University of Technology
Computer Science

Wireless Fundamental

2023-2024

Fourth Class

Dr. Asia Ali

Wireless Network

1st course lecture 1

- **Introduction to the WIRELESS Networks**

Lecturer: Dr. Asia Ali

OBJECTIVES Of This Course:

- **To study about Wireless networks, protocol stack and standards.**
- **To study about fundamentals of 3G Services, its protocols and applications.**
- **To study about evolution of 4G Networks, its architecture and applications.**

First Course lectures(plan)

1- introduction to the WIRELESS LAN

WLAN technologies: Infrared, UHF narrowband, spread spectrum.

IEEE802.11: System architecture, protocol architecture, physical layer, MAC layer, 802.11b, 802.11a

– **Hiper LAN**: WATM, BRAN, HiperLAN

– **Bluetooth**: Architecture, Radio Layer, Baseband layer, Link manager Protocol, security.

IEEE802.16-WIMAX: Physical layer, MAC, Spectrum allocation for WIMAX.

2- MOBILE NETWORK LAYER Introduction

– **Mobile IP**: IP packet delivery, Agent discovery, tunneling and encapsulation. IPV6

-Network layer in the internet.

- Mobile IP session initiation protocol

- mobile ad-hoc network: Routing, Destination Sequence distance vector, Dynamic source routing

3- MOBILE TRANSPORT LAYER -TCP enhancements for wireless protocols.

Wireless networks

Introduction

The availability of high performance, low power, and low-cost digital signal processors, and advances in digital communication techniques over the radio frequency spectrum have resulted in the widespread availability of wireless network technology for mass consumption.

Wireless networks are best known in the context of first- and second generation mobile telephony (AT&T's analog AMPS, Advanced Mobile Phone System,in the first generation (1 G), and the GSM and CDMA digital systems in the second generation(2 G)).

Figure 1-the first generation (1 G), and the GSM and CDMA (2 G)

However, networks carry the flows of information between distributed applications such as

- telephony
- teleconferencing
- media-sharing, World Wide Web access, e-commerce, etc.

Wireless networking is concerned with *algorithms for resource allocation between* devices sharing a portion of the radio spectrum. On the other hand, in **wireline networks** the resource allocation algorithms are concerned with sharing the fixed resources of a bit transport infrastructure.

How Wireless Networks Work?

Moving data through a wireless network involves three separate elements:

- radio signals
- The data format
- The network structure.

In terms of the OSI reference model, the radio signal operates at the physical layer, and the data format controls several of the higher layers. The network structure includes the wireless network interface adapters and base stations that send and receive the radio signals.

In a wireless network, the network interface adapters in each computer and base station convert digital data to radio signals, which they transmit to other devices on the same network, and they receive and convert incoming radio signals from other network elements back to digital data.

Each of the broadband wireless data services use a different combination of radio signals, data formats, and network structure.

In wireline networks the information to be transported between the endpoints of applications is carried over a static bit-carrier infrastructure. These networks typically comprise high quality digital transmission systems over copper or optical media.

Typically, each wireless network system is constrained to operate in some portion of the RF (Radio frequency) spectrum. For example, a cellular telephony system may be assigned 5 MHz of spectrum in the 900 MHz band. Information bits are transported between devices in the wireless network by means of some physical wireless communication technique (i.e., a PHY layer technique, in terms of the ISO-OSI model) operating in the portion of the RF spectrum that is assigned to the network.

The frequency that is used for wireless network is Radio frequency signals and it has a range from: 30 KH to 300 GH.

These signals are invisible and used to send messages from one device to another.

Uses: FM Radio station use RF signal to broadcast signals. The frequency is used as the station name (like 93.5 RED FM)

Requirement to create wireless network:

- Network interface card (NIC) used for wireless.
- NIC use antenna unlike the RJ45 cable.
- Access point for generating signal and establish connection between devices.
- Devices which has wireless signal adapter.

A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.

Purpose

NIC allows both wired and wireless communications.

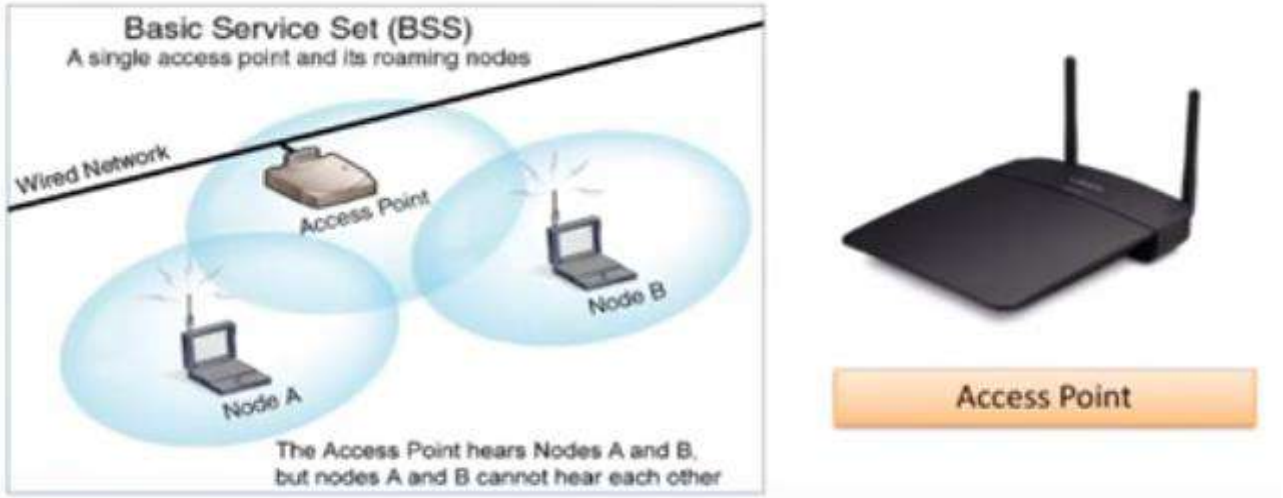
NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP).

NIC is both a physical layer and a data link layer device, i.e. it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

Types of NIC Cards

Figure 1- (a)- A wireless network adapter for installation inside a desktop computer. (b)- A wireless network adapter that attaches to a computer's USB port.

Figure 2- A PC Card wireless network interface adapter.



Types of wireless networks:

Based on the size wireless networks are divided into 4 categories

Wireless LAN

Wireless MAN

Wireless WAN

Wireless PAN

Wireless LAN (Local Area Network)

This is a network where two or more computers are connected that covers only a limited area.

The NIC is used in this connection where has a small rang to cover.

We often called this peer to peer network.

This is also called Ad Hoc Network which is being set up for temporary purposes.

Unlike switch in a wired network, a special device is used in WLAN, which is called access point.

WLAN which uses Access Point are called BSS (Basic Service Set). This acts as a coordinator between different devices.

WIFI

Wireless fidelity.

Uses the 802.11 suite of protocol (802.11 a/ b/g/n/ac/ax)

RF signal frequency :2.4 GHz or 5 GHz

Wi-fi technology is only used in WLAN.

Range: about 100 meters.

WI-FI ALLIANCE. We can see their trademarks in most of the WI-FI DEVICES.

WMAN (Wireless Metropolitan area Network)

Collected units of many WLANs located at various.

It uses WIMAX (worldwide interoperability for microwave access) which is controlled by WiMAX.

Maximum speed 1 Gbits/sec.

IEEE 802.16

NOTE: Microwave is a line-of-sight wireless communication technology that uses high frequency beams of radio waves to provide high-speed wireless connections that can send and receive voice, video, and data information.

Microwaves signals are often divided into three categories:

Ultra high frequency (UHF)(0.3-3 GHz)

Super high frequency (SHF) (3-30 GHz)

Extremely high frequency (EHF)(30-300 GHz)

WWAN (Wireless wide area network)

WWAN is a very large network which is spread over a very large area. It connects many cities together.

Mobile phones use WWAN to make communication possible.

The technology in WWAN are subdivided in many generations.

2G, 3G and 4 G

The communication system which was used before the emergence of 2 G is called 1 G used in 1980.

This technology used in most of the analog devices.

- **2 G**

Examples of 2nd generation technologies are

GPRS (General Packet Radio Service)

EDGE (Enhanced Data rates for GSM Evoluation)

- **3G- 4G**

- High speed network accessibility can be achieved in this technologies
- *The examples of 4th generation technologies are*
  - *LTE (Long Term Evolution)*
  - *VoLTE (Voice Over long term Evolution)*

1G First Generation of Mobile Phone

- The first handheld mobile cell phone was demonstrated by Motorola in 1973.
- The first commercial automated cellular network was launched in Japan by NTT in 1979.
- These '1G' systems could support far more calls but still used analog technology.
- Basic Mobility
- Basic Services
- Incompatibility
- Analog System

2G Second Generation of Mobile Phone

- In 1991, the second generation (2G) digital cellular technology was launched in Finland by Radiolinja on the GSM standard, which sparked competition in the sector as the new operators challenged the incumbent 1G network operators.
- Advanced mobility (Roaming)
- More services (Data presence)
- Towards global solution
- Digital system

WPAN (Wireless Personal Area Network)

The wireless networks that are used in smaller distances are known as a PAN(802.15, ZigBee, Bluetooth and infrared data Association)

The communication between a mobile phone and its Bluetooth headset is a typical example of WPAN.

Two kinds of wireless technologies are used for WPAN.

Wireless Network

1st course lecture 2

- **Lecture outlines**
- Continue with to the Introduction to the Wireless Networks
- Radio Spectrum: The Key Resource

Lecturer: Dr. Asia Ali

Security options in Wireless Network

Data can be easily hacked in wireless network without using proper security. The RF signal can be intercepted by Antenna

Three commonly used security system:-

Wired Equivalent Privacy (WEP)

Wi-Fi Protected Access (WPA)

Wi-Fi protected Access II (WPA2)

Wired Equivalent Privacy (WEP)

Security standard released in 1997

The encryption algorithm used in WEP was easily breakable by hackers.

Encryption refers to the technique of converting data in such a way that it's understood only by the Sender and Receiver.

Wi-Fi Protected Access (WPA)

Released in 2003

Invented by Wi-Fi Alliance

Required firmware upgradation instead of changing any hardware component.

Uses TKIP (Temporal Key Integrity Protocol) algorithm

Better security than WEP

Wi-Fi protected Access II (WPA2)

Released in 2004

Advanced security features are available

advanced encryption standard (AES) algorithm is used for better security.

IEEE Standards

There are various types of standards decide for wireless networks. IEEE is the authority which determines various standards for functioning of wireless networks.

Most of the networking standards are designed by 802 standards committee.

IEEE Wireless Standards

First wireless LAN came into existence in 1997

IEEE 802.11 standard was designed for that.

Frequency used : 2.4 GHz

Maximum Speed: 2 Mbps

This standard is now called 802.11 legacy.

IEEE Wireless Standards

802.11a (year 1999's, frequency 5 GHz, Maximum speed 54Mbps)

802.11 b (year 1999's, frequency 2.4 GHz, Maximum speed 11Mbps)

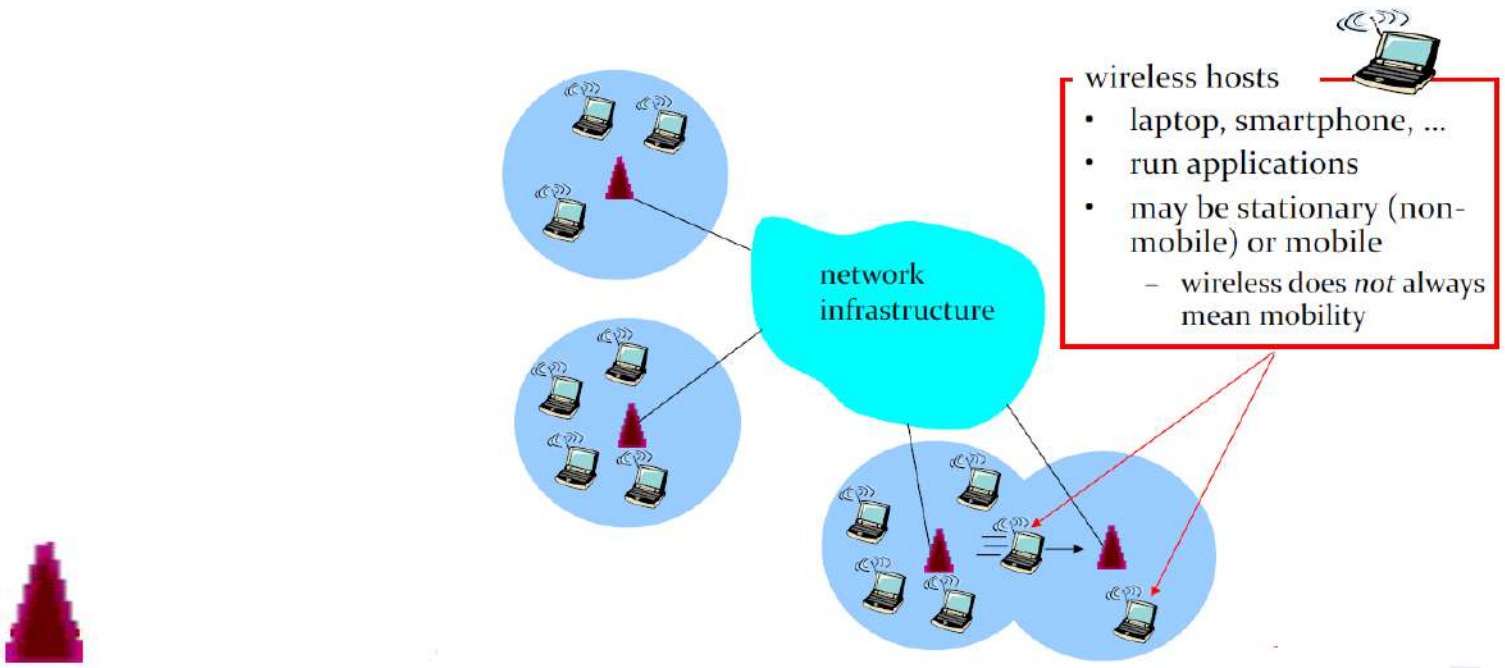
802.11g (year 2003, frequency 2.4 GHz, speed 54 Mbps)

802.11n (year 2009, frequency 2.4 GHz and 5 GHz, speed 300 Mbps)

Drawbacks

- RF signal strength gets weaken while going through a certain distance.
- This signal is affected by opaque body such as concrete wall, big objects and even by human body.
- As the signal is transmitted as RF signal it is easy for the hacker to hack by using an antenna.

A Simple and Common Wireless Network Model



wireless link: connects wireless host (s) to base station can also be used as backbone link, multiple access protocol coordinates, link access various data rates, transmission distance

Base station: typically connected to a wired network
• relay - responsible for sending packets between wired network and wireless host(s) in its "area"– e.g., Wi-Fi access points, cell towers.

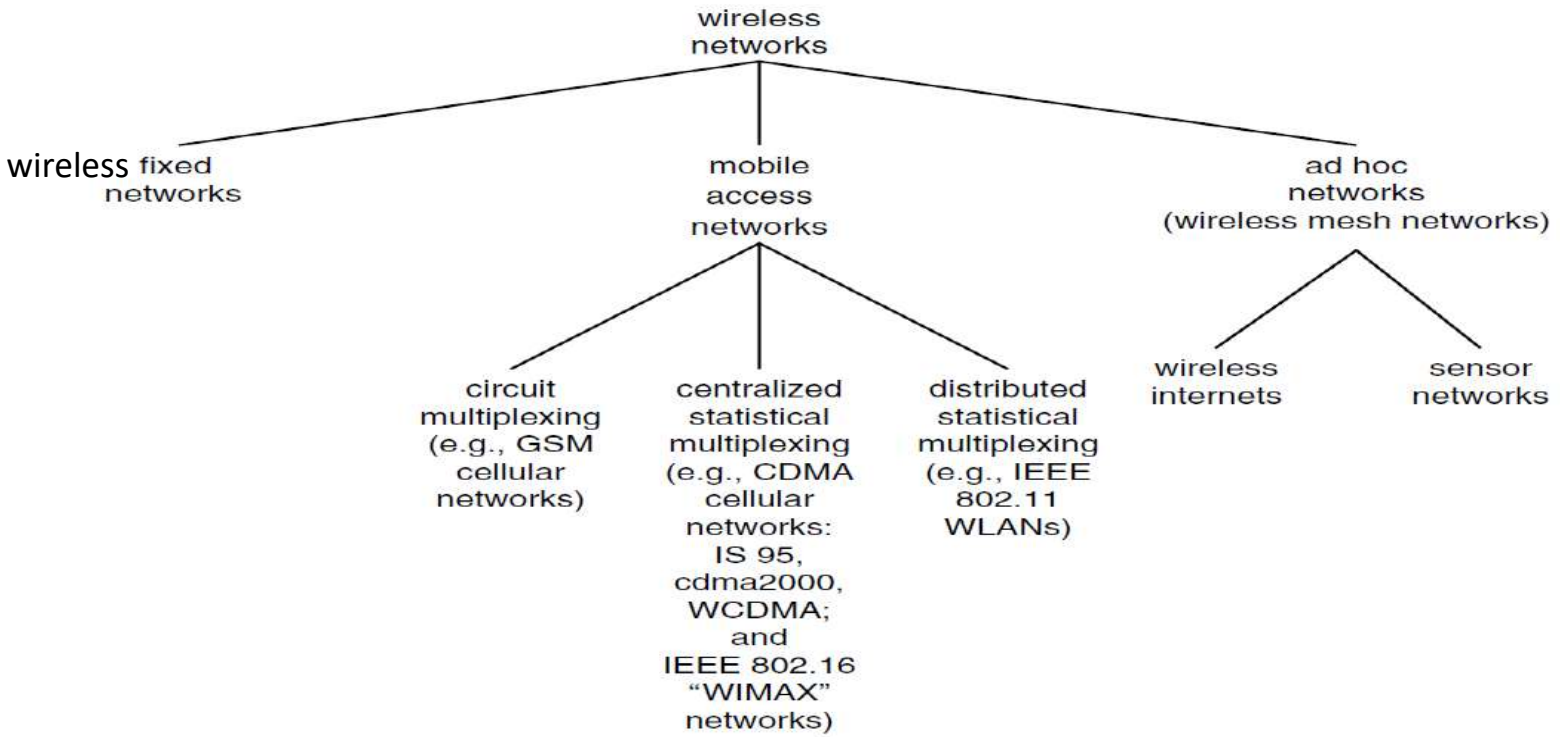
Why we use wireless network?

It is helpful for portable devices such as Laptops, mobiles, tablet
Establish a network connection is easy
Introducing a new device in the network is easy.
Security system is more featured in wireless networks.

Broadband Access

- ***Wired Broadband Access***
- **FTTx: FTTH (Fibre to the Home), FTTC (Fibre to the Cabinet), etc.**
- **ADSL, Ethernet.**
- ***Wireless Broadband Access***
- **Cellular Networks (3G, 4G, LTE-A (Long-term Evolution Advanced), 5G, WiFi, WiMAX, etc.)**

A Taxonomy of wireless networks



A compression table (1) between infrastructure (AP) and no infrastructure

	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station, which connects to larger Internet (e.g., Wi-Fi, cellular, WiMax)	host may have to relay through several wireless nodes to connect to larger Internet (e.g., mesh nets)
no infrastructure	no base station, no connection to larger Internet (e.g., Bluetooth, ad hoc nets, Wi-Fi Direct)	no base station, no connection to larger Internet. May have to relay to reach another given wireless node (e.g., MANET, VANET)

A simplified reference model

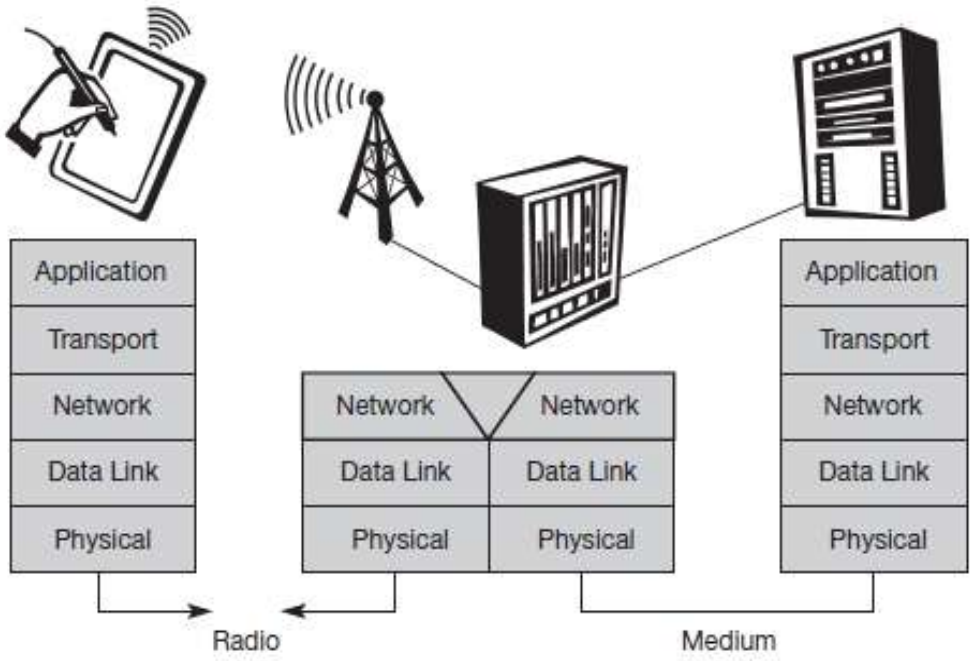


Figure 3- a simple network and reference model.

Figure 3 shows a personal digital assistant (PDA) which provides an example for a wireless and portable device. This PDA communicates with a base station in the middle of the picture. The base station consists of a radio transceiver (sender and receiver) and an interworking unit connecting the wireless link with the fixed link. The communication partner of the PDA, a conventional computer, is shown on the right-hand side.

➢ Radio Spectrum: The Key Resource

Wireless devices are constrained to operate in a certain frequency band.

Each **band** has an associated *bandwidth*, which is simply *the amount of frequency space in the band*. Bandwidth has acquired a connotation of being a measure of the data capacity of a link. As an example, an analog mobile telephony channel requires a 20-kHz bandwidth. TV signals are more complex and have a correspondingly larger bandwidth of 6 MHz. The use of a radio spectrum is controlled by regulatory authorities through *licensing* processes.

In the U.S., regulation is done by the Federal Communications Commission (FCC). Many FCC rules are adopted by other countries throughout the Americas. European allocation is performed by CEPT's European Radio communications Office (ERO). Other allocation work is done by the International Telecommunications Union (ITU). To prevent overlapping uses of the radio waves, frequency is allocated in bands, which are simply ranges of frequencies available to specified applications.

Table 1- lists some common frequency bands used in the U.S.

Transmission type	*Frequency*	*Wavelength*
Very low frequency (VLF)	9–30 kHz	33–10 km
Low frequency (LF)	30–300 kHz	10–1 km
Medium frequency (MF)	300–3000 kHz	1000–100 m
High frequency (HF)	3–30 MHz	100–10 m
Very high frequency (VHF)	30–300 MHz	10–1 m
Ultra high frequency (UHF)	300–3000 MHz	1000–100 mm
Super high frequency (SHF)	3–30 GHz	100–10 mm
Extremely high frequency (EHF)	30–300 GHz	10–1 mm

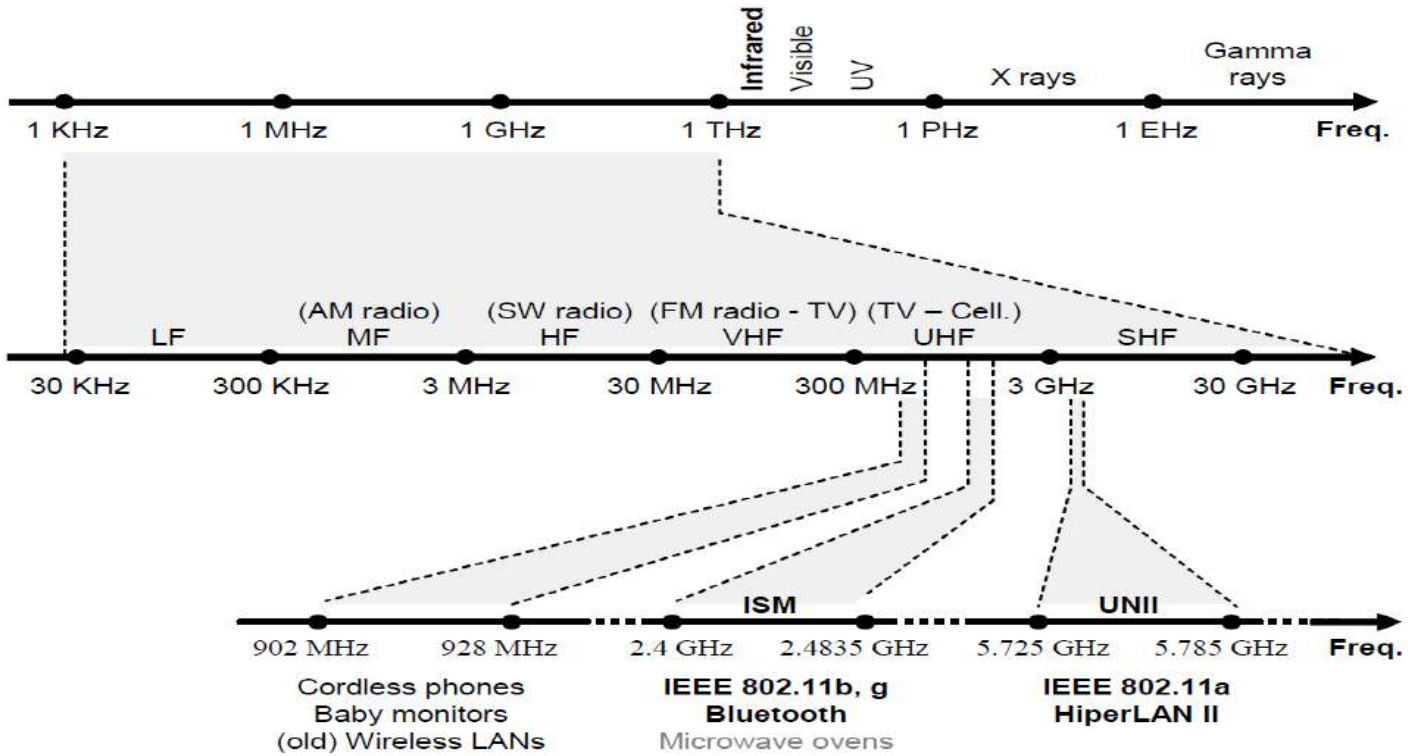
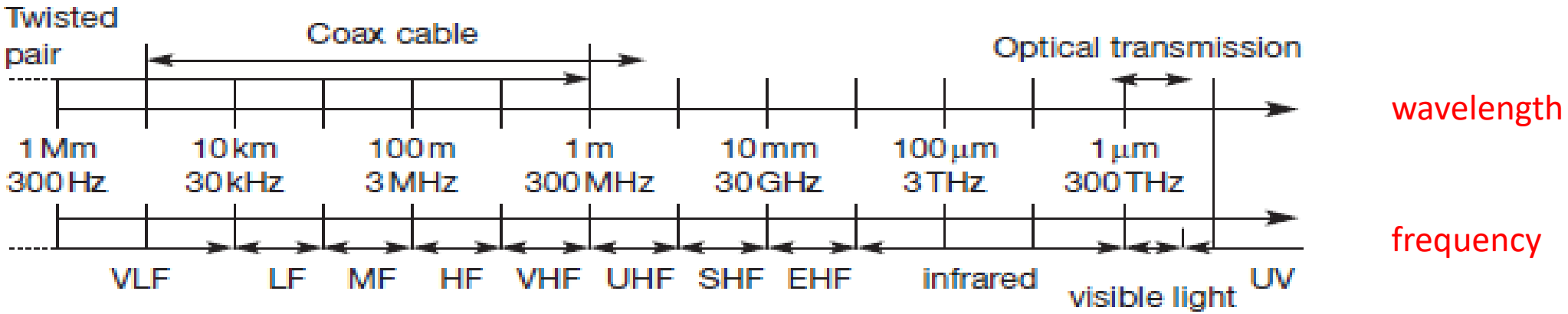


Figure 1-The electromagnetic spectrum allocation. ISM = Industry, Science & Medicine, UNII = Unlicensed National Information Infrastructure.



VLF = Very Low Frequency

LF = Low Frequency

MF = Medium Frequency

HF = High Frequency

VHF = Very High Frequency

UHF = Ultra High Frequency

SHF = Super High Frequency

EHF = Extra High Frequency

UV = Ultraviolet Light

Figure 2-Frequency spectrum for communication

Example:

Wireless Fidelity (Wi-Fi) is a wireless network technology used for connecting to the Internet. The frequencies wi-fi works at are 2.4Ghz or 5Ghz, ensure no interference with cell phones, broadcast radio, TV antenna and two-way radios are encountered during transmission.

Microwave signals are often divided into three categories:

ultra high frequency (UHF) (0.3-3 GHz);
super high frequency (SHF) (3-30 GHz); and
extremely high frequency (EHF) (30-300 GHz).

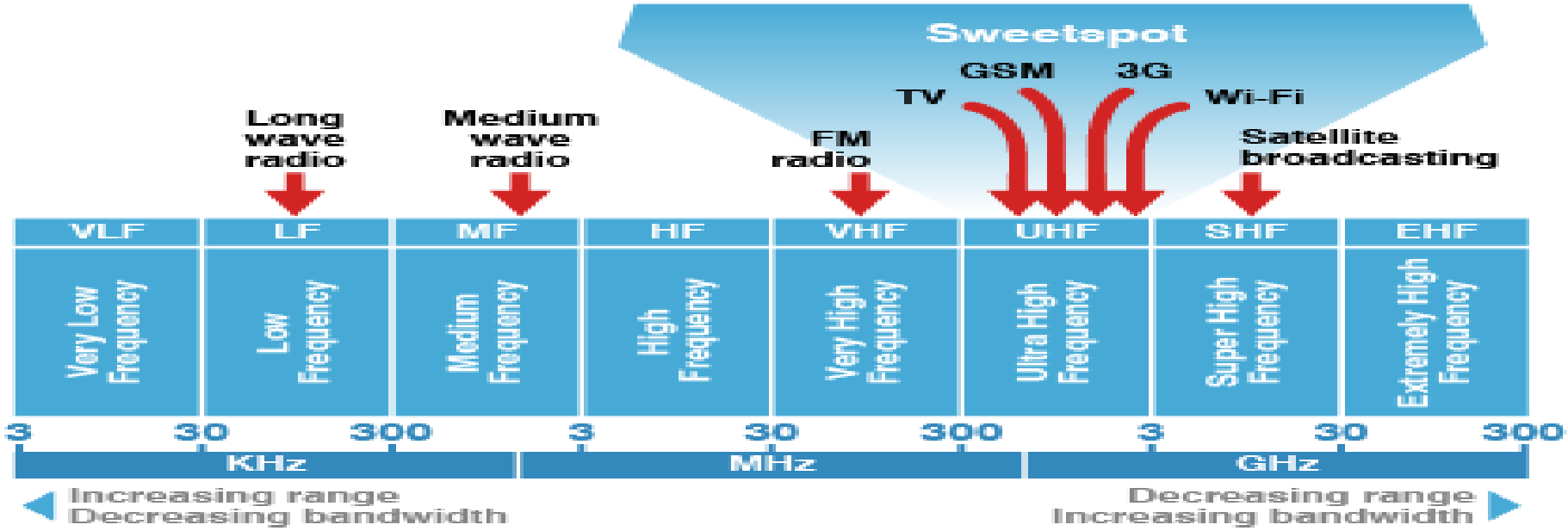


Figure 3 Radio Frequency Spectrum (2)

The Infrared (Ir) Spectrum

Infrared radiation takes over from extremely high frequency (EHF) at 300 GHz and extends to just below the red end of the visible light spectrum at 1mm wavelength. The radio frequency or infrared communication technologies are at the heart of the physical layer of wireless networks.

Spread Spectrum

Spread spectrum is a family of methods for transmitting a single radio signal using a relatively wide segment of the radio spectrum. Wireless Ethernet networks use several different spread spectrum radio transmission systems, which are called:

Frequency-hopping spread spectrum (FHSS)

Direct-sequence spread spectrum (DSSS)

Spread spectrum radio offers some important advantages over other types of radio signals that use a single narrow channel. Spread spectrum is extremely efficient, so the radio transmitters can operate with very low power. Because the signals operate on a relatively wide band of frequencies.

The Wi-Fi standards are less sensitive to interference from other radio signals and electrical noise, which means they can often get through in environments where a conventional narrow-band signal would be impossible to receive. And because a frequency-hopping spread spectrum (FHSS) signal shifts among more than one channel, it can be extremely difficult for an unauthorized listener to intercept and decode the contents of a signal.

Wireless network topologies

- **Point-to-Point**
- **Point-to-Multipoint**
- **Multipoint-to-Multipoint**

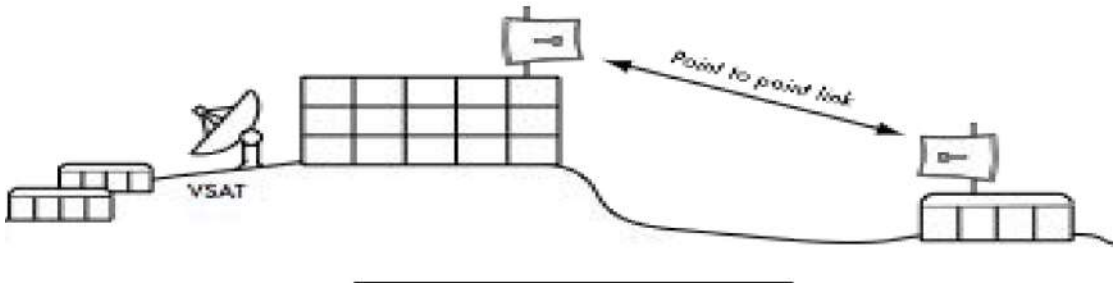


Figure 1- Point to point connection link

Point to Multipoint

When more than one node communicates with a central point, this is a **point-to-multipoint** network

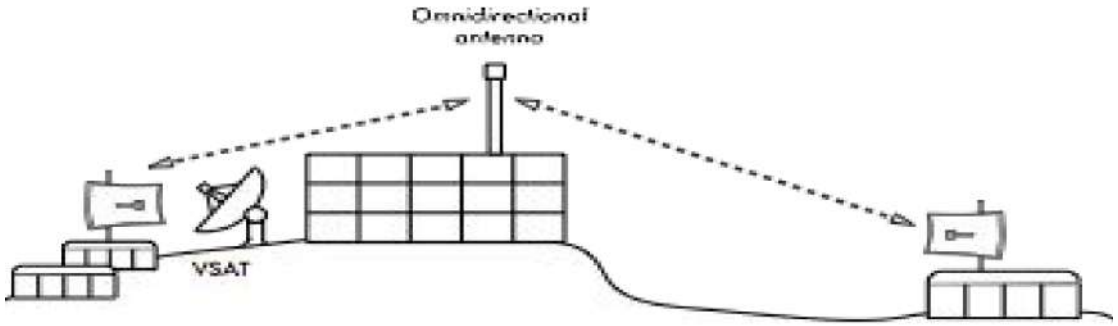


Figure 2-Point to multipoint network

Multipoint to Multipoint

When any node of a network may communicate with any other, this is a **multipoint-to-multipoint** network (also known as an **ad-hoc** or **mesh** network).

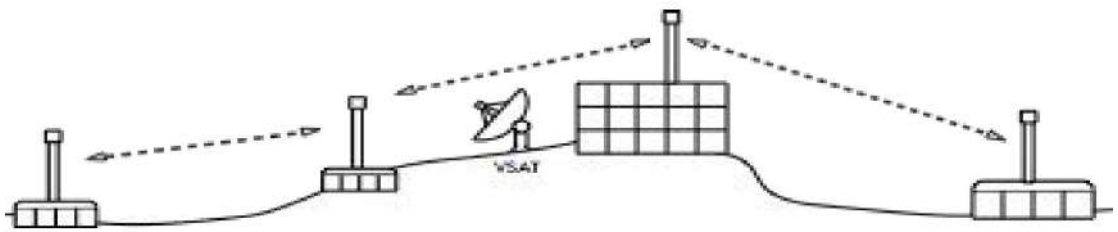


Figure 3- Multipoint-to-multipoint network

Point to Multipoint

When more than one node communicates with a central point, this is a **point-to-multipoint** network

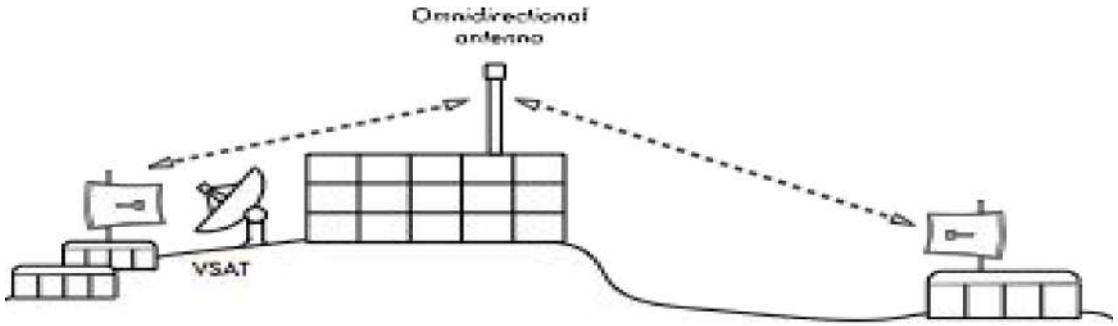


Figure 2-Point to multipoint network

Multipoint to Multipoint

When any node of a network may communicate with any other, this is a **multipoint-to-multipoint** network (also known as an **ad-hoc** or **mesh** network).

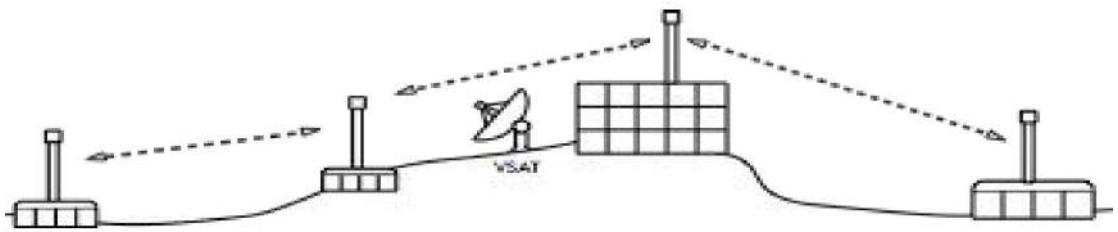


Figure 3- Multipoint-to-multipoint network

Wireless Networks

1st course lecture 3

- **Lecture outlines**
- **CHARACTERISTIC OF WLAN**
- **Basic transmission technologies used for WLANs**

Lecturer: Dr. Asia Ali

➢ CHARACTERISTIC OF WLAN

1. Advantages of WLANs

Flexibility: Within radio coverage, nodes can communicate without further restriction means within the reception area. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc).

Planning: Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans. As long as devices follow the same standard, they can communicate.

Design: Wireless networks allow for the design of small, independent devices which can for example be put into a pocket. Cables not only restrict users but also designers of small PDAs, notepads etc. Wireless senders and receivers can be hidden in historic buildings, i.e., current networking technology can be introduced without being visible.

Robustness: Wireless networks can survive disasters, e.g., earthquakes or users pulling a plug. If the wireless devices survive, people can still communicate. Networks requiring a wired infrastructure will usually break down completely.

Cost: After providing wireless access to the infrastructure via an access point for the first user, adding additional users to a wireless network will not increase the cost. This is, important for e.g., lecture halls, hotel lobbies or gate areas in airports where the numbers using the network may vary significantly.

2. WLANs also have several disadvantages:

● **Quality of service:** The main reasons for WLAN lower quality than their wired counterparts:

-The lower bandwidth due to limitations in radio transmission (e.g., only 1–10 Mbit/s user data rate instead of 100–1,000 Mbit/s),

- Higher error rates due to interference (e.g., 10 ^–4 instead of 10 ^–12 for fiber optics)

-Higher delay/delay variation due to extensive error correction and detection mechanisms.

● **Proprietary solutions:** Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardized functionality plus many enhanced features (typically a higher bit rate using a patented coding technology or special inter-access point protocols). However, these additional features only work in a homogeneous environment, i.e., when adapters from the same vendors are used for all wireless nodes. At least most components today adhere to the basic standards IEEE 802.11b or (newer) 802.11a.

● **Restrictions:** All wireless products have to comply with national regulations. WLANs are limited to low-power senders and certain license-free frequency bands, which are not the same worldwide.

● **Safety and security:** Using radio waves for data transmission might interfere with other high-tech equipment in, e.g., hospitals. Senders and receivers are operated by laymen and, radiation has to be low. All standards must offer (automatic) encryption, privacy mechanisms, support for anonymity etc.

➢ WLAN technologies

➢ Basic transmission technologies used for WLANs

Three different basic transmission technologies

1. Infrared light (e.g., at 900 nm wavelength).
2. UHF narrowband (radio transmission in the GHz range (e.g., 2.4 GHz in the license-free ISM band)
3. Spread spectrum.

Both (1, 2) technologies can be used to set up ad-hoc connections for work groups, to connect, e.g., a desktop with a printer without a wire, or to support mobility within a small area.

Infrared LAN

In this section, we begin with a comparison of the characteristics of infrared LANs with those of radio LANs and then look at some of the details of infrared LANs. An individual cell of an IR LAN is limited to a single room, because infrared light does not penetrate opaque walls.

Infrared offers a number of significant advantages over the Spread spectrum and UHF narrowband **radio approaches.**

First: the spectrum for infrared is virtually unlimited, which presents the possibility of achieving extremely high data rates.

Second: The infrared spectrum is unregulated worldwide, which is not true of some portions of the microwave spectrum.

Third: infrared shares some properties of visible light that make it attractive

MORE ADVANTAGES:

Four:

infrared communications can be more easily secured against eavesdropping than other spectrums;

Five:

a separate infrared installation can be operated in every room in a building without interference, enabling the construction of very large infrared LANs.

Six:

Infrared light is reflected by light-colored objects; thus it is possible to use ceiling reflection to achieve coverage of an entire room. Infrared is that the equipment is relatively inexpensive and simple.

The main disadvantages are **the shielding problems of infrared**. WLANs should, e.g., cover a whole floor of a building and not just the one room where LOSs exist. Future mobile devices may have to communicate while still in a pocket or a suitcase so cannot rely on infrared.

2.Narrowband microwave: These LANs operate at microwave frequencies but do not use spread spectrum. Some of these products operate at frequencies that require FCC licensing, while others use one of the unlicensed ISM bands. all narrowband microwave LAN products have used a licensed microwave band. More recently, at least one vendor has produced a LAN product in the ISM band.

3.Spread Spectrum LANS

The most popular type of wireless LAN uses spread spectrum techniques. In most cases, this is done by spreading the signal over a range of frequencies, that consist of the industrial, scientific, and medical (ISM) bands of the electromagnetic spectrum. The ISM bands these LANs operate in the ISM (Industrial, Scientific, and Medical) bands so that no FCC licensing is required for their use in the United States.

- **Advantages of radio transmission**

- Radio transmission can cover larger areas and can penetrate (thinner) walls, furniture, plants etc.
- Additional coverage is gained by reflection. Radio typically does not need a LOS(Line of Sight) if the frequencies are not too high.
- Furthermore, current radio-based products offer much higher transmission rates (e.g., 54 Mbit/s) than infrared (directed laser links, which offer data rates well above 100 Mbit/s. These are not considered here as it is very difficult to use them with mobile devices).

➢ Disadvantage Of Radio Transmission.

- Shielding is not so simple.
- Radio transmission can interfere with other senders, or electrical devices can destroy data transmitted via radio.
- radio transmission is only permitted in certain frequency bands.
- Very limited ranges of license-free bands are available worldwide.

Design goals for wireless LANs

- global, seamless operation
- low power for battery use
- no special permissions or licenses needed to use the LAN
- robust transmission technology
- simplified spontaneous cooperation at meetings
- easy to use for everyone, simple management
- protection of investment in wired networks
- security (no one should be able to read my data), privacy (no one should be able to collect user profiles), safety (low radiation)
- transparency concerning applications and higher layer protocols, but also location awareness if necessary

Note:

WLAN (IEEE 802.11) standardized infrared transmission in addition to radio transmission.

The other two (HIPERLAN and Bluetooth) rely on radio.

Table -1- shows different IEEE 802.11 standards

IEEE 802.11 b	IEEE 802.11 a	IEEE 802.11g
Appears in 1999	Introduced in 2001	Introduced in 2003
2.4Ghz radio spectrum	5.0 Ghz radio spectrum	combine the feature of both standards (a,b)
11 Mbps) actual speed)	15-20 Mbps (Actual speed)	54Mbps speed
100-150 feet range	50-75 feeet range	100-150 feet range
Most popular and less expensive	More expesive	
Interference from mobile phones and Bluetooth devices which can reduces the transmission speed	Not compatible with IEEE 802.11b	Compatible with b

802.11 –Classical architecture of an infrastructure network

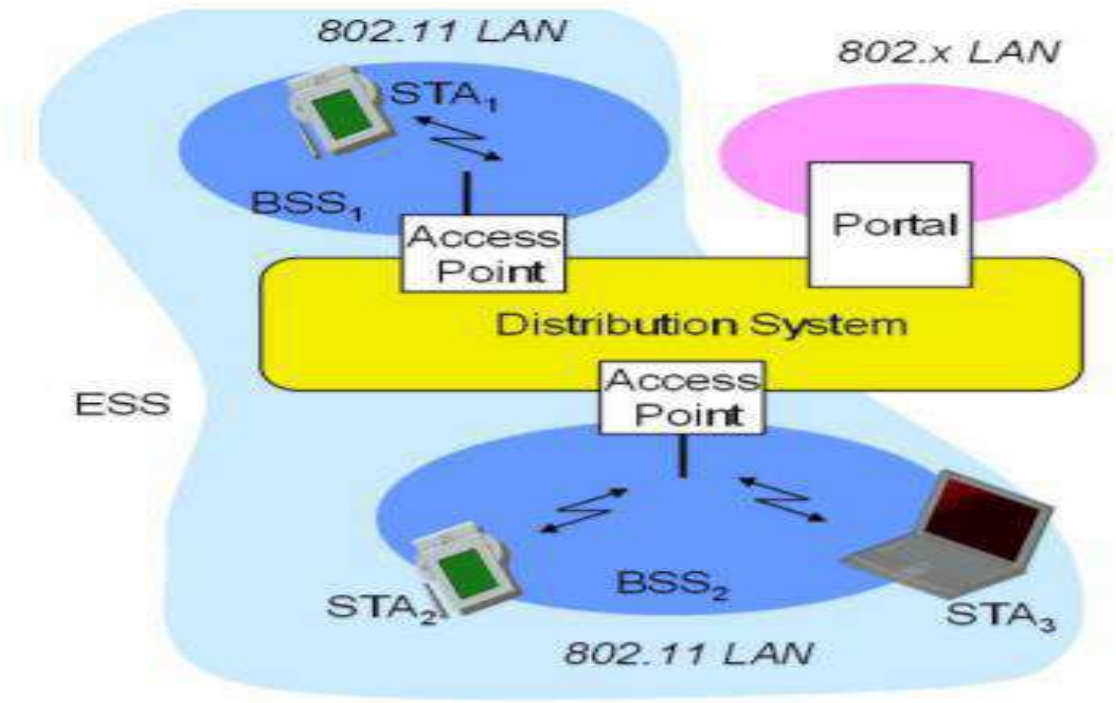


Figure 2-Architecture of an infrastructure-based IEEE 802.11

Station (STA)

Terminal with access mechanisms to the wireless medium and radio contact to the access point.

Basic Service Set (BSS)

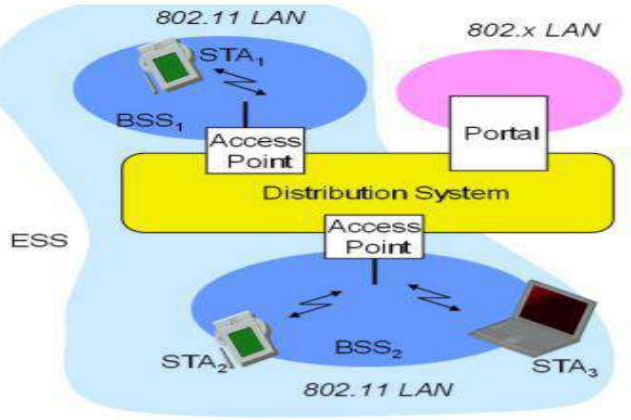
Group of stations using the same radio frequency. When all of the stations in the BSS are mobile stations and there is no connection to a wired network, the BSS is called independent BSS (IBSS). IBSS is typically short-lived network, with a small number of stations, which is created for a particular purpose. When a BSS includes an access point (AP), the BSS is called infrastructure BSS. When there is a AP, If one mobile station in the BSS must communicate with another mobile station, the communication is sent first to the AP and then from the AP to the other mobile station. This consume twice the bandwidth that the same communication. While this appears to be a significant cost, the benefits provided by the AP far outweigh this cost.

Access Point

Station integrated into the wireless LAN and the distribution system.

Portal

Bridge to other (wired) networks

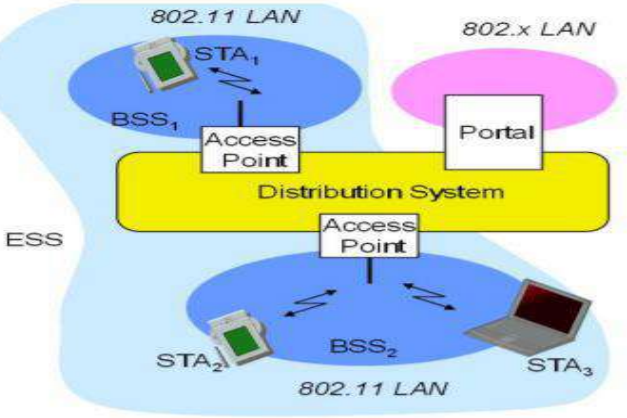


Distribution System

Interconnection network to form one logical network (EES: Extended Service Set) based on several BSS. The distribution system (DS) is the mechanism by which one AP communicates with another to exchange frames for stations in their BSSs.

Infrastructure wireless LAN is a term often referred to wireless LANs that deploy AP, with the infrastructure being the APs along with wired Ethernet infrastructure that connects APs and router, hub or switch.

Extended Service Set (ESS) A ESS is a set of infrastructure BSSs, where the APs communicate among themselves to forward traffic from one BSS to another and to facilitate the movement of mobile stations from one BSS to another. The APs perform this communication via an abstract medium called the distribution system (DS). To network equipment outside of the ESS, the ESS and all of its mobile stations appears 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.



➢ System architecture (WLAN)

Comparison: infrastructure vs. ad-hoc vs. mesh networks

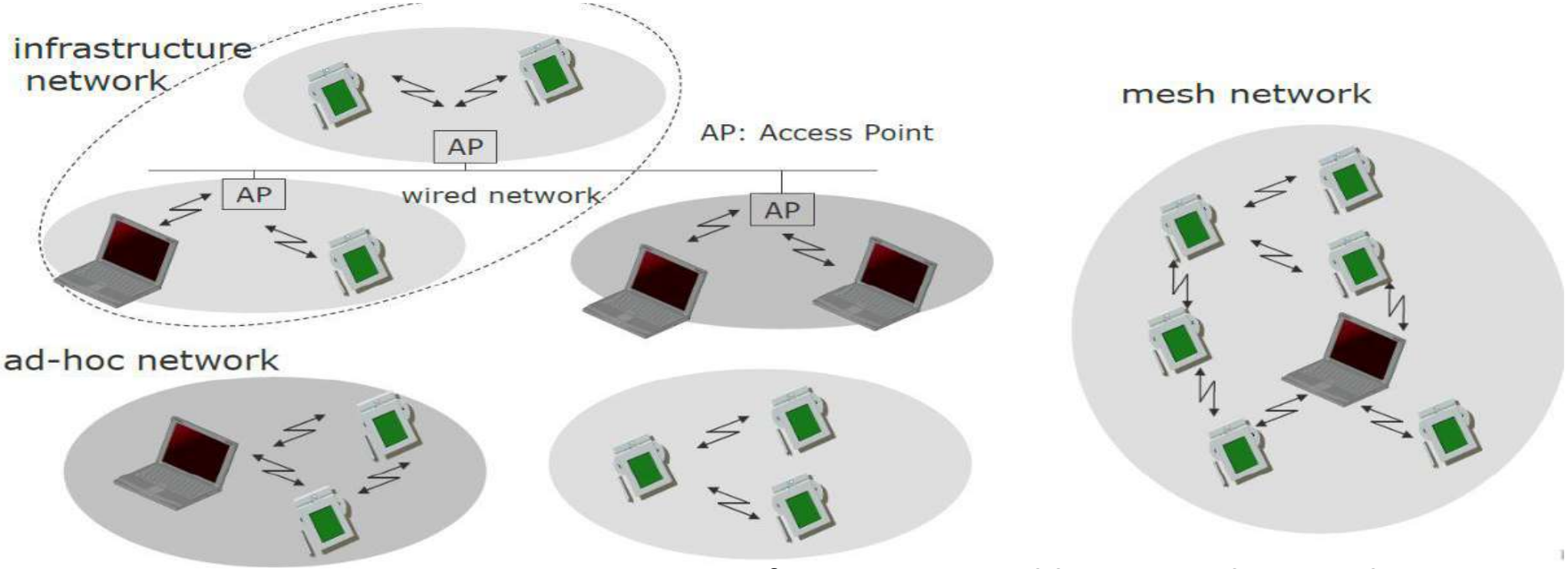


Figure 1- **: infrastructure vs. ad-hoc vs. mesh networks**

ad hoc network it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks.

Mesh network: It is built of peer radio devices that do not have to be cabled to a wired port like traditional WLAN access points (AP) do.

➢ 802.11 -Architecture of an ad-hoc network

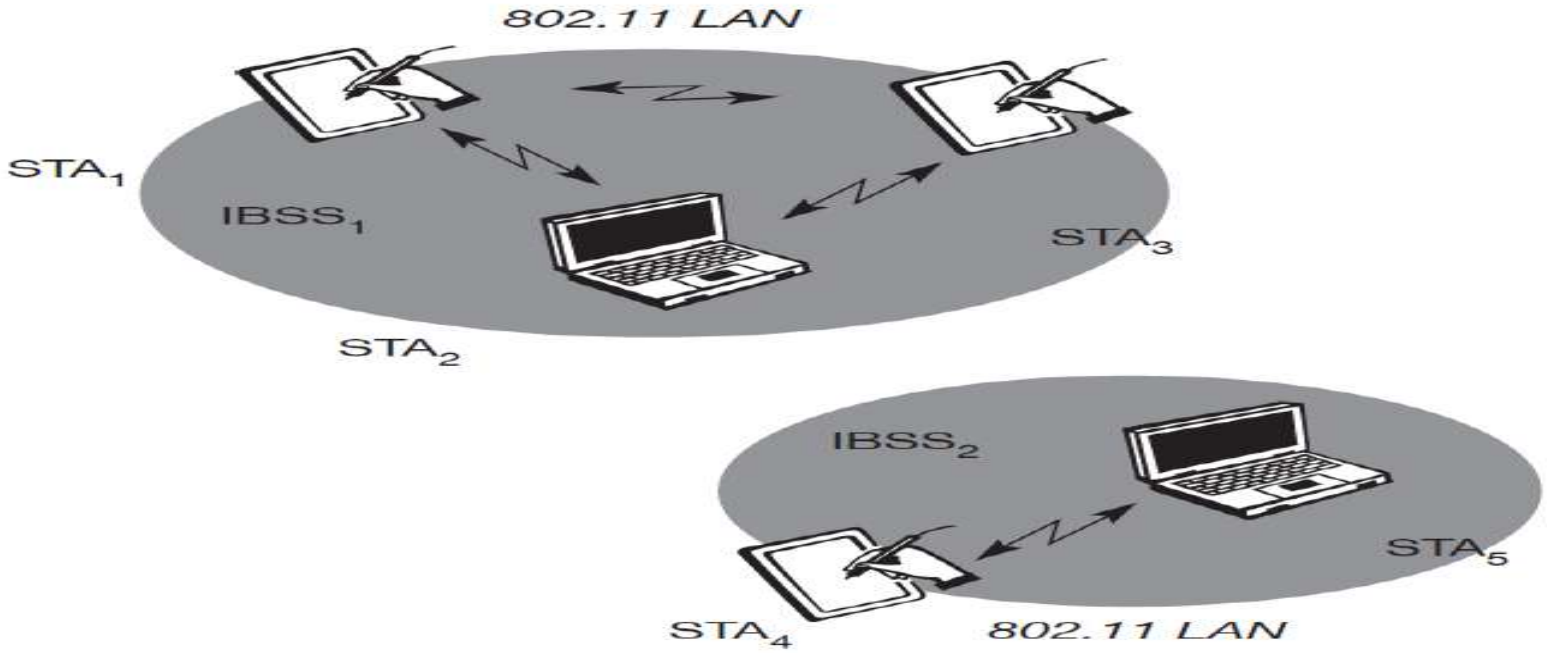


Figure 3- Direct communication within a limited range

Station (STA): terminal with access mechanisms to the wireless medium.

Independent Basic Service Set (IBSS): group of stations using the same radio frequency.

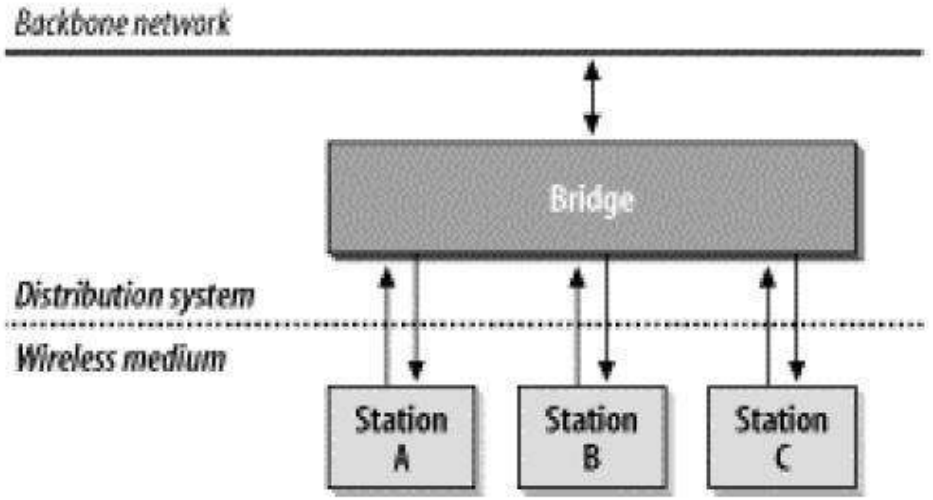


Figure 4--Distribution system in common 802.11 access point implementations

Every frame sent by a mobile station in an infrastructure network must use the distribution system. It is easy to understand why interaction with hosts on the backbone network must use the distribution system. After all, they are connected to the distribution system medium. Wireless stations in an infrastructure network depend on the distribution system to communicate with each other because they are not directly connected to each other. The only way for station A to send a frame to station B is by relaying the frame through the bridging engine in the access point. However, the bridge is a component of the distribution system.

Wireless Networks

1st course lecture 4

Lecture outlines

- **Protocol architecture**
- **The physical layer**

Lecturer: Dr. Asia Ali

2. Protocol architecture

IEEE 802.11 can fit into the other 802.x standards for wired LANs. Figure 1 shows the most available scenario: an IEEE 802.11 wireless LAN connected to a switched IEEE 802.3 Ethernet via a bridge.

- Applications should not notice any difference apart from the lower bandwidth and perhaps higher access time from the wireless LAN.
- The WLAN behaves like a slow-wired LAN. Consequently, the higher layers (application, TCP, IP) look the same for wireless nodes as for wired nodes.
- The upper part of the data link control layer, the logical link control (LLC), covers the differences of the medium access control layers needed for the different media.

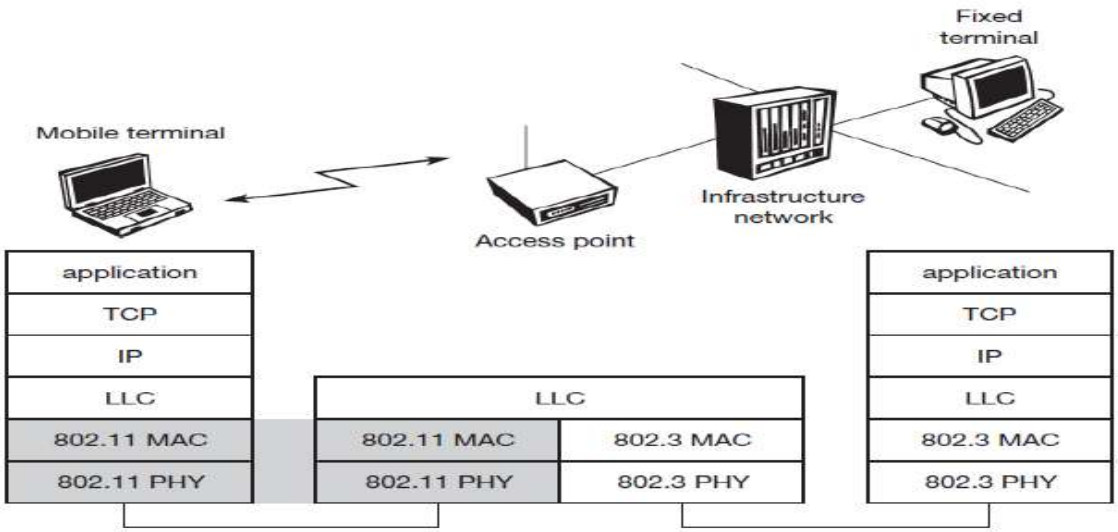


Figure 1- IEEE 802.11 protocol architecture and bridging

Figure 2- shows the WLAN layers a general view.

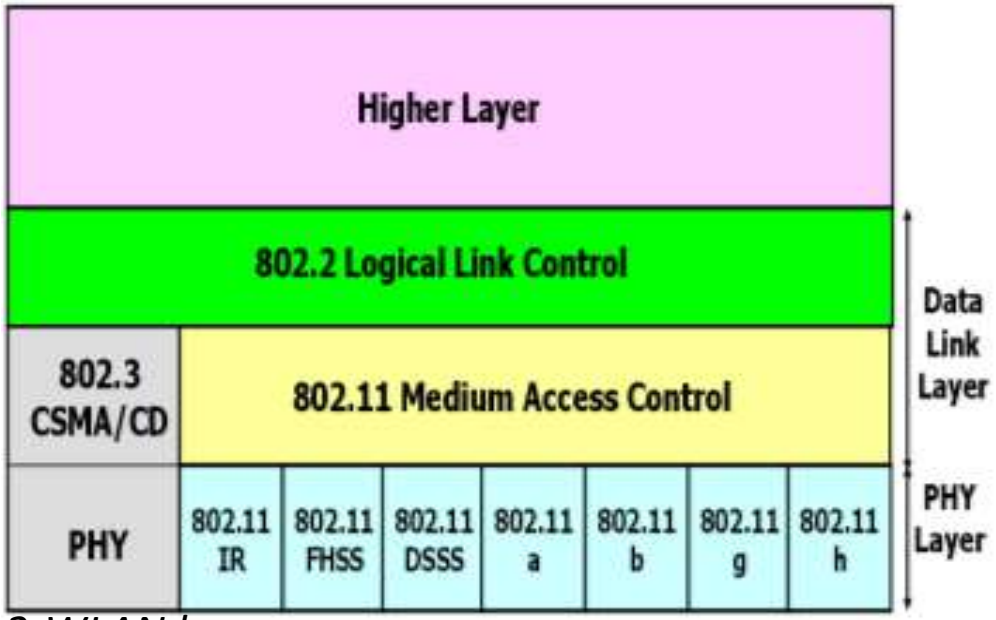


Figure 2-WLAN layers

The IEEE 802.11 standard only covers the physical layer PHY and medium access layer MAC like the other 802.x LANs do.

The physical layer is subdivided into

- The physical layer convergence protocol (PLCP)
- The physical medium dependent sublayer PMD (see Figure 3).

The Media access control MAC

- access mechanisms, fragmentation, and encryption
- MAC Management
- Synchronization, roaming, Management Information Base(MIB), power management.

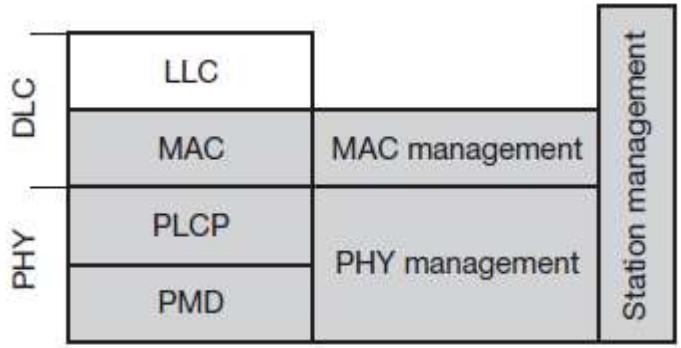


Figure 3-Detailed IEEE 802.11 protocol architecture and management

Physical Layer Convergence Protocol(**PLCP)**

- provides a carrier sense signal, called clear channel assessment (CCA).
- provides a common PHY service access point(SAP)

The Physical Dependent Sublayer (**PMD**) sublayer handles : modulation and encoding/decoding of signals.

PHY management include channel selection and PHY MIB maintenance.

Station management coordination of all management functions.

1. PHYSICAL LAYER

Historically, IEEE 802.11 supports three different physical layers**: 2 radio (type ISM band at 2.4 GHz), 1 IR.** The PHY layer offers a service access point (SAP) with 1 or 2 Mbit/s transfer Data rate to the MAC layer.

1.1- The Frequency Hopping Spread Spectrum (FHSS)

FHSS is a spread spectrum technique, which allows for the coexistence of multiple networks in the same area by separating different networks using different hopping sequences. two-level (Gaussian shaped frequency shift keying) GFSK modulation. 1 Mbit/s data rate.

The fields of the frame fulfill the following functions:

- **Synchronization:** The PLCP preamble starts with 80 bit synchronization, which is a 010101... bit pattern. This pattern is used for synchronization of potential receivers and signal detection by the clear channel assessment(CCA).

- **Start frame delimiter (SFD):** The following 16 bits indicate the start of the frame and provide frame synchronization. The SFD pattern is 0000110010111101.

- **PLCP_PDU length word (PLW):** This first field of the PLCP header indicates the length of the payload in bytes including the 32 bit CRC at the end of the payload. PLW can range between 0 and 4,095.

● **PLCP signaling field (PSF):** This 4 bit field indicates the data rate of the payload following. All bits set to zero (0000) indicates the lowest data rate of 1 Mbit/s. The granularity is 500 Kbit/s, thus 2 Mbit/s is indicated by 0010 and the maximum is 8.5 Mbit/s (1111).

● **Header error check (HEC)**: Finally, the PLCP header is protected by a 16 bit checksum.

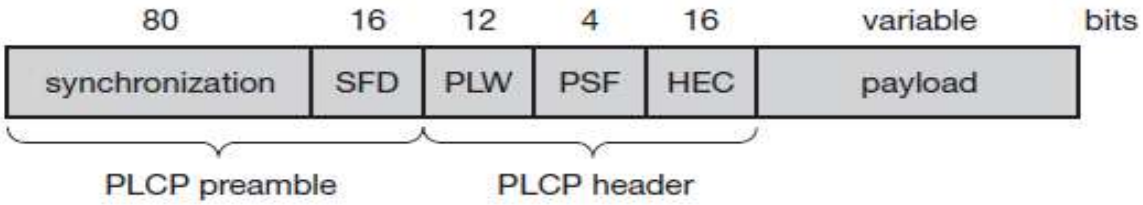


Figure 4- Format of an IEEE 802.11 PHY frame using FHSS

1.2-Direct Sequence Spread Spectrum (DSSS)

DSSS is the alternative spread spectrum method separating by code and not by frequency.

- In the case of IEEE 802.11 DSSS, spreading is achieved using the 11-chip Barker sequence (+1, –1, +1, +1, –1, +1, +1, +1, –1, –1, –1).

The key characteristics of this method are its robustness against interference and its insensitivity to multipath propagation (time delay spread). However, the implementation is more complex compared to FHSS.

- IEEE 802.11 DSSS PHY also uses the 2.4 GHz ISM band and offers both 1 and 2 Mbit/s data rates.

- The system uses differential binary phase shift keying (DBPSK) for 1 Mbit/s transmission and differential quadrature phase shift keying (DQPSK) for 2 Mbit/s as modulation schemes.

Figure 5- shows the fields of the frame which have the following functions:

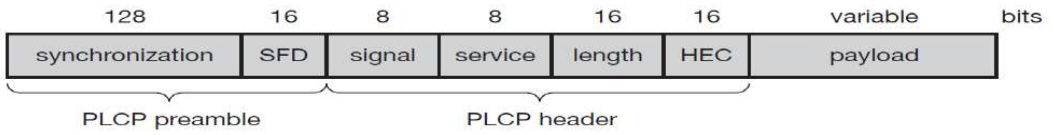


Figure 5- Format of an IEEE 802.11 PHY frame using DSSS

- Synchronization: The first 128 bits are not only used for synchronization, but also gain setting, energy detection (for the CCA), and frequency offset compensation. The synchronization field only consists of scrambled 1 bits.

- Start frame delimiter (SFD): This 16 bit field is used for synchronization at the beginning of a frame and consists of the pattern 1111001110100000.

- Signal: Originally, only two values have been defined for this field to indicate the data rate of the payload. The value 0x0A indicates 1 Mbit/s (and thus DBPSK), 0x14 indicates 2 Mbit/s (and thus DQPSK).

- Service: This field is reserved for future use; however, 0x00 indicates an IEEE 802.11 compliant frame.

- Length: 16 bits are used in this case for length indication of the payload in microseconds.

- Header error check (HEC): Signal, service, and length fields are protected by this checksum using the ITU-T CRC-16 standard polynomial.

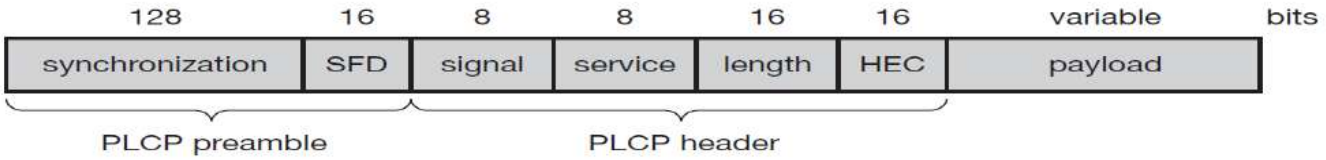


Figure 5- Format of an IEEE 802.11 PHY frame using DSSS

1.3- IR PHY Layer

The IR PHY is one of the three PHY layers supported in the standard. The IR PHY differs from DSSS and FHSS because IR uses near visible light as the transmission media.

- IR communication relies on light energy, which is reflected off objects or by line-of-sight.
- The IR PHY operation is restricted to indoor environments and cannot pass through walls, such as DSSS and FHSS radio signals.
- The maximum range is about 10 m if no sunlight or heat sources interfere with the transmission

- Data transmission over the media is controlled by the IR PMD sublayer as directed by the IR PLCP sublayer.

-The PLCP preamble and PLCP header are always transmitted at 1Mbps and the PSDU can be sent at 1 Mbps or 2 Mbps.

- carrier detection, energy detection, synchronization.

Typically, such a network will only work in buildings, e.g., classrooms, meeting rooms etc.

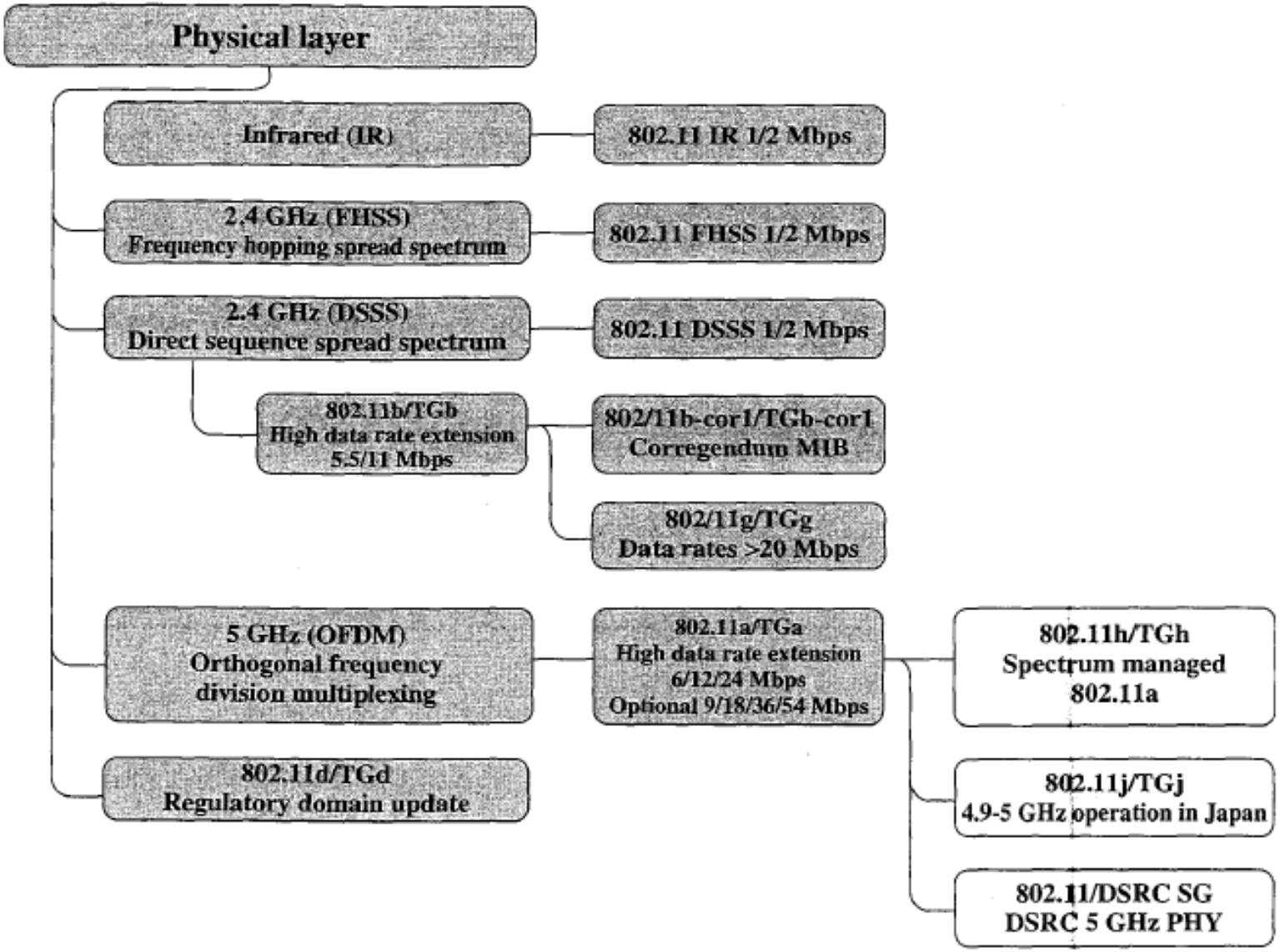


Figure 6-IEEE 802.11 Activities-Physical Layer

Wireless Networks

1st course lecture 5

Lecture outlines

- **The MAC layer**

Lecturer: Dr. Asia Ali

2. IEEE 802.11 MEDIUM ACCESS CONTROL

The IEEE 802.11 MAC layer covers three functional areas:

- Reliable data delivery.
- Medium access control.
- Security.

2.1 Mac Layer

The basic services provided by the MAC layer are (*Traffic services)*

1. Asynchronous Data Service (mandatory), support of broadcast and multicast, exchange of data packets based on “best-effort” i.e., no delay can be given for transmission.
2. Time- bounded services.

Unicast =one to one
Multicast=one to many
Broadcast= one to all

The following are three basic access methods

The mandatory basic method based on

- (1) A version of CSMA/CA, (2) an optional method avoiding the hidden terminal problem.
- (3) Contention-free polling method for time-bounded service.

The first two methods are also summarized as **distributed coordination function (DCF)**

The third method is called **point coordination function (PCF**).

DCF only offers asynchronous service, while PCF offers both asynchronous and time-bounded service but needs an access point to control medium access and to avoid contention.

The MAC mechanisms are also called **Distributed Foundation Wireless Medium Access Control (DFWMAC)**.

Example CSMA/CD

Carrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection, send when medium is free, listen to medium if collision occurs (IEEE802.3)

Problems in wireless networks

signal strength decreases with distance

sender applies CS and CD, but collisions happen at receiver sender may not “hear” collision, i.e., CD does not work

Hidden terminal: CS might not work

Several parameters for controlling the waiting time before medium access are important. The values of the parameters depend on the PHY and are defined in relation to a slot time. Slot time is derived from the medium propagation delay, transmitter delay, and other PHY dependent parameters. Slot time is 50 µs for FHSS and 20 µs for DSSS. The medium, can be busy or idle (which is detected by the CCA). If the medium is busy this can be due to data frames or other control frames, see figure 1.

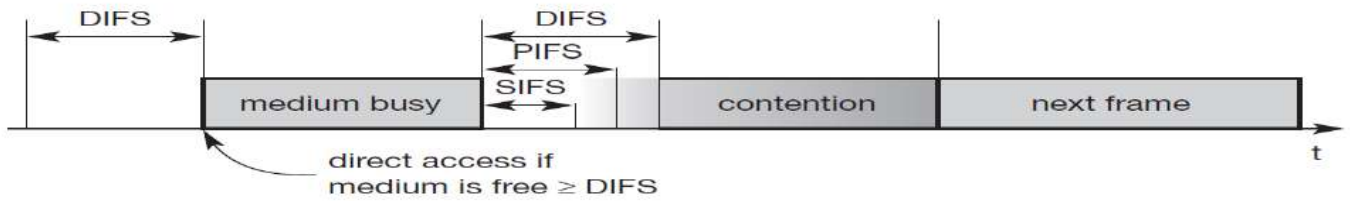


Figure 1-Medium access and inter-frame spacing

Short inter-frame spacing (SIFS): The shortest waiting time for medium access (so the highest priority) is defined for short control messages, such as acknowledgements of data packets or polling responses. For DSSS SIFS is 10 μs and for FHSS it is 28 μs.

PCF inter-frame spacing (PIFS): A waiting time between DIFS and SIFS (and thus a medium priority) is used for a time-bounded service. An access point polling other nodes only has to wait PIFS for medium access. PIFS is defined as SIFS plus one slote time.

DCF inter-frame spacing (DIFS): This parameter denotes the longest waiting time and has the lowest priority for medium access. This waiting time is used for asynchronous data service within a contention period. DIFS is defined as SIFS plus two slote times.

For all the access methods(DCF & PCF) mentioned above Figure 1 shows the three different parameters that define the priorities of medium access.

Basic DFWMAC-DCF using CSMA/CA-access method I

The mandatory access mechanism of IEEE 802.11 is based on **carrier sense multiple access with collision avoidance** (CSMA/CA), which is a random-access scheme with carrier sense and collision avoidance through random backoff.

The basic CSMA/CA mechanism is shown in Figure 2. If the medium is idle for at least the duration of DIFS (with the help of the CCA signal of the physical layer), a node can access the medium at once. This allows for short access delay under light load. But as more and more nodes try to access the medium, additional mechanisms are needed, see figure 3

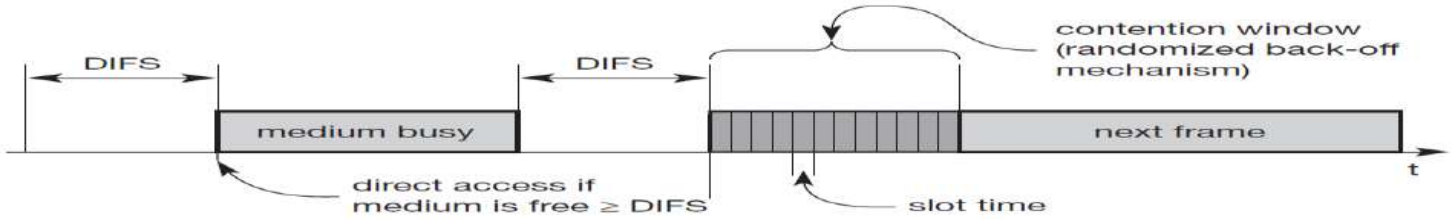


Figure 2-Contention window and waiting time

- If the medium is busy, nodes have to wait for the duration of DIFS, entering a contention phase afterwards.
- Each node now chooses a **random backoff time** within a **contention window** and delays medium access for this random amount of time.
- The node continues to sense the medium.
- As soon as a node senses the channel is busy, it has lost this cycle and has to wait for the next chance, i.e., until the medium is idle again for at least DIFS.

- But if the randomized additional waiting time for a node is over and the medium is still idle, the node can access the medium immediately (i.e., no other node has a shorter waiting time). The additional waiting time is measured in multiples of the above-mentioned slots. This additional randomly distributed delay helps to avoid collisions – otherwise all stations would try to transmit data after waiting for the medium becoming idle again plus DIFS.

To provide fairness, IEEE 802.11 adds a **back off timer. E**ach node selects a random waiting time within the range of the contention window.

If a certain station does not get access to the medium in the first cycle, it stops its back-off timer, waits for the channel to be idle again for DIFS and starts the counter again.

As soon as the counter expires, the node accesses the medium. This means that deferred stations do not choose a randomized back-off time again, but continue to count down. Stations that have waited longer have the advantage over stations that have just entered, in that they only have to wait for the remainder of their back-off timer from the previous cycle(s).

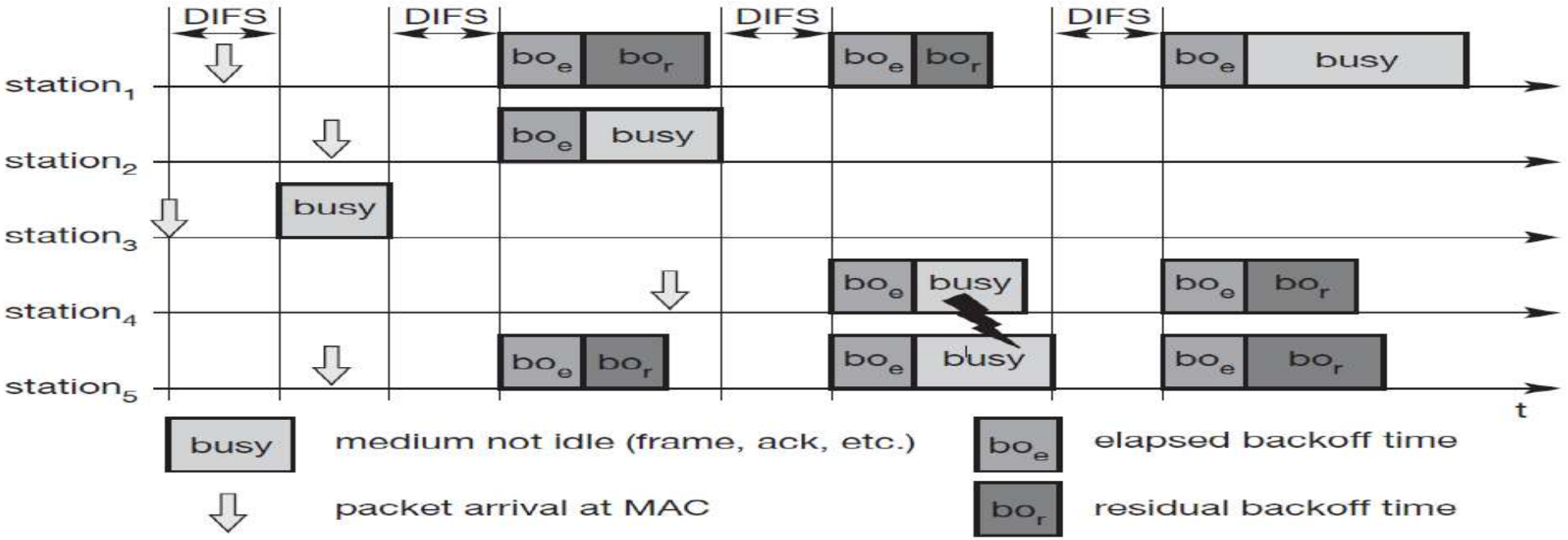


Figure 3-Basic DFWMAC–DCF with several competing senders

802.11 -CSMA/CA access method II

Sending unicast packets

- station has to wait for DIFS before sending data

- receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly.

- automatic retransmission of data packets in case of transmission errors, but exponential increase of contention window.

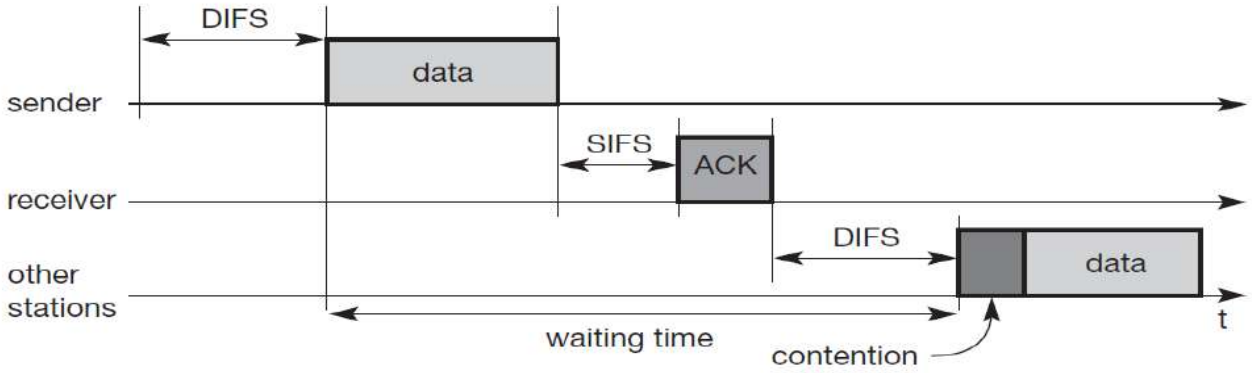


Figure 4-IEEE 802.11 unicast data transfer

11.–MAC Frame format

Types

- control frames, management frames, data frames.

Sequence numbers

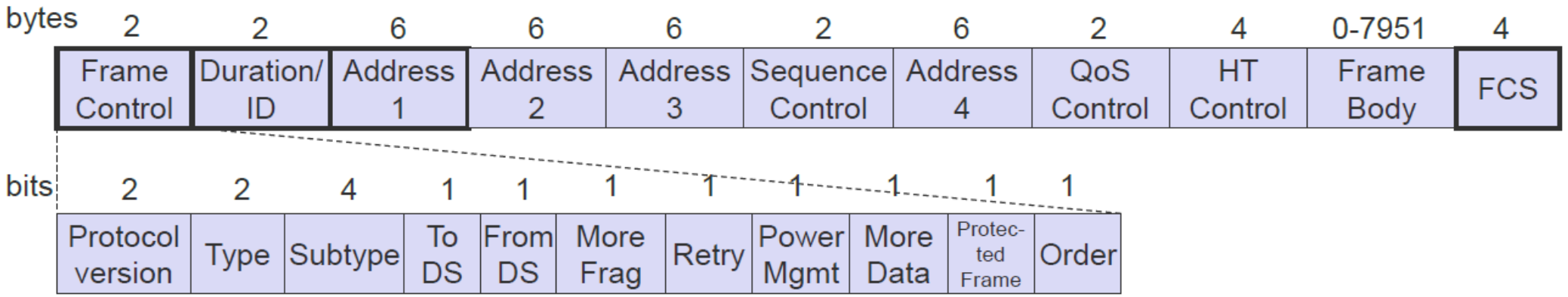
- Important against duplicated frames due to lost ACKs

Addresses

- receiver, transmitter (physical), BSS identifier, sender (logical)

Miscellaneous

- sending time, checksum, frame control, data



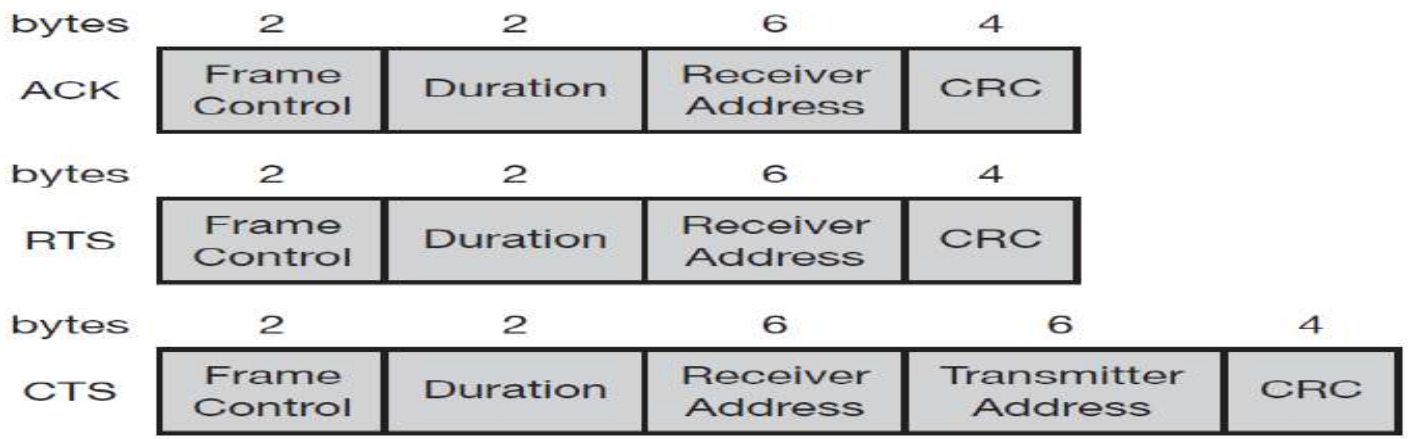
•Only the first three and the last field are present in all frames. 802.11ac allows for a variable frame body.

MAC address format (examples)

TA: Transmitter Address
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier

Example scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	RA=DA	TA=SA	BSSID	-
infrastructure network, from AP	0	1	RA=DA	TA=BSSID	SA	-
infrastructure network, to AP	1	0	RA=BSSID	TA=SA	DA	-
within mesh BSS	1	1	RA	TA	DA	SA

Special Frames: Acknowledgement (ACK), Request to send (RTS), Clear to send (CTS)



802.11 -MAC management

● **Synchronization:** Functions to support finding a wireless LAN, synchronization of internal clocks, generation of beacon signals.
- **Power management:** Functions to control transmitter activity for power conservation, e.g., periodic sleep, buffering, without missing a frame.
- **Roaming:** Functions for joining a network (association), changing access points, scanning for access points.

-Management information base (MIB): All parameters representing the current state of a wireless station and an access point are stored within a MIB for internal and external access.

Wireless Networks

1st course lecture 6

Lecture outlines

- **Bluetooth**

Lecturer: Asia Ali

BLUETOOTH

Compared to the WLAN technologies presented in our lectures, the Bluetooth technology discussed here aims at so-called **ad-hoc piconets network**.

Basics:

- WLAN technology enables device connectivity to infrastructure-based services through a wireless carrier provider.
- Personal area network (PANs) has emerged as the need for personal devices to communicate wirelessly with one another, without an established infrastructure.
- Bluetooth employs radio frequency (RF) technology for communication. It makes use of frequency modulation to generate radio waves in the ISM band.
- Low power consumption of Bluetooth technology.
- Offered range of up to 10 meters. Video and data transmission 1 M/bit
- Many of today's devices offer an infra-red data association (IrDA) interface with transmission rates of, e.g., 115 kbit/s or 4 Mbit/s.

- There are various problems with IrDA: it’s very limited range (typically 2 m for built-in interfaces), the need for a line-of-sight between the interfaces, and, it is usually limited to two participants, i.e., only point-to-point connections are supported.

- The first attempt to define a standard for PANs dates back to Ericsson's Bluetooth project in 1994 to enable communication between mobile phones using low power and low-cost radio interfaces.
- Recently, IEEE has approved a Bluetooth-based standard (IEEE 802.15.1) for wireless personal area networks (WPANs).

- One can have an interactive conference by establishing an ad hoc network of laptops. Cordless computer, instant postcard [sending digital photographs instantly (a camera is cordlessly connected to a mobile phone)], and three-in-one phone [the same phone functions as an intercom (at the office, no telephone charge), cordless phone (at home, a fixed-line charge), and mobile phone (on the move, a cellular charge)] are other indicative usage models.

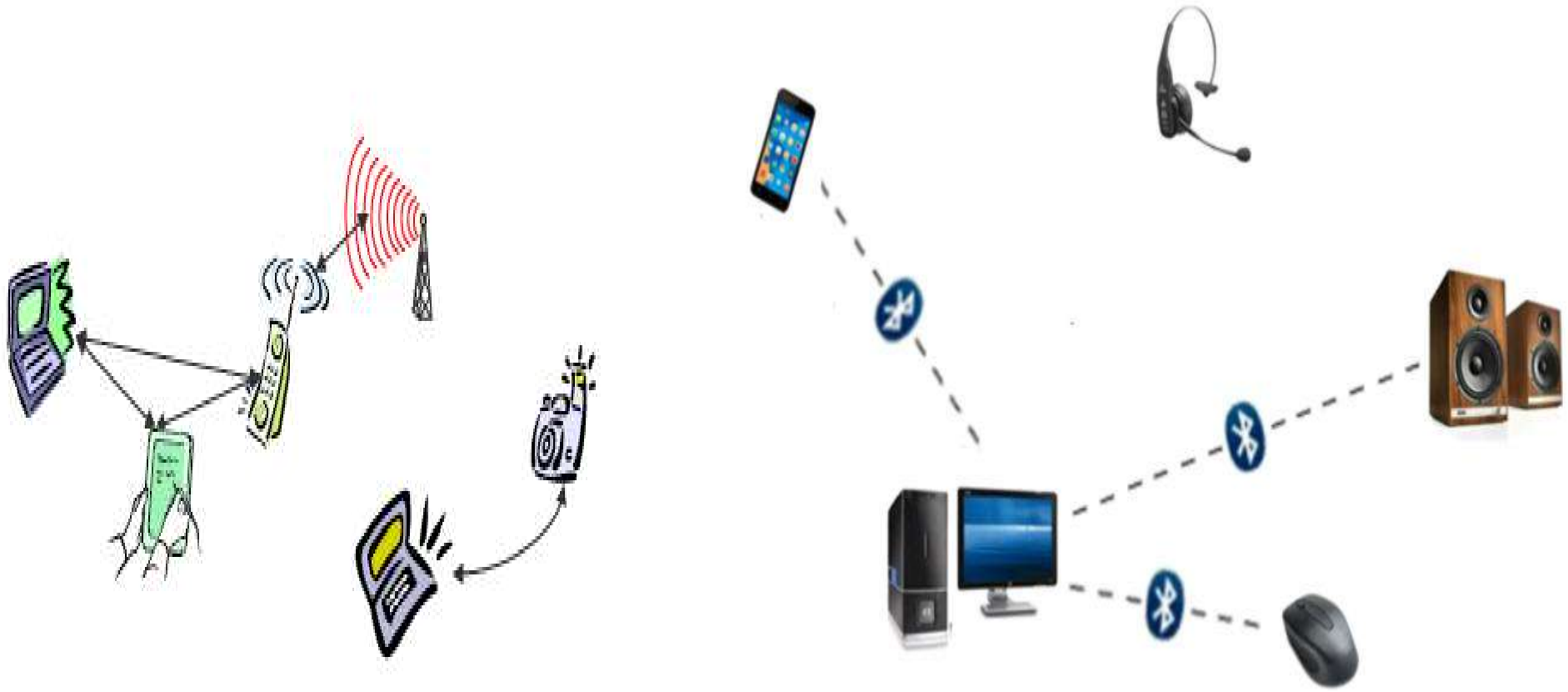


Figure 1- Bluetooth Technique

- The power of the device transmitter governs the range over which a Bluetooth device can operate.

Table -1- The classical Bluetooth systems			
Class Number		Maximum Range	Sample Devices
Class 1		100 m	USB Adapters, Access Points
Class 2		10 m	Mobile devices, Bluetooth
Class 3		1 m	Bluetooth adapters

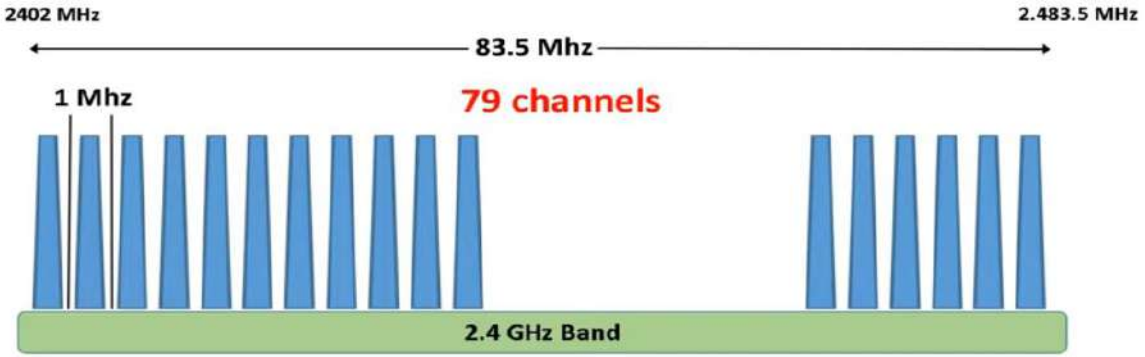
Architecture

Like **IEEE 802.11b**, Bluetooth operates in the 2.4 GHz ISM band. However, MAC, physical layer able to provide different services.

Characteristics of the classical system

2.4 GHz ISM band, 79 RF channels, 1 MHz carrier spacing per channel.

—Channel 0: 2402 MHz … ….channel 78: 2480 MHz



The transmitter hops in a pseudo random fashion determine by the master in the network. To hop from one channel to another using frequency hopping channel. And makes 1600 hops per second. Hopping sequence in a pseudo random fashion, determined by a master Time division duplex for send/receive separation.

Networking

Two types of Bluetooth Topology

The piconets and scatternet.

—*Note: Overlapping piconets (stars) forming a scatternet*

Piconet

- Collection of devices connected in an ad hoc fashion
- One-unit acts as master and the others as slaves for the lifetime of the piconet
- Master determines hopping pattern, slaves have to synchronize
- Each piconet has a unique hopping pattern
- Participation in a piconet= synchronization to hopping sequence
- Each piconet has one master and up to 7 simultaneous slaves (> 200 could be parked)

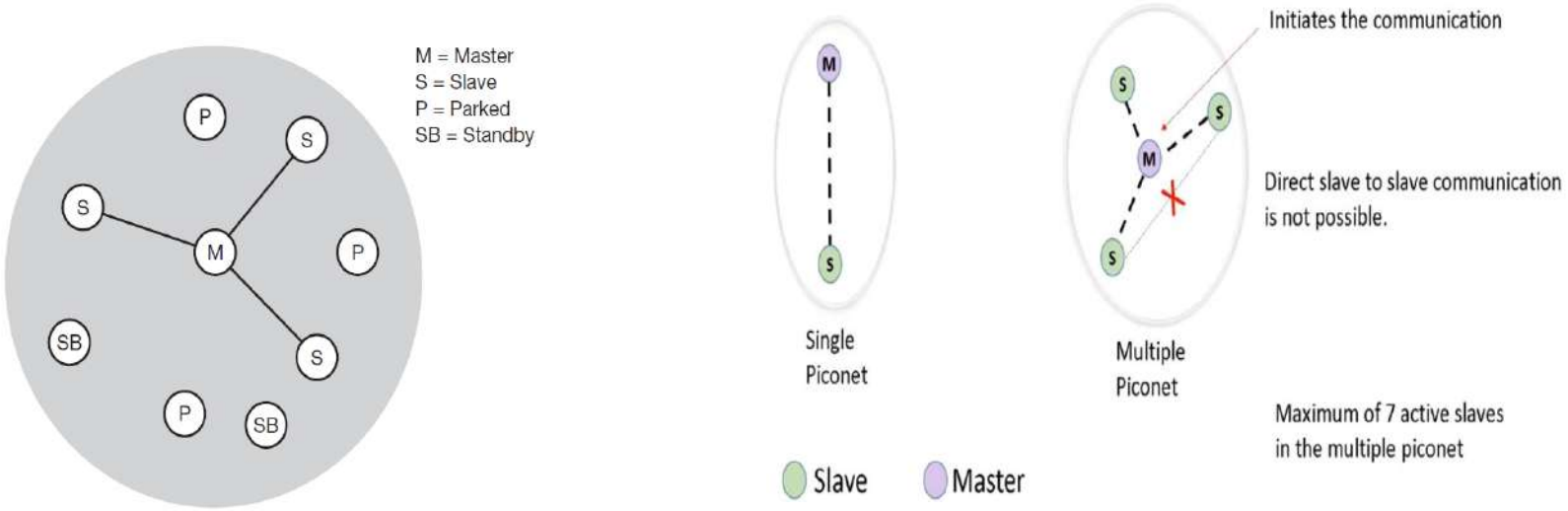


Figure 2- the left side Simple Bluetooth piconet. A- master with number of nodes not exceeding 7 nodes. The right side-A single piconet and multiple piconet

- parked devices (P) cannot actively participate in the piconet (i.e., they do not have a connection), but are known and can be reactivated within some milliseconds.

Devices in stand-by (SB) do not participate in the piconet. Each piconet has exactly one master and up to seven simultaneous slaves. More than 200 devices can be parked.

- The reason for the upper limit of eight active devices, is the 3-bit address used in Bluetooth. If a parked device wants to communicate and there are already seven active slaves, one slave has to switch to park mode to allow the parked device to switch to active mode.

The Formation of a Piconet

- All active devices have to use the same hopping sequence they must be synchronized.
- The first step involves ding its clock and device ID.
- All Bluetooth devices have the same networking capabilities, i.e., they can be master or slave.
- There is no distinction between terminals and base stations, any two or more devices can form a piconet.
- The unit establishing the piconet automatically becomes the master, all other devices will be slaves.
- The hopping pattern is determined by the device ID- a 48-bit worldwide unique identifier.
- The phase in the hopping pattern is determined by the master's clock. After adjusting the internal clock according to the master a device may participate in the piconet.
- All active devices are assigned a 3-bit **active member address** (AMA).
- All parked devices use an 8-bit **parked member address** (PMA).
- Devices in stand-by do not need an address. All users within one piconet have the same hopping sequence and share the same 1 MHz channel.
- As more users join the piconet, the throughput per user drops quickly (a single piconet offers less than 1 Mbit/s gross data rate).

See figure 3. (Only having one piconet available within the 80 MHz in total is not very efficient.) led to the idea of forming groups of piconets called scatternet.

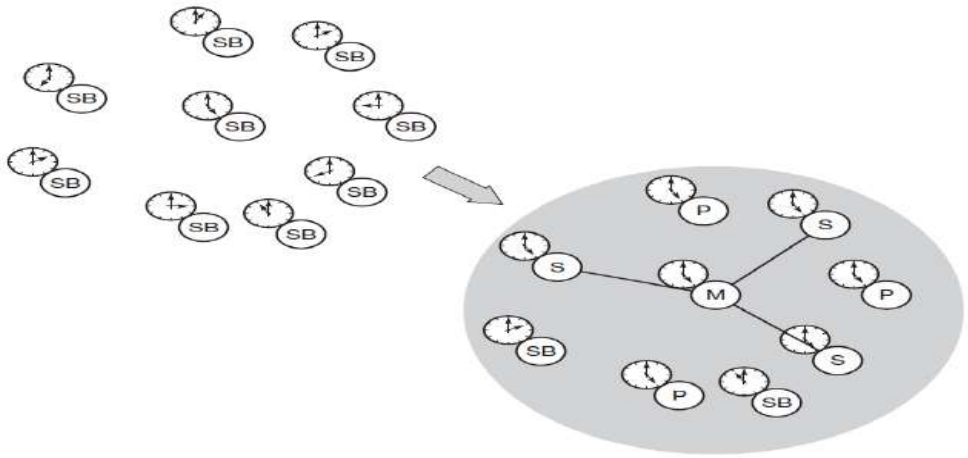


Figure 3- Forming a Bluetooth piconet

Scatternet

In the example, figure 4-A-, the scatternet consists of two piconets, in which one device participates in two different piconets.
Both piconets use a different hopping sequence, always determined by the master of the piconet.
It is clearly not possible for a master of one piconet to act as the master of another piconet as this would lead to identical behaviour (both would have the same hopping sequence, which is determined by the master per definition).
As soon as a master leaves a piconet, all traffic within this piconet is suspended until the master returns. Devices can be slave in one piconet and master of another.

Communication between different piconets takes place by devices jumping back and forth between theses nets. If this is done periodically, for instance, isochronous data streams can be forwarded from one piconet to another. However, scatternets are not yet supported by all devices.

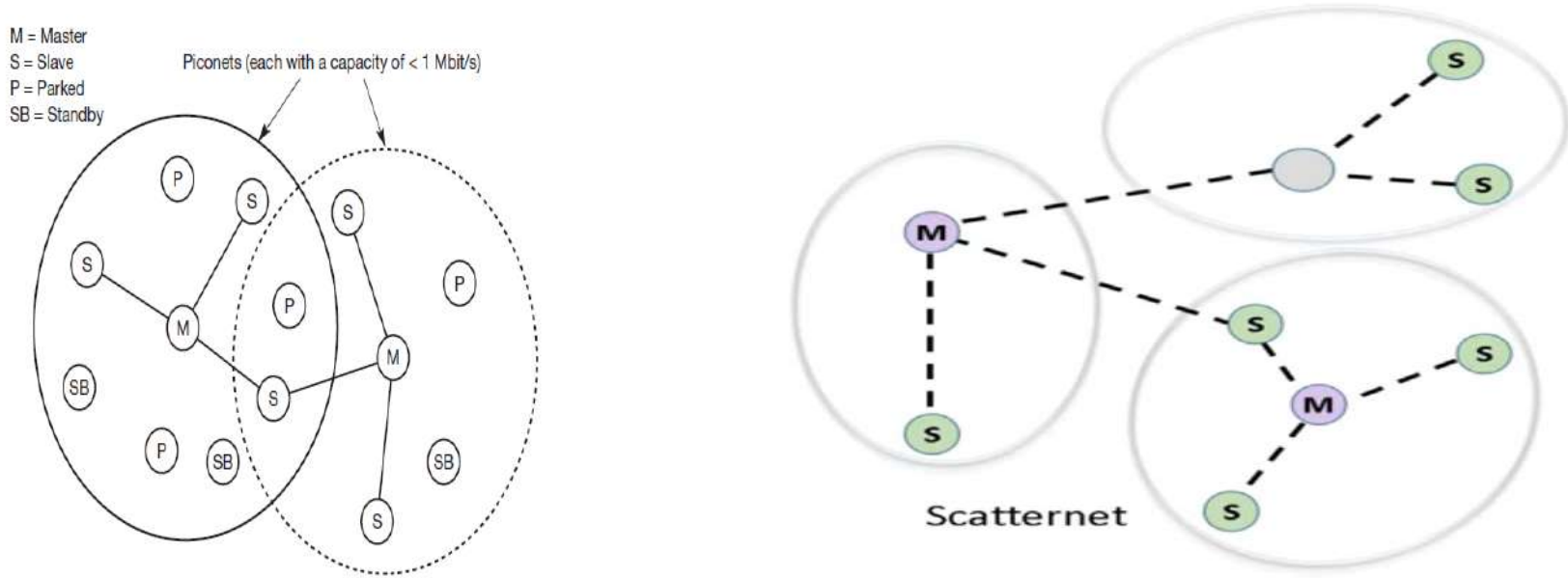


Figure 4- left side is a Scatternet-A-overlapped piconets to create a scatternet, the right side- the master in piconet can not be a master in another piconet.

Example:

In figure 5, we have a smart phone sending a file (packets of data) to a computer. Using the frequency technique. The first packet will be sent on a randomly selected channel in the figure channel 56 then channel 4 untill all the packets will send in the same fashion. 1600 hops/sec which means every 625 microsecond a packet will be sent on a different frequency. Every 625 microsecond the frequencies are changing to prevent the interference with other wireless networks which are using the ISM band.

Advantages

The Minimize eavesdropping

The frequencies will be changing every 625 microsecond which means no interference with other wireless network that are using the same ISM band such as cordless phone and wifi.

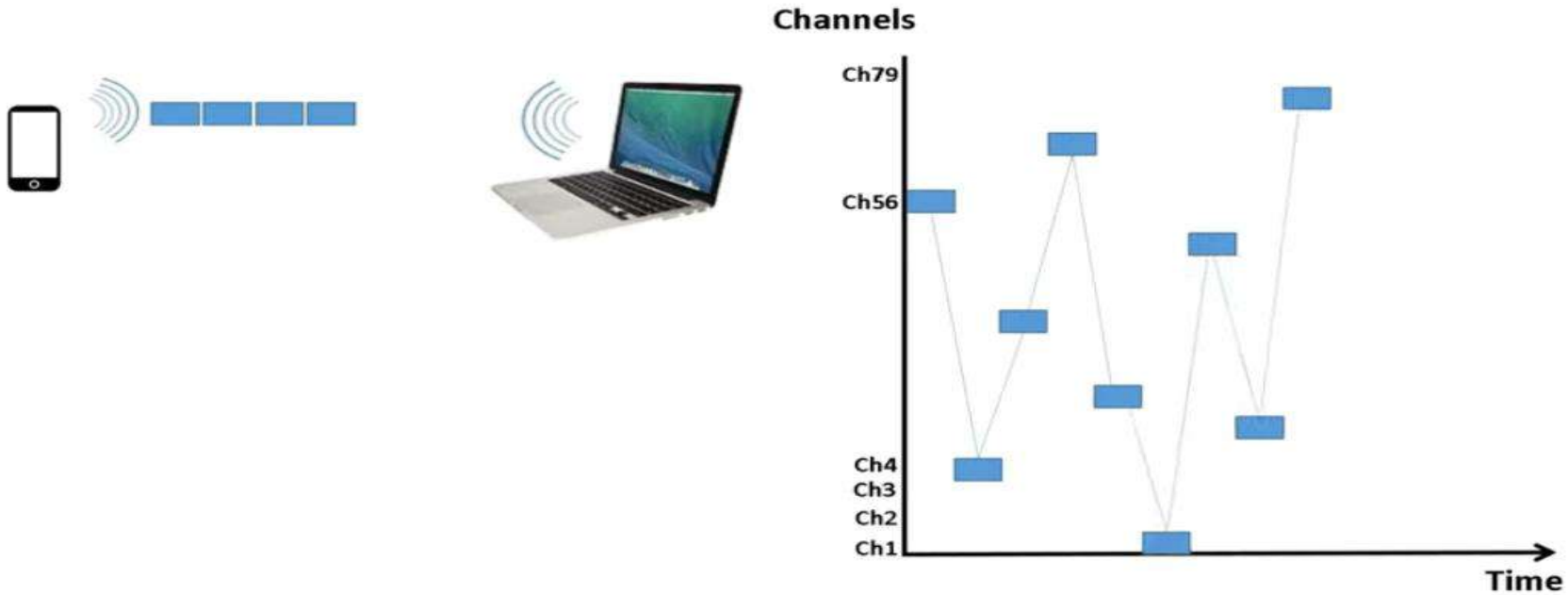


Figure 5-Sending data using Bluetooth technique.

Protocol stack

- The protocols in a stack determine the interconnectivity rules for a layered network model such as in the OSI or TCP/IP models.

- The **core protocols** of Bluetooth comprise the following elements:
- **Radio:** Specification of the air interface, i.e., frequencies, modulation, and transmit power.
- **Baseband:** Description of basic connection establishment, packet formats, timing, and basic QoS parameters.
- **Link manager protocol:** Link set-up and management between devices including security functions and parameter negotiation.
- **Logical link control and adaptation protocol (L2CAP):** Adaptation of higher layers to the baseband (connectionless and connection-oriented services.
- **Service discovery protocol:** Device discovery in close proximity plus querying of service characteristics.

Wireless Networks

1st course lecture 6

Lecture outlines

- **Continue with Bluetooth**
- **Worldwide Interoperability for Microwave Access (WiMax)**
- **Wi-Fi and WiMAX**
- **The broadband radio access networks (BRAN)**

Lecturer: Asia Ali

Power Management in the Bluetooth

The Bluetooth units can be in several modes of operation during the connection state, namely, active mode, sniff mode, hold mode, and park mode. These modes are…….

• **Active mode:** In this mode, the Bluetooth unit actively participates in the piconet. Various optimizations are provided to save power. For instance, if the master informs the slave when it will be addressed, the slave may sleep until then. The active slaves are polled by the master for transmissions.

• **Sniff mode:** This is a low-power mode in which the listening activity of the slave is reduced. The Link manager protocol (LMP) in the master issues a command to the slave to enter the sniff mode, giving it a sniff interval, and the slave listens for transmissions only at these fixed intervals.

• **Hold mode:** In this mode, the slave temporarily does not support Asynchronous Connection-Less (ACL) packets on the channel. In this mode, capacity is made available for performing other functions such as scanning, paging, inquiring, or attending another piconet.

• **Park mode:** This is a very low-power mode. The slave gives up its active member address and is given an eight-bit parked member address. The slave, however, stays synchronized to the channel. Any messages to be sent to a parked member are sent over the broadcast channel characterized by an active member address of all zeros. Apart from saving power, the park mode helps the master to have more than seven slaves (limited by the three-bit active member address space) in the piconet.

Bluetooth: Radio layer

Bluetooth devices will be integrated into typical mobile devices and rely on battery power. This requires small, low power chips which can be built into handheld devices.

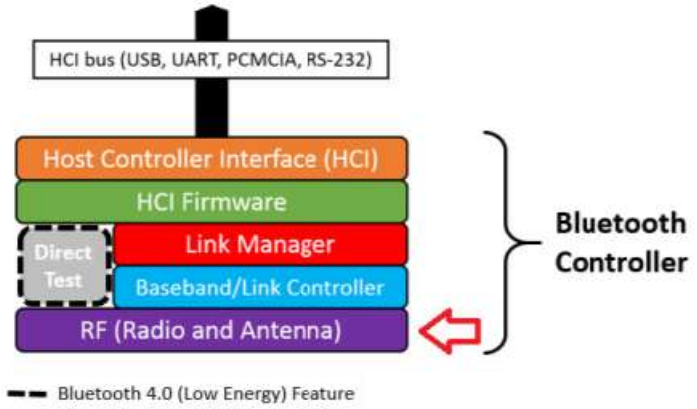
Bluetooth has to support multi-media data.

A frequency-hopping/time-division duplex scheme is used for transmission.

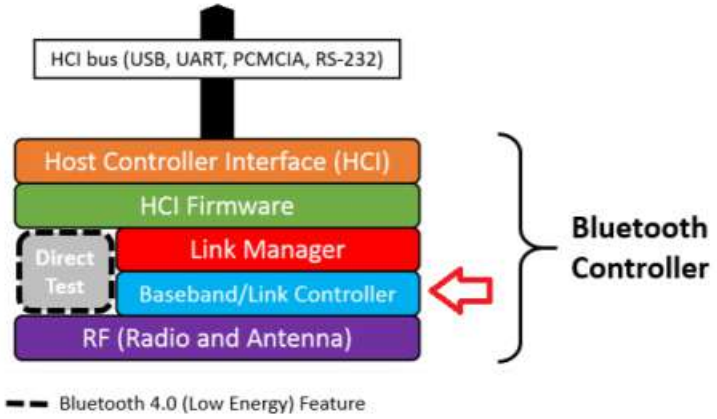
A fast hopping rate of 1,600 hops per second.

Bluetooth transceivers use Gaussian FSK for modulation and are available in three classes:

- **Power class 1:** Maximum power is 100 mW and minimum is 1 mW (typ.100 m range without obstacles). Power control is mandatory.
- **Power class 2**: Maximum power is 2.5 mW, nominal power is 1 mW, and minimum power is 0.25 mW (typ. 10 m range without obstacles). Power control is optional.
- **Power class 3**: Maximum power is 1 mW.

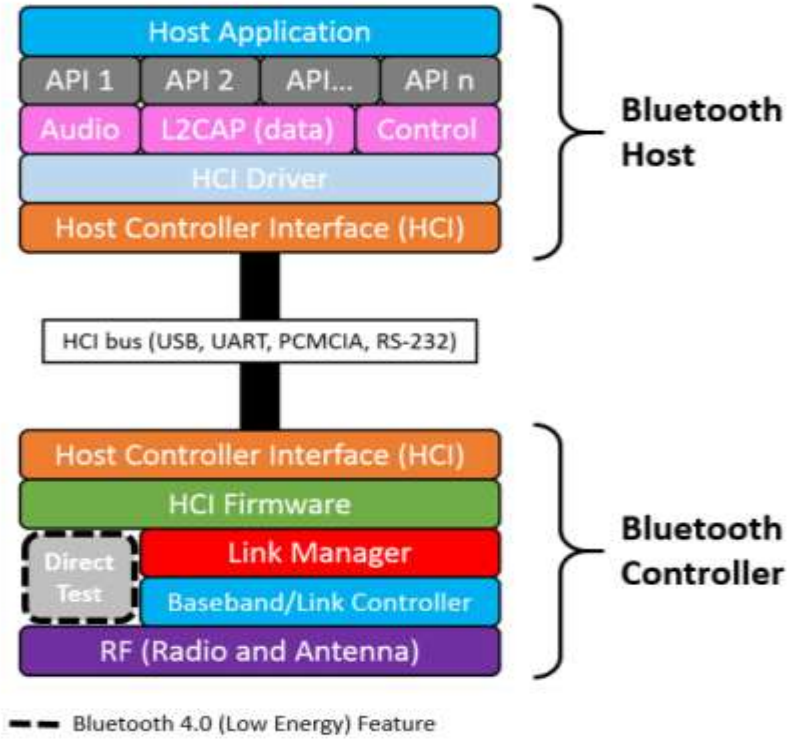


Location of RF Physical Layer in Bluetooth Protocol Stack



Location of Baseband Physical Layer in Bluetooth Protocol Stack

- A BlueTooth module is usually **a hardware component that provides**. **a wireless product to work with the computer**; or in some cases, the. bluetooth may be an accessory or peripheral, or a wireless headphone. or other product (such as cellphones can use.)



Bluetooth System Stack

Bluetooth module consists of four main components: radio transceiver, baseband/link controller, link manager and a host controller interface (HCI). HCI connects a Bluetooth system with the host system and provides a uniform interface method of accessing the Bluetooth hardware capabilities by the host system

Baseband layer

The functions of the baseband layer not only performs frequency hopping for interference and medium access, but also defines physical links and many packet formats. Figure 1, shows the components of a Bluetooth packet at baseband layer. The packet typically consists of the following three fields:

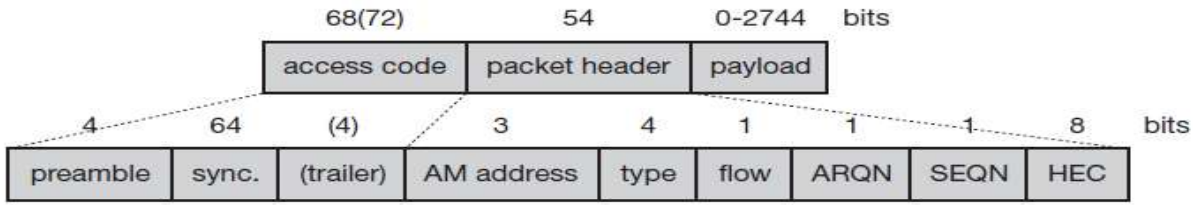


Figure 1-Baseband packet

- Access code: This first field of a packet is needed for timing synchronization and piconet identification (channel access code). The access code consists of a 4 bit preamble, a synchronization field, and a trailer (if a packet header follows).

- Packet header: This field contains typical layer 2 features: address, packet type, flow and error control, and checksum. The 3-bit active member address represents the active address of a slave. Active addresses are temporarily assigned to a slave in a piconet. If a master sends data to a slave the address is interpreted as receiver address. If a slave sends data to the master the address represents the sender address. The zero value is reserved for a broadcast from the master to all slaves.

Bluetooth offers two different types of **Physical Links**, a synchronous connection-oriented link (SCO) and an asynchronous connectionless link (ACL).

ACL (Asynchronous Connectionless Link) This is a control data link.

SCO (Synchronous Connection Oriented Link) This is a voice data link.

While Bluetooth is the technology used to connect devices from different manufacturers without wires, the devices still have to talk to each other while providing service they are designed for.

Headsets (combines a headphone with a microphone) are audio devices for speech, talk and listen; but when a headset is not doing its job it is still communicating with the other device referred to as the audio gateway (AG). This would be a cell phone for instance.

Once the headset has completed its pairing to the AG it goes into a stand by mode. As long as the headset and AG are within range they are connected by the ACL. If the AG receives a call and the headset ACL is working, the AG will signal the headset. The headset will be active to let the user know a call has arrived. Pressing the call control on the headset lets the AG know it is okay to open the SCO and voice data will be exchanged between the headset and AG. **Q- can we call this a single biconet? Whish one is the master and which one is the slave?**

Bluetooth Security

In Bluetooth communications, devices may be authenticated and links may be encrypted. The authentication of devices is carried out by means of a challenge response mechanism which is based on a commonly shared secret link key generated through a user-provided personal identification number (PIN). The authentication starts with the transmission of an LMP challenge packet and ends with the verification of result returned by the claimant. Optionally, the link between them could also be encrypted.

Bluetooth versions

Bluetooth 1.1

1. also IEEE Standard 802.15.1-2002
2. initial stable commercial standard

Bluetooth 1.2

1. also IEEE Standard 802.15.1-2005
2. eSCO(extended SCO): higher, variable bitrates, retransmission for SCO
3. AFH (adaptive frequency hopping) to avoid interference

Bluetooth 2.0 + EDR (2004, no more IEEE)

1. EDR (enhanced date rate) of 3.0 Mbit/s for ACL and eSCO
2. lower power consumption due to shorter duty cycle

Bluetooth 2.1 + EDR (2007)

1. better pairing support, e.g. using NFC
2. improved security

Bluetooth 3.0 + HS (2009)

1. Bluetooth 2.1 + EDR + IEEE 802.11a/g = 54 Mbit/s

Bluetooth 4.0 (2010), 4.1 (2013), 4.2 (2014)

1. Low Energy, much faster connection setup

Bluetooth 5 (2016)

1. Longer range (100 m) or higher data rate (2 Mbit/s without EDR), localization, no more park state

Worldwide Interoperability for Microwave Access (WiMax)

WiMax is characterized under the IEEE 802.16 standard.

- It is a broadband wireless access technology that provides fixed, nomadic, reliable and mobile communication across wired and wireless connectivity.
- The 802.16 standard was created to attend to specifications for wireless Metropolitan Area Networks (WMANs).

There are two main types of WiMAX:

1. **802.16-2004 (Fixed WiMax) -** 802.16-2004 transmission to stationary devices and replaces earlier specifications i.e. 802.16 and 802.16a.

1. **802.16e or 802.16-2005 (mobile WiMAX) –**

802.16e is an extension of 802.16 -2004 for mobile use in the 2 to 6 GHZ band.

- It allows people to communicate while walking or riding in cars.
- provides a mobile voice over IP and higher speed data alternative to the cellular networks (Global System for Mobile Communication (GSM), Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA)).
- In WiMAX central modulation technique is OFDM (i.e. Orthogonal Frequency Division Multiplexing), and both systems utilize MIMO (i.e. multiple inputs multiple outputs) techniques.

Defining two scenarios for a wireless deployment as shown below in Figure 2:

(a) point-to-point (P2P):- Point to point is used where there are two points of interest (mainly the sender and receiver) .

(b) point-to-multipoint (PMP):- Point-to-multipoint is as the name suggests a distribution from a single point to multiple receivers. In the Point-to-multipoint technique, a sender sends data to multiple receivers with used many types of security (authentication, authorization). It means one base station can service hundreds of dissimilar subscribers in terms of bandwidth and offered services.

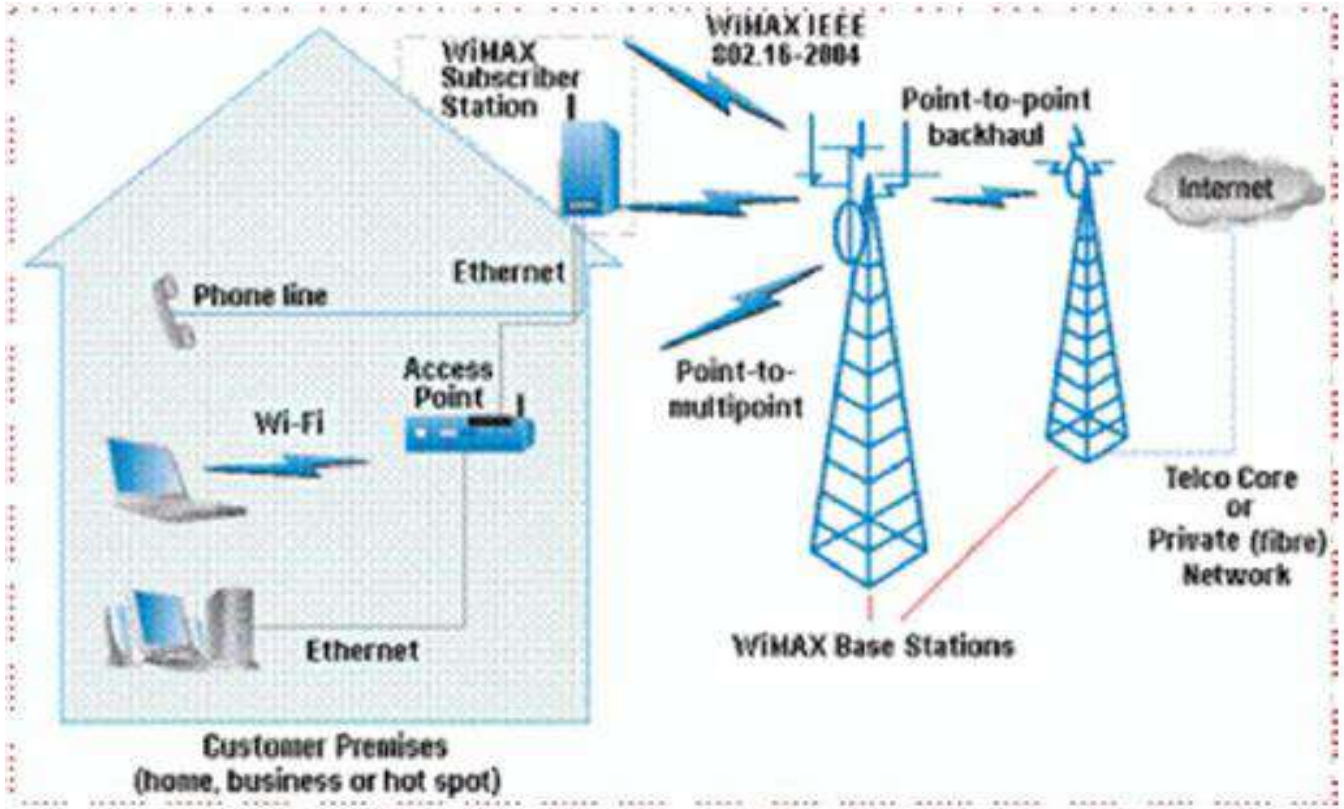


Figure 3-WiMax

Wi-Fi and WiMAX

Wi-Fi and WiMAX are two *broadband technologies but these technologies may have few similarities, and they differ in the technical execution.

WiMAX is similar to the wireless standard known as Wi-Fi, but on a larger scale and at faster speeds.

If we compare between the Wi-Fi and WiMAX.

- Wifi offer local network access for a few hundred feet with the speed of up to 54 Mbps.
- A single WiMAX antenna expected to have a range of up to 40 miles with the speed of 70 Mbps or more.
- The main goal of WiMAX is to offer cheap and fast connectivity of both voice and data communication.

On dual channel devices, data transmission can exceed up to 450Mbps limit. A user with a mobile computing device such as a laptop, cell phone, or PDA which is Wi-Fi enabled can connect to the global Internet when it is within a range of an access point (**as shown below in Figure 1)**.

Dual channel: it means the devices can work on 2.4 GHZ and 5 GHZ. Therefore, data transmission can exceed up to 450Mbps.

The region which is covered by one or more access points called a **hotspot**. **Hotspots** *can range from a single room to thousands of square feet's of overlapping hotspots*

Note: IEEE 802.11a cannot co-exist with 802.11b and 802.11g as they operate on different frequency bands.

***Broadband technology refers to a high-speed, higher bandwidth connection to the Internet than is offered by a standard telephone line. The greater bandwidth of a broadband connection allows for more data to be transmitted at higher speeds than a conventional telephone line.**

If Wireless technology (Wi-Fi and WiMax) can be integrated and overlay, it means that WiMAX and Wi-Fi will support each other.

WiMAX and Wi-Fi operators can be applied various configurations if they were integrated are as follows:

(A) Backhaul it is a synonym for "backbone": It is the first configuration, in this, we combined these two technologies then WiMAX functioning as a backhaul while Wi-Fi connected directly to the subscriber.

Devices that provide connectivity to a WiMAX network are known as subscriber stations (SS) they are able to connect multiple devices such as (mobile, broadband TV, LAPTOPs). Examples of such devices are routers and network switches.

(B) Backhaul inter WI-FI mesh network: WiMAX has been used directly as a part of Wi-Fi Mesh Network. Wi-Fi network automatically will be more reliable in a wider coverage area and reduce cost connection that is caused by cable drawing in each AP installation when in this network Subscriber Terminal of WiMAX is put on access point of Wi-Fi Mesh Network. The solution in this network can increase performance and robustness of the Wi-Fi network.

(C) Wi-Fi and WiMAX full integrated: WiMAX coverage is overlapping with Wi-Fi coverage. It gives better service choices, more flexible to the changes of network and is more user-friendly with connection ease compatible with a terminal that has been owned.

- Broadband access not only provides faster Web surfing and quicker file downloads but also enables several multimedia applications, such as real-time audio and video streaming, multimedia conferencing, and interactive gaming.
- Broadband connections are also being used for voice telephony using voice-over-Internet Protocol (VoIP) technology.

- **Hotspots**
- A Hotspot is a geographical area that has a readily accessible wireless network. Hotspots are equipped with Broadband Internet connection and one or more Access points that allow users to access the internet wirelessly. Hotspots can be setup in any public location that can support an Internet connection.

HOW HOTSPOTS WIFI WORKS

•A Wi-Fi hotspot is created by installing an access point to an internet connection. An access point acts as a base station.

•When Wi-Fi enabled device encounters a hotspot the device can then connect to that network wirelessly.

A single access point can support up to 30 users and can function within arrange of 100–150 feet indoors and up to 300 feet outdoors.

The broadband radio access networks (BRAN)

Standardized by the European Telecommunications Standards Institute (ETSI), could have been an RAL for WATM (ETSI, 2002b). The primary market for BRAN includes private customers and small to medium-sized companies with Internet applications, multi-media conferencing, and virtual private networks. The BRAN standard and IEEE 802.16 (Broadband wireless access, IEEE, 2002b) have similar goals.

- transfer rates of 25–155 Mbit/s.
- and a transmission range of 50 m–5 km.

HIPERLAN

The European counterparts to the IEEE 802.11 standards are the high performance radio LAN(HIPERLAN) standards defined by the European Telecommunications Standards Institute (ETSI). It is to be noted that while the IEEE 802.11 standards can use either radio access or infrared access, the HIPERLAN standards are based on radio access only.

The standards have been defined as part of the ETSI broadband radio access networks (BRAN) project. In general, broadband systems are those in which user data rates are greater than 2 Mbps (and can go up to 100s of Mbps). Four standards have been defined for wireless networks by the ETSI.

HIPERLAN/1 is a wireless radio LAN (RLAN) without a wired infrastructure, based on one-to-one and one-to-many broadcasts. It can be used as an extension to a wired infrastructure, thus making it suited to both ad hoc and infrastructure

- based networks. It employs the 5.15 GHz and the 17.1 GHz frequency bands and provides a maximum data rate of 23.5 Mbps.

- **The HIPERLAN/2 standard intends to provide:**

- short-range (up to 200 m) wireless access to Internet protocol (IP).
- asynchronous transfer mode (ATM: ATM networks are connection-oriented and require a connection to set up prior to transfer of information from a source to a destination.
- All information to be transmitted — voice, data,image, and video — is first fragmented into small, fixed-size packets known as cells.
- These cells are then switched and routed using packet switching principles) ,and other infrastructure-based networks and, more importantly, to integrate WLANs into cellular systems.
- It employs the 5 GHz frequency band and offers a wide range of data rates from 6 Mbps to 54 Mbps.

HIPERLAN/2 has been designed to meet the requirements of future wireless multimedia services. as shown in Figure 5. The figure shows MTs being centrally controlled by the APs which are in turn connected to the core network (infrastructure-based network). It is to be noted that, unlike the IEEE standards, the core network for HIPERLAN/2 is not just restricted to Ethernet. Also, the AP used in HIPERLAN/2 consists of one or many transceivers called access point transceivers (APTs) which are controlled by a single access point controller (APC).

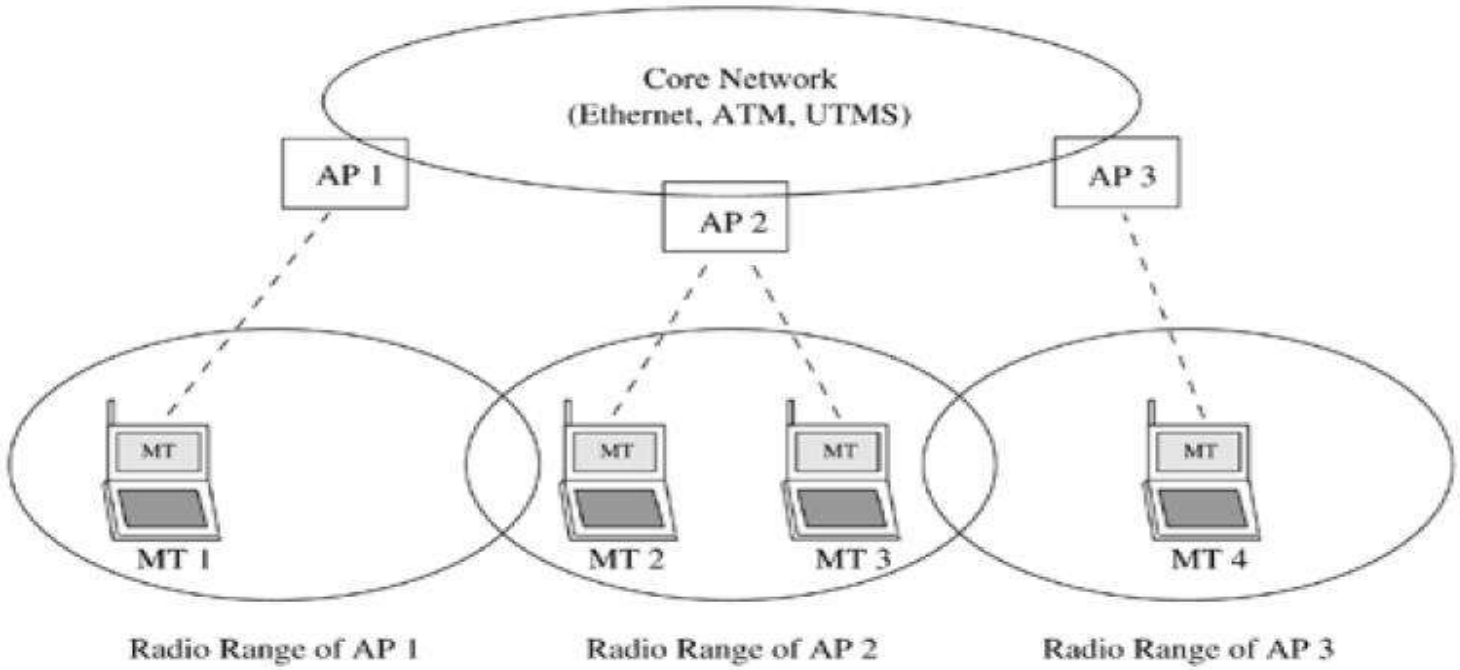


Figure 5- A typical deployment of HIPERLAN/2.

Wireless ATM working group

The ATM Forum formed the **Wireless ATM Working Group** in 1996, which aimed to develop a set of specifications that extends the use of ATM technology to wireless networks. These wireless networks should cover many different networking scenarios, such as private and public, local and global, mobility and wireless access (Raychaudhuri, 1996a and b).

The main goals of this working group

- ensuring the compatibility of all new proposals with existing ATM Forum standards.
- certain functions to support mobility and radio access if required.

WATM systems had to be designed for transferring voice, classical data, video (from low quality to professional quality), multimedia data, short messages etc.

Wireless Network

1st course lecture 8

- **Mobile Network Layer**

Lecturer: Dr. Asia Ali

Mobile Network Layer

Mobile IP: IP packet delivery, Agent discovery, tunneling and encapsulation. IPV6-Network layer in the internet.

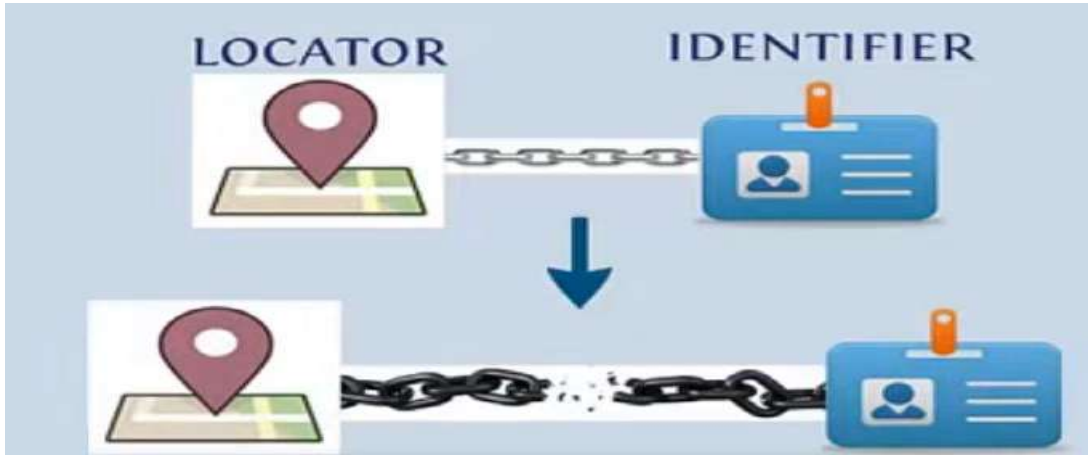
Mobile ad-hoc network: Routing, Destination Sequence distance vector, Dynamic source routing

Introduction

Here we introduce protocols and mechanisms developed for the network layer to support mobility. The most prominent example is *Mobile IP*. The internet is the network for global data communication with hundreds of millions of users.

The IP (Internet protocol) designers have designed it to be the locator and the identifier of a node and combined them together.

Mobile IP is the standard that allows users using mobile devices whose IP is associated with one network to stay connected when moving to other networks.



Mobile IP Goals, assumptions and requirements

Why not simply we use a mobile computer in the internet?

The reason is quite simple: you will not receive a single packet as soon as you leave your home network, i.e., the network your computer is configured for, and reconnect your computer (wireless or wired) at another place (if no additional mechanisms are available). For example, the destination address 129.13.42.99 shows that the receiver must be connected to the physical subnet with the network prefix 129.13.42.

Routers in the internet now look at the destination addresses of incoming packets and forward them according to internal look-up tables. **To avoid an explosion of routing tables, only prefixes are stored and further optimizations are applied**.

A router would otherwise have to store the addresses of all computers in the internet, which is obviously not feasible. As long as the receiver can be reached within its physical subnet, it gets the packets; as soon as it moves outside the subnet, a packet will not reach it. A host needs a so-called **topologically correct address.** temporarily change routing table entries for mobile host is not good solution because routing table does not scale if many mobile hosts or frequent location changes.

Quick 'solutions'

One might think that a quick solution to this problem would be to assign to the computer a new***, topologically correct IP address (***Change mobile host IP-address***)***.

-Adjust the host IP address depending on the current location (DHCP)

- Domain Name System (DNS) updates take to long time

- Old TCP connections break.

Requirements

Since the quick 'solutions' obviously did not work, a more general architecture had to be designed.

mobile IP as a standard to enable mobility in the internet. Several requirements accompanied the development of the standard:

Transparency

- mobile end-systems keep IP address
- Continuous service after link interruption
- point of connection to the fixed network can be changed

Compatibility

- No changes to current hosts, OS, routers
- A mobile IP implementation should still be able to communicate with fixed systems without mobile IP.

Security

- All the messages related to the management of Mobile IP are authenticated.

Efficiency and scalability

- only few additional messages to mobile system (low bandwidth)
- Global support for large number of mobile systems

The goal of a mobile IP: *'supporting end-system mobility while maintaining scalability, efficiency, and compatibility in all respects with existing applications and Internet protocols*'.

Terminology used with understand mobile IP

The following defines several entities and terms needed to understand mobile IP. See Figure 1.

Mobile Node (MN)

- Laptop, PDA, etc.. that may move about

Correspondent Node (CN)

- Node that wants to communicate with MN, the CN can be a fixed or mobile node.

Home Agent (HA)

- Router in home network of the MN, helps in forwarding
- registers current MN location, tunnels IP datagrams to COA

Foreign Agent (FA) Router in current foreign network of MN

- forwards tunnelled datagrams to the MN Care-of Address (COA)
- address of the current tunnel end-point for the MN (at FA or MN)
- can be chosen, e.g., via DHCP

NOTE: **Care-of address (COA):** The COA defines the current location of the MN from an IP point of view.

Home Network

- No mobile IP support is needed within the home network

Foreign network

- The foreign network is the current subnet the MN visits and which is not the home network.

Session continuity from foreign network to local network. Reachability communication must be possible where the mobile node is (moving or stable in the same place)

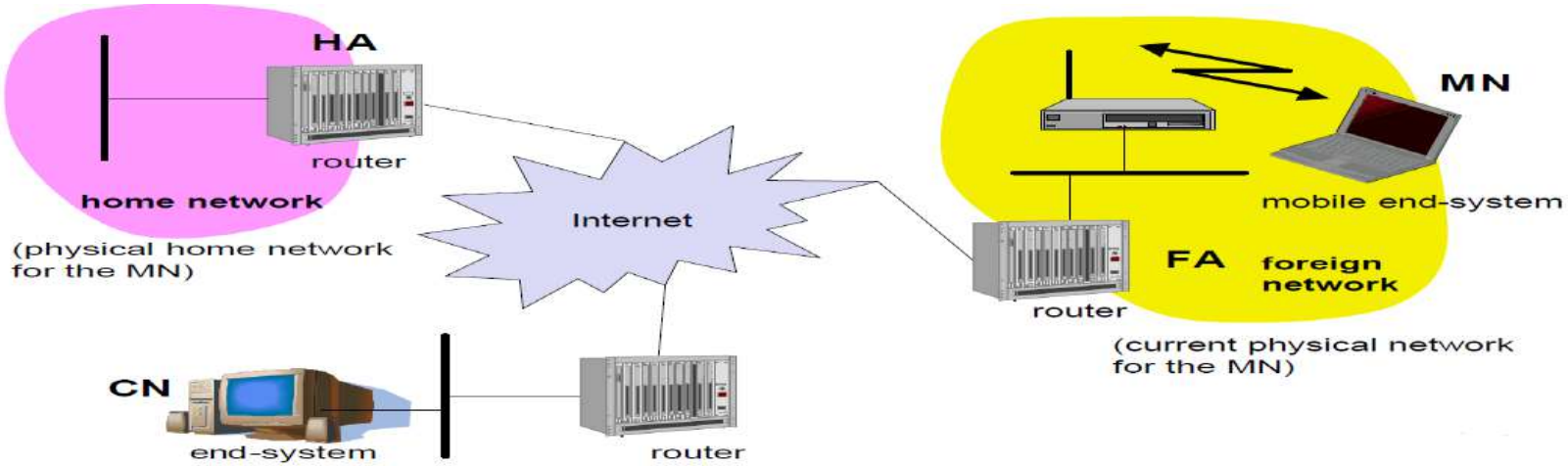
Mobility not including mobile phone or a laptop. It can be any of the following (1) terminal (host) mobility where the host change his point of attachment when a node change the access point to another access point. (2) Network mobility change its point of attachment. A train with a Wi-Fi can be the network that in a train that is moving and keeps changing its association. For example, a network is the train and its keep on changing the access points as it is moving.

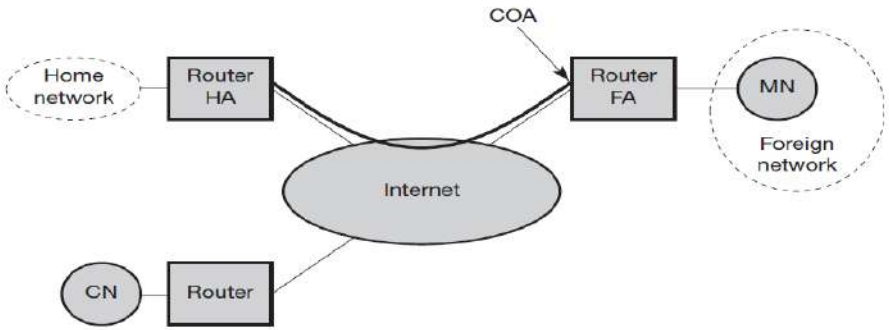
(3) Session mobility: communication session means transfer from one device to other one. For example, you are watching on your mobile some video and wanted to transfer it or continue it on the TV.

How mobile IP works?

Suppose a home network with a home agent connected to it and to the Internet. If the MN moves from its home network to a foreign network and while the MN in the foreign network, there is a corresponding node that tries to send messages to the MN. The corresponding node will use the home address of MN that the corresponding node already knows. The message will be intercepted by the home agent, which will look up for the new address of the MN in the care of address or the new network. The home agent will encapsulate the message it just received and set the destination address to the MN care of address using **tunnelling protocol***. The message then tunnelled to the MN new address in the foreign network.

***t**unneling protocol is a communications protocol that allows for the movement of data from one network to another. It involves allowing private network communications to be sent across a public network (such as the Internet) through a process called encapsulation





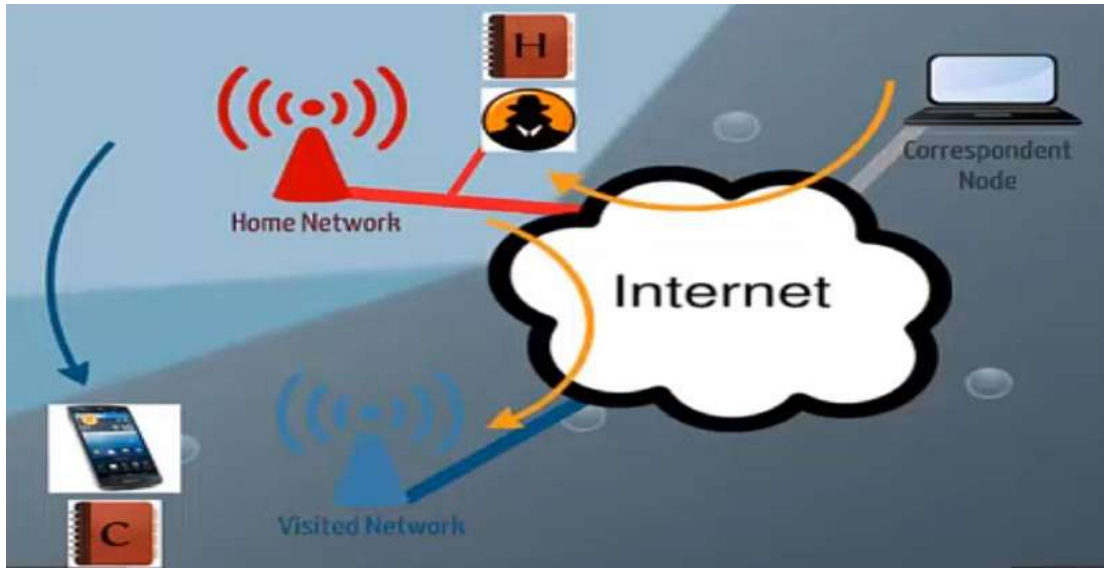


Figure 1-Mobile IP example network

IP packet delivery

Figure 2 illustrates packet delivery to and from the MN using the example network of Figure 1 correspondent node CN wants to send an IP packet to the MN. One of the requirements of mobile IP was to support hiding the mobility of the MN.

CN does not need to know anything about the MN's current location and sends the packet as usual to the IP address of MN (step 1). This means that CN sends an IP packet with MN as a destination address and CN as a source address. The internet, not having information on the current location of MN, routes the packet to the router responsible for the home network of MN. This is done using the standard routing mechanisms of the internet. The HA now intercepts the packet, knowing that MN is currently not in its home network. The packet is not forwarded into the subnet as usual, but encapsulated and tunnelled to the COA. A new header is put in front of the old IP header showing the COA as new destination and HA as source of the encapsulated packet (step 2).

The foreign agent now decapsulates the packet, i.e., removes the additional header, and forwards the original packet with CN as source and MN as destination to the MN (step 3).

Again, for the MN mobility is not visible. It receives the packet with the same sender and receiver address as it would have done in the home network.

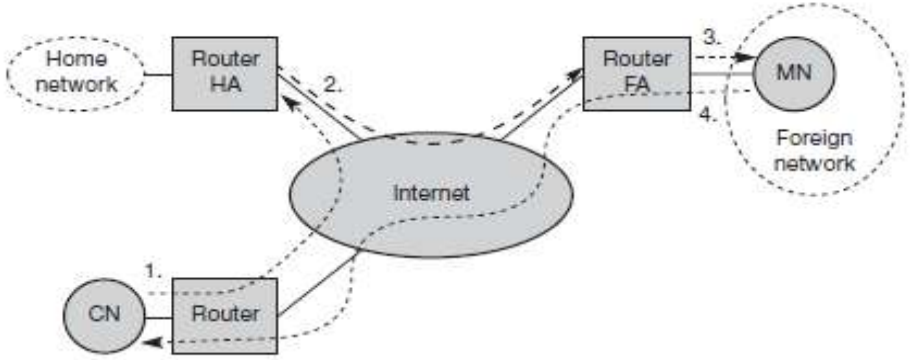


Figure 2- Packet delivery to and from the mobile node

Figure 2-Packet delivery to and from the mobile node. To summarize the scenario is 1. Sender sends to the IP address of MN, HA intercepts packet 2. HA tunnels packet to COA by encapsulation 3. FA forwards the packet to MN 4. Reverse: Sender sends to IP address of receiver; FA is default router.

Agent discovery

How does the MN discover that it has moved? For this purpose mobile IP describes two methods: agent advertisement and agent solicitation, which are in fact router discovery methods plus extensions.

Agent advertisement

For the first method, foreign agents and home agents advertise their presence periodically using special **agent advertisement** messages.

Agent Advertisement

- HA and FA periodically send advertisement messages into their subnets
- MN reads a COA from the FA advertisement messages

Registration

- MN signals COA to the HA via the FA, HA acknowledges
- Messages need to be secured by authentication

Advertisement

- HA advertises the MN IP address (as for fixed systems)
- routers adjust their entries, (HA responsible for a long time)
- All packets to MN are sent to HA

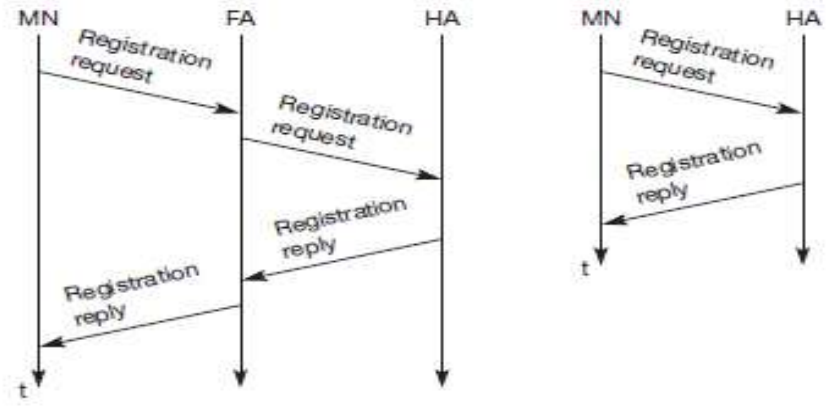


Figure 3- Registration of a mobile node via the FA or directly with the HA

Tunneling and encapsulation

Tunneling and encapsulation are the mechanisms used for forwarding packets between the HA and the COA, as shown in Figure 3 , step 2.

A **tunnel** establishes a virtual pipe for data packets between a tunnel entry and a tunnel endpoint. Packets entering a tunnel are forwarded inside the tunnel and leave the tunnel unchanged. Tunneling, i.e., sending a packet through a tunnel, is achieved by using encapsulation.

Encapsulation is the mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet. The reverse operation, taking a packet out of the data part of another packet, is called **decapsulation**. Encapsulation and decapsulation are the operations typically performed when a packet is transferred from a higher protocol layer to a lower layer or from a lower to a higher layer respectively. Here these functions are used within the same layer. This mechanism is shown in Figure 4 and describes exactly what the HA at the tunnel entry does. The HA takes the original packet with the MN as destination, puts it into the data part of a new packet and sets the new IP header in such a way that the packet is routed to the COA. The new header is also called the **outer header** for obvious reasons. Additionally, there is an **inner header** which can be identical to the original header as this is the case for IP-in-IP encapsulation, or the inner header can be computed during encapsulation.

Encapsulation of one packet into another as payload e.g. IP-in-IP-encapsulation tunnel between HA and COA

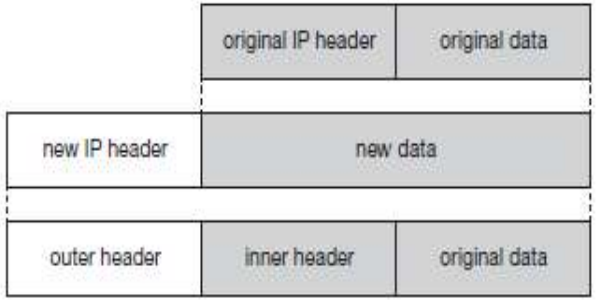


Figure 4-IP encapsulation

IPV6-Network layer in the internet.

Mobile IP was developed for IPv4, but IPv6 simplifies the protocols. Security is integrated with regard to authentication. No special mechanisms as add-ons are needed for securing mobile IP registration.

Every IPv6 node masters address auto-configuration the mechanisms for acquiring a COA are already built in. Neighbor discovery as a mechanism mandatory for every node is also included in the specification; special foreign agents are no longer needed to advertise services. Combining the features of autoconfiguration and neighbor discovery means that every mobile node is able to create or obtain a topologically correct address for the current point of attachment.

Every IPv6 node can send binding updates to another node, so the MN can send its current COA directly to the CN and HA. These mechanisms are an integral part of IPv6.

A soft handover is possible with IPv6. The MN sends its new COA to the old router servicing the MN at the old COA, and the old router encapsulates all incoming packets for the MN and forwards them to the new COA.

The FA is not needed any more. A CN only has to be able to process binding updates, i.e., to create or to update an entry in the routing cache. The MN itself has to be able to decapsulate packets, to detect when it needs a new COA, and to determine when to send binding updates to the HA and CN. A HA must be able to encapsulate packets.

However, IPv6 does not solve any firewall or privacy problems. Additional mechanisms on higher layers are needed for this.

Wireless Network

1st course lecture 9

Mobile ad-hoc network

Lecturer: Dr. Asia Ali

Mobile/wireless ad-hoc network (WANET/MANET):

Wireless networks typically work by one of the configuration network topology either Ad-Hoc or Infrastructure network. **WANET/MANET** is a local area network (LAN) that is built spontaneously to enable two or more wireless devices to be connected to each other without requiring typical network infrastructure equipment, such as a wireless router or access point.

Mobility support the existence of at least some infrastructure. Mobile IP requires, e.g., a home agent, tunnels, and default routers.

DHCP requires servers and broadcast capabilities of the medium reaching all participants or relays to servers.
Cellular phone networks require base stations, infrastructure networks etc.
However, sometimes, users of a network cannot rely on an infrastructure, it is too expensive, or there is none at all. In these situations, mobile ad-hoc networks are the only choice here we focus on so-called multi-hop ad-hoc networks when describing ad-hoc networking.
In most cases, a PC, laptop or smartphone Wi-Fi interface is used to build an ad hoc network (Figure 1). In other situations, devices such as wireless sensors are designed to work primarily in an ad hoc mode.

How does an ad hoc network work?

- Devices configured for ad hoc functionality require a wireless network adapter or chip, and they need to be able to act as a wireless router when connected. When setting up a wireless ad hoc network, each wireless adapter must be configured for ad hoc mode instead of infrastructure mode. All wireless devices connecting to an ad hoc device need to use the same service set identifier (SSID) and wireless frequency channel number.
- The individual wireless endpoints connected to an ad hoc network forward packets to and from each other. Ad hoc wireless networks are most useful when wireless infrastructure isn't available -- for example, if there aren't any access points or routers within range and cabling cannot extend to reach the location where additional wireless communication is needed.
- Ad hoc networks are also commonly set up to provide temporary wireless network access created by a computer or smartphone.
- An example of ad-hoc is to use a cellular-connected smartphone that is configured in Wi-Fi ad hoc mode so that Wi-Fi capable laptops can connect to the Wi-Fi ad hoc network to gain internet access over the smartphone's cellular internet link. This method bypasses any need for a WAP or WLAN controller.

Instant infrastructure: Unplanned meetings, spontaneous interpersonal communications etc. cannot rely on any infrastructure. Therefore, ad-hoc connectivity has to be set up.

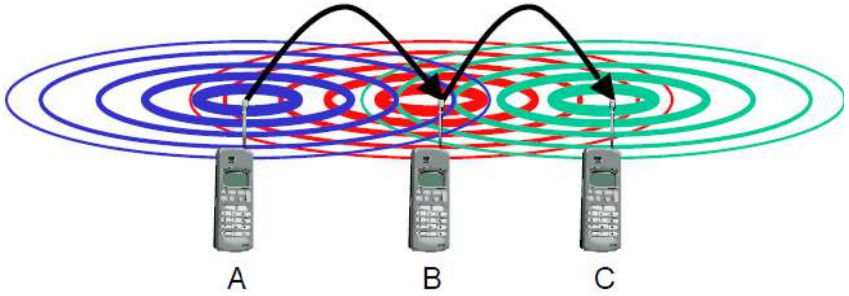
● **Disaster relief:** Infrastructures typically break down in disaster areas. Hurricanes cut phone and power lines, floods destroy base stations, fires burn servers.

● **Remote areas:** Even if infrastructures could be planned ahead. it is sometimes too expensive to set up an infrastructure in sparsely populated areas. cost can also be argument against infrastructure

Main topic: routing

- no default router available. The nodes in this network also serve as routers that are responsible for finding and dealing with the route to every node in the network. Some characteristics of MANET are: dynamic network configuration, limited bandwidth power constraints for each operation. The MANET network layer has two parts, namely the network layer and the transport layer. In the network layer of MANET is the IP (Internet protocol) and the ad hoc routing layer uses the AODV protocol (ad hoc on demand distance vector)

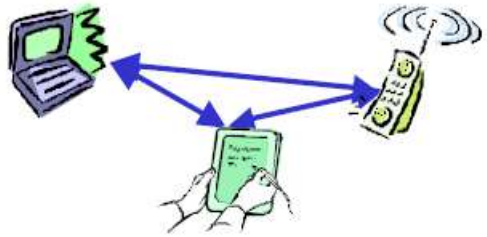
- every node should be able to forward



Solution: Wireless ad-hoc networks

Network without infrastructure

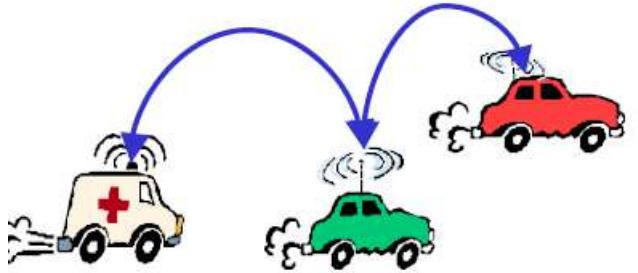
- Use components of participants for networking



Examples

- Single-hop: All partners max. one hop apart
  - Bluetooth piconet, PDAs in a room, gaming devices…

- Multi-hop: Cover larger distances, circumvent obstacles
  - Bluetooth scatternet, *TETRA police network, car-to-car networks…



A mobile ad hoc network is an autonomous collection of mobile devices (laptops, smart phones, sensors, etc.) that communicate with each other over wireless links and cooperate in a distributed manner in order to provide the necessary network functionality in the absence of a fixed infrastructure. This type of network, operating as a stand-alone network or with one or multiple points of attachment to cellular networks or the Internet, paves the way for numerous new and exciting applications. Application scenarios include, but are not limited to: emergency and rescue operations, conference or campus settings, car networks, personal networking, etc.

➢Ad-Hoc network is divided into 7 Ad Hoc network types are as follows:

WANET (Wireless Ad Hoc Network)

MANET (Mobile Ad Hoc Network)

VANET (Vehicular Ad Hoc Network)

SPANs (Smart Phone Ad Hoc Network)

iMANETs (Internet Based Mobile Ad Hoc Network)

Military / Tactical MANETs SPAN (Self Powered Ad Hoc Network).

Internet: MANET (Mobile Ad-hoc Networking) group

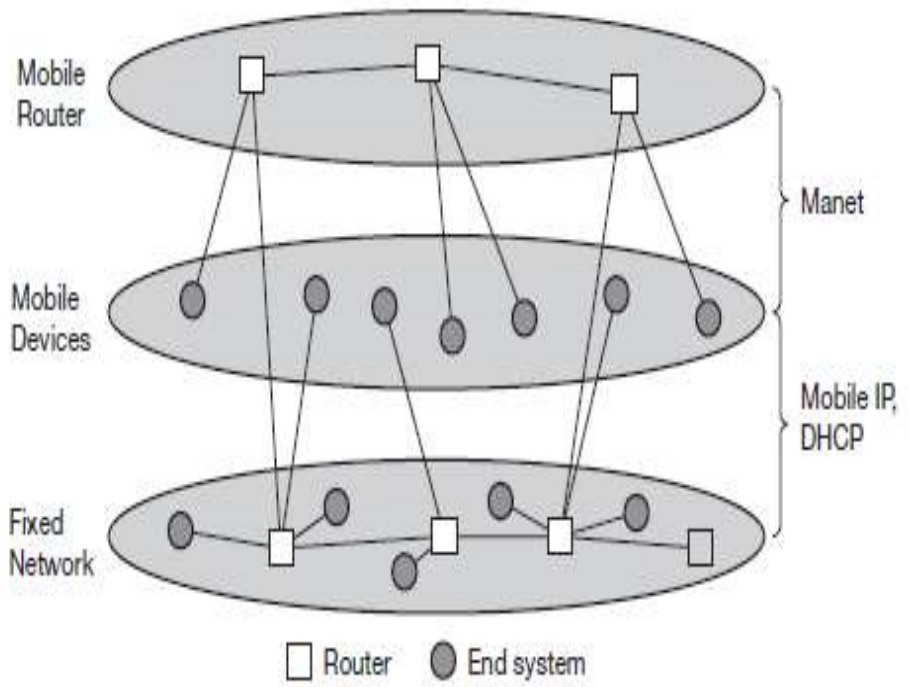


Figure 1-MANETs and mobile IP

Figure 1 shows the relation of MANET to mobile IP and DHCP. While mobile IP and DHCP handle the connection of mobile devices to a fixed infrastructure, MANET comprises mobile routers, too. Mobile devices can be connected either directly with an infrastructure using Mobile IP for mobility support and DHCP as a source of many parameters, such as an IP address.

Routing

While in wireless networks with infrastructure support a base station always reaches all mobile nodes, this is not always the case in an ad-hoc network. A destination node might be out of range of a source node transmitting packets. Routing is needed to find a path between source and destination and to forward the packets appropriately.

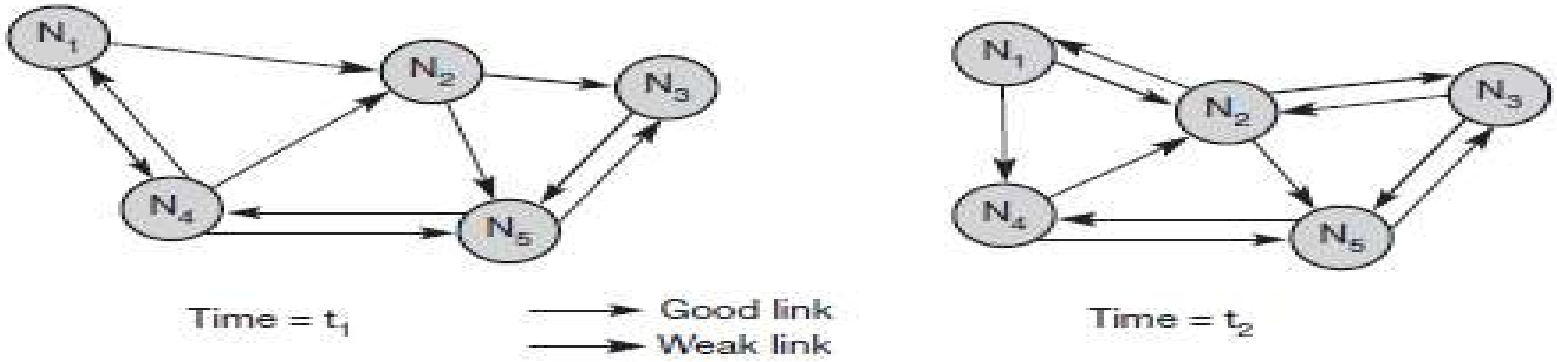


Figure 2-Example ad-hoc network

Figure 2 gives a simple example of an ad-hoc network. At a certain time t1 the network topology might look as illustrated on the left side of the figure. Five nodes, N1 to N5, are connected depending on the current transmission characteristics between them. In this snapshot of the network, N4 can receive N1 over a good link, but N1 receives N4 only via a weak link. Links do not necessarily have the same characteristics in both directions. The reasons for this are, e.g., different antenna characteristics or transmit power. N1 cannot receive N2 at all, N2 receives a signal from N1.

This situation can change quite fast as the snapshot at t2 shows. N1 cannot receive N4 any longer, N4 receives N1 only via a weak link. But now N1 has an asymmetric but bi-directional link to N2 that did not exist before.

This very simple example already shows some fundamental differences between wired networks and ad-hoc wireless networks related to routing.

Traditional routing algorithms

Traditional routing algorithms known from ***wired networks*** will not work efficiently (e.g., distance vector algorithms such as RIP (Hendrik, 1988), (Malkin, 1998) converge much too slowly) or fail completely (e.g., link state algorithms such as OSPF (Moy, 1998) exchange complete pictures of the network).

Problem 1: traditional Routing algorithms cannot be used because, Highly dynamic network topology

- Device mobility and varying channel quality
- Asymmetric connections possible

Distance Vector

- periodic exchange of cost to everyone else, with neighbours
- selection of shortest path if several paths available

Link State

- periodic notification of all routers about the current cost to neighbors
- routers get a complete picture of the network, run Djikstra's algorithm

Example

- ARPA packet radio network (1973), DV-Routing
- every 7.5s exchange of routing tables including link quality
- Receive packets, update tables

Routing in ad-hoc networks

The big topic in many research projects

- Far > 50 different proposals exist
- The most simplest one: Flooding!

Reasons

- Classical approaches from fixed networks fail
  - Fast link quality changes, slow convergence, large overhead
- Highly dynamic, low bandwidth, low computing power

Metrics for routing

- Minimize: Number of hops, loss rate, delay, congestion, interference … Maximal:l Stability of logical network, battery run-time, time of connectivity …

Problems of traditional routing algorithms

- Dynamic of the topology
- frequent changes of connections, connection quality, participants

Limited performance of mobile systems

- Periodic routing table updates need energy, sleep modes difficult
- limited bandwidth further reduced due to routing info exchange
- links can be asymmetric, directional transmission quality

Destination sequence distance vector(DSDV)

routing is an enhancement to distance vector routing for ad-hoc networks (Perkins, 1994). Distance vector routing is used as routing information protocol (RIP) in wired networks. It performs extremely poorly with certain network changes due to the count-to-infinity problem. Each node exchanges its neighbor table periodically with its neighbours. Changes at one node in the network propagate slowly through the network (step-by-step with every exchange). The strategies to avoid this problem which are used in fixed networks (poisoned-reverse/splithorizon (Perlman, 1992)) do not help in the case of wireless ad-hoc networks,
due to the rapidly changing topology. This might create loops or unreachable regions within the network.

DSDV now adds two things to the distance vector algorithm:

- **Sequence numbers for all routing updates**: Each routing advertisement comes with a sequence number. Within ad-hoc networks, advertisements may propagate along many paths. Sequence numbers help to apply the advertisements in correct order.
  - assures in-order execution of all updates
  - avoids loops and inconsistencies
- **Decrease of update frequency**
  - store time between first and best announcement of a path
  - inhibit update if it seems to be unstable (based on the stored time values)

Dynamic source routing

divides the task of routing into two separate problems according to (Johnson, 1996), (Johnson, 2002a):

- **Route discovery:** A node only tries to discover a route to a destination if it has to send something to this destination and there is currently no known route.

- **Route maintenance:** If a node is continuously sending packets via a route, it has to make sure that the route is held upright. As soon as a node detects problems with the current route, it has to find an alternative.

The basic principle of source routing is also used in fixed networks, e.g. token rings. Dynamic source routing eliminates all periodic routing updates and works as follows. If a node needs to discover a route, it broadcasts a route request with a unique identifier and the destination address as parameters. Any
node that receives a route request does the following.

- If the node has already received the request (which is identified using the unique identifier), it drops the request packet.
- If the node recognizes its own address as the destination, the request has reached its target.
- Otherwise, the node appends its own address to a list of traversed hops in the packet and broadcasts this updated route request.

➢Conclusion

- Reactive protocol is a on demand process that means determine routes whenever needed (is divides in two types – Ad hoc On-Demand Distance Vector (AODV) and Temporary Ordering Routing Algorithms (TORA)). while the proactive protocols traditional process but provides the shortest path.
- The packet data is delivered in more efficiently in the reactive protocol than in proactive protocol.
- Proactive protocols (Destination Sequence Vector or DSDV router is utilized in this type of protocol) are much slower than the reactive protocols in terms of performance.
- For the different topographies, reactive protocol is more efficient and adaptive than the proactive protocols.
- For the reactive protocol, the time taken or average end to end delay by the data to reach the destination from the source is quite variable while in proactive it is constant for the a given Ad hoc network.