ITMC412 PAN
شبكات المنطقة الشخصية

WiFi (IEEE802.11)
L6

By: Dr. Abdussalam Nuri Baryun
abaryun.teaching@gmail.com

Mobile Computing Department, Faculty of Information Technology, University of Tripoli

5G WiFi vs mobile 5G

- The 5G WiFi which shouldn't be confused with mobile 5G, the successor to 4G LTE. The former refers to WiFi on the 5GHz frequency band. You have to know that WiFi operates on 2.4GHz(802.11 a/b/g/n), 5Ghz(802.11 ac) and 60GHz(802.11 ad).
- WiFi-specific functions aren't compatible with cellular networks, however, For home networks that have infrastructure like this, WiFi is, and will remain to be the most viable option.

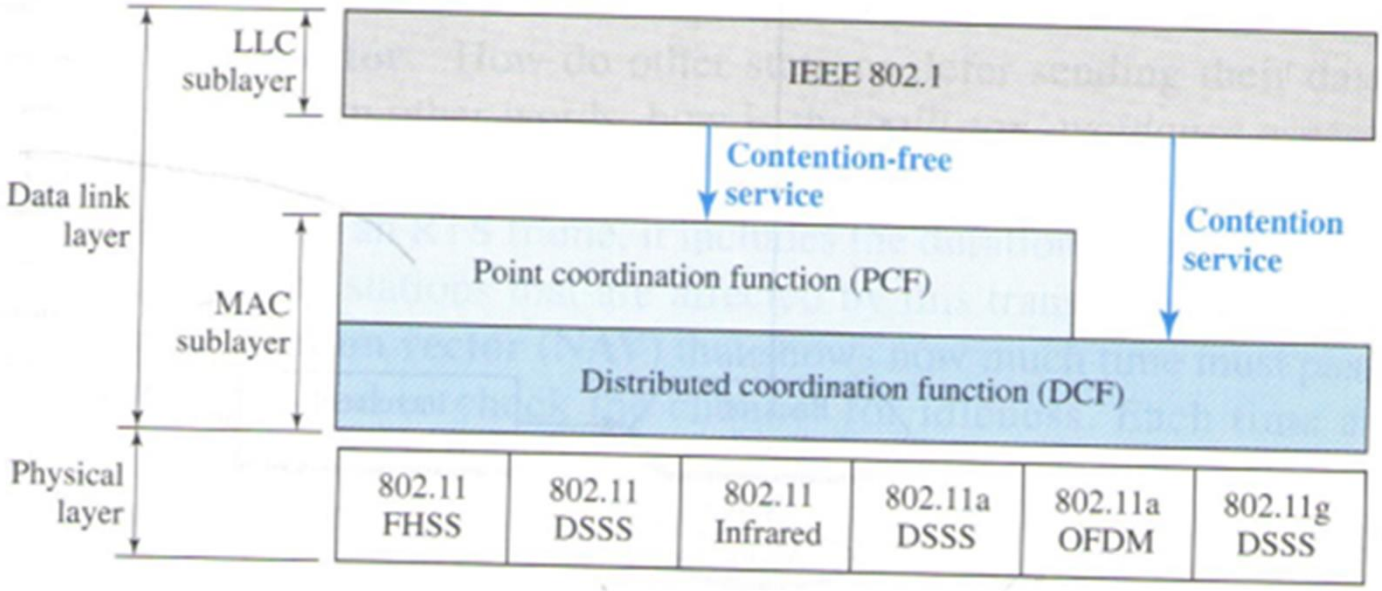
Year	WiFi Versions/Protocols	Old name	New name
1999	First Generation	WiFi 802.11b	WiFI 1
1999	Second Generation	WiFi 802.11a	WiFi 2
2003	Third Generation	WiFI 802.11g	WiFi 3
2009	Four Generation	WiFi 802.11n	WiFi 4
2014	Fifth Generation	WiFi 802.11ac	WiFi 5
2019	Sixth Generation	WiFi 802.11ax	WiFi 6

WiFi

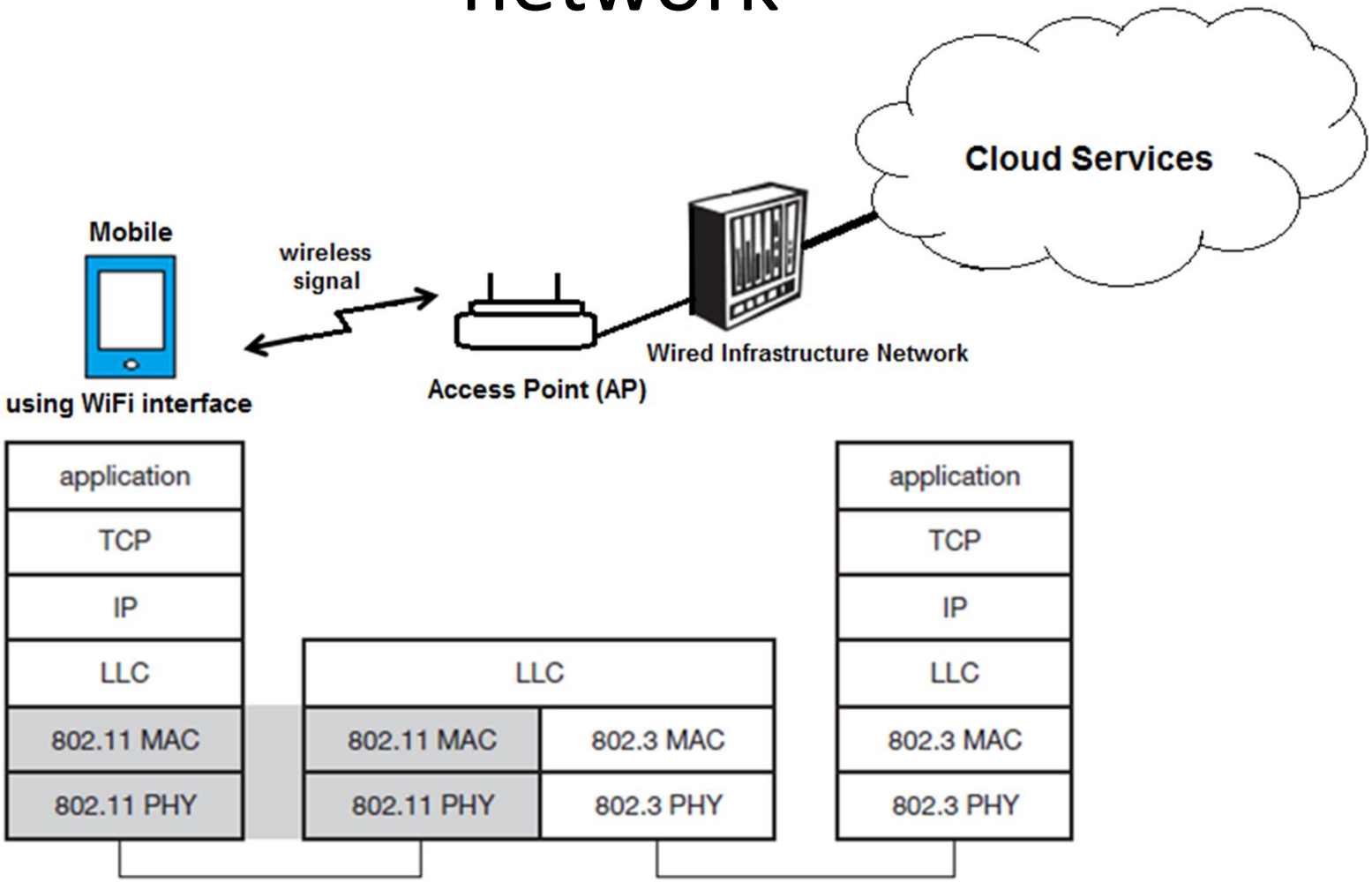
- While the development of including WiFi technology into personal devices as mobile phone the WiFi IEEE802.11 is being considered by many as a personal area network technology.
- In this lecture we study WiFi while notice that IEEE802.11 is a standard of Wireless LAN, however, it is used currently within personal devices that also uses WPAN technologies as well.

WiFi System Architecture

MAC layers in IEEE 802.11 standard **Ref [1]**



Bridging WiFi to infrastructure network

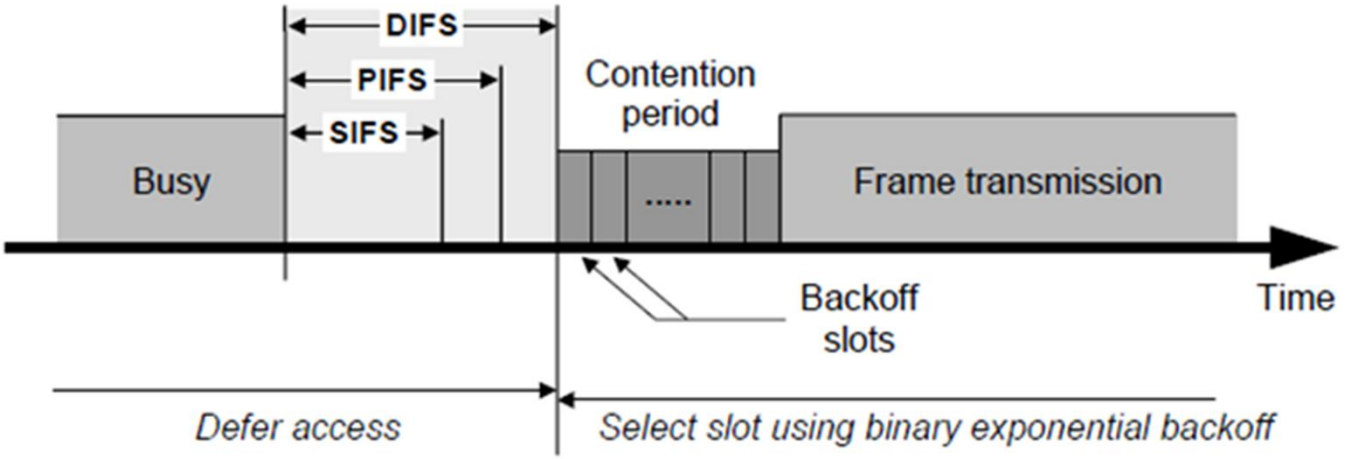


WiFi Medium Access Control

- IEEE802.11 uses for Contention Access Period (CAP); the Carrier Sense Multiple Access - Collision Avoidance protocol (CSMA/CA).
- Distributed Coordination Function (DCF):
  - CSMA/CA used for access control
  - When a collision is detected, a random backoff timer is set
  - Positive acknowledgements are used (to be explained below)
- Point Coordination Function (PCF):
  - Built on top of DCF: the point coordinator uses DCF to seize the medium
  - A point coordinator determines which station currently has the right to transmit by polling as the contention free period.

- Some drawbacks of PCF are:
  - Introduces considerable additional complexity
  - Needs to choose a coordinator to do the polling (a leader election problem)
  - Needs to provide for failure of the coordinator
  - A station cannot access the medium unless explicitly polled from the coordinator
  - All stations need to hear the poll
  - The number of stations in a BSS can scale with no penalty in the performance. However, different BSSs need to be carefully planned not to overlap even when the density of the BSSs is very small. Therefore, it requires coordination between the point coordination functions within peer APs.

WiFi interframe spacing



IEEE 802.11 interframe spacing relationships. Different length IFSs are used by different priority stations. **Ref [2]**

WiFi interframe Definition

- ***SIFS: Short interframe Space****; is used for the highest priority transmissions, such as control frames,* or to separate transmissions belonging to a single dialog (e.g. Frame-fragment–ACK). This value is a fixed value per PHY and is calculated in such a way that the transmitting station will be able to switch back to receive mode and be capable of decoding the incoming packet. For example, for the 802.11 FH PHY this value is set to 28 microseconds.
- ***PIFS: PCF (or priority) interframe Space****; is used by the PCF during contention-free operation.* The coordinator uses PIFS when issuing polls and the polled station may transmit after the SIFS has elapsed and preempt any contention-based traffic. PIFS is equal to SIFS plus one slot time.
- ***DIFS: DCF (or distributed) interframe Space****; is the minimum medium idle time for asynchronous* frames contending for access. Stations may have immediate access to the medium if it has been free for a period longer than the DIFS. DIFS is equal to SIFS plus two slot times.

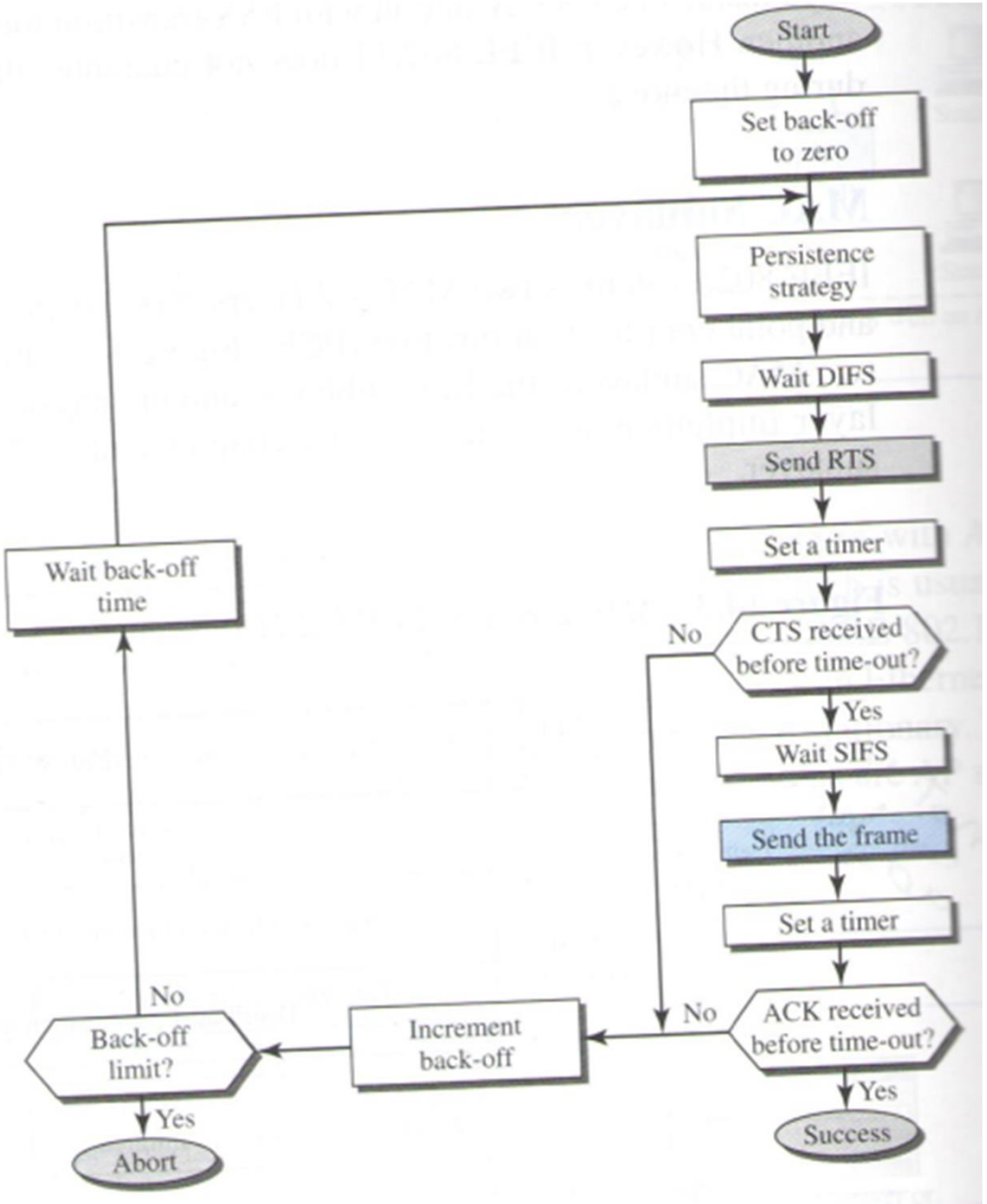
WiFi PHY Parameters

IEEE 802.11b system parameters. (PHY preamble serves for the receiver to distinguish silence from transmission periods and detect the beginning of a new packet.) **Ref [2]**

Parameter	Value for 1Mbps channel bit rate
Slot time	20 μsec
SIFS	10 μsec
DIFS	50 μsec (DIFS = SIFS + 2 × Slot time)
EIFS	SIFS + PHY_preamble + PHY_header + ACK + DIFS = 364 μsec
CW_{min}	32
CW_{max}	1024
PHY_preamble	144 bits (144 μsec)
PHY_header	48 bits (48 μsec)
MAC data header	28 bytes = 224 bits
ACK	14 bytes + PHY_preamble + PHY_header = 304 bits (304 μsec)
RTS	20 bytes + PHY_preamble + PHY_header = 352 bits (352 μsec)
CTS	14 bytes + PHY_preamble + PHY_header = 304 bits (304 μsec)
MTU*	Adjustable, up to 2296 bytes

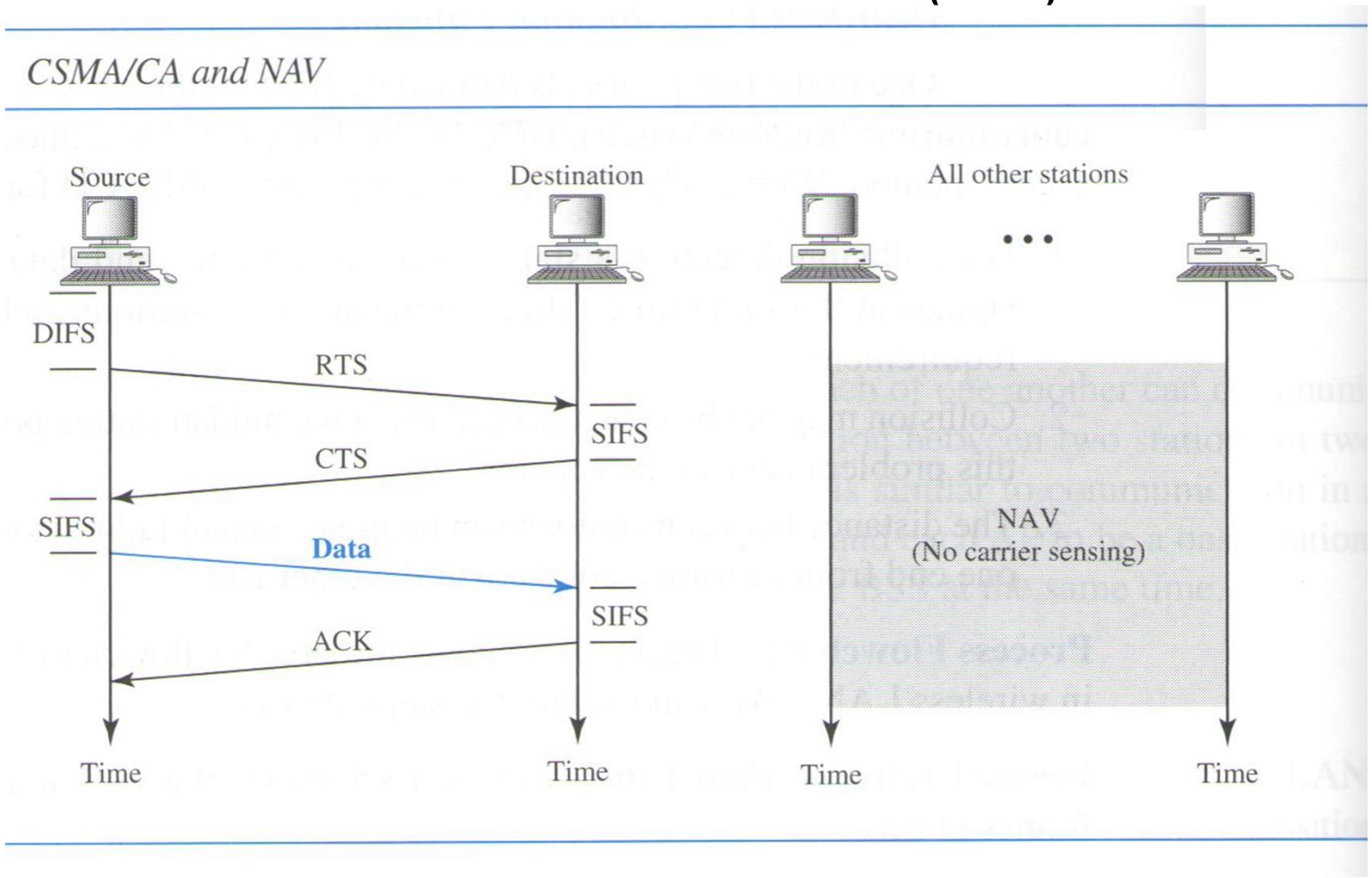
(*) The Maximum Transmission Unit (MTU) size specifies the maximum size of a physical packet created by a transmitting device.

WiFi CAP Period using CSMA/CA with RTS/CTS [1]



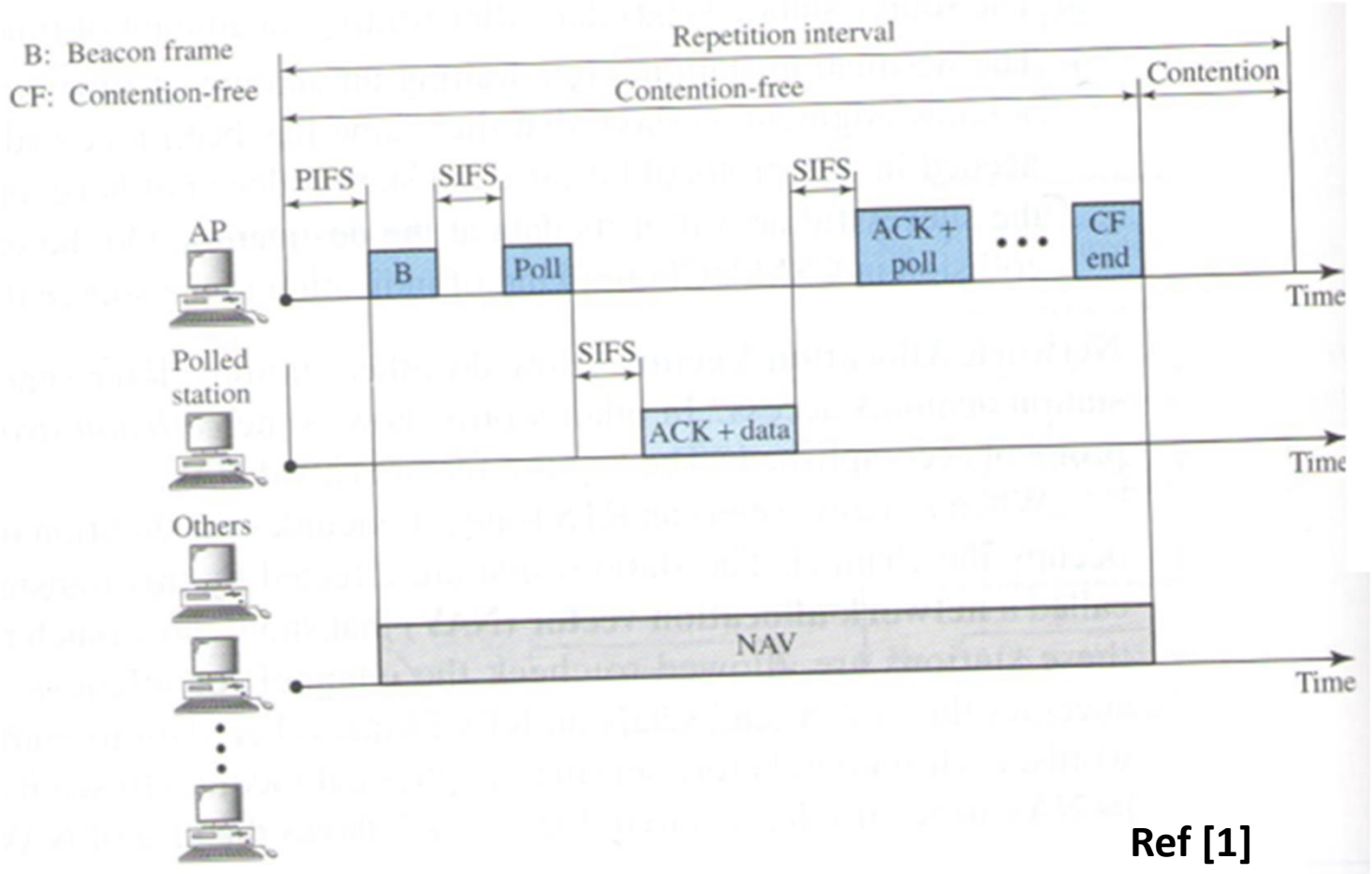
Using *Virtual reservation* mechanism:

Network Allocation Vector (NAV)



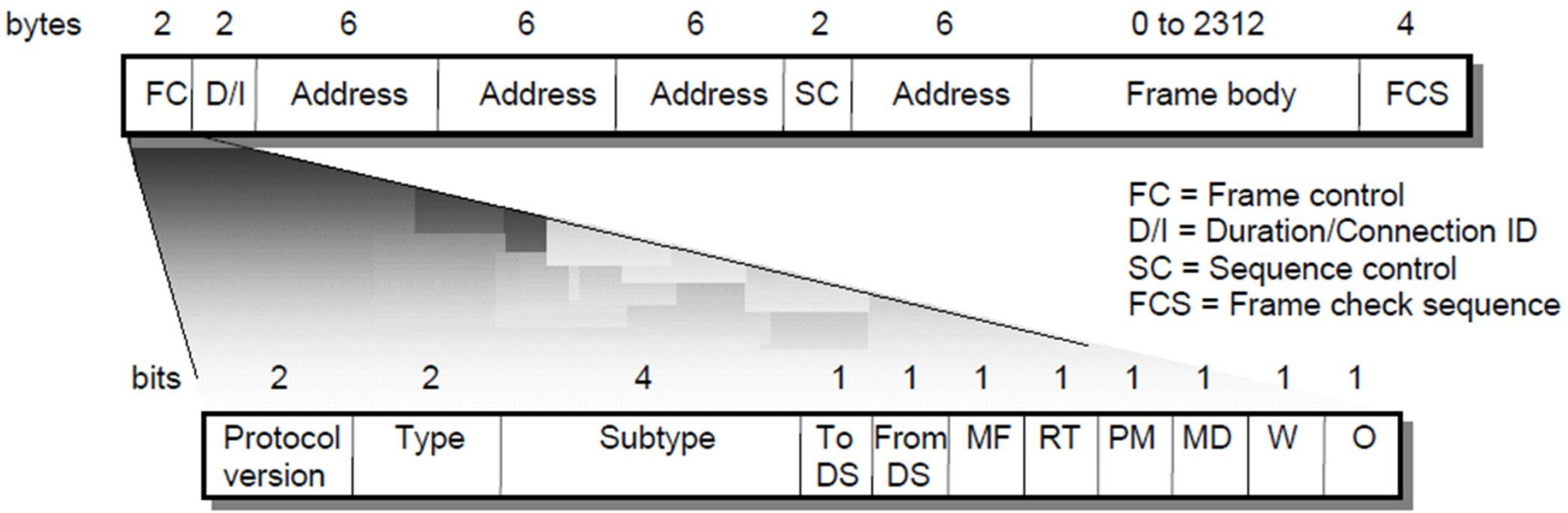
When other stations hears RTS or CTS they stop sensing for NAV time which is indicated in the Duration field of the control frame. **Ref [1]**

WiFi AP uses Repetition interval for CF period



Ref [1]

General MAC packet/frame Structure



Ref [2]

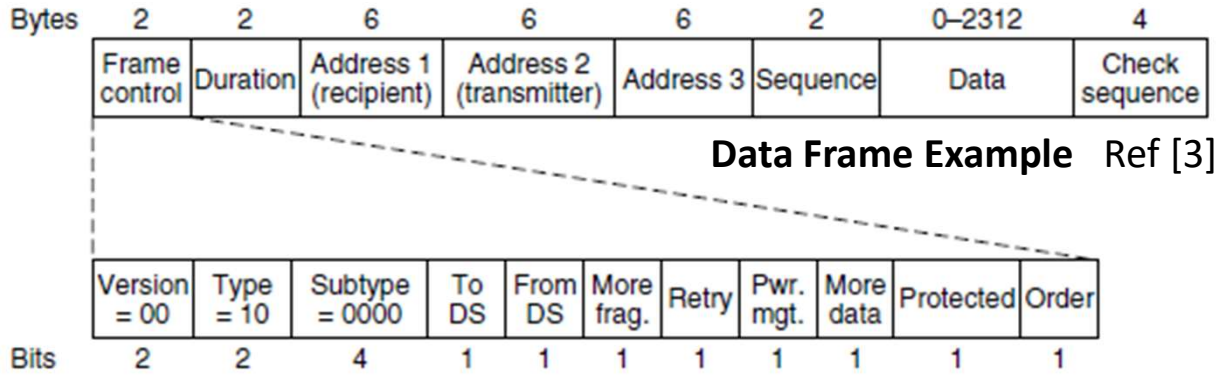
WiFi MAC Frame Fields

- **Frame control:** The first 2 bytes serve several purposes. They contain several sub-fields as explained after the MAC frame.
- **Duration/ID:** If the field value is less than 32,768, the duration field contains the value indicating the period of time in which the medium is occupied (in *micro-seconds). This field is used for setting the NAV for the virtual reservation* mechanism using RTS/CTS and during fragmentation. Certain values above 32,768 are reserved for identifiers.
- **Address 1 to 4:** The four address fields contain standard IEEE 802 MAC addresses (6 bytes each), as they are known from other 802.x LANs. The meaning of each address depends on the DS bits in the frame control field and is explained in more detail in a separate paragraph.
- **Sequence control:** Due to the acknowledgement mechanism frames may be duplicated. Therefore a sequence number is used to filter duplicates.
- **frame body (Data):** The MAC frame may contain arbitrary data (max. 2,312 byte), which is transferred transparently from a sender to the receiver(s).
- **Checksum (CRC):** Finally, a 32 bit checksum is used to protect the frame as it is common practice in all 802.x networks.

Frame Control Subfield

- **Protocol version:** This 2 bit field indicates the current protocol version and is fixed to 0.
- **Type:** The type field determines the function of a frame: management (=00), control (=01), or data (=10). The value 11 is reserved. Each type has several subtypes as indicated in the following field.
- **Subtype:** for management frames are: 0000 for association request, 1000 for beacon. RTS subtype 1011, CTS is 1100. Shown Example of data packet.

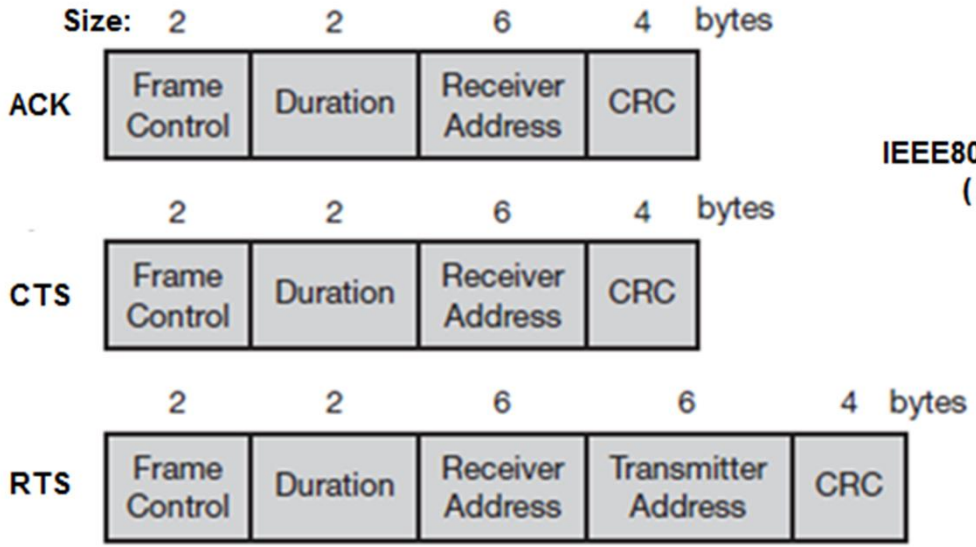
Data_type and subtype in frame control field →



Data Frame Example Ref [3]

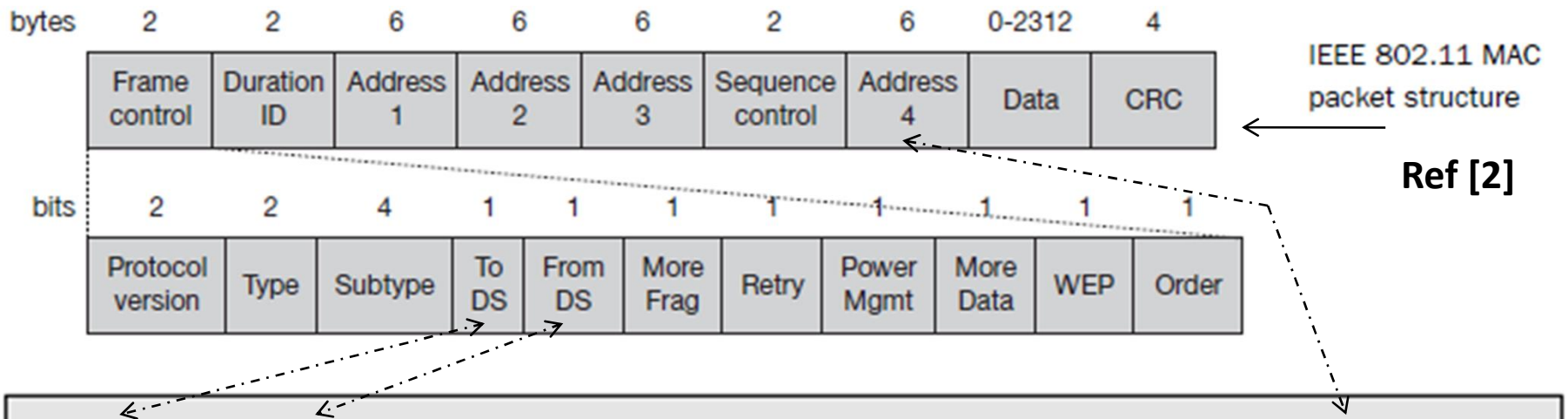
Control packets

- Three control packets: ACK, RTS, CTS
- Control Packet type field: 01 (subtype/ ACK: 1101, RTS: 1011, CTS: 1100)
- Control packets have no body field (no data) as short frames.



IEEE802.11 special control frames: Ref [1]
(ACK, CTS, RTS)

MAC Packet Addressing mechanism



Ref [2]

to DS	from DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSS ID	–
0	1	DA	TA	SA	–
1	0	RA	SA	DA	–
1	1	RA	TA	DA	SA

DA: Destination Address, SA: Source Address, RA: Receiving AP, TA: Transmitting AP

WiFi Communication Scenarios

For addressing, the following four scenarios are possible Cases:

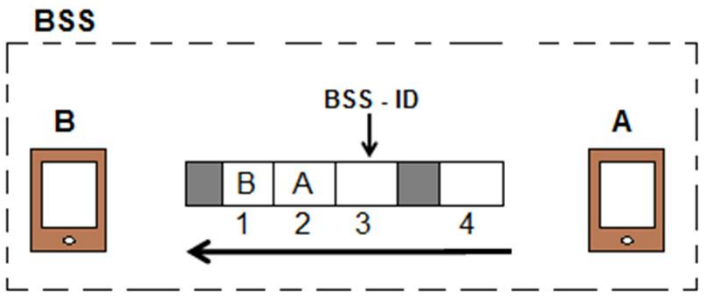
Case 1) Ad-hoc network: If both DS bits are zero, the MAC frame constitutes a packet which is exchanged between two wireless nodes without a distribution system. DA indicates the destination address, SA the source address of the frame, which are identical to the physical receiver and sender addresses respectively. The third address identifies the *basic service set (BSS ID)*, the fourth address is unused (see the following Figure).

Case 2) Infrastructure network, from AP: If only the 'from DS' bit is set, the frame physically originates from an access point. DA is the logical and physical receiver, the second address identifies the BSS, the third address specifies the logical sender, the source address of the MAC frame. This case is an example for a packet sent to the receiver via the access point.

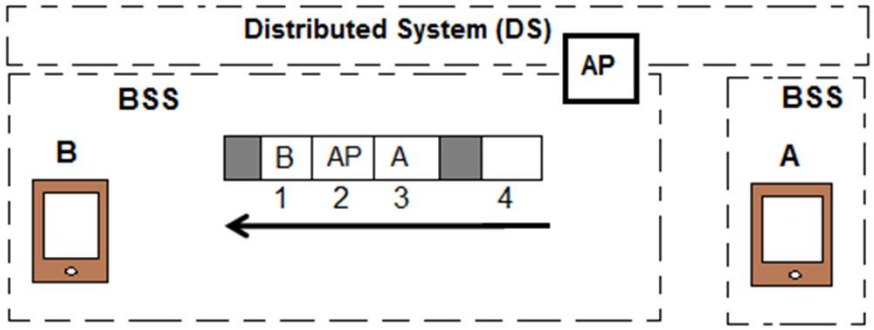
Case (3) Infrastructure network, to AP: If a station sends a packet to another station via the access point, only the 'to DS' bit is set. Now the first address represents the physical receiver of the frame, the access point, via the BSS identifier. The second address is the logical and physical sender of the frame, while the third address indicates the logical receiver.

Case (4) Infrastructure network, within DS: For packets transmitted between two access points over the distribution system, both bits are set. The first **receiver address (RA), represents the MAC address of the receiving access** point. Similarly, the second address **transmitter address (TA), identifies the** sending access point within the distribution system. Now two more addresses are needed to identify the original destination DA of the frame and the original source of the frame SA. Without these additional addresses, some encapsulation mechanism would be necessary to transmit MAC frames over the distribution system transparently.

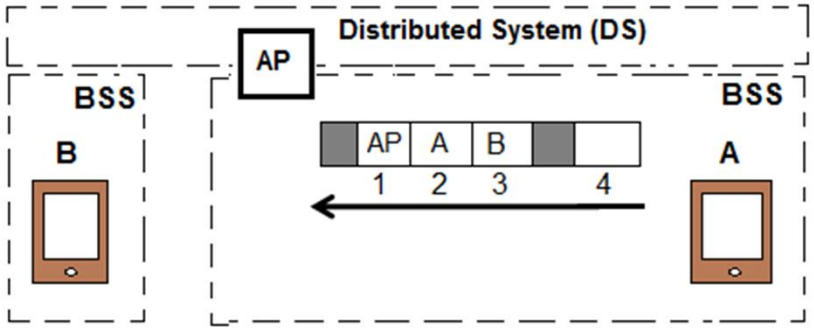
WiFi Communication Cases



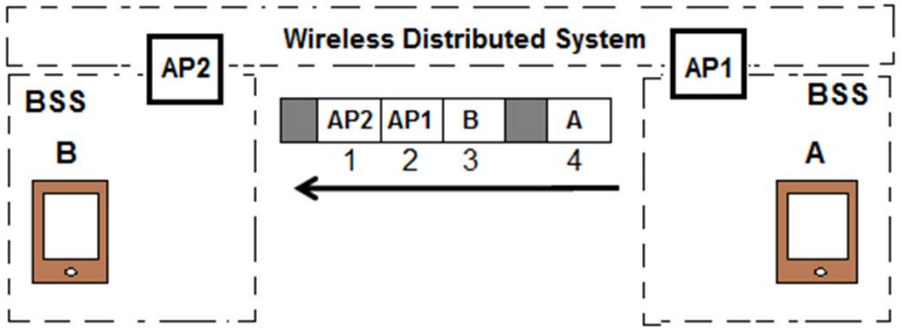
Case (1) two WiFi nodes communicating without DS
(to DS=0, from DS=0, address_1= DA, Address_2= SA)



Case(2) distributed system through AP sends to WiFi node B
(to DS=0, from DS=1, address_1= DA, address_2= TA, address_3= SA)



Case (3) WiFi node A sends to DS through AP.
(to DS=1, from DS=0, address_1=RA, address_2=SA, Address_3=DA)



Case (4) frame is going from AP1 to AP2 in the wireless DS.
(to DS=1, from DS=1, address_1=RA, address_2=TA, address_3=DA, address_4=SA

3.3.3 CSMA/CA

In wireless LANs it is not practical to do collision detection because of two main reasons:

1. Implementing a collision detection mechanism would require the implementation of a full duplex radio, capable of transmitting and receiving at once. Unlike wired LANs, where a transmitter can simultaneously monitor the medium for a collision, in many wireless LANs the transmitter's power overwhelms a collocated receiver. The dynamic range of the signals on the medium is very large. This is mainly result of the propagation loss, where the signal drops exponentially from its source (remember Figure 2-14(a)!). Thus, a transmitting station cannot effectively distinguish incoming weak signals from noise and the effects of its own transmission.

2. In a wireless environment we cannot assume that all stations hear each other, which is the basic assumption of the collision detection scheme. Again, due to the propagation loss we have the following problem. The fact that the transmitting station senses the medium free does not necessarily mean that the medium is free around the receiver area. (This is the so called "hidden station problem," to be considered below.)

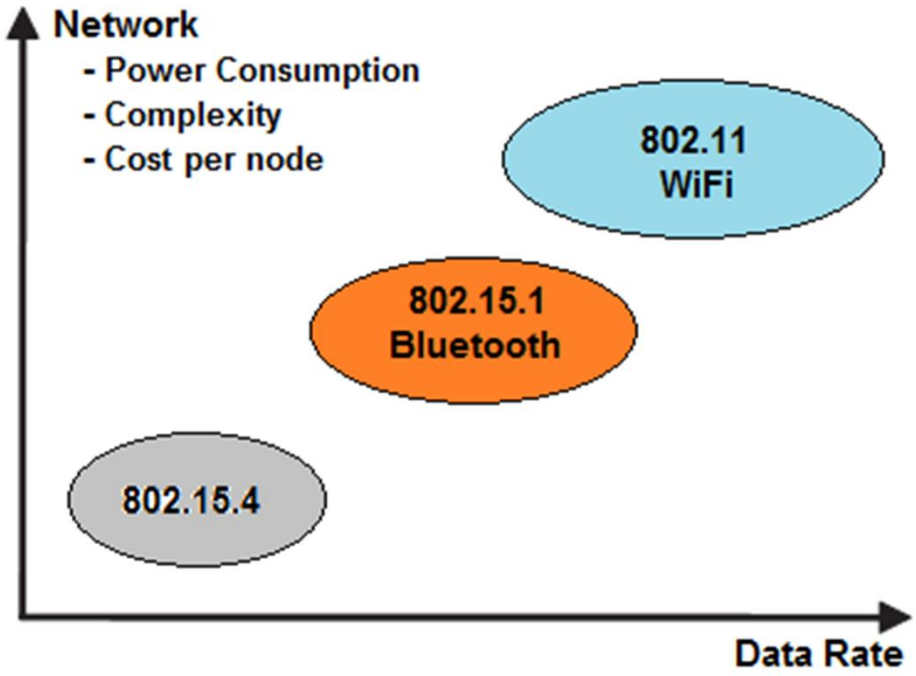
CSMA/CA is essentially *p*-persistence, with the twist that when the medium becomes idle, a station must wait for a time period to learn about the fate of the previous transmission before contending for the medium. After a packet was transmitted, the maximum time until a station detects a collision is twice the propagation time of a signal between the stations that are farthest apart plus the detection time. Thus, the station needs at least 2β units. The time interval between packets (frames) required for carrier sense mechanism to determine that the medium is idle and available for transmission is called *interframe space* (IFS). A station gets a higher priority if it is assigned a smaller interframe spacing.

When a station wants to transmit data, it first senses the medium whether it is busy. Two basic rules apply here:

1. If the medium has been idle for longer than an IFS corresponding to its priority level, transmission can begin immediately.
2. If the medium is busy, the station enters the *access deferral* state. The station continuously senses the medium, waiting for it to become idle. When the medium becomes idle, the station first waits for an IFS, then sets a *contention timer* to a time interval randomly selected in the range [0, $CW-1$], where CW is a predefined contention window length. The station can transmit the packet after this timer expires.

- WiFi devices roll-out in the coming years, WiFi Direct will pay a big role in sharing content between various kinds of devices such as smart tvs, tablets, smartphone, Monitors and projectors.

Comparing WiFi with other personal technologies



	Data Rate	Coverage (Range)
IEEE802.15.4	20 to 250 Kbps	10–100 m
Blutooth	1 Mbps	2–10 m
WiFi	1 to 11 Mbps	30–100 m

Comparing WiFi with other personal technologies

WPAN / Properties	WiFi	Bluetooth	IEEE802.15.4
Max Network Size	32	8	65,535
Range	100 m	10 m	70 – 100 m
MAC protocol	CSMA/CA	TDMA/TDD	CSMA/CA
Modulation (PHY)	DSSS/CCK	FHSS/BPSK	DSSS/QPSK DSSS/BPSK
Number of channels	14	79	27
Data Rate	11 Mbps	1 Mbps	250 Kbps
Latency	3 ms	200 – 300ms	30 ms
RTT	4 - 200ms		
Power Consumption	hours	days	months
Network Complexity	high	medium	simple

References

[1] Forouzan, B., Data Communications and Networking, 4ed.

[2] Marsic, I., Wireless Networks, Local and ad hoc networks, Rutger University.

[3] Tanenbaum, Computer Networks, 5ed.