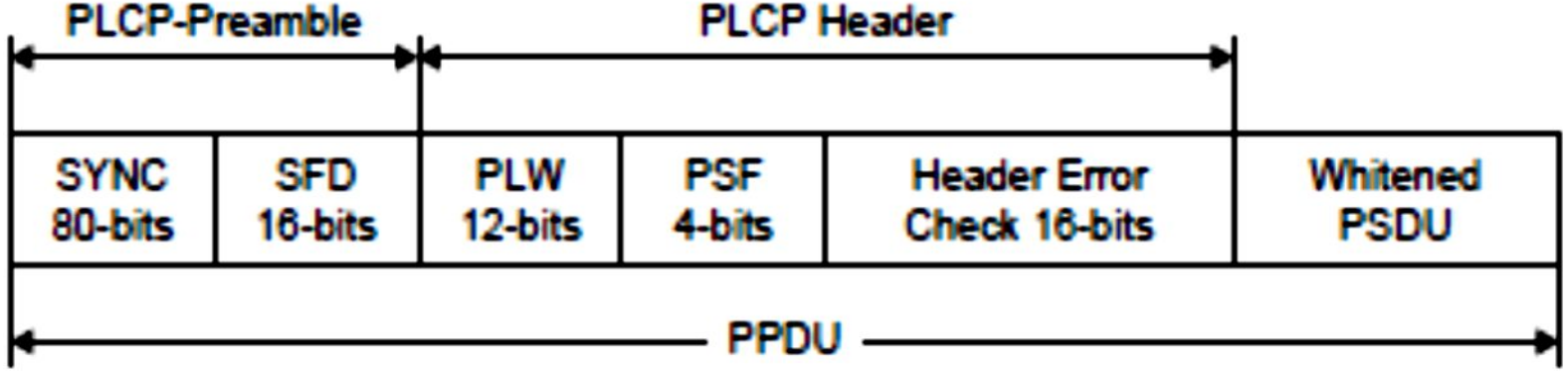


Figure 21.11 FHSS PHY PPDU frame.

IEEE 802.11 Data Link Layer

- The data link layer within 802.11 consists of two sublayers:
  - ✔ Logical link control (LLC) and
  - ✔ Media access control (MAC).
- 802.11 uses the same 802.2 LLC and 48-bit addressing as the other 802 LAN, allowing for simple bridging from wireless to IEEE wired networks, but the MAC is unique to WLAN.
- The sublayer above MAC is the LLC, where the framing takes place. The LLC inserts certain fields in the frame such as the source address and destination address at the head end of the frame and error handling bits at the end of the frame

- The 802.11 MAC is similar in concept to 802.3, in that it is designed to support multiple users on a shared medium by having the sender sense the medium before accessing it.
- In an 802.11 WLAN, collision detection is not possible due to the *near/far* problem .
- To detect a collision, a station must be able to transmit and listen at the same time, but in radio systems the transmission drowns out the ability of a station to hear a collision.

IEEE 802.11 Medium Access Control

- Wireless local area networks operate using a shared, high bit rate transmission medium to which all devices are attached and information frames relating to all calls are transmitted.

MAC sublayer defines how a user obtains a channel when he or she needs one.

- ✔ MAC schemes include random access, order access, deterministic access, and mixed access. The random access MAC protocols are:
- ✔ ALOHA (asynchronous, slotted),
- ✔ Carrier-sense multiple-access (CSMA) (CSMA/collision-detection (CD),
- ✔ CSMA/collision-avoidance (CA), non-persistent, and p-persistent).
- The maximum throughput of slotted ALOHA protocol is about 36% of the data rate of the channel .It is simple, but not very efficient.
- The CSMA peaks at about 60%. When the traffic becomes heavy, it degrades badly.

Table 21.10 Comparison of MAC access schemes in wireless networks.

Access	Protocols	Characteristics
Random	CSMA	• Under light load—fast response time • Under heavy load—throughput declines • Simple to implement
Deterministic	FDMA	• Able to provide guaranteed bandwidth
	TDMA	• Larger average delay compared to random access
	CDMA	• Smaller delay variance
Mixed	CSMA/TDMA	• Under light load—fast response time • Under heavy load—throughput approaches TDMA • Higher overhead compared to random and deterministic access

- Deterministic MAC schemes improve throughput and response time when traffic is heavy. They offer the guaranteed bandwidth for isochronous traffic.
- When the traffic is light, it is left to be mostly random.
- When the traffic is heavy and throughput is in danger of declining or if a node requires isochronous bandwidth, the control point allocates bandwidth deterministically. CSMA/TDMA approaches CSMA performance under light traffic, so it has fast access time.
- It approaches TDMA performance when the traffic becomes heavy, so its throughput can rise close to 100% of the data rate.

carrier sense multiple access with collision avoidance (*CSMA/CA*) or distributed coordination function (DCF).

- CSMA/CA attempts to avoid collisions by using *explicit packet acknowledgment* (ACK), which means an ACK packet is sent by the receiving station to confirm that the data packet arrived intact.
- The CSMA/CA protocol is very effective when the medium is not heavily loaded since it allows stations to transmit with minimum delay.
- But there is always a chance of stations simultaneously sensing the medium as being free and transmitting at the same time, causing a collision.

- These collisions must be identified so that the MAC layer can retransmit the packet by itself and not by the upper layers, which would cause significant delay.

Why not CSMA/CD?(Why collision detection is not possible in wireless environments?)

- In the Ethernet with CSMA/CD the collision is recognized by the transmitting station, which goes into a retransmission phase based on an exponential random backoff algorithm.
- While these collision detection mechanisms are a good idea on a wired LAN, they cannot be used on a WLAN environment for two main reasons:

1.Implementing a collision detection mechanism would require the implementation of a full duplex radio capable of transmitting and receiving at the same time, an approach that would increase the cost significantly.

2.In a wireless environment we cannot assume that all stations hear each other (which is the basic assumption of the collision detection scheme), and the fact that a station wants to transmit and senses the medium as free does not necessarily mean that the medium is free around the receiver area.

- To overcome these problems, the 802.11 uses a CA mechanism together with a positive ACK.

Exponential Backoff Algorithm

Explain Exponential Backoff algorithm.

- used to resolve contention problems among different stations wishing to transmit data at the same time.
- When a station goes into the backoff state, it waits an additional, randomly selected number of time slots.
- During the wait, the station continues sensing the medium to check whether it remains free or another transmission begins.
- At the end of its contention window, if the medium is still free the station can send its frame.
- If during the contention window another station begins transmitting data, the backoff counter is frozen and counting down starts again when the channel returns to the idle state.

- There is a problem related to the CW dimension.
- ✔ With a small CW, if many stations attempt to transmit data at the same time it is very possible that some of them may have the same backoff interval. This means that there will continuously be collisions, with serious effects on the network performance.
- ✔ On the other hand, with a large CW, if few stations wish to transmit data they will likely have long backoff delays resulting in the degradation of the network performance. The solution is to use an exponentially growing CW size.
- ✔ It starts from a small value (*CW*min =31) and doubles after each collision, until it reaches the maximum value *CW*max (*CW*max =1023).

In 802.11 the backoff algorithm must be executed in three cases:

- ✔ When the station senses the medium is busy before the first transmission of a packet
- ✔ After each retransmission
- ✔ After a successful transmission

  - This is necessary to avoid a single host wanting to transmit a large quantity of data, occupying the channel for too long a period, and denying access to all other stations.
  - The backoff mechanism is not used when the station decides to transmit a new packet after an idle period and the medium has been free for more than the DIFS (see Figure 21.14).

$$\text{The transmission time for a data frame} = \left\{\text{PLCP} + \frac{D}{R}\right\}\mu s$$

PLCP = the time required to transmit the physical layer convergence protocol

D = the frame size

R = the channel bit rate

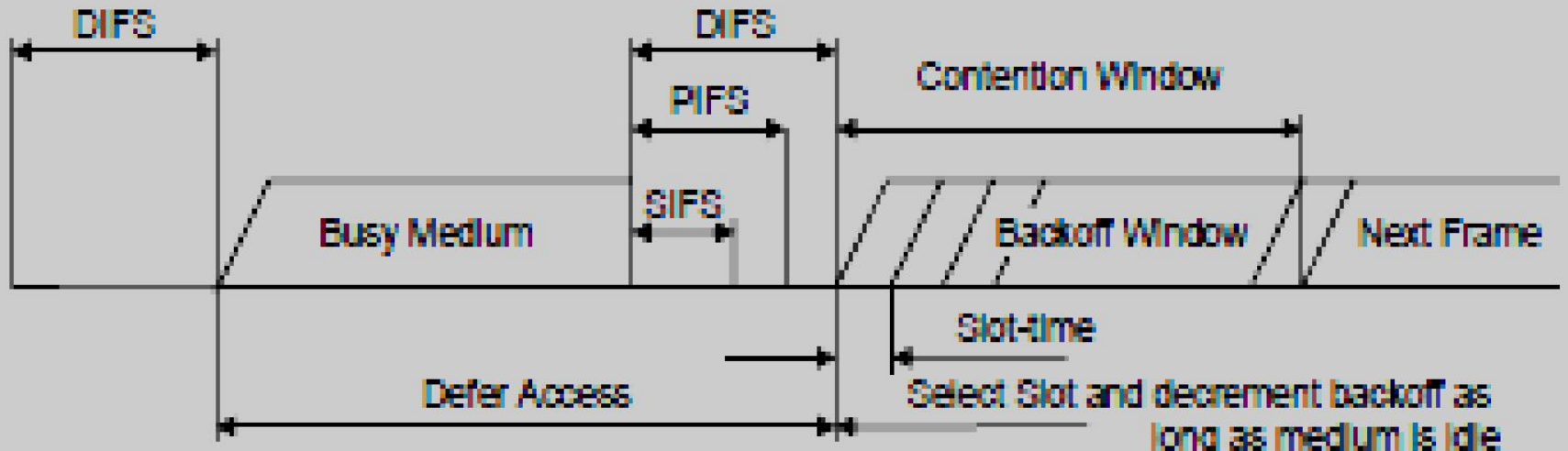


Figure 21.14 CSMA/CA in IEEE 802.11b.

$$\text{CSMA/CA packet transmission time} = BO + DIFS + 2PLCP + \frac{D}{R} + SIFS + \frac{A}{R}\,\mu s$$

where:

A = the ACK frame size
BO = the backoff time
DIPS = the distributed inter-frame space
SIPS = the short inter-frame space

The 802.11 standard defines the following four inter-frame spaces to provide different priorities.

- **Short inter-frame space (SIFS):** It is used to separate transmissions belonging to a single dialog (e.g., fragment-ACK), and is the minimum inter-frame space. There is always at most one single station to transmit at any given time, therefore giving it priority over all other stations. For the 802.11 DSSS PHY the value is 10 µs.

- **Point coordinate inter-frame space (PIFS):** It is used by the AP to gain access to the medium before any other station. This value is SIFS plus a slot time (i.e.,30 s).
- **Distributed inter-frame space (DIFS):** It is the inter-frame space used for a station willing to start a new transmission. It is calculated as PIFS plus one slot time (i.e., 50 s).
- **Extended inter-frame space (EIFS):** It is the longer inter-frame space used by a station that has received a packet which it could not understand. This is required to prevent the station from colliding with a future packet belonging to the current dialog.

Hidden and Exposed Node Problem

Another major MAC layer problem specific to a WLAN is the *hidden node* issue, in which two stations on opposite sides of an AP can both hear activity from an AP, but not from each other, usually due to distance or an obstruction (see Figure 21.15a).

What is hidden node and exposed node problems in WLAN? Explain with suitable illustration.

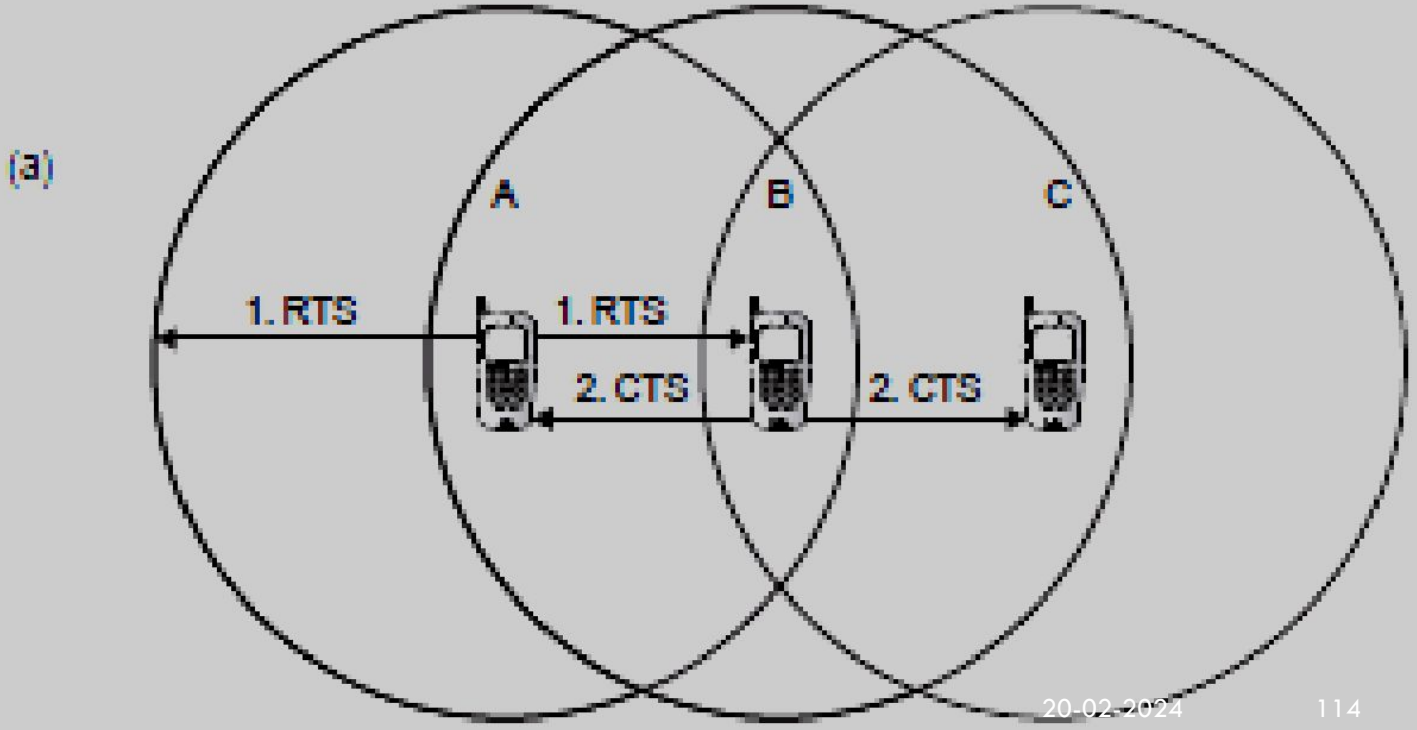


Figure 21.15(a) Hidden and exposed node problem.

- To solve this problem, 802.11 specifies an optional *request to send/clear to send* (RTS/CTS) protocol at the MAC layer.
- When this feature is in use, a sending station transmits an RTS and waits for the AP to reply with a CTS.
- Since all stations in the network can hear the AP, the CTS causes them to delay any intended transmissions, allowing the sending station to transmit and receive a packet acknowledgment without any chance of collision.
- Since RTS/CTS adds additional overhead to the network by temporarily reserving the medium, it is typically used only on the largest-sized packets, for which transmission would be expensive from a bandwidth standpoint.

- ✔ This mechanism reduces the probability of a collision on the receiver area by a station that is hidden from the transmitter to the short duration of the RTS transmission, because all stations hear the CTS and make the medium busy until the end of the transaction.
- ✔ The duration information on the RTS also protects the transmitter area from collisions during the ACK (from stations that are out of range of the acknowledged station).
- ✔ It should also be noted that, due to the fact that RTS and CTS are short frames, the mechanism also reduces the overhead of collisions, since these frames are recognized faster than if the whole packet were to be transmitted.
- ✔ The mechanism is controlled by a parameter called RTS threshold, which, if used, must be set on both the AP and the client side.

The time required to transmit a frame, taking into account the RTS/CTS four-way handshake is given as:

$$\mathrm{BO} + \mathrm{DIFS} + 4\mathrm{PLCP} + \frac{\mathrm{RTS} + \mathrm{CTS} + D + A}{R} + 3\mathrm{SIFS}\,\mu\mathrm{s}$$

BO = backoff time (μs)
DIFS = distributed inter-frame space (50 μs)
PLCP = time required to transmit physical layer convergence protocol (μs)
RTS = request to send frame size (bits)
CTS = clear to send frame size (bits)
D = frame size (bits)
A = acknowledgement frame size (bits)
R = channel bit rate (bits per second)
SIFS = short inter-frame space (10 μs)

Exposed node problem

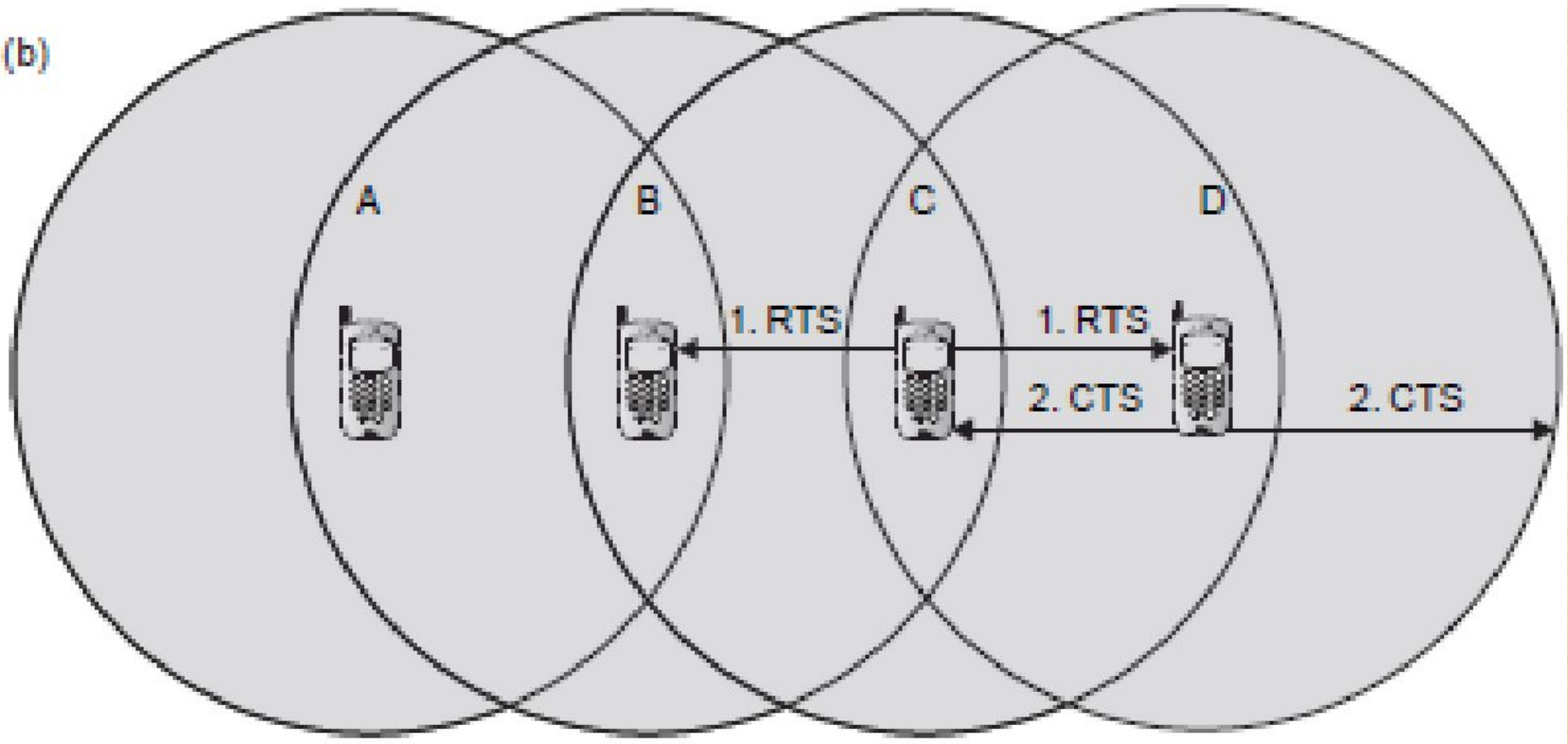


Figure 21.15(b) Hidden and exposed node problem.

- Assume that node B and C intend to transmit data only without receiving data. When node C is transmitting data to node D, node B is aware of the transmission.
- This is because node B is within the radio coverage of node C. Without exchanging RTS and CTS frames, node B will not initiate data transmission to node A because it will detect a busy medium.
- The transmission between node A and node B, therefore, is blocked even if both of them are idle.
- This is referred as the ***exposed node problem***.
- To alleviate this problem, a node must wait a random backoff time between the two consecutive new packet transmission times.

IEEE 802.11 MAC Sublayer

- In IEEE 802.11, the MAC sublayer is responsible for asynchronous data service (e.g., exchange of MAC service data units (MSDUs)), security service (confidentiality, authentication, access control in conjunction with layer management), and MSDU ordering.
- The MAC sublayer accepts MSDUs from higher layers in the protocol stack to send them to the equivalent layer of the protocol stack in another station.
- The MAC adds information to the MSDU in the form of headers and trailers to generate a MAC protocol data unit (MPDU). The MPDU is then passed to the physical layer to be sent over the wireless medium to other stations.

- The MAC may fragment MSDUs into several frames to increase the probability of each individual frame being delivered successfully.
- The MAC frame contains addressing information, information to set the network allocation vector (NAV), and a frame check sequence to verify the integrity of the frame.

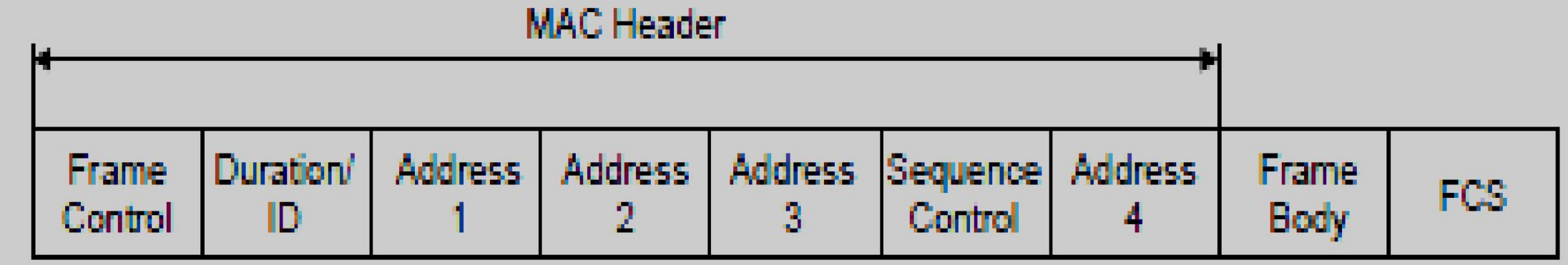


Figure 21.16 IEEE 802.11 MAC frame format.

- The MAC frame format contains four address fields. Any particular frame type may contain one, two, three, or four address fields.
- The address format in IEEE 802.11-1997 is a 48-bit address, used to identify the source and destination of MAC addresses contained in a frame, as IEEE 802.3.
- In addition to source address (SA) and destination address (DA), three additional address types are defined:

✔ the transmitter address,

✔ the receiver address (RA), and

✔ the basic service set identifier (BSSID).

- The BSSID is a unique identifier for a particular basic service set of the IEEE 802.11 WLAN. In an infrastructure basic service set, the BSSID is the MAC address of the AP.
- The *transmitter address* is the address of the MAC that transmitted the frame onto the wireless medium. This address is always an individual address. The transmitter address is used by stations receiving a frame to identify the station to which any responses in the MAC frame exchange protocol will be sent.
- The *receiver address* (*RA*) is the address of the MAC to which the frame is sent over the wireless medium. This address may be either an individual or group address.

- The *source address* (*SA*) is the address of the MAC that originated the frame.
- This address is always an individual address. This address does not always match the address in the transmitter address field because of the indirection that is performed by the distribution system of an IEEE 802.1 WLAN. It is the SA field that should be used to identify the source of a frame when indicating that a frame has been received to higher layer protocols.
- The *destination address* (*DA*) is the address of the final destination to which the frame is sent. This address may be either an individual or group address. This address does not always match the address in the RA field because of the indirection that is performed by the DS.

- The *sequence number subfield* contains numbers assigned sequentially by the sending station to each MSDU. This sequence number is incremented after each assignment and wraps back to zero when incremented from 4095.
- The *fragment number subfield* contains a 4-bit number assigned to each fragment of an MSDU. The first, or only, fragment of an MSDU is assigned a fragment number of zero. Each successive fragment is assigned a sequentially incremented fragment number. The fragment number is constant in all transmissions or retransmissions of a particular fragment.

- The *frame body field* contains the information specific to the particular data or management frames. This field is variable in length. It may be as long as 2034 bytes without encryption, or 2312 bytes when the frame body is encrypted. The value of 2304 bytes as the maximum length of this field was chosen to allow an application to send 2048-byte pieces of information, which can be encapsulated by as many as 256 bytes of upper layer protocol headers and trailers.
- The *frame check sequence (FCS) field* is 32 bits in length. It contains the result of applying the C-32 polynomial to the MAC header and frame body.

The original 802.11 standard suffers from some serious limitations which prevent it from becoming a leading technology and a serious alternative to wired LAN. The following are some of the problems:

- ✔ Low data rate: The 802.11 protocol imposes very high overhead to all packets
- ✔ That reduce real data rate significantly
- ✔ No QoS guarantees

Several extensions to the basic 802.11 standard have been introduced by IEEE to provide higher data rates or QoS guarantees. 802.11a, 802.11b, and 802.11g focus on higher data rates whereas 802.11e is aimed at providing QoS guarantees.

Joining an Existing Basic Service Set

- The 802.11 MAC sublayer is responsible for how a station associates with an AP. When an 802.11 station enters the range of one or more APs, it chooses an AP to associate with (also known as joining a basic service set), based on signal strength and observed packet error rates.
- Once accepted by the AP, the station tunes to the radio channel to which the AP is set. Periodically it surveys all 802.11 channels in order to access whether a different AP would provide it with better performance characteristics.
- If it determines that this is the case, it reassociates with the new AP, tuning to the radio channel to which that AP is set.

Explain the concept of Joining an Existing Basic Service Set

- Reassociating usually occurs because the wireless station has physically moved away from the original AP, causing the signal to be weakened.
- In other cases, reassociating occurs due to changes in radio characteristics in the building, or due to high network traffic on the original AP.
- In the latter case this function is known as load balancing, since its primary function is to distribute the total WLAN load most efficiently across the available wireless infrastructure.
- The process of dynamically associating and reassociating with APs allows network managers to set up WLANs with very broad coverage by creating a series of overlapping 802.11b cells throughout a building or across a campus.

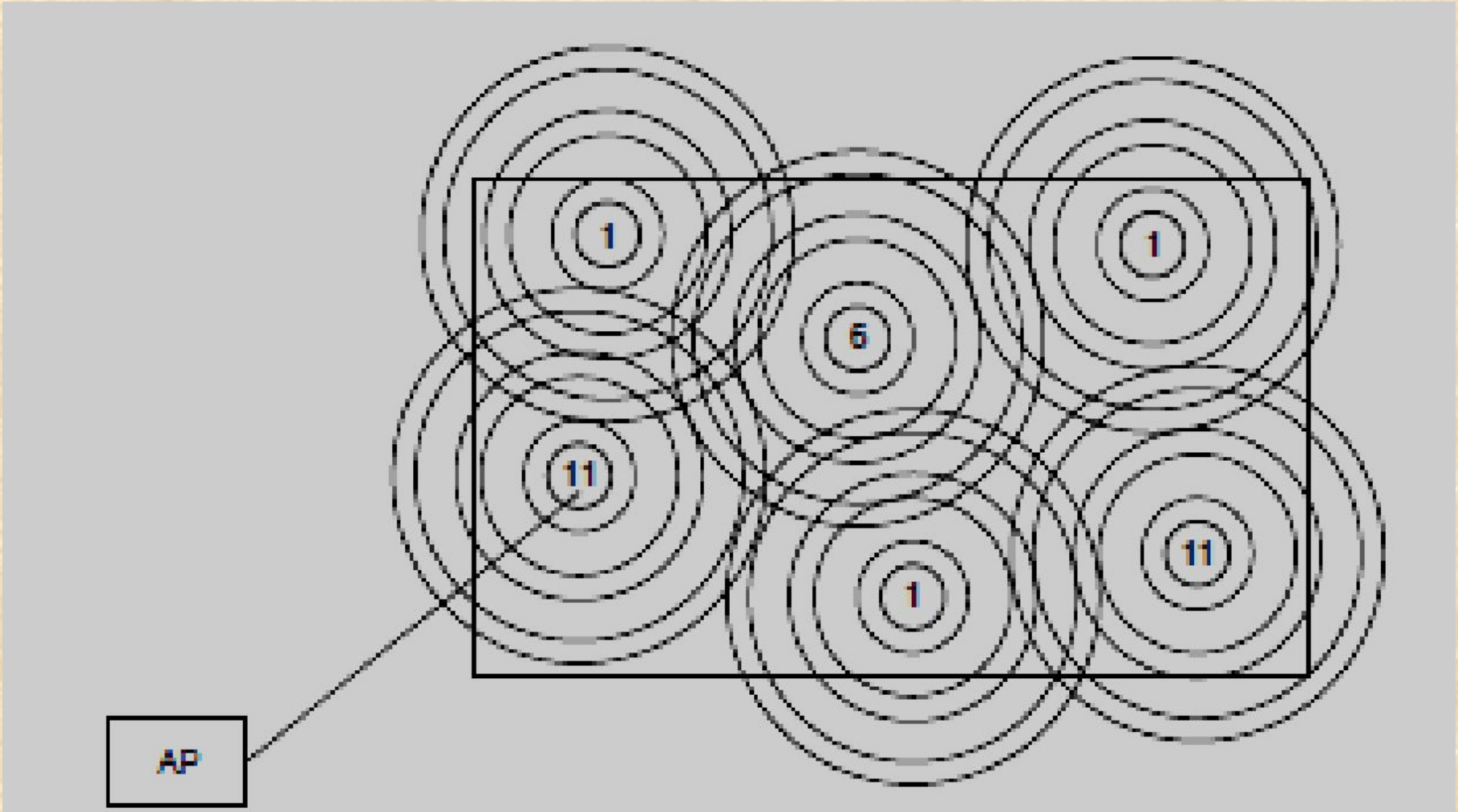


Figure 21.17 DSSS channel without overlap with a channel used by neighbor AP.

- To be successful, the IT manager ideally will employ channel reuse, taking care to set up each access point on an 802.11 DSSS channel that does not overlap with a channel used by a neighboring AP .
- If two APs are in range of one another and are set to the same or partially overlapping channels, they may cause some interference for one another, thus lowering the total available bandwidth in the area of overlap.

- When a station wishes to access an existing basic service set, it needs to get synchronization information from the AP. The station can get this information in one of two ways:
  - *Passive scanning:* In this case the station waits to receive a beacon frame from the AP. The beacon frame is a frame sent out periodically by the AP containing synchronization information.
  - *Active scanning:* In this case the station tries to locate an AP by transmitting *probe request frame*, and waits for *probe response* from the AP.
- A method is chosen according to the power consumption/performance tradeoff. Once the station has located an AP, and decides to join its basic service set, it goes through the authentication process.

- This is the interchange of information between the AP and the station, where each side proves the knowledge of a given password.
- This is necessary because WLANs have limited physical security to prevent unauthorized access.
- The goal of authentication is to provide access control equal to a wired LAN. The authentication service provides a mechanism for one station to identify another station. Without this proof of identity, the station is not allowed to use the WLAN for data delivery.
- All 802.11 stations, whether they are part of an independent basic service set or extended service set (ESS) network, must use the authentication process prior to communicating with another station. IEEE 802.11 uses authentication services defined in IEEE 802.11i.

- Once the station is authenticated, it then starts the association process.
- It is used to make a logical connection between a mobile station and an AP and to exchange information about the station and basic service set/capabilities, which allows the distribution system service (DSS) to know about the current position of the station.
- This is necessary so that the AP can know where and how to deliver data to the mobile station.
- A station is allowed to transmit data frames through the AP only after the association process is completed.

- When a station determines that the existing signal is poor, it begins scanning for another AP.
- This can be done by passively listening or actively probing each channel and waiting for a response.
- Once information has been received, the station selects the most appropriate signal and sends an association request to the new AP.
- If the new AP sends an association response, the client connects to the new AP.

- This feature is known as *roaming* and is similar to the cellular handover, with two main differences:

✔ On a packet-based LAN system, the transition from cell to cell may be performed between packet transmissions as opposed to a cellular system where the transition may occur during a phone conversation. This makes WLAN roaming a little easier.

✔ On a voice system, a temporary disconnection may not affect the conversation, while in a packet-based data system it significantly reduces performance because retransmission is performed by the upper layer protocols.

- The 802.11 standard does not define how roaming should be performed, but defines the basic tools including active/passive scanning, and a re-association process, in which a station roaming from one AP to another becomes associated with the new AP.

- The 802.11 standard also provides a mechanism to remove a station from the basic service set. The process is called de-authentication.

- De-authentication is used to prevent a previously authenticated station from using the network any further.

- Once a station is de-authenticated, it is no longer able to access the WLAN without performing the authentication process again.
- De-authentication is a notification and cannot be refused. When a station wishes to be removed from a basic service set, it can send a de-authentication management frame to the associated AP.
- An AP could also de-authenticate a station by sending a de-authentication frame to the station.

Security of IEEE 802.11 Systems

- The IEEE 802.11 provides for MAC access control and encryption mechanisms. Earlier, the wireline equivalent privacy (WEP) algorithm was used to encrypt messages.

- WEP uses a Rivest Cipher 4 (RC4) pseudo-random number generator with two key structures of 40 and 128 bits.

- Because of the inherent weaknesses of the WEP, the IEEE 802.11i committee developed, a new encryption algorithm and worked on the enhanced security and authentication mechanisms for 802.11 systems.

- For access control, ESSID (also known as a WLAN service area ID) is programmed into each AP and is required knowledge in order for a wireless client to associate with an AP.

- In addition, there is provision for a table of MAC addresses called an access control list to be included in the AP, restricting access to stations whose MAC addresses are not on the list.

- Beyond layer 2, 802.11 WLANs support the same security standards supported by other 802 LANs for access control and encryption.

- These higher-level technologies can be used to create end-to-end secure networks encompassing both wired LAN and WLAN components, with the wireless piece of the network gaining additional security from the IEEE 802.11i feature set.

Explain WEP frame security mechanism.

Power Management

- Power management is necessary to minimize power requirements for battery powered portable mobile units.
- The standard supports two power-utilization modes, called *continuous aware mode* and *power save polling mode*.

✔ *Continuous aware mode:* The radio is always on and draws power,

✔ *Power save polling mode*: The radio is dozing with the AP and is queuing any data for it. A power saver mode or sleep mode is defined when the station is not transmitting in order to save battery power. However, critical data transmissions cannot be missed. Therefore APs are required to have buffers to queue messages.

- ✔ Sleeping stations are required to periodically wake up and retrieve messages from the AP.
- ✔ Power management is more difficult for peer-to-peer IBSS configurations without central AP. In this case, all stations in the IBSS must be awakened when the periodic beacon is sent.
- ✔ Stations randomly handle the task of sending out the beacon. An announcement traffic information message window commences.
- ✔ During this period, any station can go to sleep if there is no announced activity for it during this short period.

✔ Students are suggested to read more about power saving in WLAN.

Table 21.16 Comparisons of various WLAN standards.

	IEEE 802.11	IEEE 802.11b	IEEE 802.11a	IEEE 802.11g	HIPERLAN/1	HIPERLAN/2	MMAC HiSWAN
Rectification	June 1997	Sept. 1999	Sept. 1999	June 2003	early 1993	Feb. 2000	April 1997
RF bandwidth (GHz)	2.4	2.4	5.0	2.4	5	5	5
Max. data rate (Mbps)	2	11	54	54	23.5	54	27
Physical layer (PHY)	FHSS, DSSS, IR	DSSS	OFDM	OFDM	GMSK	OFDM	OFDM
Range (m)	50–100	50–100	50–100	50–100	50	50 indoor, 300 outdoor	100–150