Chapter 4

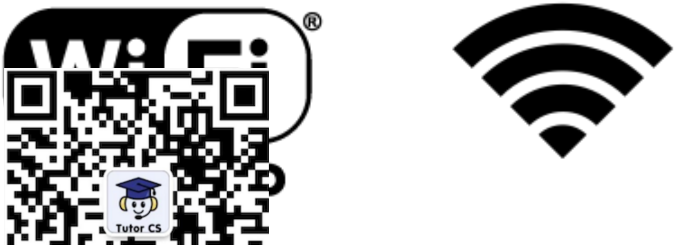
WiFi

WiFi, which sta[illegible]delity”, is one of the most widely used wireless networking tec[illegible] millions of them deployed in our homes and workplaces. WiFi is also increasingly available in many indoor and outdoor public places such as airports, shopping malls, parks and university campuses. All personal mobile devices, such as smartphones, tablets, and laptops are fitted with WiFi interfaces, making them very easy to be connected to such networks wherever they are available. In most cases, WiFi is available for free to use or at least there is no limit imposed on the volume of data for paid subscriptions, making it the most desired option to get connected to the Internet. WiFi has gone through many years of developments and upgrades over the last decade, resulting in increased level of complexity adopted in its recent standards. This chapter will explain the basic features and functions of the WiFi technology, while the more advanced versions will be examined at later chapters.

4.1 WiFi vs. IEEE 802.11

Both IEEE 802.11 and WiFi basically refer to wireless LANs. There is however a subtle difference between them. 802.11 is an IEEE standard for wireless LANs. Unfortunately, to satisfy a large number of different vendors contributing to the standardization process, 802.11 specification comes with many different options to implement. This raises a practical interoperability issue if different vendors choose to implement different options of the same 802.11 standard.

To overcome the potential interoperability problem of 802.11, an industry alliance was formed, called Wireless Fidelity or WiFi Alliance. This alliance commits to a selected set of options that all members will implement, essentially guaranteeing the ultimate interoperability that was envisaged by IEEE 802.11. Now, any product displaying the WiFi logo is guaranteed to work with any other product displaying the same, irrespective of who manufactures them. With WiFi, wireless LAN now has its “fidelity”, i.e., its ability to work with others. Note that the display of the WiFi icon, i.e., a small radar symbol, when trying to connect a device to a WiFi network is not about certifying the WiFi product, but to basically indicate that the device is connected to WiFi. Figure 4.1 shows the difference between WiFi logo and WiFi icon. Details of WiFi can be found from wi-fi.org, while IEEE 802.11 details are available from ieee.org.



ogo (left) vs. WiFi Icon (right)

4.2 IEEE Standards Numbering System

IEEE has a peculiar numbering system for all its standards. Anyone trying to follow the IEEE standards for wireless LANs must be familiar with this numbering system.

In early 1980s, a group was formed called 802, which defined logical link control (802.2), bridging and management (802.1) and security (802.10) functionalities for communication networks. Later, many different types of wired and wireless networks were formed and numbered starting from 802.3, such as Ethernet (802.3), WiFi (802.11), and so on. All these networks starting from 802.3 onwards are defined by the same link control, bridging, management, and security standards. Consequently, IEEE 802.11 follows 802.1 and 802.2. The hierarchy of the numbering system is shown in Figure 4.2

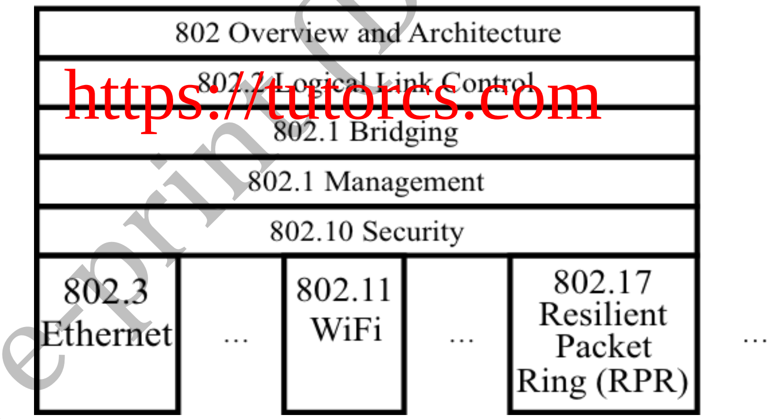

802 Overview and Architecture
802.2 Logical Link Control
802.1 Bridging
802.1 Management
802.10 Security
802.3 Ethernet
...
802.11 WiFi
...
802.17 Resilient Packet Ring (RPR)
...

Figure 4.2: Hierarchy of IEEE 802 numbering system

Standards with letters appended after an 802 standard applies only to that particular 802 networks, but not others. For example, 802.11i will apply to WiFi devices, but not Ethernet (802.3) devices.

When letters are appended, they can be either lower case or upper case. Lower case letters represent temporary or interim revisions (also called "amendments"), which will eventually disappear before merging with a standard with an uppercase letter. Standards with upper case letters are permanent and are called "base standards". For example, IEEE 802.1w-2001 was merged with IEEE 802.1D-2004. Standards were originally numbered sequentially, such as 802.1a, …, 802.1z, 802.1aa, 802.1ab, and so on. Now base standard letters are being shown during the amendments, such as IEEE 802.1Qau-2010, where Q is the base standard and au is the amendment.

It is interesting to note that while IEEE uses letters to refer to different versions of the technology, Wi[illegible]ently opted to use numbers to name the WiFi versions. For ex[illegible] to IEEE 802.11n, 5 refers to 802.11ac and so on. Table 4.1 shows [illegible]umbers and their corresponding IEEE standards.

Table 4.1 WiF[illegible]nd their corresponding IEEE Standards

WiFi Alliance [illegible]	[illegible]EEE Standard
WiFi 4	802.11n
WiFi 5	802.11ac
WiFi 6	802.11ax
WiFi 7	802.11be

4.3 IEEE 802.11 Features

The original 802.11 standard in 1997 specified only 1 and 2 Mbps. Newer versions offered successively higher speeds at 11 Mbps, 54 Mbps, 108 Mbps, 200 Mbps, and so on. All these versions were specified for “license-exempt” or “license-free” spectrum, i.e., spectrum which we are not required to license by law.

When the spectrum is license-exempt, a technology is required to prevent spectrum hogging. 802.11 employs spread spectrum techniques at the physical layer to solve the hogging problem. More specifically, for the Industrial, Scientific, and Medical (ISM) bands, it uses either Direct Sequence (DS) spread spectrum or Frequency Hopping spread spectrum. 802.11 specifies a third physical layer called Diffused Infrared to be used with the infrared band in 850-900nm.

802.11 supports multiple priorities to deliver both time-critical, such as voice, and data traffic over the same LAN infrastructure. It also supports power management, which enables nodes to go to sleep mode when there is no traffic to conserve power.

4.4 ISM Bands

The license-exempt spectrum to be used by wireless LANs is called the Industrial, Scientific, and Medical (ISM) band. As shown in Table 4.2, there are many different available ISM bands of varying bandwidth [ITU2018]. The bands available in the lower frequency has understandably smaller bandwidth whereas increasing bandwidth is available at higher frequency ISM bands. For example, the 6.765 MHz band has only 30 kHz bandwidth whereas a massive 150 MHz bandwidth is available at 5.725 GHz.

The original WiFi started with the 2.4 GHz band. However, 2.4 GHz was already in use by a large variety of products such as medical equipment, microwave, garage door openers and so on. When the WiFi usage started to grow, 2.4 GHz became saturated, prompting the opening of a new WiFi band at 5.725 GHz, which is simply referred to as 5 GHz band. Most recent WiFi routers can operate over both bands, hence they are marketed as “dual band” routers. In recent years, many more bands have been released to support new types of WiFi, which are listed in Table 4.3.

Table 4.2 ISM Bands	
Frequency Range	Bandwidth
6.765MHz – 6.795MHz	30kHz
13.553MHz -1[illegible]	14kHz
26.957MHz – 2[illegible]	326kHz
40.660MHz – 4[illegible]	40kHz
433.050MHz – [illegible]	1.74MHz
902MHz – 928[illegible]	26MHz
2.4GHz – 2.5G[illegible]	100MHz
5.725GHz – 5.8[illegible]GHz	150MHz
24.000GHz – 24.250GHz	250MHz
61GHz – 61.5GHz	500MHz
122GHz – 123GHz	1GHz
244GHz – 246GHz	2GHz

Table 4.3 WiFi bands	
WiFi Standard	Frequency Band
802.11b/g/n	2.4 GHz
802.11a/n/ac/ax	5 GHz
802.11be	6 GHz (not confirmed yet)
802.11p (car-to-car)	5.9 GHz (licensed band)
802.11ah (IoT)	900 MHz
802.11af (Rural)	700 MHz (unused TV channels)
802.11ad/ay (Multi Gbps wireless applications: e.g., cable replacement, VR, …)	60 GHz

4.5 IEEE 802.11 Channels

The WiFi bands are divided into separate channels to facilitate better management of congestion when multiple wireless LANs operate in close proximity. Two different LANs then can simply choose to operate in two different channels of the same band and yet avoid collisions and interference from each other. It should be noted that an AP and any WiFi devices connected to it operate over a single channel, the channel that is selected by the AP at any given time.

Each channel is usually 20 or 22 MHz wide. WiFi operating in the 2.4 GHz band uses 22 MHz channels, while 5 GHz band uses 20 MHz channels. With newer WiFi versions, it is possible to combine two or more channels to get a wider channel for higher data rates.

2.4 GHz WiFi has a total of 14 channels although not all channels are available in all countries. Table 4.4 lists the lower, center, and upper frequencies for these 14 channels. As can be seen, each channel is 22 MHz wide while their center frequencies are 5 MHz apart from each other with the exception of channel 14. Table 4.4 also shows that with 20-MHz, only a small number of non-overlapping channels are possible. Specifically, for 2.4 GHz WiFi, we can choose from 3 available non overlapping channels numbered as 1, 6, and 11. Most WiFi routers select channel 6 as default.

In contrast to 2.4 GHz, 5 GHz WiFi has 20 MHz non-overlapping channels. 5 GHz uses two types of cha[illegible] channels is always available, while the others are actually shared [illegible] Dynamic Frequency Selection (DFS) algorithm. With DFS, 5 GH[illegible] radar channels and immediately vacate them, i.e., switch to anothe[illegible] detected in the operating channel. User devices connected to su[illegible] en will also need to switch to the new channel, which may caus[illegible] tion drop.

Table 4.4 Channel frequencies for 2.4 GHz WiFi

Channel Number	Lower Frequency (MHz)	Center Frequency (MHz)	Upper Frequency (MHz)
1	2401	2412	2423
2	2406	2417	2428
3	2411	2422	2433
4	2416	2427	2438
5	2421	2432	2443
6	2426	2437	2448
7	2431	2442	2453
8	2436	2447	2458
9	2441	2452	2463
10	2446	2457	2468
11	2451	2462	2473
12	2456	2467	2478
13	2461	2472	2483
14	2473	2484	2495

4.6 Physical Layers

The physical layer technology directly affects the data rate achievable with WiFi. In the first version defined in 1997, spread spectrum was used to achieve only 1 and 2 Mbps, which was soon proved to be too slow for the emerging LAN applications. Two years later, in 1999, an advanced version of spread spectrum was introduced for 2.4 GHz, while OFDM was introduced for the 5-GHz band to increase the data rate to 54 Mbps. In 2003, OFDM was also successfully used in 2.4 GHz to achieve 54 Mbps channels, which was named 802.11g. OFDM has proved so successful that it still defines the physical layer standard for today's WiFi.

4.7 Hidden Node Problem

Unlike wired LAN (Ethernet), Wireless LAN suffers from a specific collision detection problem called *hidden node problem*. Let's consider the three wireless nodes, A, B, and C, as shown in Figure 4.3. Let us assume that A can hear B, B can hear C, but C cannot hear A. Now, C may start transmitting to B while A is also transmitting to B. Clearly, collisions will be experienced at B, making it difficult for B to understand either of the communications. Unfortunately, the transmitters A and C cannot detect the collision. Only the receiver, B, can detect it. Therefore, unlike Ethernet, where transmitters can detect collision a[illegible] LAN must implement some other techniques that can avoid such [illegible]st place. Wireless LANs therefore use collision avoidance (CA) [illegible]n detection (CD) used in Ethernet.

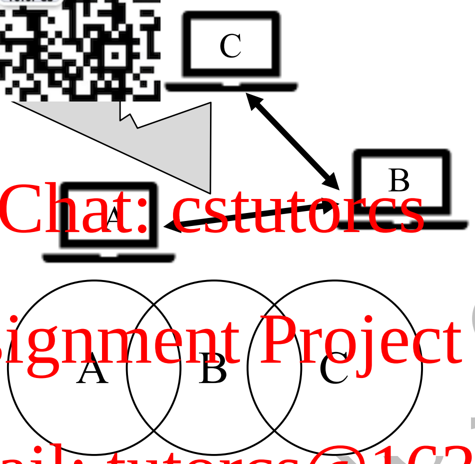


Figure 4.3 Hidden node problem in 802.11.

4.8 Collision Avoidance with 4-way Handshake

In wireless LAN, CA is achieved by a 4-way handshake process as shown in Figure 4.4. Essentially, four packets are transmitted for each data packet, i.e., three control packets are needed to avoid collision for each data packet transmitted.

The 4-way handshake begins with the transmitter first transmitting a ready-to-send (RTS) packet. If the receiver receives it and wishes to allow the transmitter to go ahead, then it will transmit a clear-to-send (CTS) packet. The transmitter sends the data packet only if and when it receives the CTS, which avoids collision with other potential transmitters as they defer their transmissions upon hearing the CTS. Finally, the receiver transmits an acknowledgment to confirm the correct reception of the data packet from the transmitter. This procedure needs to be repeated for each data packet.

Although it may sound like too much overhead to avoid collision, the actual overhead of the 4-way handshake has to be analyzed more carefully. The RTS and CTS packets are very short lasting only a few microseconds. The data packets, on the other hand, are long lasting, tens to hundreds of milliseconds depending on the speed of the network. Thus, avoiding collision of a long data packet with tiny RTS/CTS packets is worth the effort.

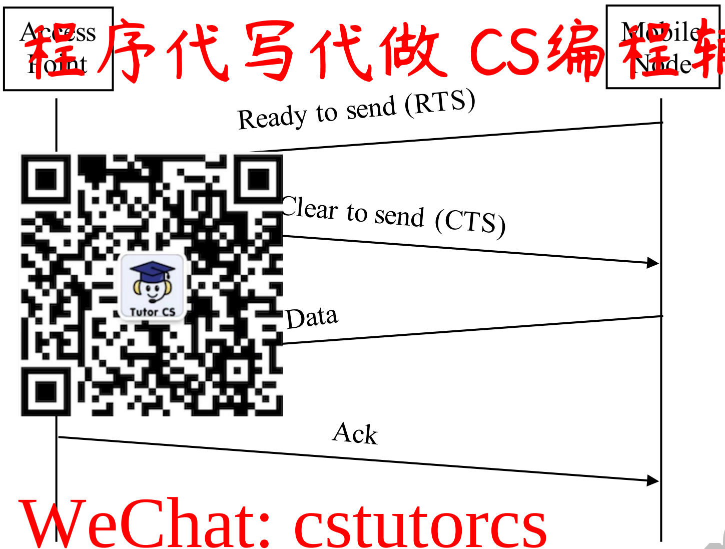


Figure 4.4 4-way handshake using RTS/CTS to avoid collision in 802.11

4.9 IEEE 802.11 Medium Access Control (MAC)

To completely realize the medium access control (MAC), the 4-way handshake must work in conjunction with the carrier sense multiple access (CSMA) function. CSMA basically says that a wireless node must first listen the channel before even attempting the 4-way handshake and backoff for a random period if it finds the channel busy. The 4-way handshake is launched only if the channel was found idle.

The RTS and CTS packets contain the duration of the data packet, which allows other nodes who hear the CTS to stay away from attempting channel sensing. Finally, to achieve reliability, the transmitter must retransmit the data packet if it does not receive the ACK from the receiver.

4.9.1 IEEE 802.11 Priorities

Wireless LAN has different priorities for control and data packets. These priorities are achieved by enforcing different amounts of interframe space (IFS) as shown in Figure 4.5. After the channel busy period ends, the RTS, CTS, and ACK packets can be transmitted by waiting only a short IFS (SIFS), but medium priority time-critical frames, such as those used for periodic channel reservation in Point Coordination Function (PCF) mode, will have to wait slightly longer than SIFS. Finally, the data frames, which use Distributed Coordination Function (DCF), will wait a bit more before attempting transmission.

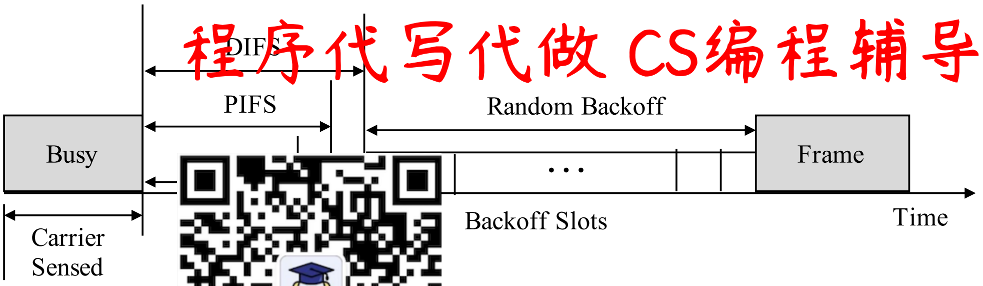


Figure 4.5 Inter priorities in 802.11

4.9.2 Time Crit

The wireless LAN base station uses the PCF to achieve a contention-free period (CFP) to allow transmission of data from time-critical services. The base station periodically transmits a beacon and then using a polling frame grants one node to access the channel without any contention. During the CFP, no other nodes will attempt access to the channel. The duration of CFP will vary with the load of the time critical data. The channel will be opened for contention as soon as the PCF ends. Thus, the channel access alternates between PCF and DCF, which is shown in Figure 4.6.

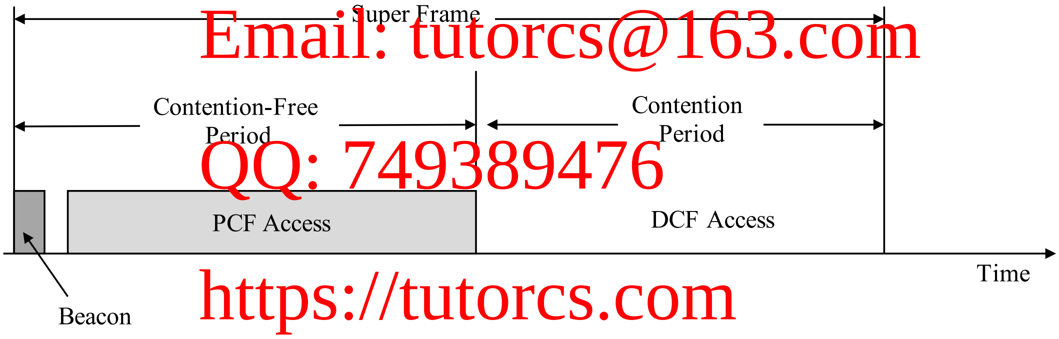


Figure 4.6 Time critical services using the PCF function. DCF follows PCF.

4.9.3 IEEE 802.11 DCF Backoff

For effective sharing of the channel with many users, DCF uses a sophisticated backoff mechanism to prevent a node from hogging the channel. Each node maintains a FIFO (first in first out) queue to store the data packets to be transmitted. For transmitting the head of the queue, the node implements the DCF backoff mechanism, which requires three variables, Contention Window (CW), Backoff Count (BO), and Network Allocation Vector (NAV), to be maintained.

If a frame (RTS, CTS, Data, Ack) is heard, NAV is set to the duration in that frame. Nodes are allowed to sense the media only after NAV expires. NAV therefore is basically a timer that prevents a node from even sensing the channel if the node has explicit knowledge about the future busy time of the channel.

If the medium is idle for DIFS, and backoff (BO) is not already active, the node draws a random BO in [0, CW] and sets the backoff timer. The node can only start transmission if the channel continues to be idle during this backoff time. If the medium becomes busy during backoff, the timer is paused, and a new NAV is set. After NAV, i.e., when the channel becomes idle again, the back off continues from the previous BO value.

Because collisions can still occur after transmission, each transmitted packet is acknowledged l CF backoff time increases exponentially with successive failec smission attempts, i.e., when no ACK is received, to make it mor heavy load. Initially and after each successful transmission (A ets CW = CW_{min}. Then after each unsuccessful attempt: CW = r ax}. It should be noted that CW is in units of slot time, which vari ards as shown in Table 4.5. We also have PIFS = SIFS+1 slot time 2 slot time.

Table 4.5 Slot time and MAC parameters for WiFi standards

WLAN	Slot-time (µs)	SIFS (µs)	CWmin	CWmax
11a	9	16	15	1023
11b	20	10	31	1023
11g	9 or 20	10	15 or 31	1023
11n (2.4 GHz)	9 or 20	10	15	1023
11n (5 GHz)	9	16	15	1023
11ac	9	16	15	1023

Example 4.1

Assume that we have CW_{min}=3 and CW_{max}=127 configured for a given WLAN. What would be the values of CW if there were 8 successive unsuccessful attempts after initalizing the network?

Solution:

After initialization, CW = CWmin = 3
After 1st unsuccessful attempt, CW = min(7,127) = 7
After 2nd unsuccessful attempt, CW = min(15,127) = 15
Then on, 31, 63, 127, 127, 127, …

Example 4.2

What is the duration of PIFS and DIFS for IEEE 802.11b?

Solution:

Slot time = 20 µ
SIFS = 10 µs
PIFS = SIFS + s 0 µs
DIFS = SIFS + 2 0 = 50 µs

4.9.5 Virtual Carrier Sense

Continuous carrier sensing for a prolonged period of time can drain the batteries of wireless nodes. To avoid unnecessary carrier sensing, WiFi uses virtual carrier sensing using the NAV parameter. This is possible because every frame has a Duration ID field which indicates how long the medium will be busy for transmitting this frame. Table 4.6 shows how this duration is calculated for different types of frames.

Table 4.6 Durations for different types of frames

Frame Type	Duration
RTS	RTS + SIF + CTS + SIF + Frame + SIF + Ack
CTS	CTS + SIF + Frame + SIF + Ack
Frame	Frame + SIF + Ack
Ack	Ack

Once a node hears a frame, it sets a NAV timer for the Duration ID of the frame and can go to sleep for conserving its battery. No physical carrier sensing is done during this period. The node wakes up after the NAV period to start sensing again.

Example 4.3:

Consider an 802.11b WLAN. A station estimates the transmission times of RTS, CTS, and ACK as 10 µs, 10 µs, and 25 µs, respectively. What would be the value of the Duration field in the RTS header if the station wants to send a 250 µs long data frame?

Solution:

802.11b has a SIFS duration of 10 µs.
Duration field in RTS = RTS_time + CTS_time + ACK_time + data_time + 3xSIFS
= 10+10+25+250+3x10 = 325 µs

4.9.6 DCF Example

Figure 4.7 shows an example of how DCF works, where A, D, C, and R, represent ACK, Data, CTS, and RTS, respectively, and Table 4.7 traces the events at different points in time.

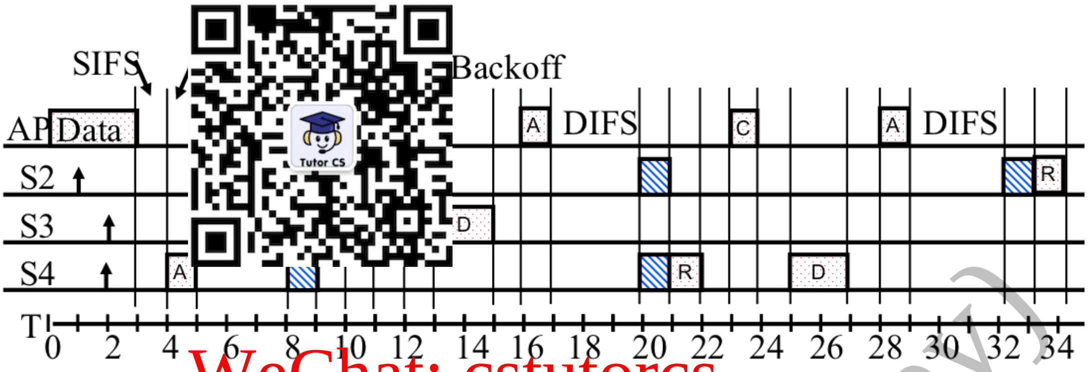


Figure 4.7 DCF example

Table 4.7 Event trace for DCF example

Time	Event
T1	Station 2 wants to transmit but the media is busy
T2	Stations 3 and 4 want to transmit but the media is busy
T3	Station 1 finishes transmission.
T4	Station 1 receives ack for its transmission (SIFS=1); Stations 2, 3, and 4 set their NAVs to 1.
T5	Medium becomes free
T8	DIFS expires. Stations 2, 3, 4 draw backoff count between 0 and 5. The counts are 3, 1, 2
T9	Station 3 starts transmitting and announces a duration of 8 (RTS + SIFS + CTS + SIFS + DATA + SIFS + ACK). Station 2 and 4 pause their backoff counters at 2 and 1, respectively.
T15	Station 3 finishes data transmission
T16	Station 3 receives Ack.
T17	Medium becomes free
T20	DIFS expires. Station 2 and 4 notice that there was no transmission for DIFS. Stations 2 and 4 start their backoff counters from 2 and 1, respectively.
T21	Station 4 starts transmitting RTS

4.10 IEEE 802.11 Architecture

Figure 4.8 shows how the various elements of WiFi networks are connected to each other. The architecture has the following elements:

Basic Service Set (BSS): Set of all nodes associated with one AP. Like the “cell ID” in cellular networks, each BSS is identified with a unique Service Set ID (SSID), which is usually the 48-bit MAC address of the AP.

Distribution System (DS): A system of multiple APs connected together via a wired backbone. Usually the wired backbone is made from Ethernet and is hidden against ceiling or other infrastructure, so it is not visible to public.
Independent Basic Service Set (IBSS): Set of nodes connecting independently in *ad-hoc mode* withou the WiFi infrastructure. Ad-hoc networks coexist and inter ucture-based networks

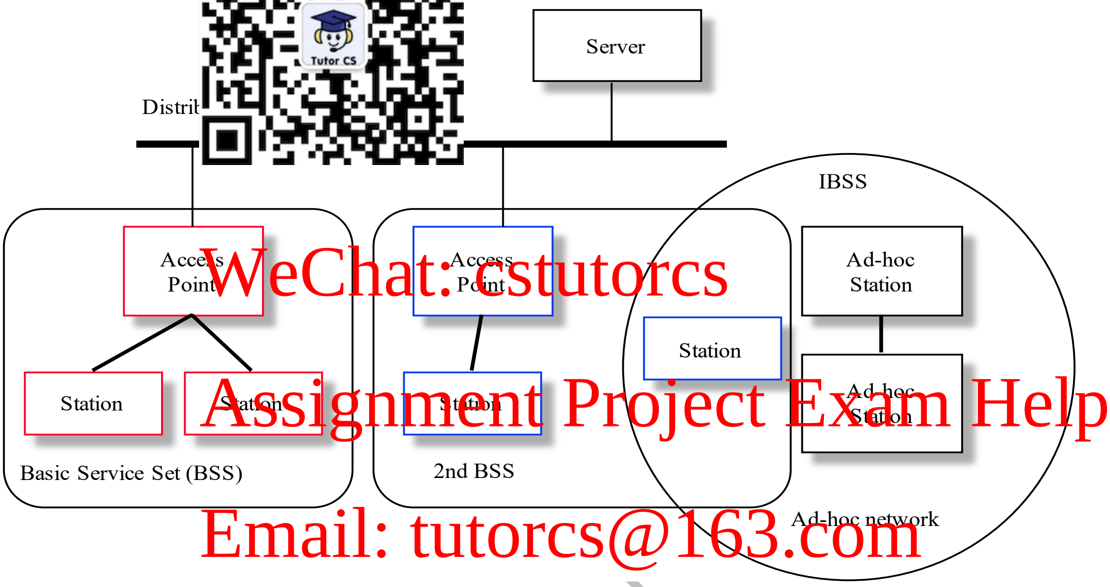
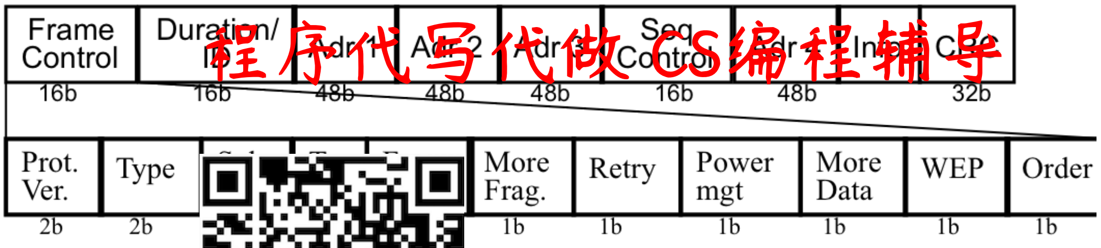


Figure 4.8 Elements of IEEE 802.11 Architecture

4.11 IEEE 802.11 Frame Format

Figure 4.9 shows the WiFi frame format, all fields and their relative positions in the frame. There are a total of 9 main fields in the frame as explained below:

Frame Control: A 16-bit field that defines many control functions for the frame, which will be described later.
Duration/ID: A 16-bit field that follows the Frame Control field. If used as duration field, indicates the time in micro seconds the channel will be allocated for successful transmission of MAC frame, which includes time until the end of Ack. In some control frames, it contains association or connection identifier.
Adr 1/2/3/4: These are 48-bit address fields. It is interesting to see that WiFi uses four address fields, while most other networks, such as Ethernet, uses only two. Use of four address fields will be explained later.
Seq Control: It is a 16-bit field. Its main function is to number frames between a pair of transmitter and receiver using 12 bits and manage fragmentation and reassembly using a 4-bit fragment sub-field.
Info: the field that carried user data or payload.
CRC: 32-bit cyclic redundancy check to detect frame errors.



[illegible]me format of IEEE 802.11

The Frame Cont[illegible]ields:

Protocol Version: It provides the version number.
Type: Control, management, or data
Sub-Type: Association, disassociation, re-association, probe, authentication, de-authentication, CTS, RTS, Ack . . .
To DS: Going to Distribution System
From DS: Coming from Distribution System
More Fragment: Used to indicate whether this is the last fragment or more fragments are following. This helps with fragment reassembly at the receiver.
Retry: Whether it is a retransmission or original transmission.
Power mgt: Node indicating whether it is going to sleep (Power Save mode)
More data: Whether there is more buffered data at AP for a station in power save mode
Wireless Equivalent Privacy (WEP): Security info in this frame
Order: Strict ordering

4.12 Use of 802.11 Address Fields

There are four address fields to provide greater control of how packets can be "routed" from source to destination. Figure 4.10 illustrates the various use contexts of these four addresses, where Source/Destination refers to the ultimate network devices that prepare and decode the frame for network layer, Tx/Rx could be the source/destination, or intermediate radio devices, e.g., access point (AP). The 4 address fields are defined by the 2 DS bits as shown in Table 4.8 [GAST2005]. Uses of the four address fields in wireless client-server communications are further illustrated in Figures 4.11 and 4.12.

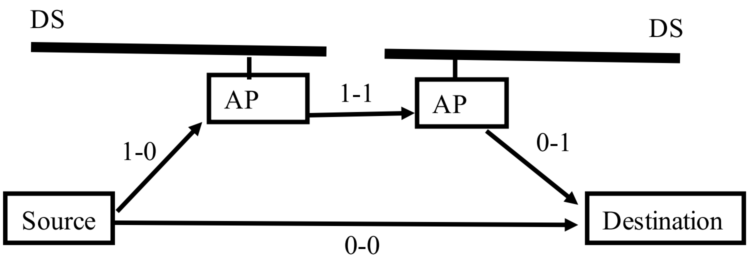
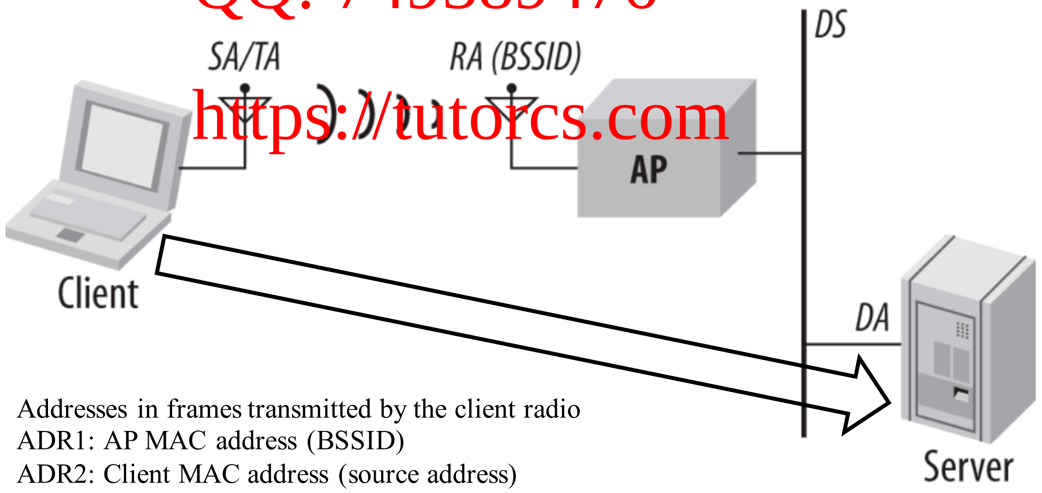


Figure 4.10 802.11 address fields and their use

Table 4.8 Meaning of WiFi address fields

Purpose	ToDS	FromDS	ADR1 (Rx)	ADR2 (Tx)	ADR3	ADR4
IBSS			DA	SA	IBSSID	N/A
From AP (from infra.)	0	1	DA	BSSID	SA	N/A
To AP (to infra.)	1	0	BSSID	SA	DA	N/A
AP-to-AP (W'less Brdg)	1	1	RxA	TxA	DA	SA



Addresses in frames transmitted by the client radio
ADR1: AP MAC address (BSSID)
ADR2: Client MAC address (source address)
ADR3: Server MAC address (destination address)
ADR4: Not applicable

Figure 4.11 Wireless client transmitting to a wired server

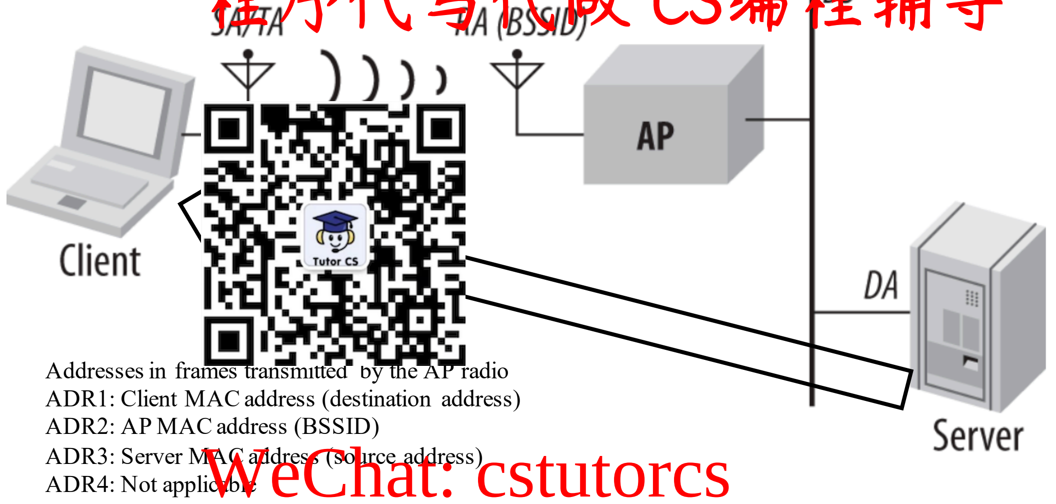

SA/TA
RA (BSSID)
AP
Client
DA
Server
Addresses in frames transmitted by the AP radio
ADR1: Client MAC address (destination address)
ADR2: AP MAC address (BSSID)
ADR3: Server MAC address (source address)
ADR4: Not applicable

Figure 4.12 Wired server transmitting to a wireless client

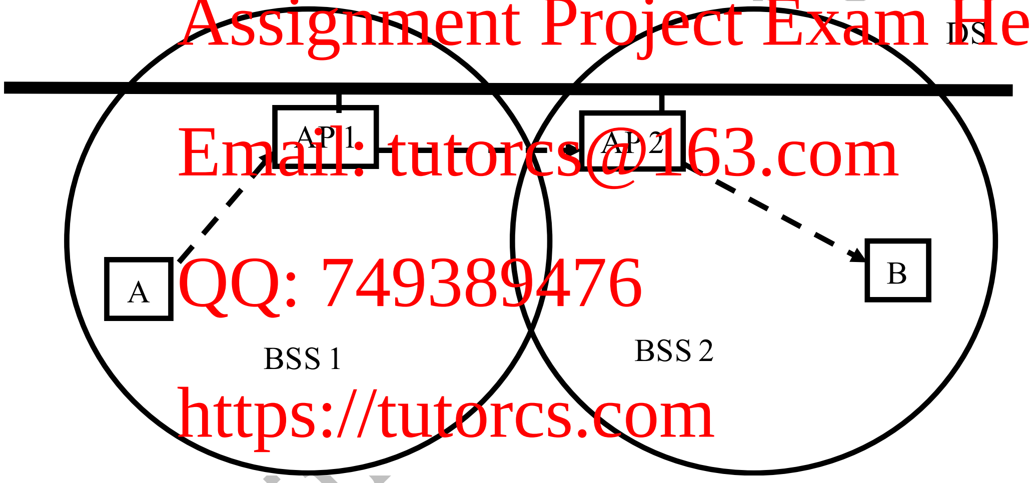


Figure 4.13 Example of two BSSs interconnected via a DS

Example 4.4:

Consider the example WLAN in Figure 4.13 where two BSSs are connected via a distribution system. What is the content of the Address 3 field when Station A wants to send a packet to Station B via AP 1?

Solution:

In this case (To DS=1, From DS=0), Address 3 field should contain the address of the destination station. Therefore, it should be the address of B.

4.13 802.11 Power Management

Extending the battery life of portable devices is one of the main challenges of wireless networks. As the battery technology itself is not advancing fast, mechanisms must be devised to let th[illegible]ch as possible and wake up only when it needs to transmit or recei[illegible]ckets to be received, a receiver could go to sleep and save battery[illegible]e this kind of power saving, WiFi has a power management fun[illegible]

To invoke the p[illegible]nction, the node uses the Power Management bit in the frame cont[illegible] to the AP that it is going to sleep. Upon receiving this information, the AP buffers all packets for this node. When the node wakes up, it waits for the beacon packet periodically sent by the AP. In the beacon packet, Traffic Indication Map (TIM) is a structure used by the AP to indicate which nodes has packets buffered.

If a node sees its bit turned on in the TIM, it does not go back to sleep. Instead, it sends a PS-Poll message to the AP and waits for the packet from the AP. The AP then sends one frame with buffered data and sets the More Data bit in the header if more data is waiting in the buffer. The client does not go back to sleep after receiving one frame if More is set.

4.14 Chapter Summary

1. 802.11 PHYs: Spread spectrum in earlier versions, but OFDM in new versions
2. 2.4 GHz channels (22 MHz) are mostly overlapped, while5 GHz channels (20 MHz) are non-overlapped, but some are shared with the radar service
3. 802.11 uses SIFS, PIFS, DIFS for priority
4. WLAN frames have four address fields
5. 802.11 supports power saving mode

References

[GAST2005] Matthew S. Gast, 802.11 Wireless Networks: The Definitive Guide, 2nd Edition, O'Reilly, 2005.

[ITU2018] Recommendation ITU-R SM.1896-1, International Telecommunication Union, September 2018.

End of Chapter 4 (Wireless and Mobile Networking, M. Hassan, 2022, CRC Press)