University of Hertfordshire

Wireless Mobile & Multimedia Networking

7COM1076

WiFi 1

Dr Tazeen Syed

t.s.syed@herts.ac.uk

School of Physics Engineering and Computer Science (SPECS)

Outline

- **IEEE 802.11 WLAN**
  - Introduction
  - Architecture
  - Services
- **IEEE 802.11 MAC Layer**
  - DCF, PCF
  - RTS, CTS, DATA ACK
- **IEEE 802.11 Physical Layer**
  - DSSS
  - FHSS
  - OFMD
  - 802.11 standards

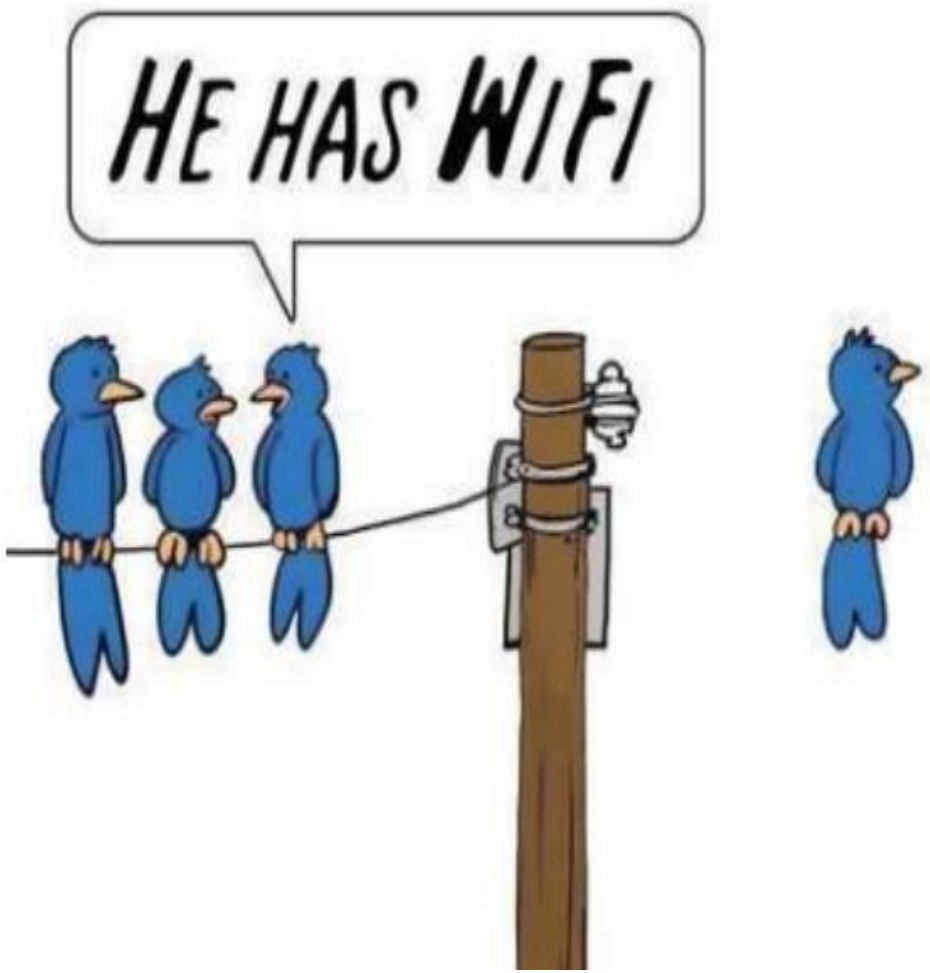
IEEE 802.11 Wireless LAN

- IEEE 802.11 is a standard specified by Institute of Electrical and Electronics Engineers (IEEE) for wireless LAN.

- It has set of rules that governs how to transmit electromagnetic waves in our LAN and communications. Everything from the frequency that we're using, to data rates that we can have, to the power that is allowed to transmit this type of signals, is governed under this standard.

IEEE 802.11 Wireless LAN

- What medium is used for wired communication?
- What medium is used for wireless communication?
- Does higher frequency give higher bandwidth, throughput and higher data rates?
- What is the issue with higher frequency?
- What is ISM band?
  - Free to transmit
  - 2.4GHZ & 5GHZ
  - They are highly occupied
  - The frequencies are high



IEEE 802.11 Wireless LAN Architecture

- **Access Point (AP)**
  Is a WLAN device that serves as a centre point of a wireless network or used as a connection point between wired and wireless networks. APs centralizes access and control over a group of wireless devices.
- **Station (STAs)**
  Are wireless devices that have access mechanism to the wireless medium
- **Basic Service Set (BSS)**

  Wireless LAN established using an Access Point and a group of stations. a group of wireless devices. All wireless devices do not communicate directly with each other but instead they communicate with the AP, and the AP forwards the frames to the destination stations. The BSS is the topology building block.

IEEE 802.11 Wireless LAN Architecture

- **Basic Service Area**

  The coverage area within which the wireless clients of the BSS may remain in communication. This area is called the Basic Service Area (BSA). If a wireless client moves out of its BSA, it can no longer directly communicate with the other wireless clients within the BSA.

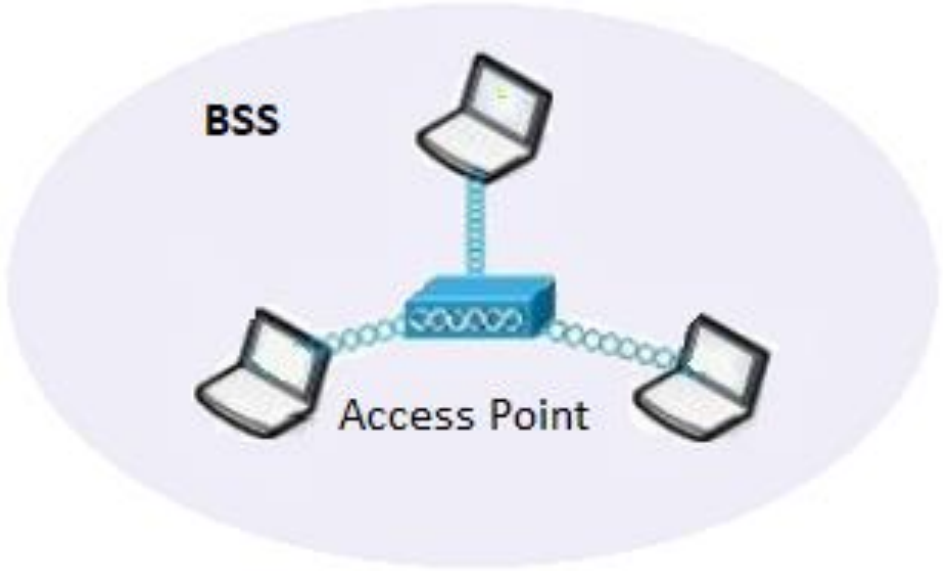
- **Basic Service Set identifier (BSSID)**

  The Layer 2 MAC address of the AP is used to uniquely identify each BSS, which is called the Basic Service Set Identifier (BSSID). Therefore, the BSSID is the formal name of the BSS and is always associated with only one AP.

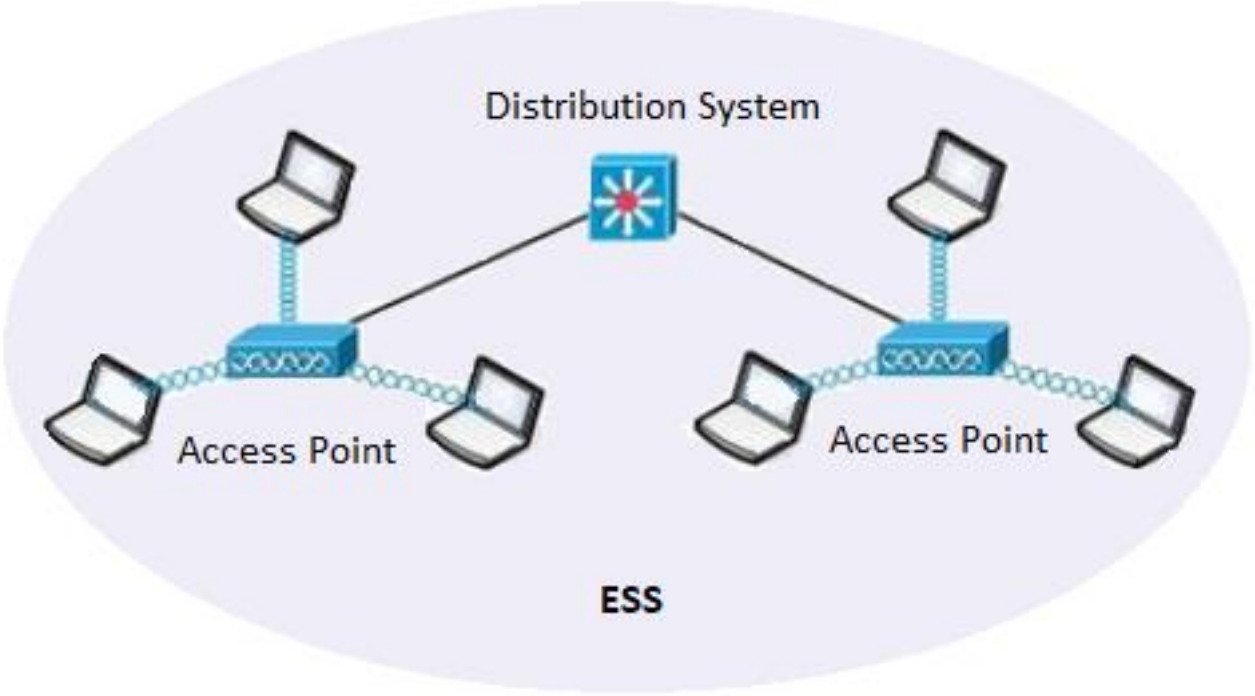
- **Extended Service Set (ESS)**

  When a single BSS provides insufficient RF coverage, two or more BSSs can be joined through a common distribution system (DS) into an ESS. An ESS is the union of two or more BSSs interconnected by a wired distribution system.

IEEE 802.11 Wireless LAN Architecture



Basic Service Set



Extended Service Set

IEEE 802.11 Wireless LAN Architecture

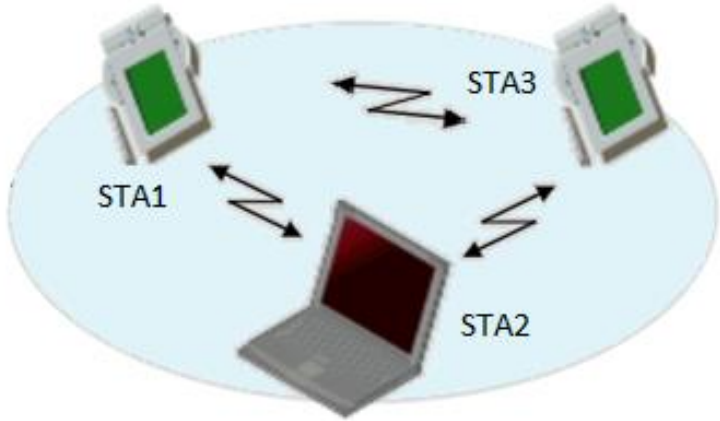
802.11 wireless technology identifies two main wireless topology modes

1. **Ad-hoc**

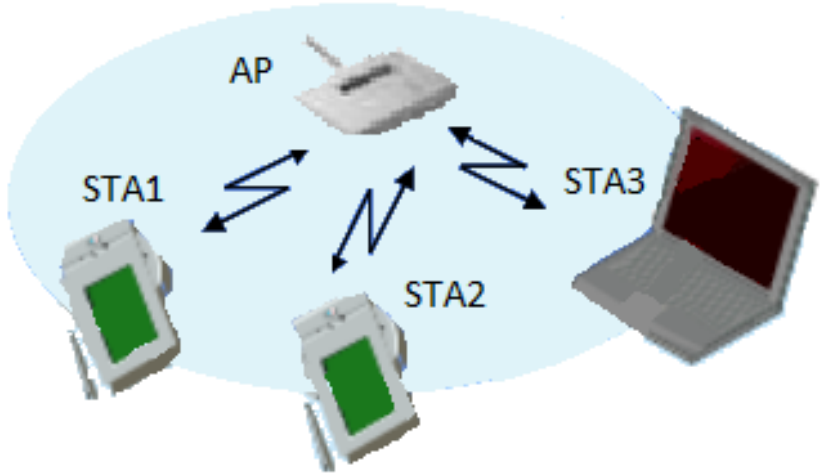
   The Ad hoc Mode is used when two devices connect wirelessly without the aid of an infrastructure devices, such a wireless router or Access Points, for example, using Bluetooth or Wi-Fi Direct connect to each other, creating a personal hotspot.

2. **Infrastructure**

   The Infrastructure Mode is used when wireless clients interconnect via a wireless router or AP, such as in WLANs.



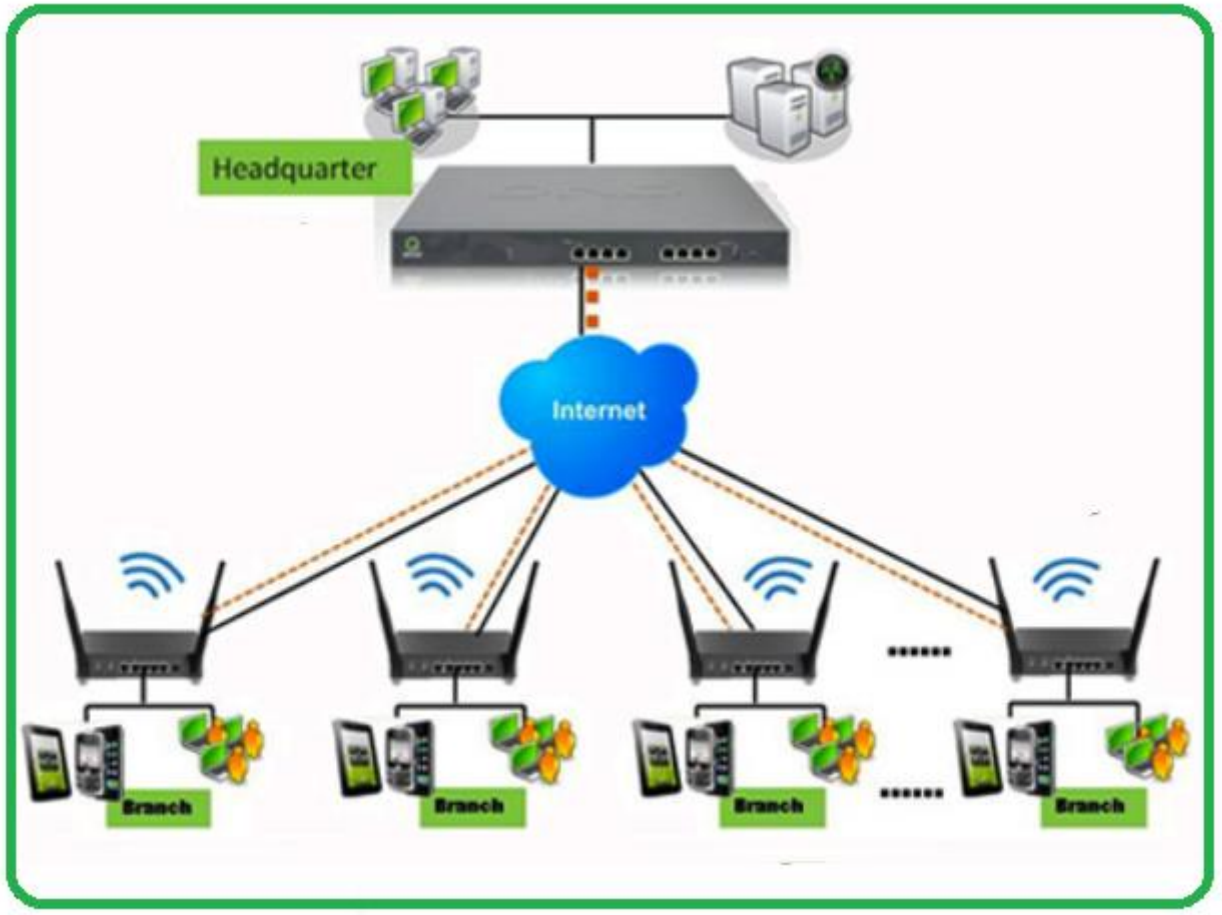
Ad-hoc mode



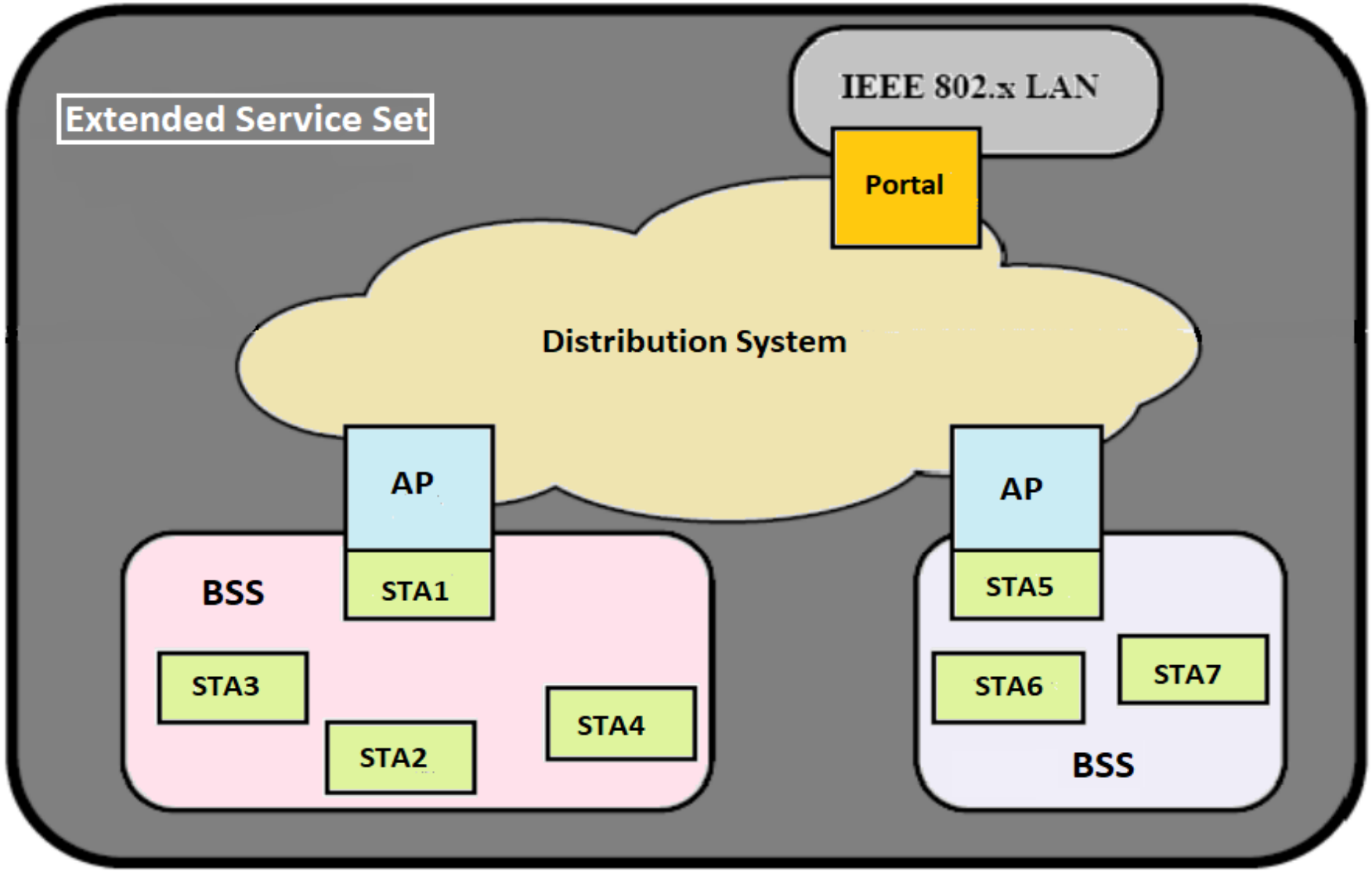
Infrastructure mode

Access point Controller

When we have multiple access points, we need to have access point controller (AP controller). Basically the goal of having multiple access points is that through roaming, the end-user devices should always have connectivity to the wireless network.



IEEE 802.11 Services



IEEE 802.11 Services

Services offered by IEEE 802.11 network can be broadly divided into two categories: *AP services* and *STA services*

- AP services are provided by the distribution System.
- STA services are provided by every station including APs

AP Services	STA Services
Association	Authentication
Reassociation	Deauthentication
Disassociation	Privacy
Distribution	Data delivery
Integration	

Access and Privacy Services

- **Authentication**
  - Establishes identity of stations to each other. The authentication scheme can range from relatively insecure handshaking to public-key encryption schemes. Example, login
- **De-authentication**
  - Invoked when existing authentication is terminated.
- **Privacy**
  - Prevents messages from being read by unintended recipient.

Association-Related Services

- **Association**
  - Establish initial association between station and AP
- **Disassociation**
  - Association termination from station or AP
- **Reassociation**
  - Enables transfer of association from one AP to another allowing station to move from one BSS to another.

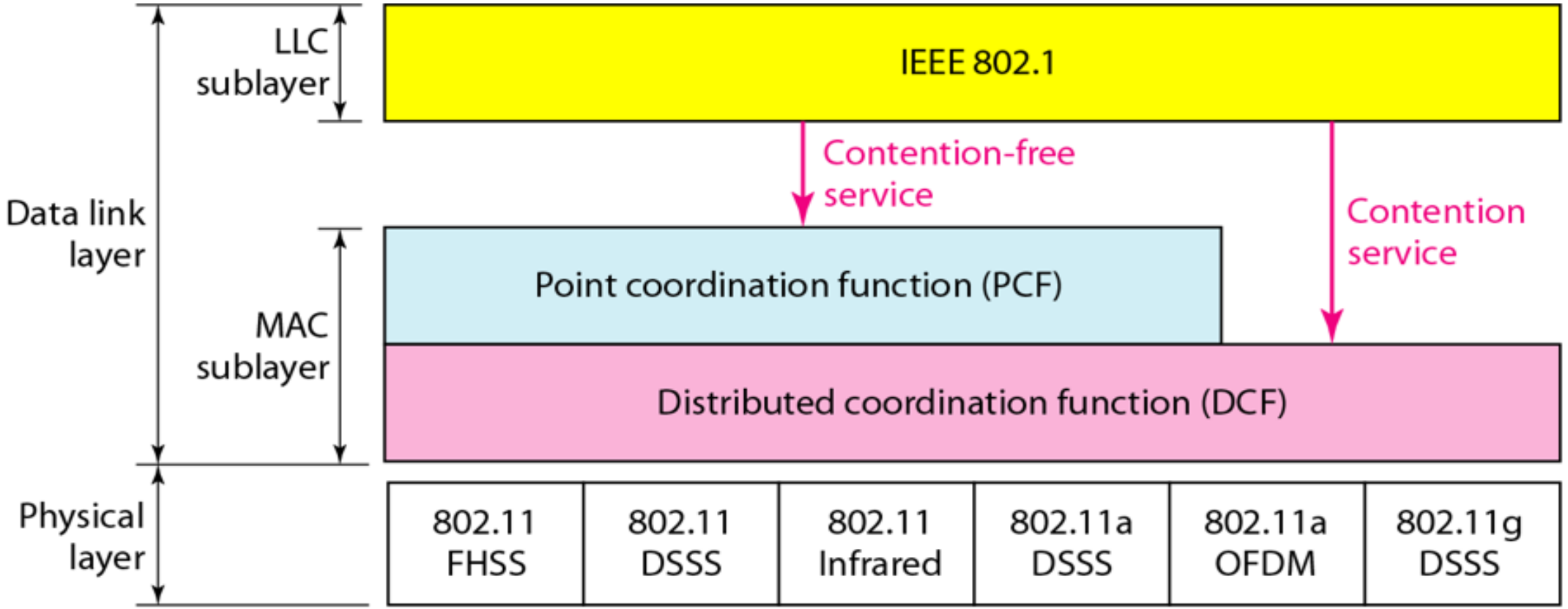
Distribution of Messages within DS

- **Distribution Service**
  - Used to exchange MAC frames from station in one BSS to station in another BSS.
- **Integration Service**
  - Transfer of data between station on IEEE 802.11 LAN and station on integrated IEEE 802.x LAN
- **Data Delivery**
  - IEEE 802.11 naturally provides a way to transmit and receive data. However, like ethernet the transmission is not guaranteed to be completely reliable

IEEE 802.11 Services

Provider	Services	Used to support
Station	Authentication (Login)	LAN access and security
Station	De-authentication (Logout)	LAN access and security
Station	Privacy	LAN access and security
Station	Data Delivery	MSDU delivery
Distribution System	Association	MSDU delivery
Distribution System	Disassociation	MSDU delivery
Distribution System	Reassociation	MSDU delivery
Distribution System	Integration	MSDU delivery
Distribution System	Distribution	MSDU delivery

IEEE 802.11 Medium Access Control Layer



FHSS - frequency hopping spread spectrum
DSSS - direct sequence spread spectrum
OFDM - orthogonal frequency division multiplexing

IEEE 802.11 Media Access Control

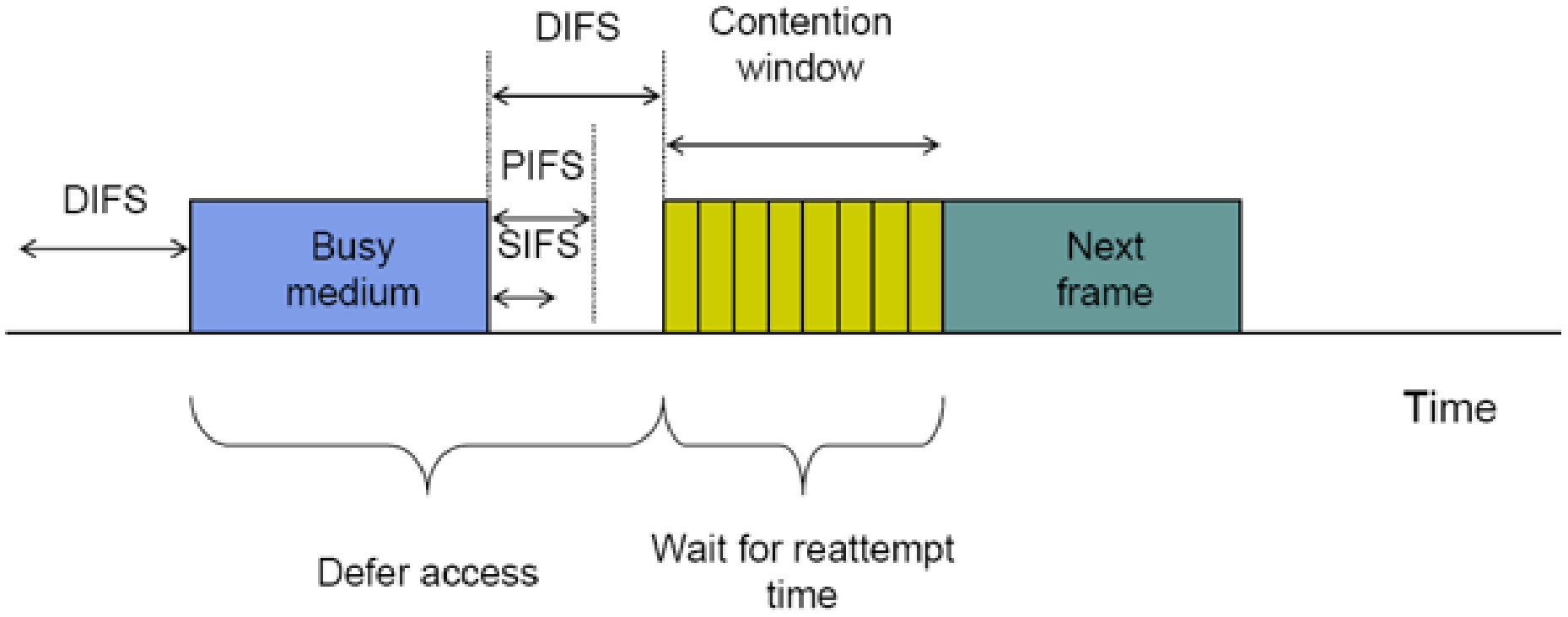
- *Distributed coordination function* (DCF) is the fundamental access method of IEEE 802.11. It is based on *carrier sense multiple access with collision avoidance* (CSMA/CA) along with the RTS-CTS mechanism.

- *Point Coordination Function* (PCF) is a polling-based access scheme with no contention. It is implemented to provide real-time services. AP controls medium access and avoids simultaneous transmissions by the nodes.

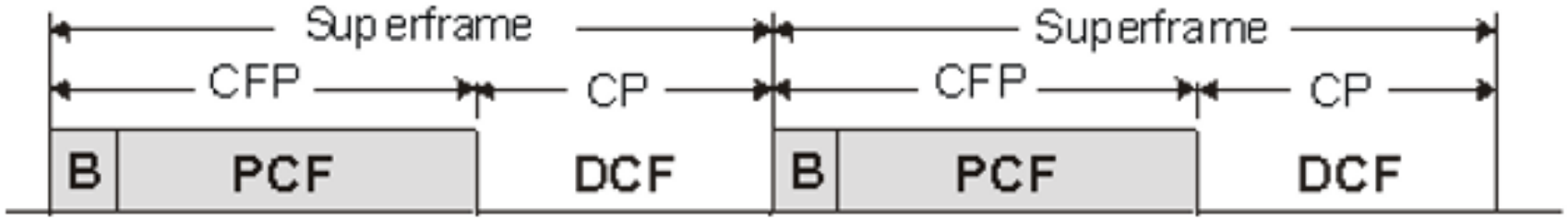
IEEE 802.11 Media Access Control

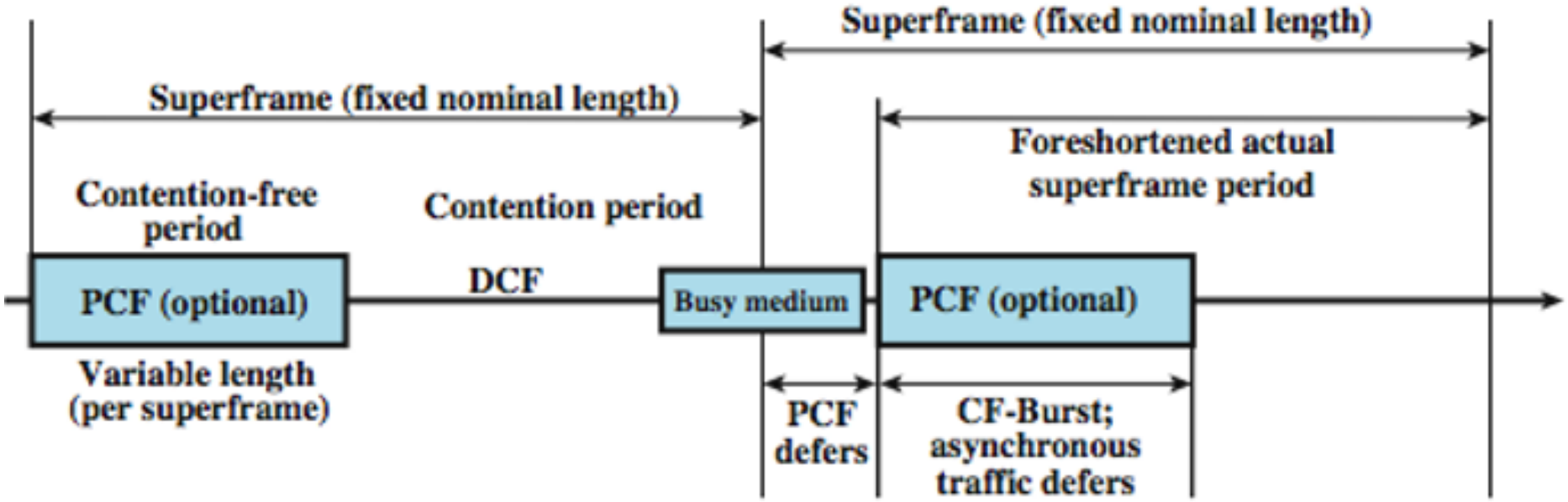
- PCF and DCF operate concurrently within the same BSS. The two access methods alternate, with a contention-free period (CFP) followed by a contention period (CP).
- The PCF mode is optional in the IEEE 802.11 standard and is always used in conjunction with the main access mechanism. Therefore, some coexistence procedure between DCF and PCF is necessary

MAC timing - Basic Access Method



MAC timing - PCF Superframe

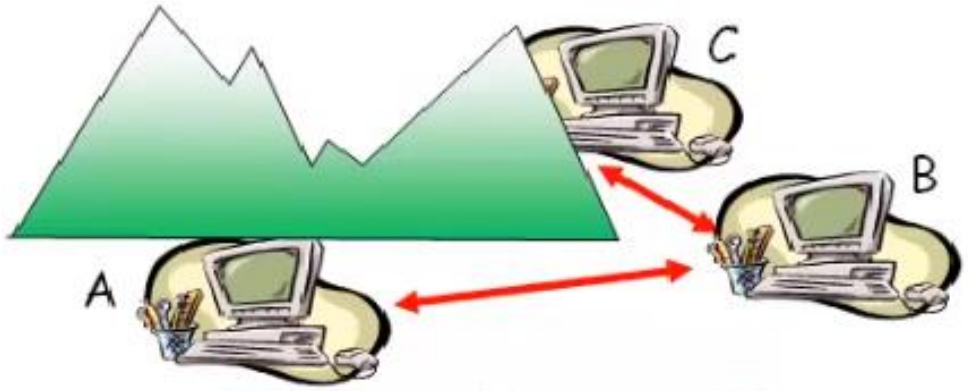


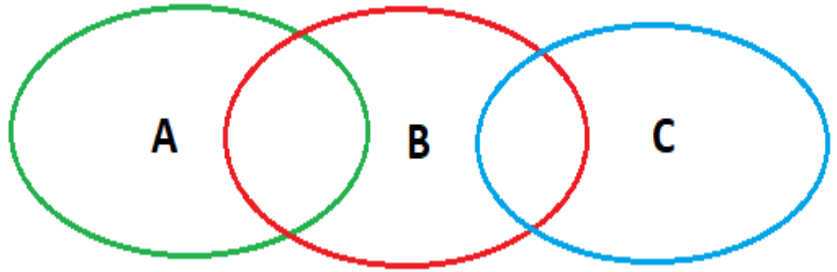


Hidden Node Problem

- A can hear B,
- B can hear C,
- but C cannot hear A

- **A** may start transmitting while **C** is also transmitting results in collision
  - **A** and **C** cannot detect collision
  - Only the receiver **B** can tell whether it received data or not





IEEE 802.11 Media Access Control

- MAC layer covers three functional areas:

1. Reliable data delivery
2. Access Control.
3. Security

Reliable Data Delivery

- There are three types of frames:

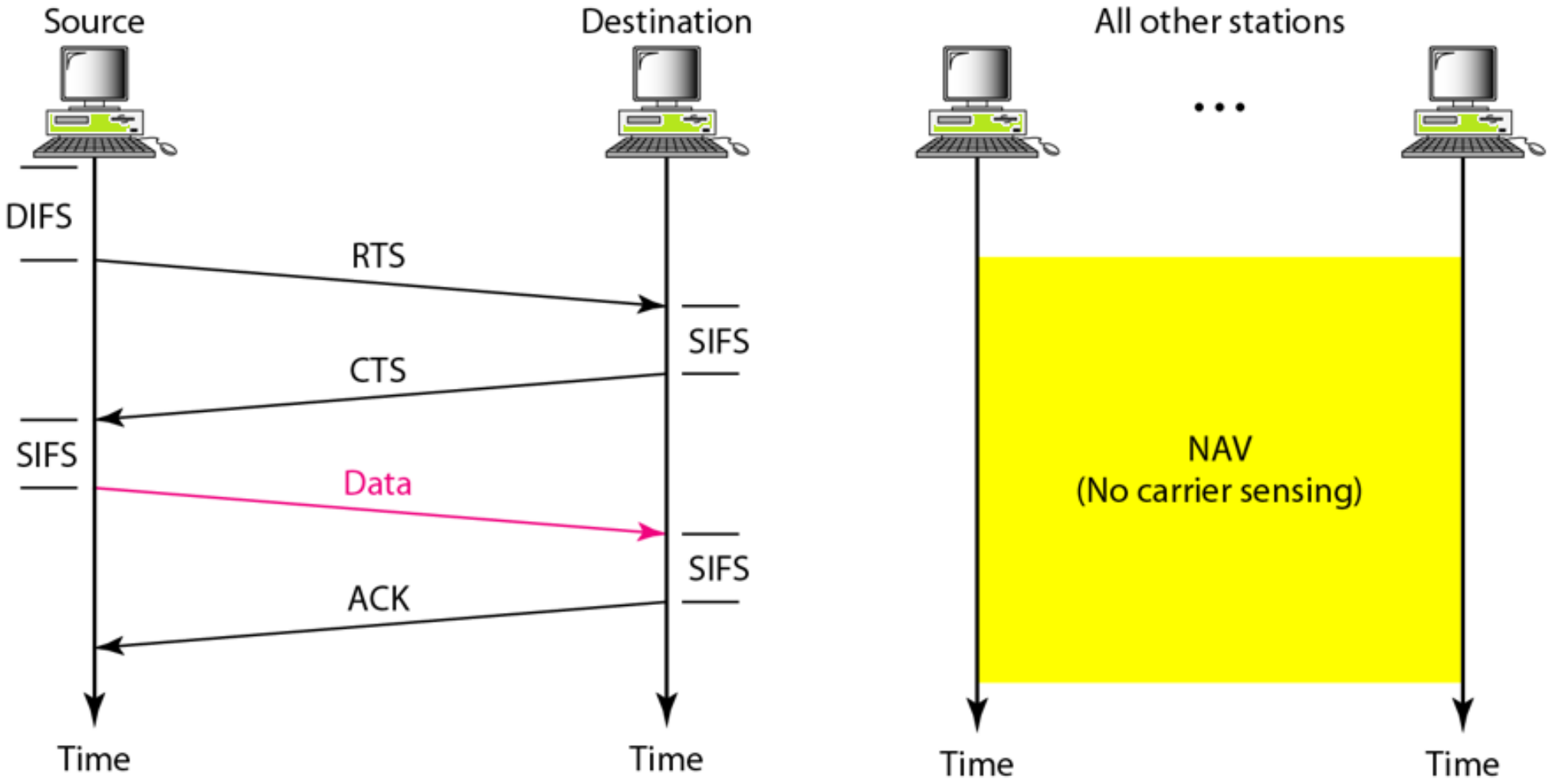
1. Management - used for initial communication between stations and access points. For example, requests, response, reassociation, dissociation, and authentication
2. Control - used for accessing the channel (RTS) and acknowledging frames (CTS or ACK)
3. Data - used for carrying data and control information

Four Frame Exchange - handshaking

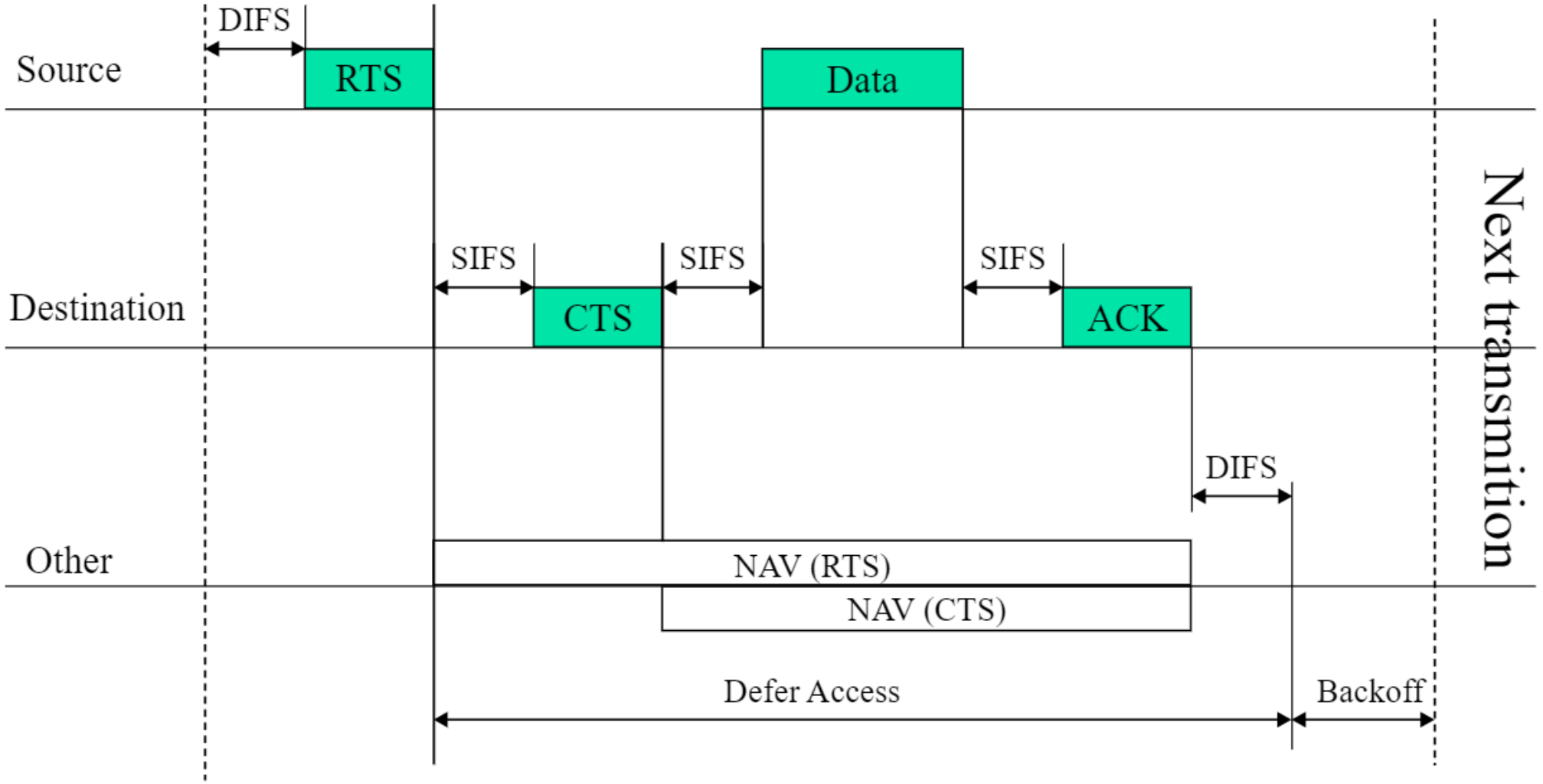
Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with RTS-CTS mechanism

1. Listen to the medium before you talk
2. If medium is busy, then the transmitter backs off for a random period
3. Transmitter sends Ready to Send (RTS) message to reserve the channel.
   - RTS consists of destination address and duration of message.
4. Receiver sends a short Clear to Send (CTS) message
5. Other stations can hear CTS and set their Network Allocation Vector (NAV) and wait for that duration. Backoff intervals are used to reduce collision probability. Other stations remain silent.
6. Transmitter transmit data
7. Receiver sends Acknowledge (ACK) message
8. If message not acknowledged, then retransmission of data will take place

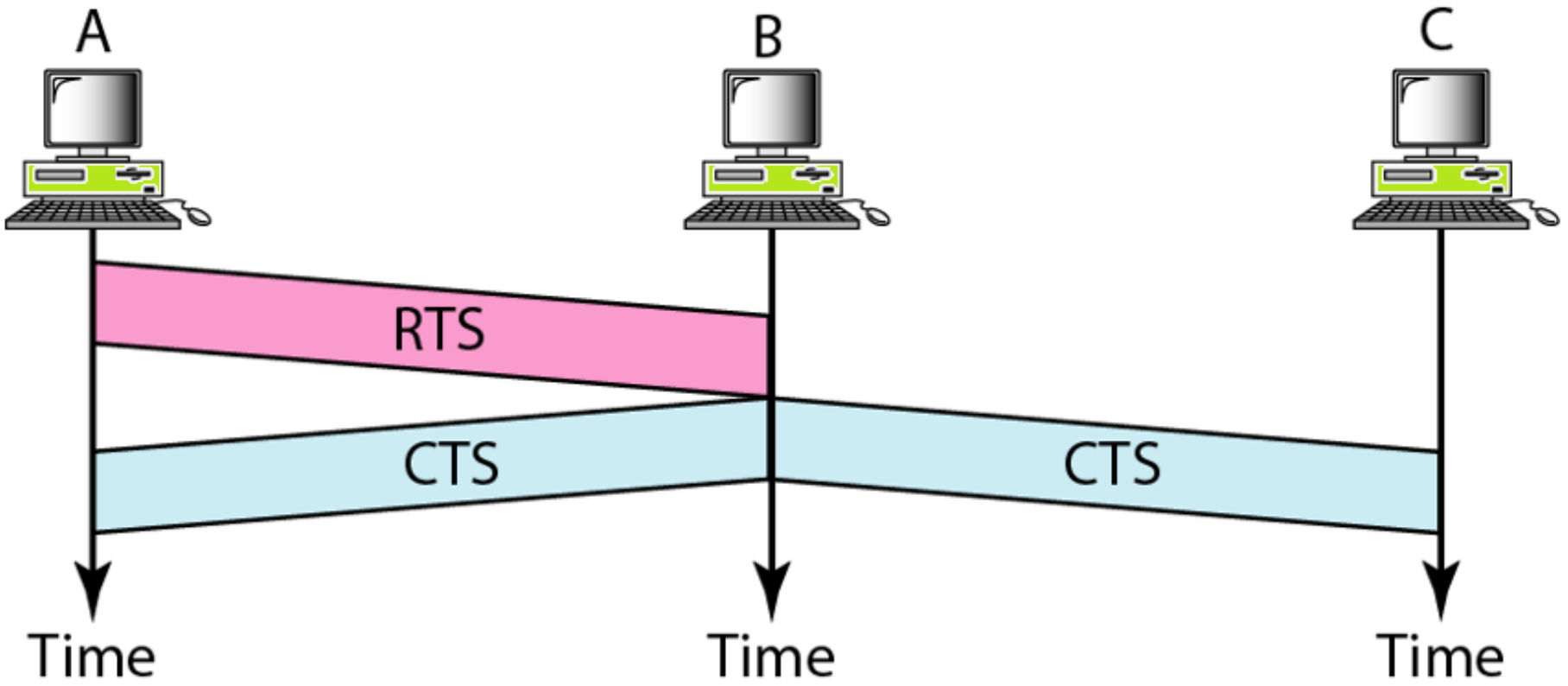
Four Frame Exchange - handshaking



IEEE 802.11 DCF and RTS-CTS Mechanism



Hidden Node problem - Solution

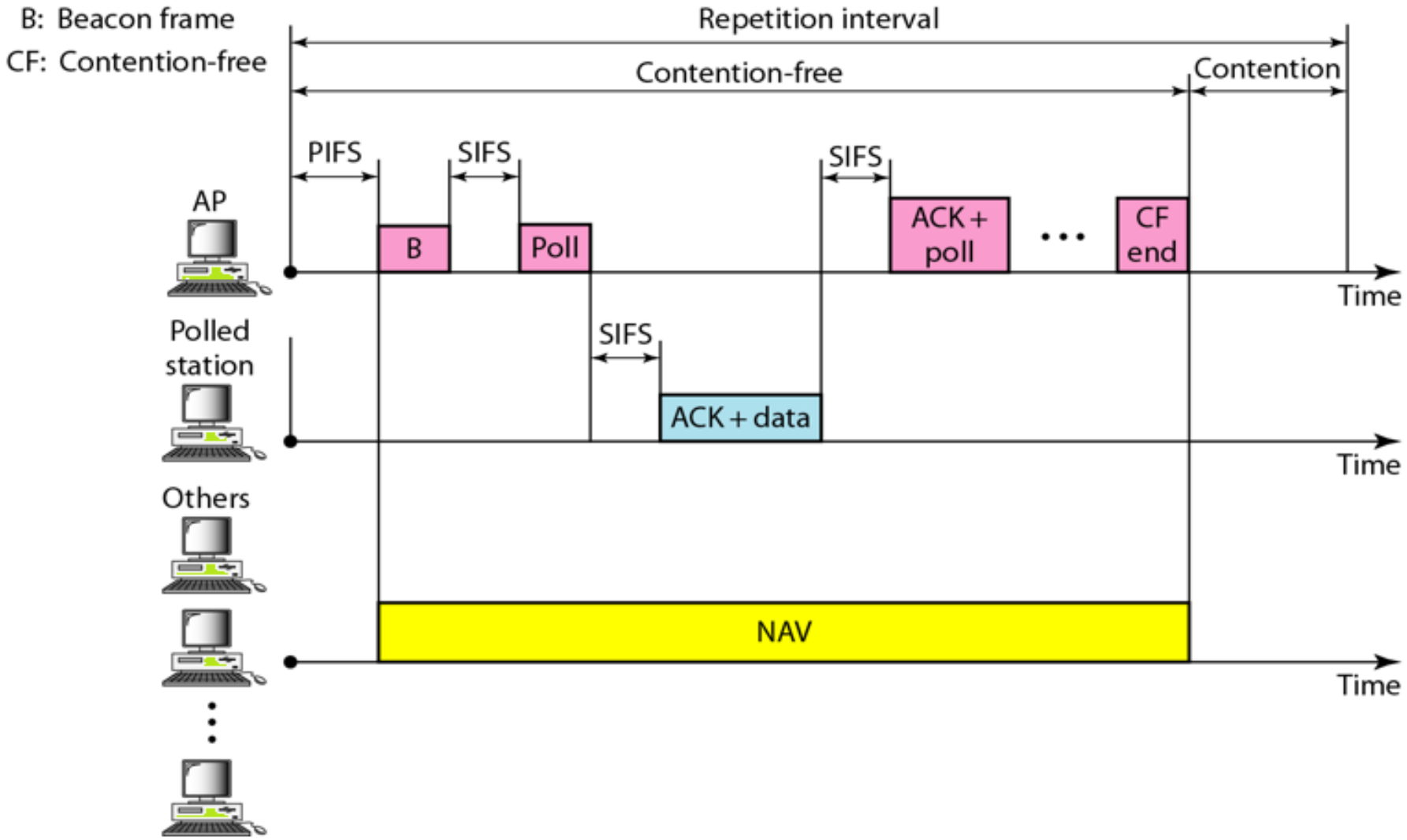


Station C doesn't hear RTS from B, but it does hear CTS from A, so it knows something is up.

Disadvantage of DCF

- High power consumption
- Hidden terminal problem not totally solved (e.g., collision of RTS)
- Fairness problem among different transmitting nodes
- Only providing best-effort service

IEEE 802.11 PCF MAC layer



Inter-frame Spacing (IFS)

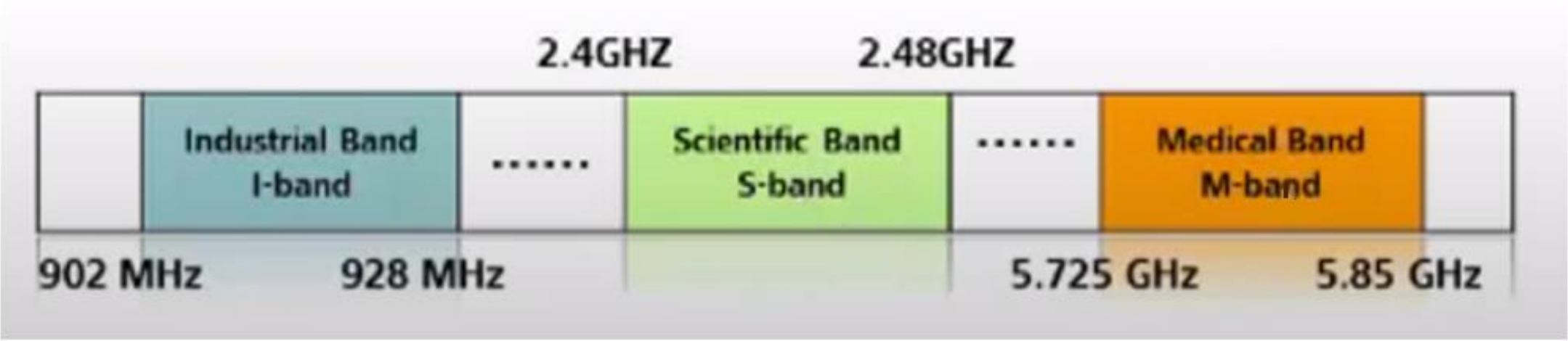
- Interframe spacing refers to the time interval between the transmissions of two successive frames by any station.
- They denote priority levels of access to the medium.
- The exact values of the IFS are obtained from the physical layer management information base (PHYMIB)
- There are 4 types of IFS:
  - **SIFS** – Short Inter-frame Spacing
  - **PIFS** – PCF Interframe Spacing
  - **DIFS** – DCF Interframe Spacing
  - **EIFS** – Extended Interframe Spacing

Inter-frame Space (IFS)

- SIFS
  - It is the shortest of all IFSs and denotes highest priority to access the medium.
  - It is defined for short control messages such as acknowledgements for data packets and polling responses.
- PIFS
  - It is the waiting time whose values lies between SIFS and DIFS.
  - This is used for real time services
- DIFS
  - It is used by stations that are operating under DCF mode to transmit packets.
  - This is for data transfer within the contention period
- EIFS
  - Longest of all IFSs. Used for resynchronisation whenever physical layer detects incorrect MAC frame reception

IEEE 802.11 Physical Layer

ISM band



IEEE 802.11 Physical Layer

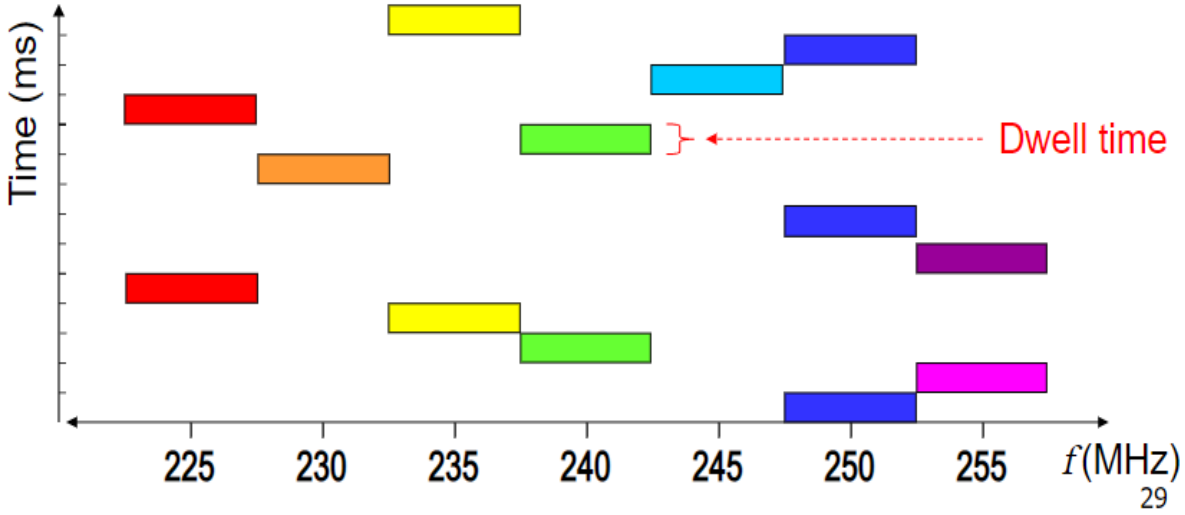
IEEE 802.11 uses four physical layer technologies

- FHSS – Frequency Hopping Spread Spectrum
- DSSS- Direct Sequence Spread Spectrum
- OFDM – Orthogonal Frequency Division Multiplexing
- Infrared

IEEE 802.11 Physical Layer

- FHSS – Frequency Hopping Spread Spectrum

  - Is a simple technique in which transmission switches (hops) across multiple narrow and frequencies in a pseudorandom manner.
  - A pre-determined hopping sequence known to both transmitter and receive before data transmission starts.
  - Bluetooth uses frequency hopping mechanism



IEEE 802.11 Physical Layer

- FHSS – Frequency Hopping Spread Spectrum
  - Operates in the 2.4 GHZ ISM band
  - Data rates of 1 and 2 Mbps
  - Each channel has a bandwidth of 1 MHz
  - The minimum hop rate is 2.5 hops per second (in United States) and minimum hopping distance in frequency is 6Mhz (in United States) and 5MHz in (in Japan)

IEEE 802.11 Physical Layer

- DSSS – Direct Sequence Spread Spectrum
  - This technique employs an encoding scheme in which information bits (data signal) are Xored with higher data rate pseudorandom number (PN) which are orthogonal.
  - PN is also called as barker chipping code.
  - This code is known at both transmitter and receiver end. Receiver uses the sequence to decode at its end

IEEE 802.11 Physical Layer

- DSSS – Direct Sequence Spread Spectrum
  - Operates in the 2.4 GHZ ISM band
  - Data rates of 1 and 2 Mbps
  - Each channel has a bandwidth of 5 MHz
- Infrared
  - Data rates of 1 and 2 Mbps
  - Wavelength between 850 and 950nm

IEEE 802.11 Physical Layer

- OFDM - Orthogonal Frequency Division Multiplexing
  - OFDM is a digital multi-carrier modulation scheme that uses multiple subcarriers within the same single channel.
  - OFDM makes use of a large number of closely spaced orthogonal subcarriers that are transmitted in parallel.
  - Each subcarrier is modulated with a conventional digital modulation scheme (such as QPSK, 16QAM, etc.) at low symbol rate.
  - Efficient use of spectrum by allowing overlap
  - High throughput and high performance achieved.

IEEE 802.11a & b standard

- IEEE 802.11a
  - Operates in the 5 GHZ ISM band
  - Provides data rates of 6, 9,12,18,24,36,48 and 54 Mbps
  - Uses Orthogonal Frequency Division Multiplexing (OFDM)
  - Subcarrier modulated using BPSK, QPSK, 16-QAM or 64-QAM
- IEEE 802.11b
  - Operates in the 2.4 GHZ ISM band
  - Provides data rates of 5.5 and 11Mbps
  - Complementary code keying modulation scheme.

IEEE 802.11 Physical Layer

- IEEE 802.11g
  - Operates in the 2.4 GHZ ISM band
  - Extends IEEE 802.11b to higher data rates.
  - Uses Orthogonal Frequency Division Multiplexing (OFDM)
- IEEE 802.11n
  - Operates in the both 2.4 & 5 GHZ ISM band
  - Uses multiple antennas to increase data rates
  - Provides data rates up to 600Mbps
  - MIMO OFDM

IEEE 802.11 Network Physical Standards

IEEE 802.11 COMMON WIFI STANDARDS							
Standard	Frequency Band	Bandwidth	Modulation Scheme	Channel Arch.	Maximum Data Rate	Range	Max Transmit Power
802.11	2.4 GHz	20 MHz	BPSK to 256-QAM	DSSS, FHSS	2 Mbps	20 m	100 mW
b	2.4 GHz	21 MHz	BPSK to 256-QAM	CCK, DSSS	11 Mbps	35 m	100 mW
a	5 GHz	22 MHz	BPSK to 256-QAM	OFDM	54 Mbps	35 m	100 mW
g	2.4 GHz	23 MHz	BPSK to 256-QAM	DSSS, OFDM	54 Mbps	70 m	100 mW
n	2.4 GHz, 5 GHz	24 MHz and 40 MHz	BPSK to 256-QAM	OFDM	600 Mbps	70 m	100 mW
ac	5 GHz	20, 40, 80, 80+80= 160 MHz	BPSK to 256-QAM	OFDM	6.93 Gbps	35 m	160 mW
ad	60 GHz	2.16 GHz	BPSK to 64-QAM	SC, OFDM	6.76 Gbps	10 m	10 mW
af	54-790 MHz	6, 7, and 8 MHz	BPSK to 256-QAM	SC, OFDM	26.7 Mbps	>1km ?	100 mW
ah	900 MHz	1, 2, 4, 8, and 16 MHz	BPSK to 256-QAM	SC, OFDM	40 Mbps	1 km	100 mW

Thank you

Any Questions?

t.s.syed@herts.ac.uk