4.1 Wireless Local Area Networks

Prof. Monali Shetty
Lecture 37
16-10-20
11.30 PM (DSPIP)

Syllabus 4.1

Introduction, Infrastructure and ad-hoc network

Wireless Local Area Network

- WLAN also called WiFi (Wireless Fidelity).
- A WLAN is a wireless computer nw that connects two or more devices using a wireless distribution method within a limited area, such as in school or an office building.
- It provides the facility of mobility to its users within the coverage area.
- A WLAN is one in which a mobile user can connect to a local area nw (LAN) through a wireless connections.

STANDARDS

Two standards that support WLAN

1. IEEE

2. ETSI (European Telecommunication Standards Institute)/ IETS

IEEE gives 802.11 for both 2.5 GHz and 5 GHz band.

ETSI gives HIPERLAN 1 & 2 stds. for 5 GHz band

Mobile Communication Technology according to IEEE (examples)

WiFi

Local wireless networks
WLAN 802.11

- 802.11a → 802.11h
- 802.11i/e/…/n/…/z/aa
- 802.11b → 802.11g

ZigBee

Personal wireless nw
WPAN 802.15

- 802.15.4 → 802.15.4a/b/c/d/e/f/g
- 802.15.5, .6 (WBAN)
- 802.15.3 → 802.15.3b/c
- 802.15.2
- 802.15.1

Bluetooth

Wireless distribution networks
WMAN 802.16 (Broadband Wireless Access) **WiMAX**

+ Mobility
[802.20 (Mobile Broadband Wireless Access)]
802.16e (addition to .16 for mobile devices)

Charactristics of wireless LANs

Advantages

- Characteristics of wireless LANs
- very flexible within the reception area
- Ad-hoc networks without previous planning possible
- (almost) no wiring difficulties (e.g. historic buildings, firewalls)
- more robust against disasters like, e.g., earthquakes, fire - or users pulling a plug…
- Cost effective – Adding new user will not increase further cost.

Disadvantages

- typically very low bandwidth compared to wired networks (1-10 Mbit/s) due to shared medium
- Provides lower transmission quality compared to wired LANs.
- High error rates due to interference. Hence low Qos
- Provides less safety & security as information transmitted on the radio channel

Comparison: infrared vs. radio transmission

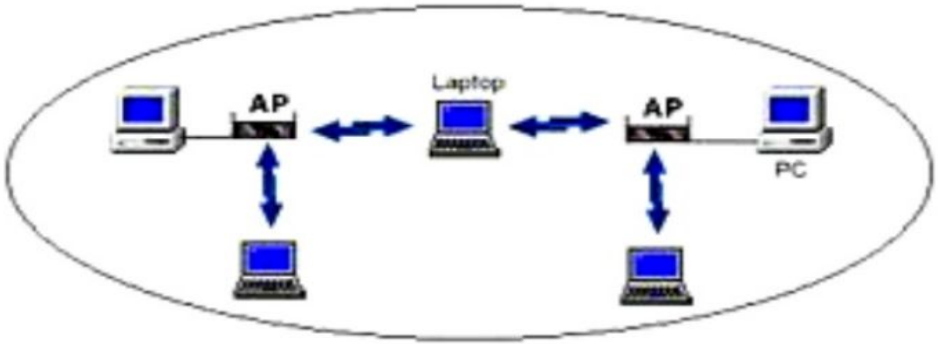
- **Infrared**
  - **uses IR diodes, diffuse light, multiple reflections (walls, furniture etc.)**
- **Advantages**
  - **simple, cheap, available in many mobile devices**
  - **no licenses needed**
  - **simple shielding possible**
- **Disadvantages**
  - **interference by sunlight, heat sources etc.**
  - **Cannot penetrate obstacles**
  - **low bandwidth**
- **Example**
  - **IrDA (Infrared Data Association) interface available everywhere, TV remote control**

- Radio
  - typically using the license free ISM band at 2.4 GHz
- Advantages
  - Higher transmission rate (11-54 Mbits)
  - coverage of larger areas possible (radio can penetrate walls, furniture etc.)
- Disadvantages
  - very limited license free frequency bands
  - interference with other electrical devices
- Example
  - Bluetooth

Wirless Nework Seup

- There are two types of wireless network types.
  - Infrastructure
  - Ad-hoc

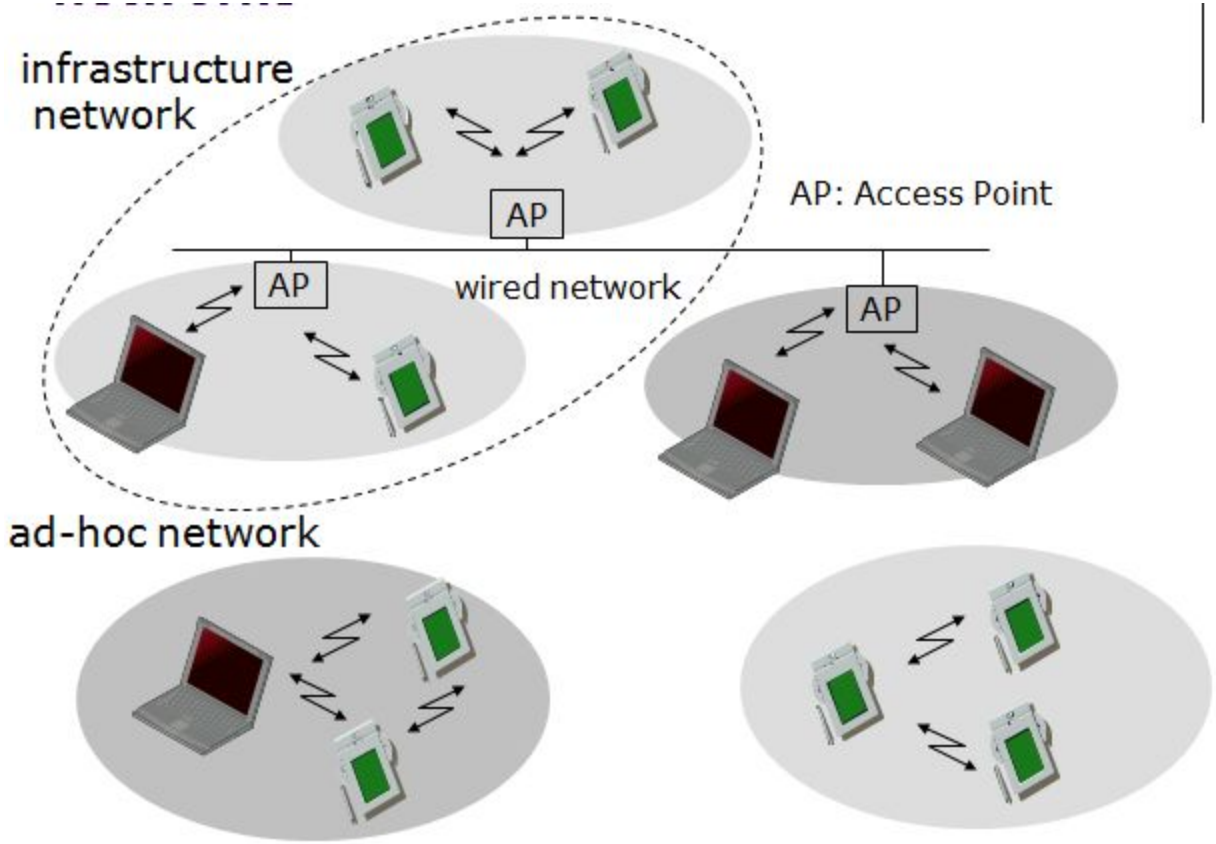
- Infrastructure
  - Referred to as a “hosted” or “managed” wireless network.
  - Consists of one or more access points (known as wireless routers) being conneced to an existing network.
  -



Ad-hoc Wireless Nework

- Also referred to as an “unmanaged” or “peer to peer” wireless network..
- It consists of each device connecting directly to each other.

Comparison: infrastructure vs. ad-hoc networks



Infrastructure – based WLAN

•A wireless n/w is connected with other wire line n/w

•Wireless nodes communicate with each other via an AP

•AP provides access to other wireless or wired n/w and also controls the medium access.

Drawback- It is not completely flexible bcoz of the existence of a fixed part of the n/w.

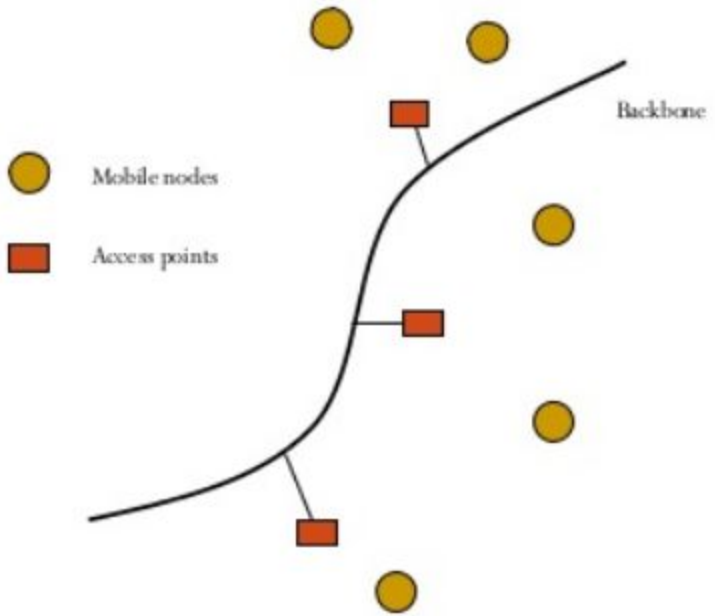
AD-HOC based WLAN

- This n/w does not have fixed part of the n/w
- Do not consist of any wired connections with other n/ws
- Temporary network composed of mobile nodes without preexisting communication infrastructure, such as Access Point (AP) and Base Station (BS).
- They are completely connected with other n/ws if they remain in the range of each other. Terminals Work as n/w nodes.
- Devices can communicate with another node that is immediately within their radio range or one that is outside their radio range.
- For the later scenario, an intermediate node is used to relay or forward the packet from the source toward the destination.
- An adhoc wireless network is self-organizing and adaptive.
- this means that a formed network can be de-formed on the fly without the need for any system administration.

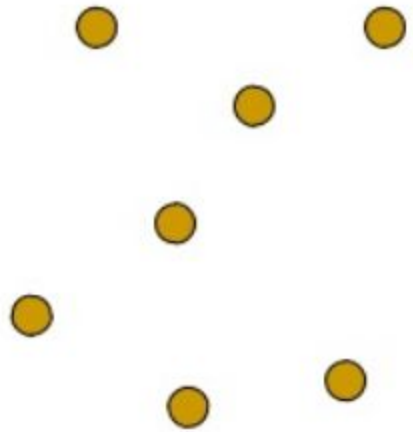
Classification of Wireless Networks

- ***Base Station*** :: all communication through an ***Access Point*** **(AP)** .Other nodes can be fixed or mobile.
- ***Infrastructure Wireless*** :: AP is connected to the wired Internet.
- ***Ad Hoc Wireless*** :: wireless nodes communicate directly with one another.
- ***MANETs* (Mobile Ad Hoc Networks) ::** ad hoc nodes are mobile.

Mobile Ad Hoc Networks (MANET)



Wireless Mobile Network



MANET

Chapter 4

4.2 IEEE 802.11

Prof. Monali Shetty

Lecture 38

27-10-20

9 AM

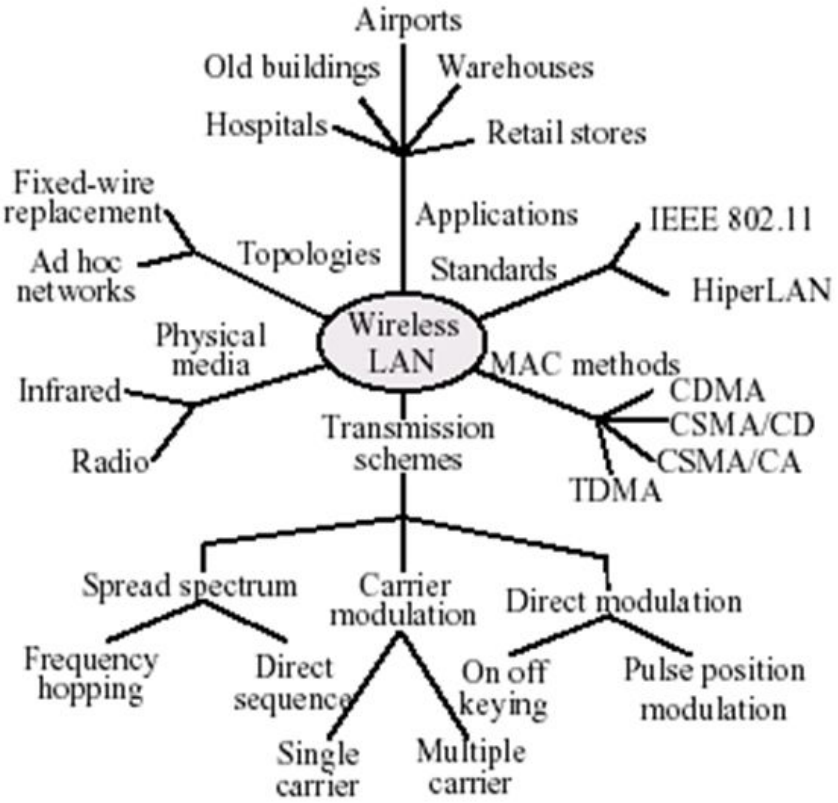
Syllabus

IEEE 802.11:System architecture , Protocol architecture , Physical layer, Medium access control layer, MAC management, 802.11a, 802.11b

Previous Quesion Paper

Q. Compare HIPERLAN 2, Bluetooth, IEEE 802.11
Q. Explain Power management in IEEE 802.11 infrastructure networks and ad-hoc networks
Q. Explain in detail IEEE 802.11 MAC sublayer

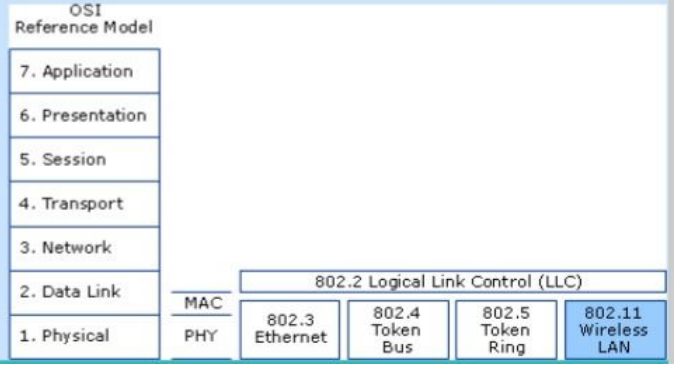
Technology Tree for Wireless LAN



IEEE 802.11 System Architecture

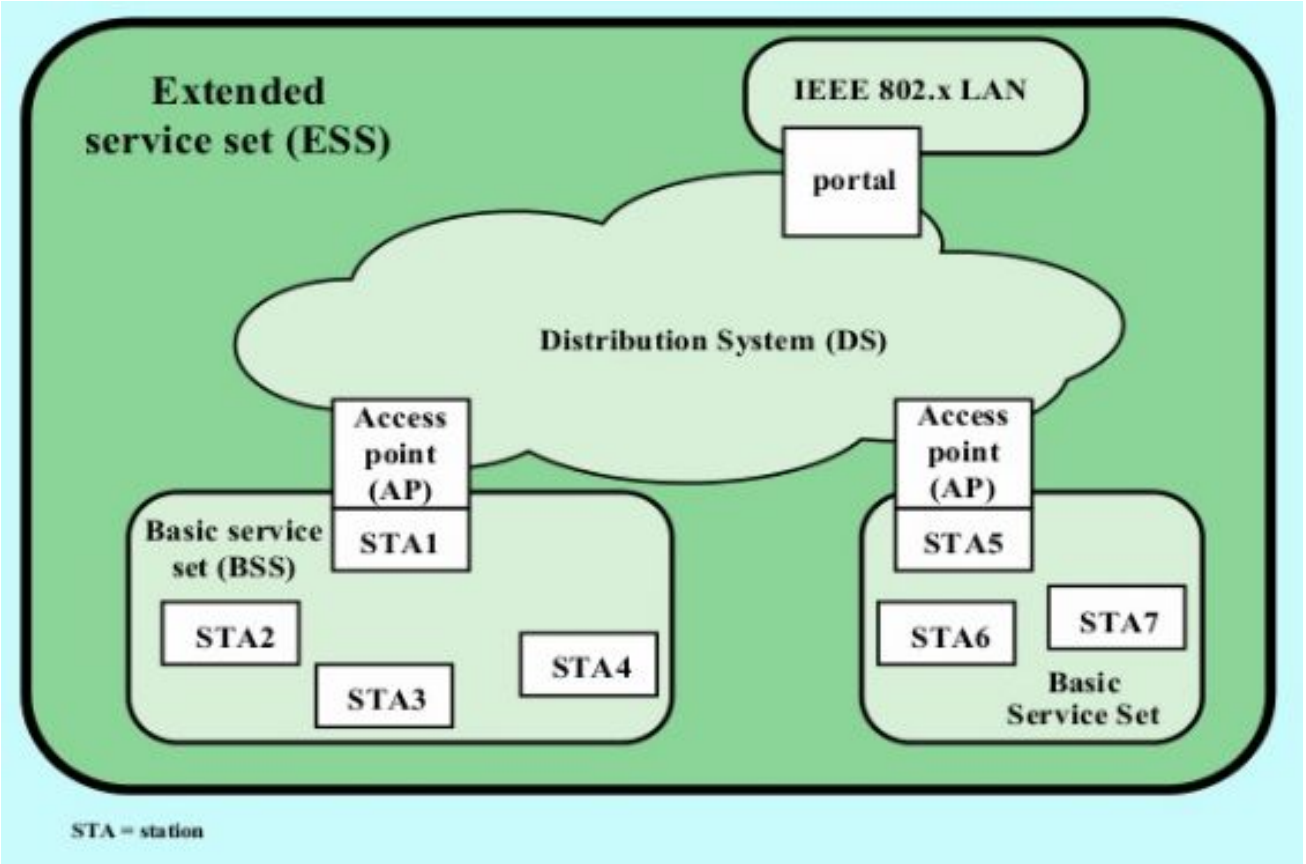
IEEE 802.11 Architecture and Services

- In 1990, IEEE 802 Committee formed a new working group, IEEE 802.11, specifically devoted to wireless LANs, with a charter to develop a MAC protocol and physical medium specification



Wi-Fi Alliance

- There is always a concern whether products from different vendors will successfully interoperate
- Wireless Ethernet Compatibility Alliance (WECA)
  - Industry consortium formed in 1999
- Renamed the Wi-Fi Alliance
  - Created a test suite to certify interoperability for 802.11 products



IEEE 802.11 Architecture

IEEE 802.11 Architecture and Services

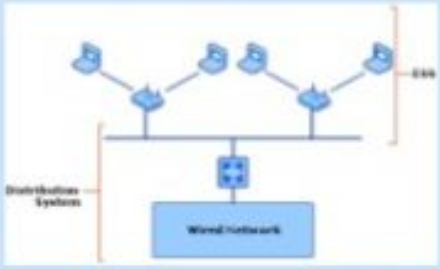
- Basic service set (BSS) consists of some number of stations executing the same MAC protocol and competing for access to the same shared wireless medium
- A BSS may be isolated or it may connect to a backbone distribution system (DS) through an access point (AP)
- In a BSS, client stations do not communicate directly with one another
- In an IBSS the stations all communicate directly
  - No AP is involved.
  - An IBSS is typically an ad hoc network.

IEEE 802.11 Architecture and Services

- An extended service set (ESS) consists of two or more basic service sets interconnected by a distribution system
- To integrate the IEEE 802.11 architecture with a traditional wired LAN, a portal is used

IEEE 802.11 Operating Modes

- 802.11 Infrastructure Mode
  - at least one wireless AP and one wireless client.



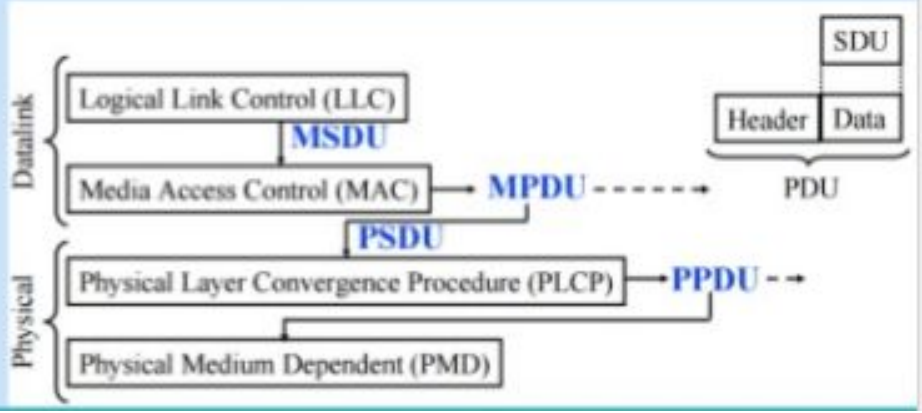
- 802.11 Ad Hoc Mode
  - wireless clients communicate directly with each other without the use of a wireless AP

IEEE 802.11 Terminology

Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations
Basic service set (BSS)	A set of stations controlled by a single coordination function
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs
Distribution system (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs
Frame	Synonym for MAC protocol data unit
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entities using the services of the physical layer
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer

IEEE 802.11 Terminology

- Each layer has Service Data Unit (SDU) as input
- Each layer makes Protocol Data Unit (PDU) as output to communicate with the corresponding layer at the other end
- SDUs may be fragmented or aggregated to form a PDU
- PDUs have a header specific to the layer



IEEE 802.11 Services

IEEE 802.11 defines nine services that need to be provided by WLAN

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Dissassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassocation	Distribution system	MSDU delivery

Chapter 4

4.2 IEEE 802.11

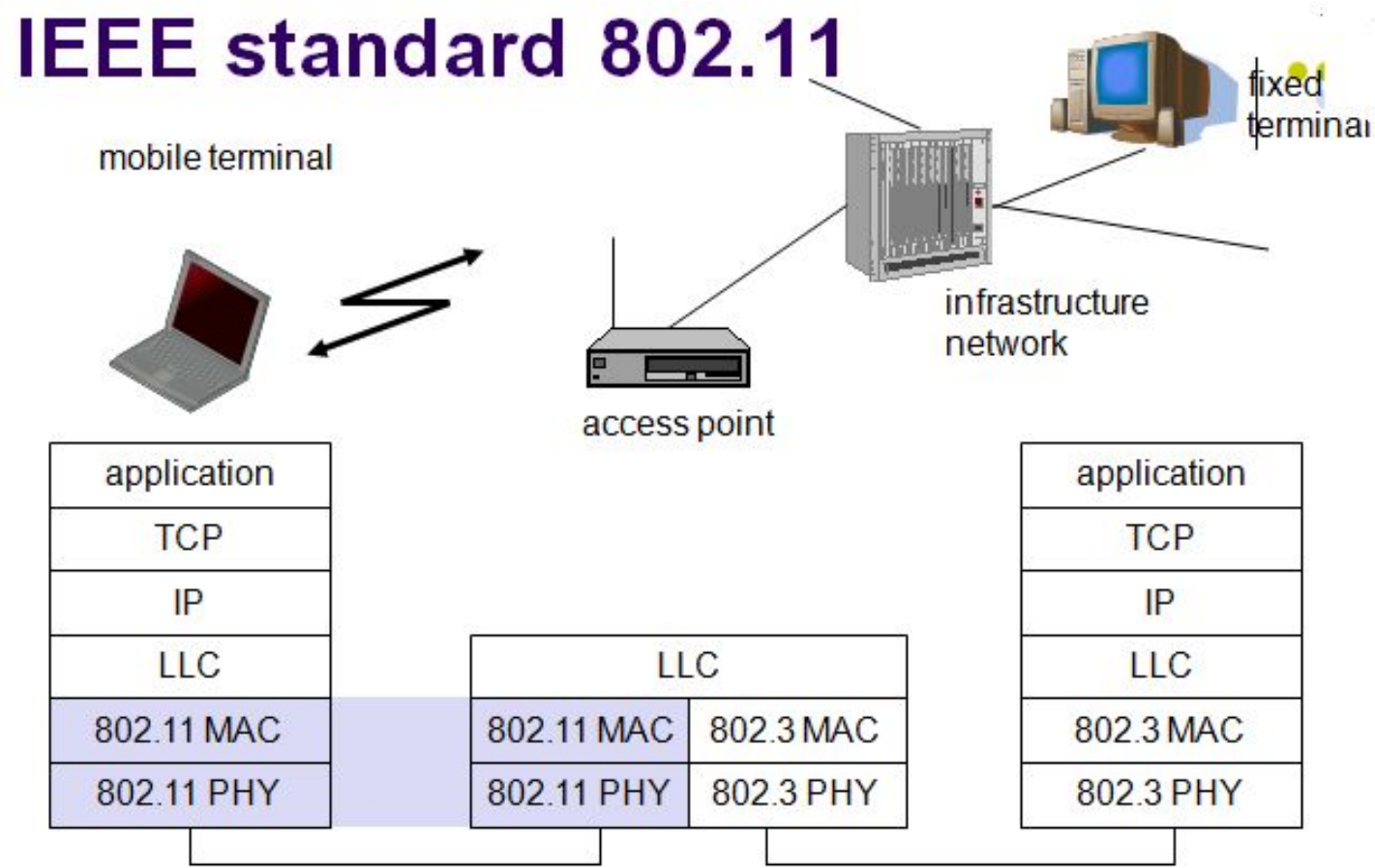
Prof. Monali Shetty

Lecture 39

28-10-20

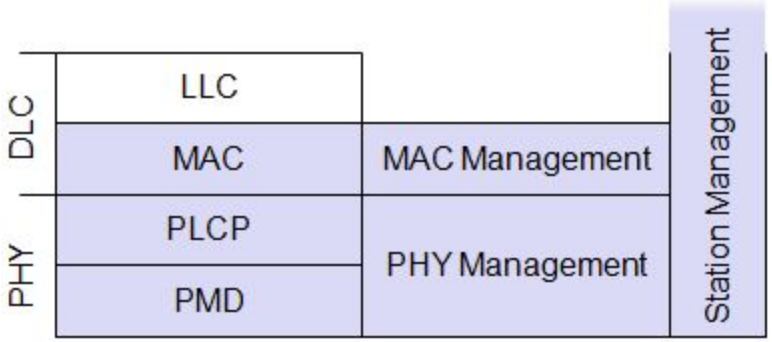
11.30 AM

IEEE 802.11 Protocol Architecture



802.11 - Layers and functions

- MAC
  - access mechanisms, fragmentation, encryption
- MAC Management
  - synchronization, roaming, MIB, power management



- PLCP Physical Layer Convergence Protocol
  - clear channel assessment signal (carrier sense)
- PMD Physical Medium Dependent
  - modulation, coding
- PHY Management
  - channel selection, MIB
- Station Management
  - coordination of all management functions

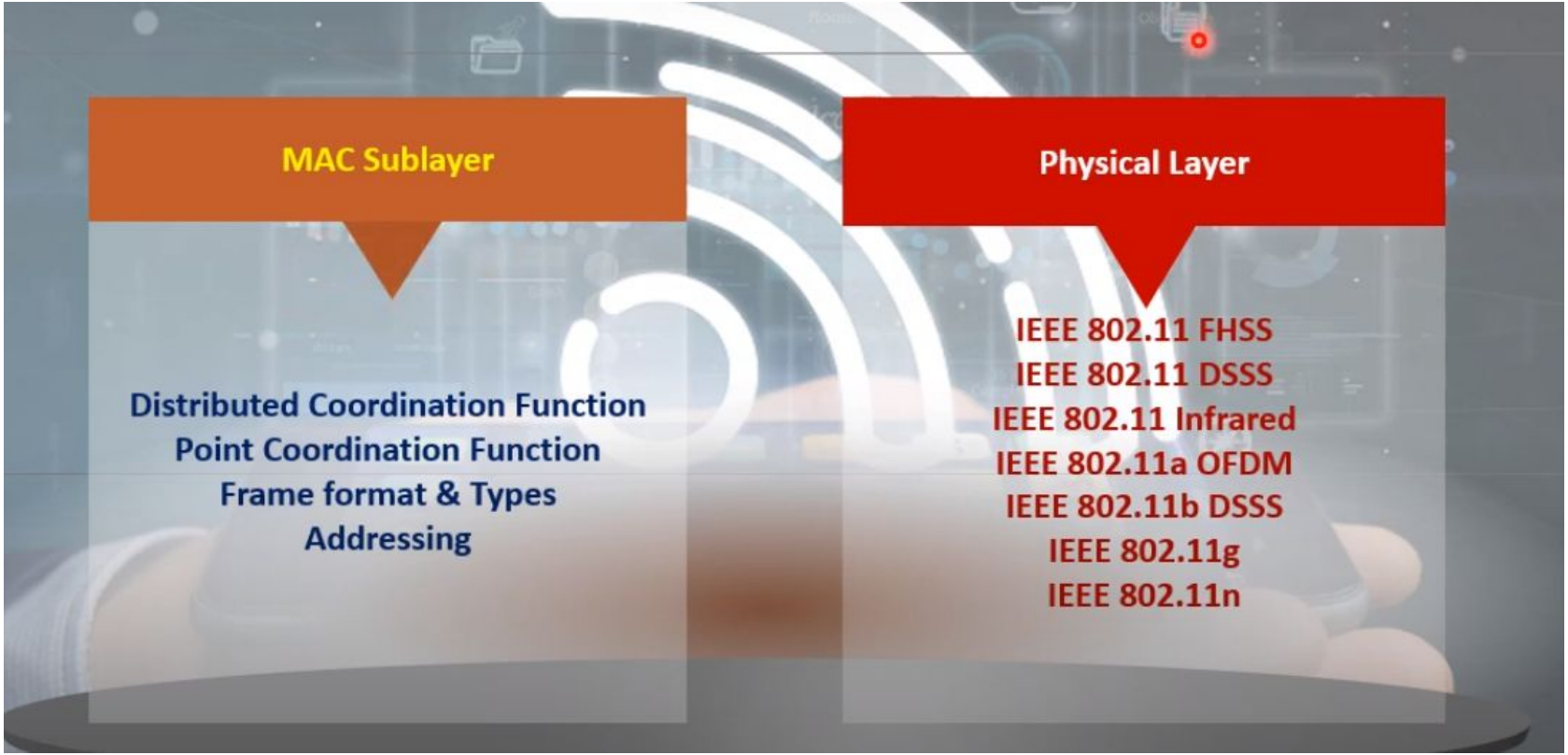
802.11 Logical architecture

- **LLC provides addressing and data link control**
- **MAC provides**
  - –access to wireless medium
    - •CSMA/CA
    - •Priority based access (802.12)
  - –joining the network
  - –authentication & privacy
  - –Services
    - •Station service: Authentication, privacy, MSDU(MAC Service Data Unit) delivery
    - •Distributed system: Association with an access point in ESS and BSS and participates to data distribution
- **Three physical layers (PHY)**
  - –FHSS: Frequency Hopping Spread Spectrum (SS)
  - –DSSS: Direct Sequence SS
  - - IR: Infrared transmission

Table *Physical layers*

IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.4 GHz	FSK	1 and 2
	DSSS	2.4 GHz	PSK	1 and 2
		Infrared	PPM	1 and 2
802.11a	OFDM	5.725 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.4 GHz	PSK	5.5 and 11
802.11g	OFDM	2.4 GHz	Different	22 and 54

MAC Sublayer and Physcial Layer- WLAN



802.11 - Physical Layer

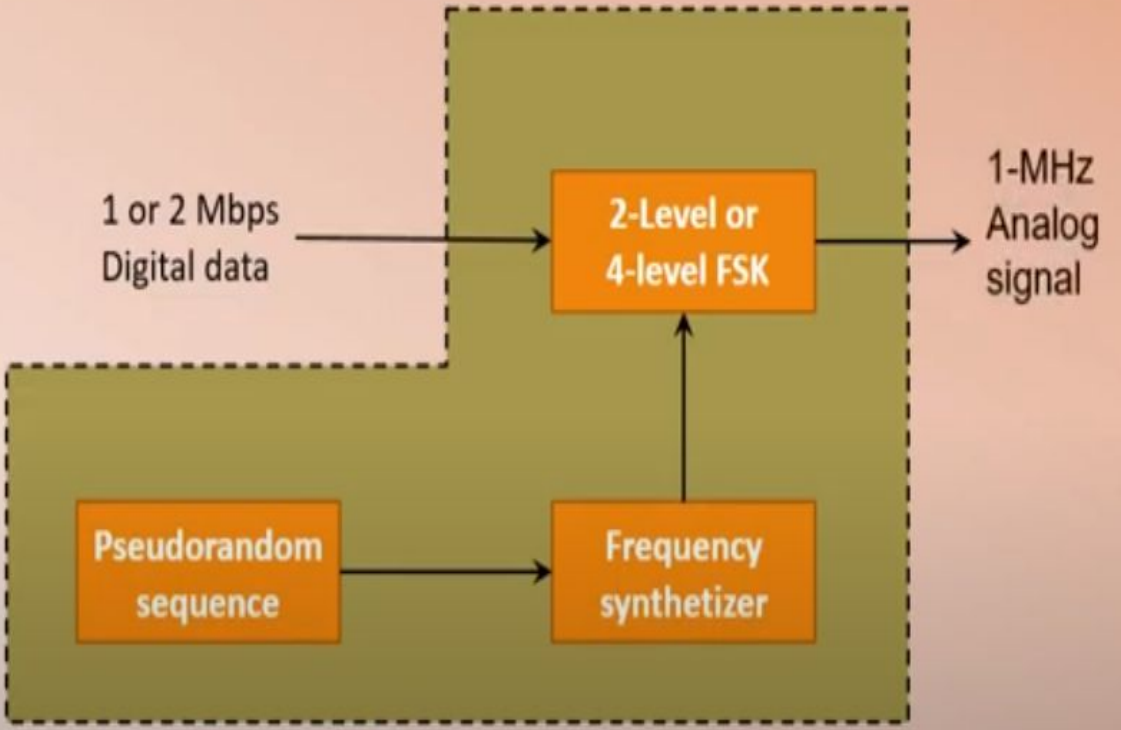
- 3 versions: 2 radio (typ. 2.4 GHz), 1 IR
  - data rates 1 or 2 Mbit/s
- **FHSS (Frequency Hopping Spread Spectrum)**
  - spreading, despreading, signal strength, typ. 1 Mbit/s
  - min. 2.5 frequency hops/s (USA), two-level GFSK modulation
- **DSSS (Direct Sequence Spread Spectrum)**
  - DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying), DQPSK for 2 Mbit/s (Differential Quadrature PSK)
  - preamble and header of a frame is always transmitted with 1 Mbit/s, rest of transmission 1 or 2 Mbit/s
  - chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
  - max. radiated power 1 W (USA), 100 mW (EU), min. 1mW
- **Infrared**
  - 850-950 nm, diffuse light, typ. 10 m range
  - carrier detection, energy detection, synchronization

Physical Layer

IEEE 802.11 Specifications

- IEEE 802.11 FHSS uses the **frequency-hopping spread spectrum (FHSS)** method
- FHSS uses the 2.400–4.835 GHz ISM band.
- The band is divided into 79 subbands of 1 MHz (and some guard bands).
- A pseudorandom number generator selects the hopping sequence.
- The modulation technique in this specification is either two-level FSK or four-level FSK with 1 or 2 bits/baud, which results in a data rate of 1 or 2 Mbps

IEEE 802.11 FHSS

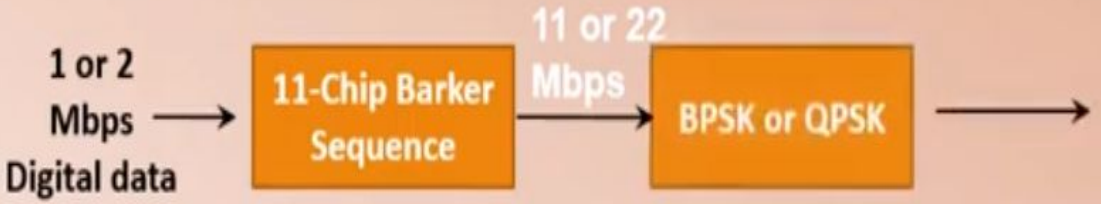


Physical Layer

IEEE 802.11 Specifications

- IEEE 802.11 DSSS uses the **direct-sequence spread spectrum (DSSS)** method, as
- DSSS uses the 2.400–4.835 GHz ISM band.
- The modulation technique in this specification is PSK at 1 Mbaud/s.
- The system allows 1 or 2 bits/baud (BPSK or QPSK), which results in a data rate of 1 or 2 Mbps

IEEE 802.11 DSSS



Physical Layer

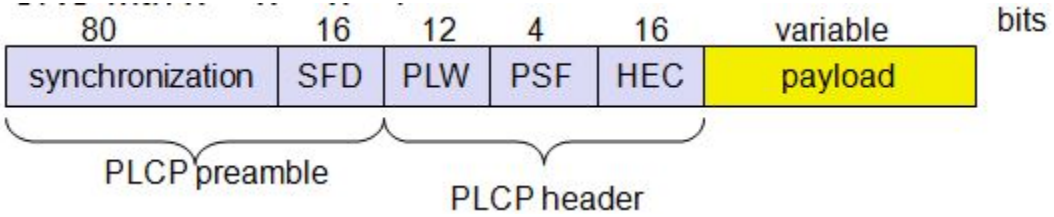
IEEE 802.11 Specifications

- IEEE 802.11 infrared uses infrared light in the range of 800 to 950 nm.
- The modulation technique is called ***pulse position modulation (PPM)***.
- For a 1-Mbps data rate, a 4-bit sequence is first mapped into a 16-bit sequence in which only one bit is set to 1 and the rest are set to 0.
- For a 2-Mbps data rate, a 2-bit sequence is first mapped into a 4-bit sequence in which only one bit is set to 1 and the rest are set to 0.
- The mapped sequences are then converted to optical signals; the presence of light specifies 1, the absence of light specifies 0.

IEEE 802.11 Infrared

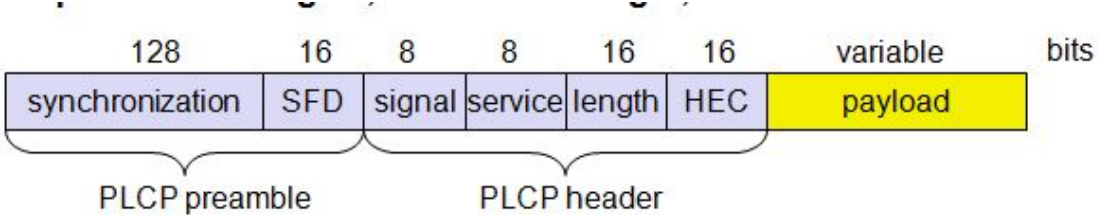
FHSS PHY packet format

- Synchronization
  - synch with 010101... pattern
- SFD (Start Frame Delimiter)
  - 0000110010111101 start pattern
- PLW (PLCP_PDU Length Word)
  - length of payload incl. 32 bit CRC of payload, PLW < 4096
- PSF (PLCP Signaling Field)
  - data of payload (1 or 2 Mbit/s)
- HEC (Header Error Check)
  - CRC with $x^{16}+x^{12}+x^{5}+1$



DSSS PHY packet format

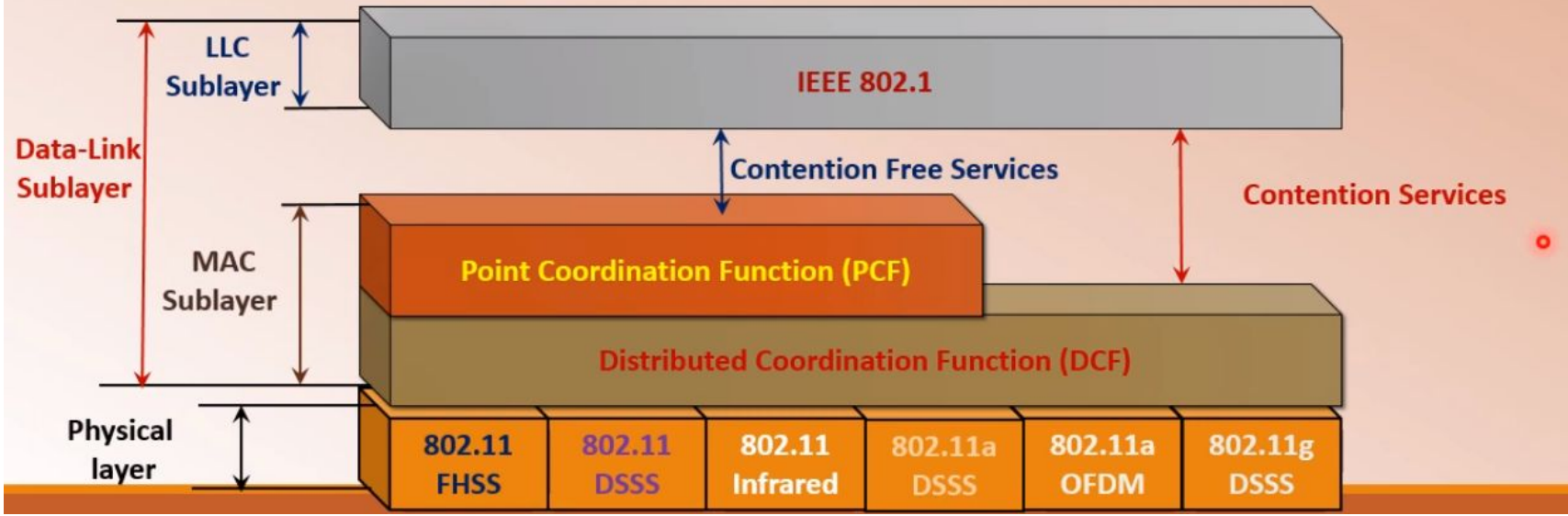
- Synchronization
  - synch., gain setting, energy detection, frequency offset compensation
- SFD (Start Frame Delimiter)
  - 1111001110100000
- Signal
  - data rate of the payload (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)
- Service
  - future use, 00: 802.11 compliant
- Length
  - length of the payload
- HEC (Header Error Check)
  - protection of signal, service and length, $x^{16}+x^{12}+x^{5}+1$



MAC Sublayer

IEEE 802.11 defines two MAC sublayers:

- The Distributed Coordination Function (DCF)
- The Point Coordination Function (PCF)



Chapter 4
4.2 IEEE 802.11

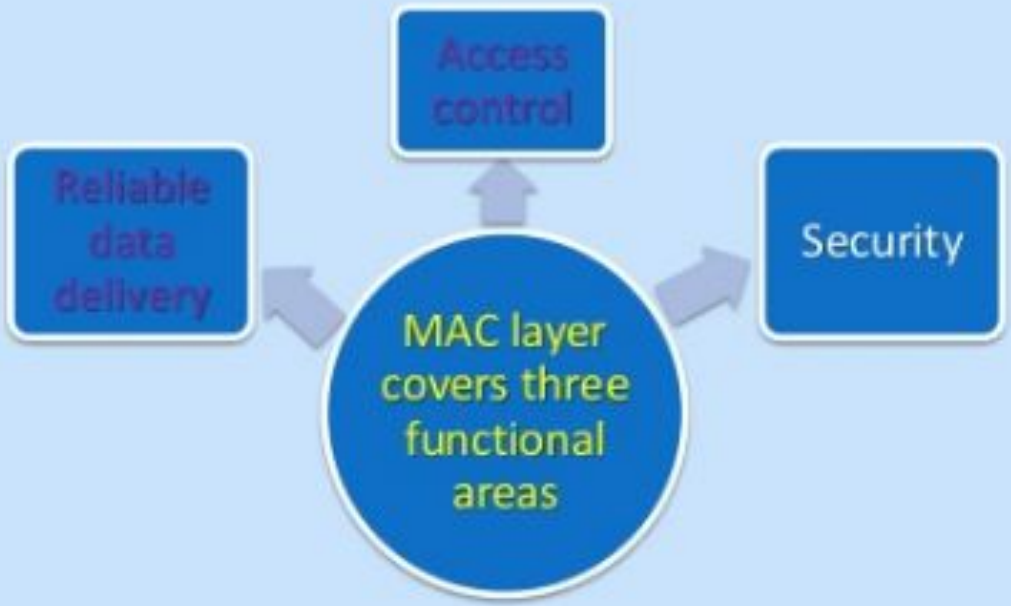
Prof. Monali Shetty

Lecture 40

29-10-20

10 AM

IEEE 802.11 Medium Access Control

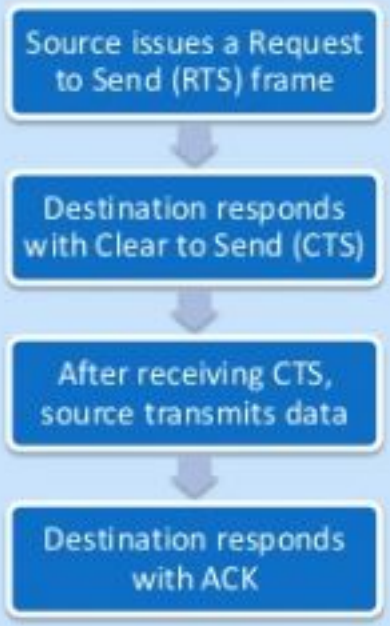


Reliable Data Delivery

- 802.11 physical and MAC layers unreliable
  - Noise, interference , and other propagation effects result in the loss of significant number of frames
  - The issue can be addressed at a higher layer such as TCP
- 802.11 includes frame exchange protocol
  - Station receiving frame returns acknowledgment (ACK) frame
  - Exchange treated as atomic unit
  - If no ACK within short period of time, retransmit

Reliable Data Delivery

- To further enhance reliability, a four frame exchange may be used
  - RTS alerts all stations within range of source that exchange is under way
  - CTS alerts all stations within range of destination
  - Other stations don't transmit to avoid collision
  - RTS and CTS exchange is a required function of MAC but may be disabled



MAC Algorithm

- Two types of proposals for a MAC algorithm
  - Distributed access protocol which distribute the decision to transmit over all the nodes using a carrier sense mechanism
  - Centralized access protocol which involve regulation of transmission by a centralized decision maker

Security

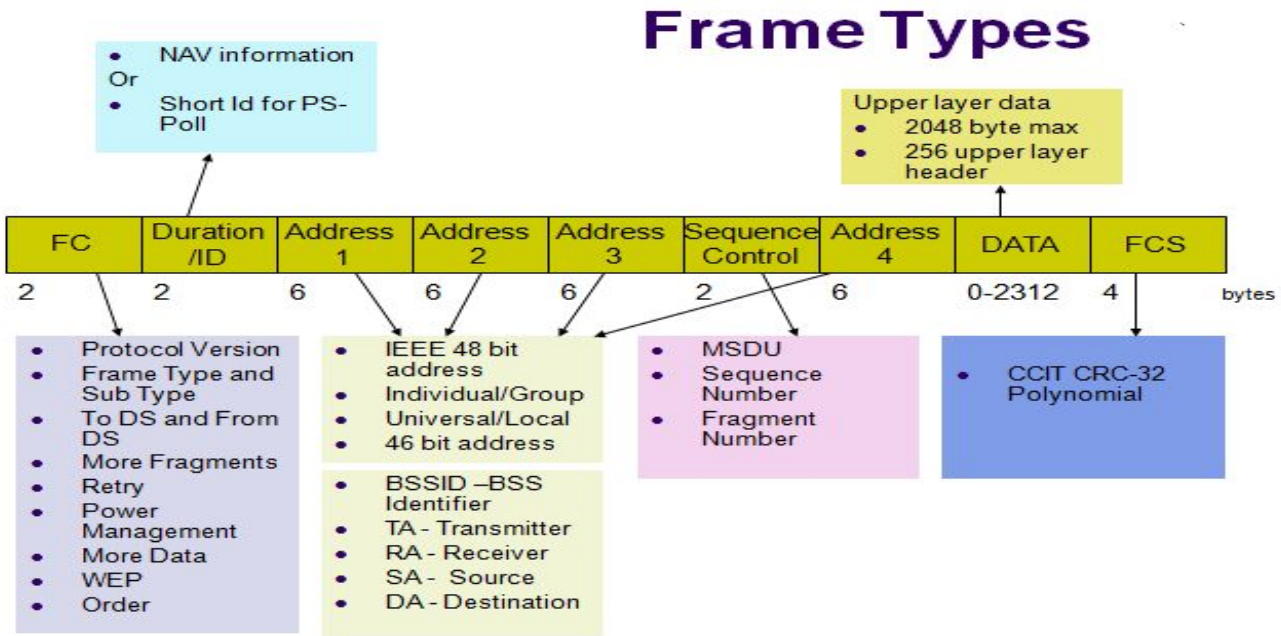
- Another function of the 802.11 MAC is to protect the data being delivered by providing security and privacy services.
- In theory, spread spectrum radio signals are inherently difficult to decipher without knowing the exact hopping sequences or direct sequence codes used.
- Security is provided by the authentication services and by wireless Equivalent Privacy (WEP), which is an encryption service for data delivered on the WLAN.
- The IEEE 802.11 standard specifies optional security called "**W**ired **E**quivalent **P**rivacy" whose goal is that a wireless LAN offer privacy equivalent to that offered by a wired LAN.

802.11 - MAC layer I - DFWMAC

- Traffic services
  - Asynchronous Data Service (mandatory)
    - exchange of data packets based on “best-effort”
    - support of broadcast and multicast
  - Time-Bounded Service (optional)
    - implemented using PCF (Point Coordination Function)
- Access methods
  - DFWMAC-DCF CSMA/CA (mandatory)
    - collision avoidance via randomized „back-off“ mechanism
    - minimum distance between consecutive packets
    - ACK packet for acknowledgements (not for broadcasts)
  - DFWMAC-DCF w/ RTS/CTS (optional)
    - Distributed Foundation Wireless MAC
    - avoids hidden terminal problem
  - DFWMAC- PCF (optional)
    - access point polls terminals according to a list

802.11 MAC Frame Structure

- Types
  - control frames(01), management frames(00), data frames(10)
- Subtype:- (control)RTS ,CTS, user data(0000)
- Sequence numbers
  - important against duplicated frames due to lost ACKs
- Addresses
  - receiver, transmitter (physical), BSS identifier, sender (logical)



MAC Sublayer

Frame Format

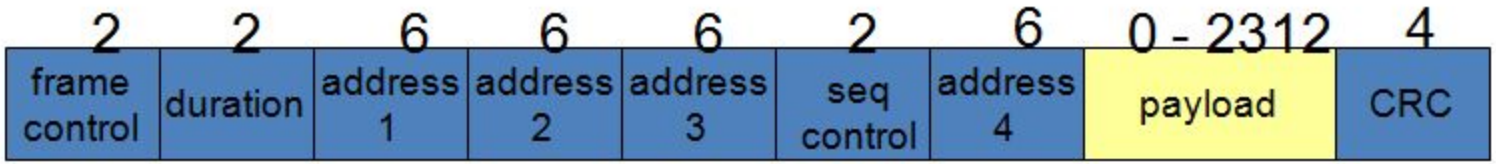
- The MAC layer frame consists of nine fields

2 Bytes

FC

Field	Explanation
Version	The current version is 0.
Type	Type of information: management (00), control (01), or data (10).
Subtype	Defines the subtype of each type (see).
To DS	Defined later.
From DS	Defined later.
More flag	When set to 1, means more fragments.
Retry	When set to 1, means retransmitted frame.
Pwr mgt	When set to 1, means station is in power management mode.
More data	When set to 1, means station has more data to send.
WEP	Wired equivalent privacy. When set to 1, means encryption implemented.
Rsvd	Reserved.

802.11 frame: addressing



Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

MAC Sublayer

Addressing Mechanism

The IEEE 802.11 addressing mechanism specifies four cases, defined by the value of the two flags in the FC field, *To DS* and *From DS*

Each flag can be either 0 or 1, resulting in four different situations

The interpretation of the four addresses (address 1 to address 4) in the MAC frame depends on the value of these flags

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

MAC Sublayer

Frame Types

A wireless LAN defined by IEEE 802.11 has three categories of frames:

- Management frames
- Control frames
- Data frames

Management frames are used for the initial communication between stations and access points.

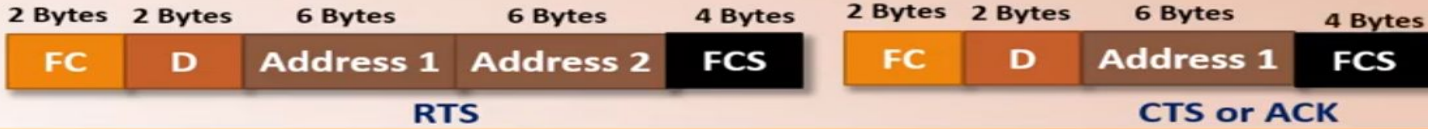
MAC Sublayer

Frame Types

A wireless LAN defined by IEEE 802.11 has three categories of frames:

- Management frames
- Control frames
- Data frames

Control frames are used for accessing the channel and acknowledging frames.
For control frames the value of the type field is 01



Subtype	Meaning
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

MAC Sublayer

Frame Types

A wireless LAN defined by IEEE 802.11 has three categories of frames:

- Management frames
- Control frames
- Data frames

Data frames are used for carrying data and control information

Chapter 4

4.5 Bluetooth

Prof. Monali Shetty

Lecture 41

3-11-20

9 AM

Syllabus

Bluetooth: Introduction, User Scenario, Architecture, protocol stack

Bluetooth Technology - Introduction

- It is a wireless technology based on mobile computing technology. Being an open wireless technology Standard, it is used to send or receive data to connected device.
- In 10th century, Harald Bluetooth the king of Denmark united Norway and Denmark into a single kingdom. Apparently he got that name from his penchant for blueberries.

- It is also known as IEEE 802.15 standard.

- The data can send or receive at a certain distance . It uses a bandwidth of 2.4 to 2.485 GHz.

- The developing unit of this technology is a group of companies called a special Interest Group which was formed in 1998. The companies are Ericsson, Intel, IBM, Nokia, Toshiba

- The range of bluetooth technology over which data can be exchanged is less than 10 mtr but the latest version Bluetooth 5.0 can exchange data in a range of about 40-400 mtrs.

- The speed at which data transmission occur is around 1 Mbps. Version 2 provides speed upto 2.1 Mbps.

- Communication devices typically belong to one individual or group
    - Sometimes categorized as Personal Area Network (PAN)

- Used for very short range communication between mobile phones, PDAs, notebook computers and other personal or peripheral devices to replace cables connecting electronic devices.

- Advantages:
  - Wireless Technology
  - It is used widely across countries and almost by everyone.
  - Robust
  - Low energy consumption
  - It has simple features.
  - It has the ability to keep our information private.

- Disadvantages:
  - Low in bandwidth
  - Data transmission range is a constraint as it is very less.

Applications of Bluetooth

- Wireless control of and communication between a mobile phone and a **hands free headset**. This was one of the earliest applications to become popular.
- **Wireless communication with pc** input and output devices, the most common being the mouse, keyboard and printer.
- **Transfer of files**, contact details, calendar appointments, and reminders between devices with obex.
- In 2004 released cars like toyota prius & lexus ls 430 have **hands free call system.**
- Sending small advertisements from bluetooth-enabled advertising hoardings to other, discoverable, bluetooth devices.
- In game consoles like sony's playstation 3 and psp go, use bluetooth for their respective wireless controllers.

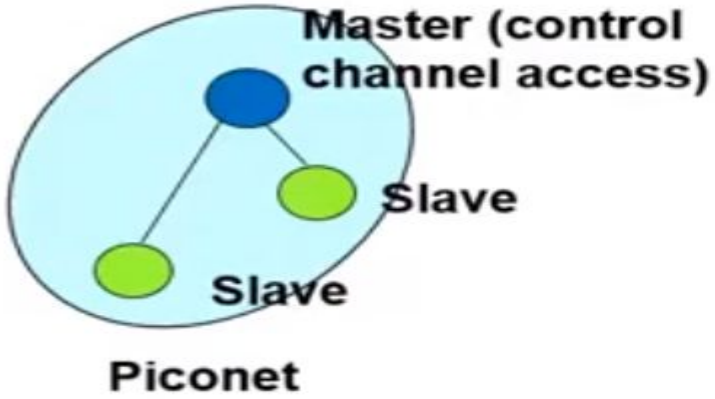
Different Versions of Bluetooth

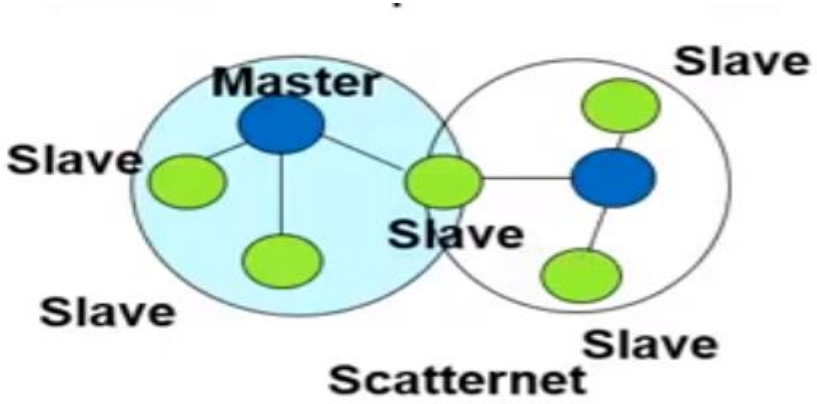
- This are the different versions of bluetooth technologies we have since 1999.

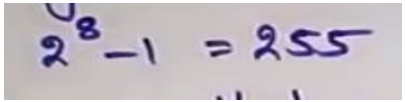
1. Bluetooth v1.0 and v1.0B (with mandatory bluetooth hardware device address)
2. Bluetooth v1.1 (ratified as IEEE standard 802.15.1-2002)
3. Bluetooth v1.2 (faster connection and discovery)
4. Bluetooth v2.0 + EDR (enhanced data rate)
5. Bluetooth v2.1 (secure simple pairing-SSP)
6. Bluetooth v3.0 (high speed data transfer)
7. Bluetooth v4.0 (low energy consumption – recently used in apple i -phone 4S)

Bluetooth Technology : Architecture

- An architecture of Bluetooth is called as “Piconet”
- Two or more devices sharing the same channel form a **piconet**.
- Piconet offers the technology with the help of which data transmission occurs, based on its nodes i.e **Master node and Slave nodes.**
- A master node is a node from which data is being sent and slave node in which the data is received.
- Ultra-high frequency and short wavelength radio waves, through which data transmission occurs.





- The piconet used the concept of multiplexing and spread spectrum i.e It is a combination of code division multiple access and frequency hopping spread spectrum.
- Bluetooth architecture defines two types of networks
  - Piconet
  - Scatternet
- Piconet: It is a bluetooth network that consists of 1 primary (master) node and 7 active secondary (slave) nodes.
- Maximum no. of nodes in piconet :: - > 8
- Maximum no. of devices that can be paired 

- No. of devices that can be parked - **infinite**
- A slave can be parked: set to an inactive , low-power state.
- A parked node is a node which is ready to connected and standby node is a node which can either become a slave or parked or either remains idle/disconnected.
- Two or more piconets form a **scatternet.**
- **Data transmission can occur only between master and slave.**
- If the connection from master node gets disconnected , the whole piconet gets disconnected.

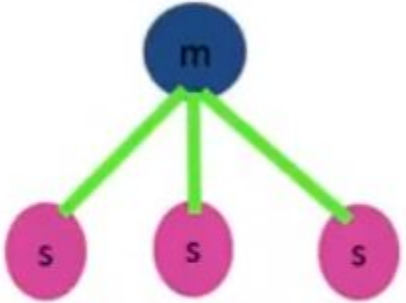
Scatter-net:

- ➔ It is formed by combination of piconets
- ➔ A slave in one piconet can act as a master or primary in other piconet.

- Master
  - Device in Piconet whose clock and hopping sequence are used to synchronize all other devices (slaves) in the Piconet.
  - It also carries out Paging procedure and also Connection Establishment.
- Slaves
  - Units within the piconet that are synchronized to the master via its clock and hopping sequence.
  - After connection establishment, Slaves are assigned a temporary 3 bit member address to reduce te no. of addressing bits required

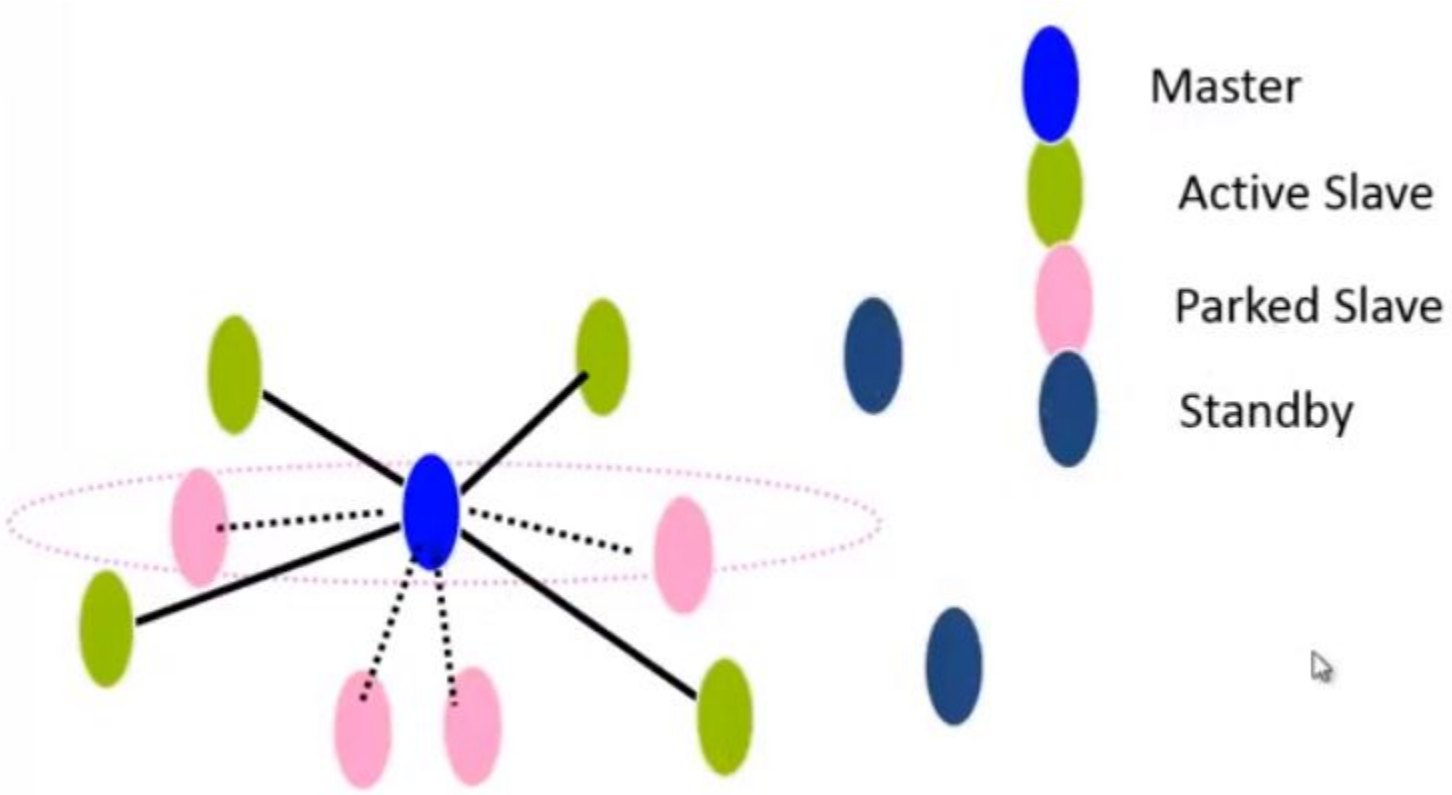
Piconets

- Point to Point Link
  - Master - slave relationship
  - Bluetooth devices can function as masters or slaves

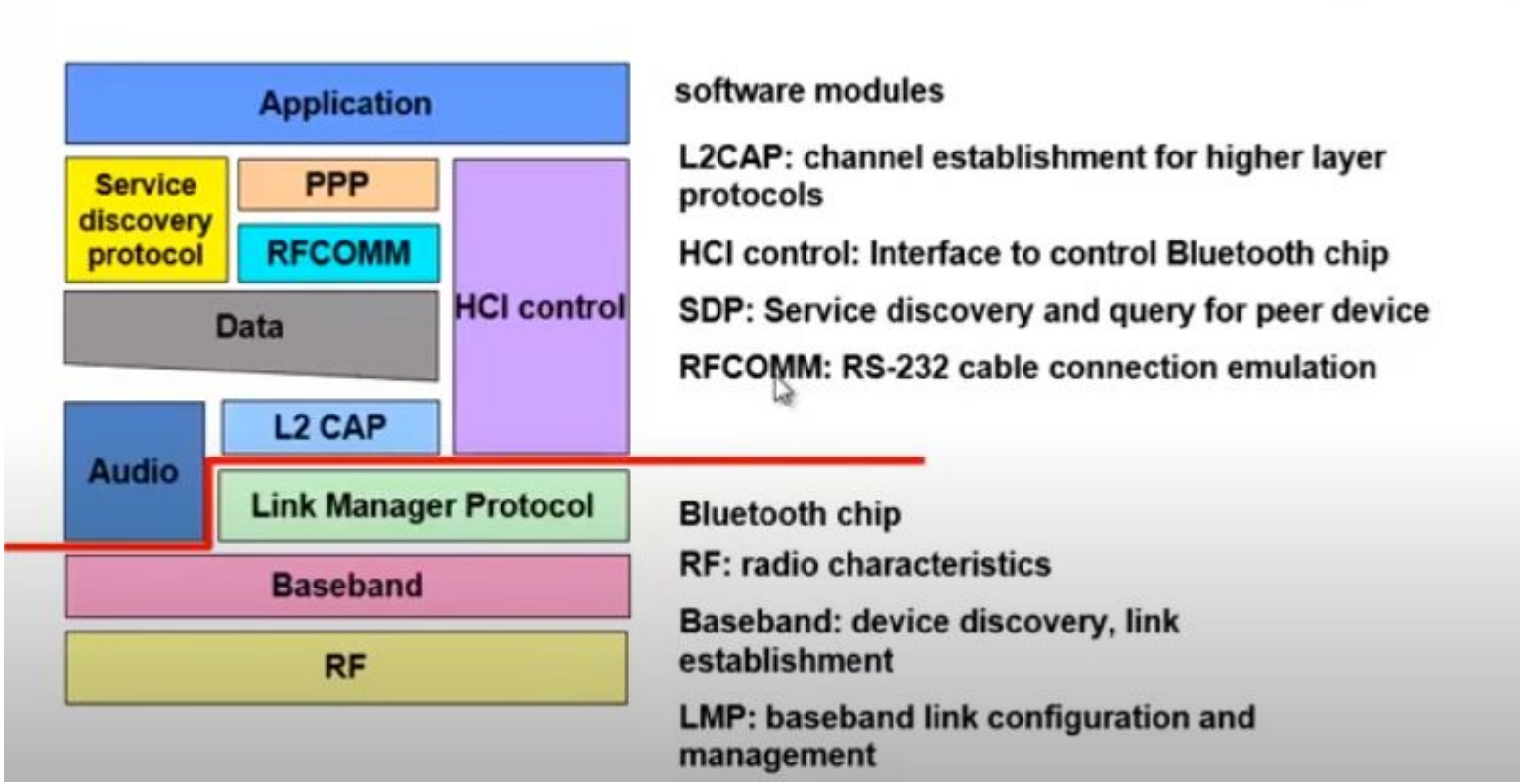


- Piconet
  - It is the network formed by a Master and one or more slaves (max 7).
  - Each piconet is defined by a different hopping channel to which users synchronize to.
  - Each piconet has max capacity (1 Mbps).
  - Hopping pattern is determined by the master.

Piconet Structure



Protocol Stack in Bluetooth



Protocol Architecture

- Protocol Architecture consists of following:

1. Core Protocols
2. Cable Replacement Protocols
3. Telephony Control Protocols
4. Adopted protocols

Core Protocols

- Core Protocols include:

1. Radio
2. Baseband
3. Link Manager Protocol
4. Logical Link Control and Adaption Protocol (L2CAP)
5. Service Discovery Protocol

Core Protocols

- **Radio:** This protocol specifies the detail of the air interface, including frequency, the use of frequency hopping, modulation scheme, and transmit power.
- **Baseband:** Addressing scheme, packet frame format , timing and power control algorithms required for establishing connection between Bluetooth devices within piconet is defined in this part of protocol specification.

Core Protocols

- **Link Manager Protocol**: It is responsible to establish link between Bluetooth devices and to maintain the link between them. This protocol also includes authentication and encryption specifications. Negotiation of packet sizes between devices can be taken care by this.
- **Logical Link Control and Adaption Protocol (L2CAP):** Adapts upper layer frame to baseband layer frame format and vice versa. L2CAP take care of both connection oriented and connectionless services.
- **Service Discovery Protocol:** Device information, services, and the characteristics of the services can be queried to enable the establishment of a connection between two or more Bluetooth devices.

Cable Replacement Protocol

- **RFCOMM** is the Cable Replacement Protocol included in the Bluetooth specification.
- It presents a virtual serial port that is designed to make replacement of cable technologies.
- RFCOMM enables the replacement of serial port with minimum of modification of existing devices.
- It provides for binary data transport and emulates RS-232 control signals over the Bluetooth baseband.

Telephony Control Protocols

- **TCS BIN:** Telephony Control Specification – Binary, is a bit-oriented protocol that defines the call control signaling for the establishment of speech and data cells between Bluetooth devices. It defines Mobility management procedures for handling group of Bluetooth TCS devices.
- **Mobility management:** It is one of the major functions of a network that allows mobile phones to work and to track where the subscribers are, allowing calls, SMS and other mobile phone services to be delivered to them.

Adapted Protocols

- These protocols are already defined by other standard bodies which are incorporated without any change in the Bluetooth protocol stack architecture.
- Adapted Protocols include:

1. PPP (Point-to-Point Protocol)
2. TCP / UDP / IP
3. OBEX (Object Exchange)
4. WAE / WAP

- **OBEX (Object Exchange):** is a session level communications protocol that facilitates the exchange of binary objects between devices. It is maintained by the Infrared Data Association but has also been adopted by the Bluetooth Special Interest Group and the SyncML wing of the Open Mobile Alliance (OMA).
- Its functionality is similar and simpler to that of HTTP.
- HTTP is normally layered above a TCP/IP link. OBEX can also be, but in Bluetooth, it is implemented on a Baseband/ ACL/ L2CAP/ RFCOMM stack.

- **WAE/ WAP (Wireless Application Environment/Wireless Application Protocol) :** WAE specifies an application framework for wireless devices and WAP is an open standard to provide mobile users access to telephony and information services.

Chapter 4

4.4 HiperLAN 1 & HiperLAN 2

Prof. Monali Shetty

Lecture 42

5-11-20

10 AM

Syllabus

HiperLAN 1 & HiperLAN 2

What is HIPERLAN?

•**High Performance Radio Local Area Networks**
•HIPERLAN type 1 or called HIPERLAN/1 is a standard, established in 1996 by ETSI.

•Goal: to achieve higher data rate than IEEE 802.11 data rates and to be used in ad hoc networking of portable devices

•Support asynchronous data transfer, carrier-sense multiple access with collision avoidance (CSMA/CA), no QoS guaranteed.
•
•Products

- ❖ Proxim's High Speed RangeLAN5 product family (24Mbps; 5GHz; QoS guaranteed)
- ❖ RadioLAN’s products for indoor wireless communication (10Mbps; 5GHz; Peer-to-Peer Topology)

Main Characteristic of HIPERLAN

- Can support both multimedia data and asynchronous data at rates as high as 23.5 Mbps
- Employs 5.15 GHz and 1.71 GHz frequency bands
- Range : 50m
- Mobility <= 10m/s
- Topology : Packet oriented
- Supports both centralized and ad-hoc communication
- HiperLANs are available in two types :
  - TYPE 1 : This has distributed MAC with QoS provisions and is based on GMSK (Gaussian minimum shift keying)
  - TYPE 2 : This has a centralized scheduled MAC and is based on OFDM.

Objectives of HiperLAN

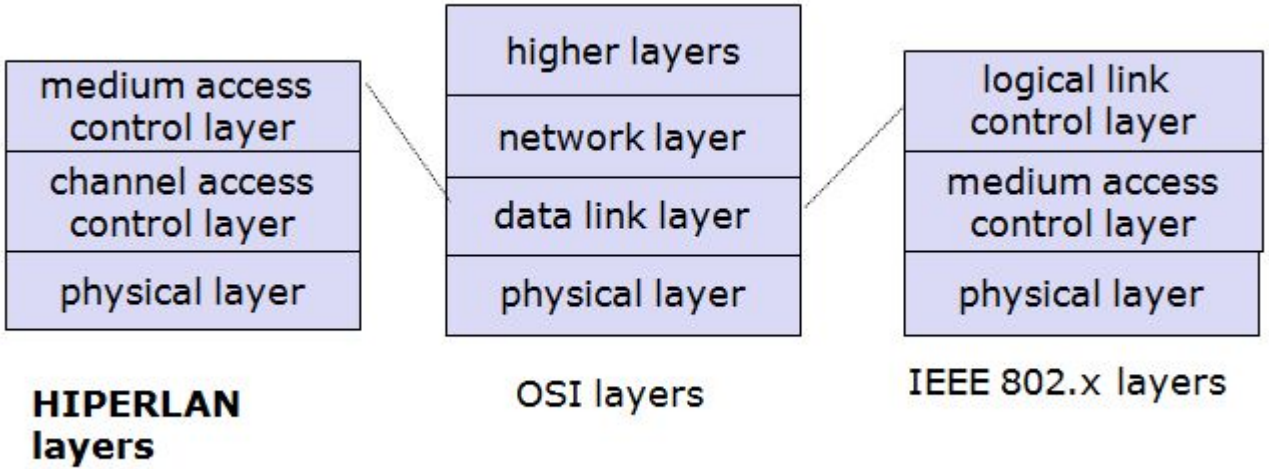
- Provide QoS to build multiservice networks
- Provide strong security
- Handoff when moving between local area and wide area
- Increase throughput
- Ease of use, deployment and maintenance
- Scalability

HIPERLAN FAMILY

•one standard cannot satisfy all requirements : range, bandwidth, QoS support, commercial constraints

	HIPERLAN 1	HIPERLAN 2	HIPERLAN 3	HIPERLAN 4
Application	wireless LAN	access to ATM fixed networks	wireless local loop	point-to-point wireless ATM connections
Frequency	5.1-5.3GHz			17.2-17.3GHz
Topology	decentralized ad-hoc/infrastructure	cellular, centralized	point-to-multipoint	point-to-point
Antenna	omni-directional		directional	
Range	50 m	50-100 m	5000 m	150 m
QoS	statistical	ATM traffic classes (VBR, CBR, ABR, UBR)		
Mobility	<10m/s		stationary	
Interface	conventional LAN	ATM networks		
Data rate	23.5 Mbit/s	>20 Mbit/s		155 Mbit/s
Power conservation	yes		not necessary	

HIPERLAN 1
20 Mbps
HIPERLAN 2
54 Mbps



HIPERLAN 2

Features

- Power Saving built into the technology
- Operates in the 5 GHz range
- Strong Security using per session keys
- DES or Triple-DES used
- Increased Throughput over other wireless technologies

(Throughput-Is how much data is passing through a network in a given time

Bandwidth-Is the amount of data that could be transferred in a given time)

- Allows convergence with other backbone technologies.

ATM – This was originally the primary use of this technology
Ethernet
3G

HIPERLAN 2 – Modes of Operation

-Operates in 2 different modes which may be used simultaneously in the same n/w

1)Centralized Mode (CM)

.Is an infrastructure based mode

.All APs are connected to core n/w and MTs are associated with Aps.

. This mode is manadatory.

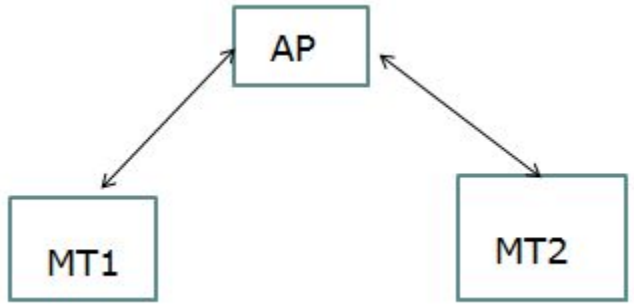
2)

Direct Mode (DM)

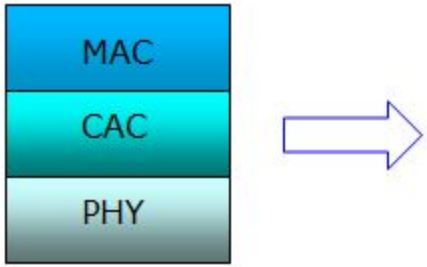
. This is the optional ad-hoc mode

. Data is directly exchanged between MTs if they can receive each other, but n/w still has to be controllled.

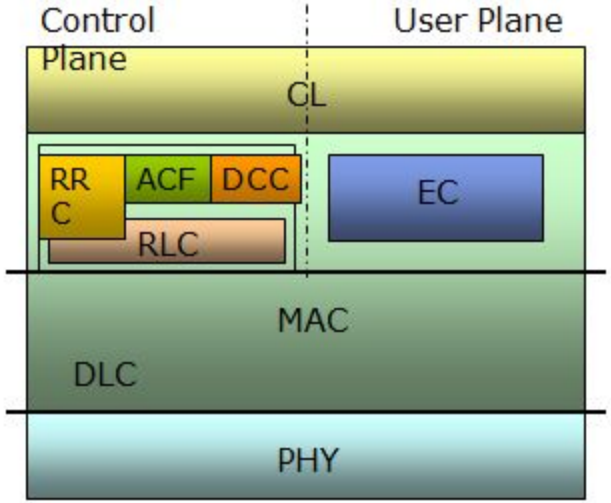
. This can be done via AP that contains a central controller (CC) or an MT that contains CC functionality



▪Architecture



HiperLAN Type 1 Reference Model



HiperLAN Type 2 Reference Model

MAC: Medium Access Sublayer
CAC: Channel Access Control Sublayer
PHY: Physical Layer
DLC: Data Link Control Layer
CL: Convergence Layer

EC: Error Control
RLC: Radio Link Control
RRC: Radio Resource Control
ACF: Association Control Function
DCC: DLC Connection Control

Parameters	HIPERLAN-1	HIPERLAN-2	802.11 WLAN
Application	Wireless LAN	Access to ATM fixed network	Wireless networks
Frequency.Band	5 GHz	5 GHz	2.4 GHZ
Maximum Data rate	23.5 Mbps	54 Mbps	2 Mbps
Topology	Decentralized adhoc/infrastructure	Cellular, centralized	Can be adhoc or infra-based
Antenna	Omni-diectional		
Range	50m	50-100m	100 m
Frequency Selection	Single carrier	dynamic frequency selection (DSS)	Frequency hopping or DSSS
Encryption	DES, 3DES	DES, 3DES	40 bit RC4

Parameters	BLUETOOTH	HIPERLAN-2	802.11 WLAN
Application	Wireless network	Access to ATM fixed network	Wireless networks
Frequency, Band	2.45GHz	5 GHz	2.4 GHZ
Maximum Data rate	1 Mbps	54 Mbps	2 Mbps
Topology	Ad-hoc	Cellular, centralized	Can be adhoc or infra-based
Error control	Arq/fec mac layer	Arq/fec phy layer	ARQ
Range	Upto 10m	50-100m	100 m
Interface	low	high	medium
Medium Access methods	Master is responsible for medium	AP centralized	CSMA/CA
Connectivity	Connection less and Oriented	Connection oriented	Connectionless
QoS (Quality of Service)	Statistical	ATM /802.1p/RSVP	PCF (optional)
Frequency Selection	Frequency hopping	dynamic frequency selection (DSS)	Frequency hopping or DSSS
Typical Outdoor Range	100 metres		
Encryption	DES, 3DES	DES, 3DES	40 bit RC4
Authentication	No	X.509	No