Wireless LAN I

IEEE 802.11 Basics

Overview

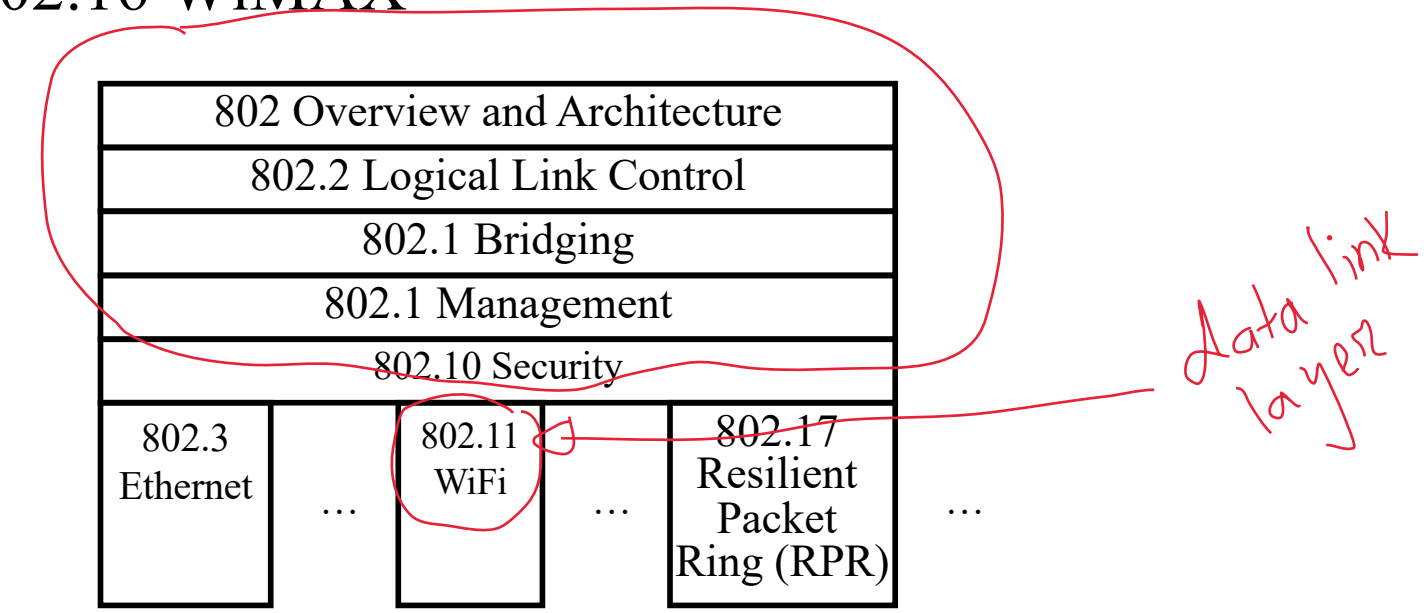
1. IEEE 802.11 vs. WiFi
2. IEEE Standards Numbering System
3. Key features of 802.11
4. 802.11 Bands and Channels
5. Hidden Node Problem and 4-Way Handshake RTS/CTS)
6. 802.11 MAC (inter-frame space, PCF, DCF)
7. 802.11 Architecture and Addressing
8. 802.11 Frame Format
9. 802.11 Power Management

IEEE 802.11 vs. WiFi

- IEEE 802.11 is a standard
- WiFi = "Wireless Fidelity" is a trademark
- Fidelity = **Compatibility** between wireless equipment from different manufacturers
- WiFi Alliance is a non-profit organization that does the compatibility testing (WiFi.org)
- 802.11 has many options and it is possible for two equipment based on 802.11 to be *incompatible*.
- All equipment with "WiFi" logo have selected options such that they will **interoperate**.

IEEE Standards Numbering System

- IEEE 802.* and IEEE 802.1* standards (e.g., IEEE 802.1Q-2011) apply to all IEEE 802 technologies:
  - IEEE 802.3 Ethernet
  - IEEE 802.11 WiFi
  - IEEE 802.16 WiMAX



Lettered vs. Numerical Versions

- IEEE 802.11 uses *letters* to name the versions
  - E.g., 802.11a/b (1999), 802.11g (2003), 802.11n (2009), 802.11ac (2013), and so on
- WiFi Alliance proposes numbers to simplify
  - E.g., WiFi 4 (802.11n), WiFi 5 (802.11ac), WiFi 6 (802.11ax) …

IEEE 802.11 Features

- Data rate (a.k.a. *speed*)
  - Original IEEE 802.11-1997 was at 1 and 2 Mbps.
  - Newer versions at 11 Mbps, 54 Mbps, 108 Mbps, 1.2 Gbps, …
- Spectrum licensing
  - All versions use *license-exempt* spectrum
- PHYs:
  - Spread spectrum (in old versions)
  - OFDM (in new versions)
- Supports multiple priorities (time-critical and data traffic)
- Power management allows a node to `doze off'
  - Longer battery life

one coin cell battery for 10 years for some sensors

IEEE 802.11 Physical Layers

- Issued in several stages
- First version in 1997: Legacy IEEE 802.11 (no longer used)
  - 3 physical layer specifications (2 in 2.4-GHz, 1 in infrared)
  - All operating at 1 and 2 Mbps
- Amendments in 1999:
  - IEEE 802.11a-1999: 5-GHz band, 54 Mbps/20 MHz, **OFDM**
  - IEEE 802.11b-1999: 2.4 GHz band, 11 Mbps/22 MHz (spread spectrum)
- Amendment in 2003:
  - IEEE 802.11g-2003 : 2.4 GHz band, 54 Mbps/20 MHz, **OFDM**

ISM Bands

- **I**ndustrial, **S**cientific, and **M**edical bands. **License exempt**

From	To	Bandwidth	Availability
6.765 MHz	6.795 MHz	30 kHz	
13.553 MHz	13.567 MHz	14 kHz	Worldwide
26.957 MHz	27.283 MHz	326 kHz	Worldwide
40.660 MHz	40.700 MHz	40 kHz	Worldwide
433.050 MHz	434.790 MHz	1.74 MHz	Europe, Africa, Middle east, Former Soviet Union
902.000 MHz	928.000 MHz	26 MHz	America, Greenland
2.400 GHz	**2.500 GHz**	**100 MHz**	**Worldwide**
5.725 GHz	**5.875 GHz**	**150 MHz**	**Worldwide**
24.000 GHz	24.250 GHz	250 MHz	Worldwide
61.000 GHz	61.500 GHz	500 MHz	
122.000 GHz	123.000 GHz	1 GHz	
244 GHz	246 GHz	2 GHz	

Ref: http://en.wikipedia.org/wiki/ISM_band

WLAN/WiFi Bands

main stream

niche

WLAN/WiFi Standard	Frequency Band
802.11b/g/n	**2.4 GHz**
802.11a/n/ac/ax	**5 GHz**
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

WiFi Channels

- The entire *band* is divided into several individual *channels*
- An AP operates over a **single channel** at any given time
- Different nearby APs can operate over different channels of the same band
  - Avoid congestion and interference
- Each channel is usually 20 or 22 MHz wide
- With newer WiFi versions, it is possible to combine two or more channels to get a wider channel
  - More bandwidth for higher data rates

only make sense when there is less interference from nearby AP (less densely populated wifi area)

2.4 GHz WiFi Channel Frequencies

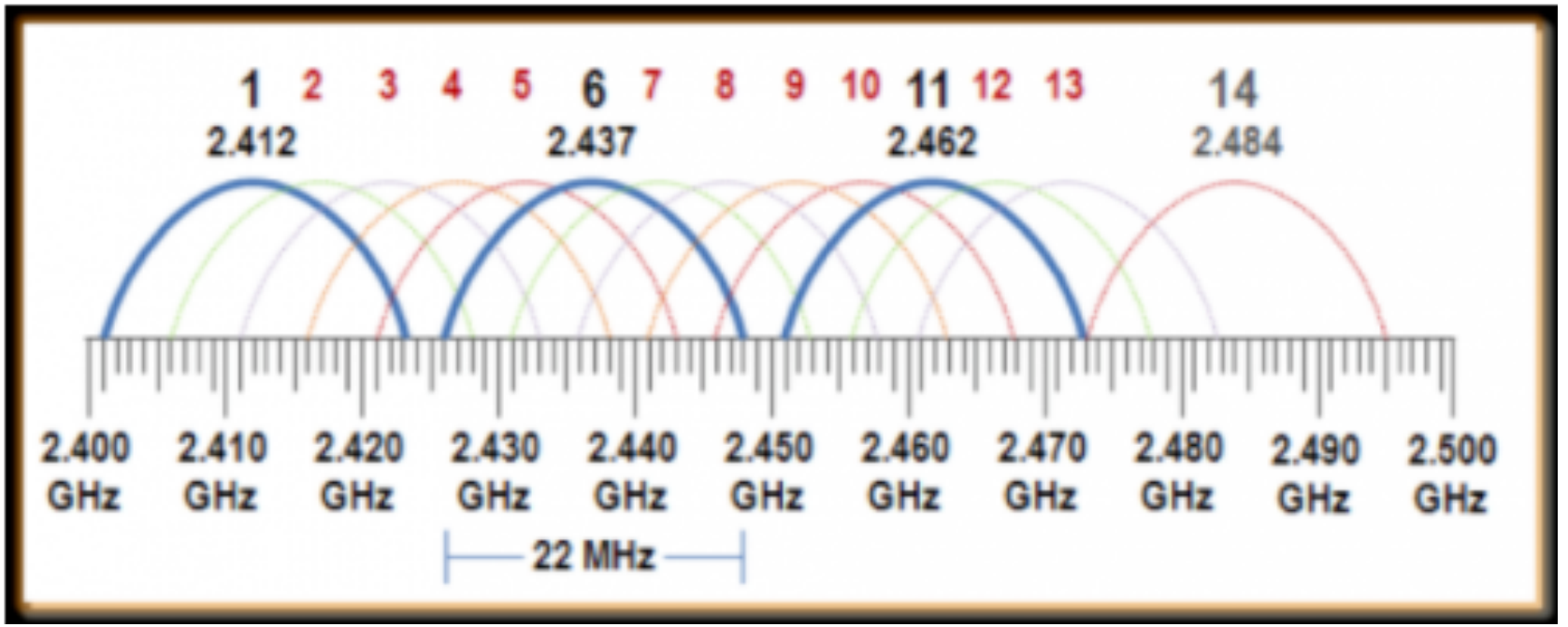
- A total of 14 channels (not all channels available in all countries)
- Centre frequencies are 5 MHz apart (except channel 14)
- Each channel is 22 MHz wide

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

From http://www.radio-electronics.com/info/wireless/wi-fi/80211-channels-number-frequencies-bandwidth.php

2.4 GHz Channel Overlaps

- Most channels in 2.4 GHz band overlap
- Maximum of three non-overlapping channels are possible
- 1-6-11 are most widely used non-overlapping channels (6 is usually default)
  - E.g., if three are three nearby APs in an enterprise, they are usually set to 1-6-11



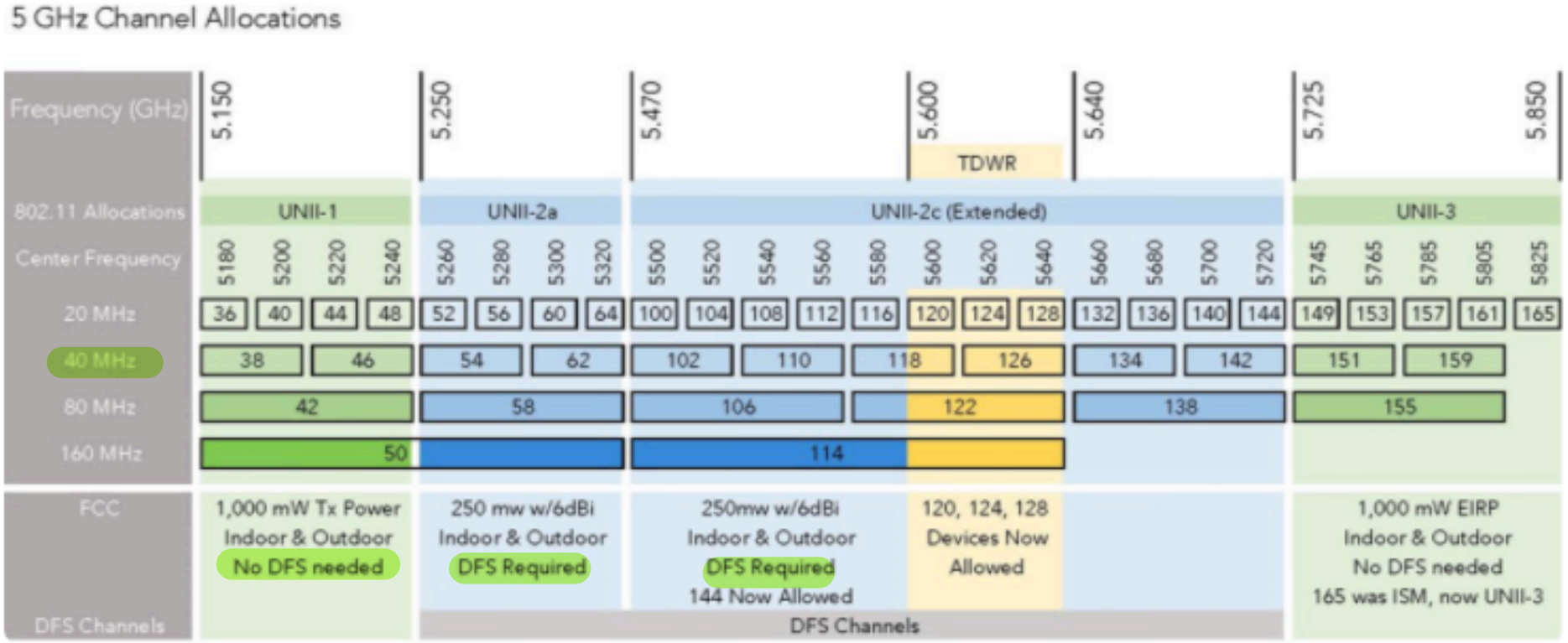
From http://boundless.aerohive.com/experts/WLAN-Channels-Explained.html

Channels in 5 GHz Band

- 20 MHz channels (c.f. 22 MHz in 2.4 GHz band)
- Non-overlapping (c.f., mostly overlapping in 2.4 GHz)
- Two types of channels
  - Always available
  - Channels used by **radar** (requires DFS)
- Dynamic Frequency Selection (DFS): WiFi AP monitors radar channels and vacate them (switch to another channel) if radar is detected
  - May cause connection drop for clients

wifi protocol has mechanisms for AP to notify the client that a channel switch is imminent

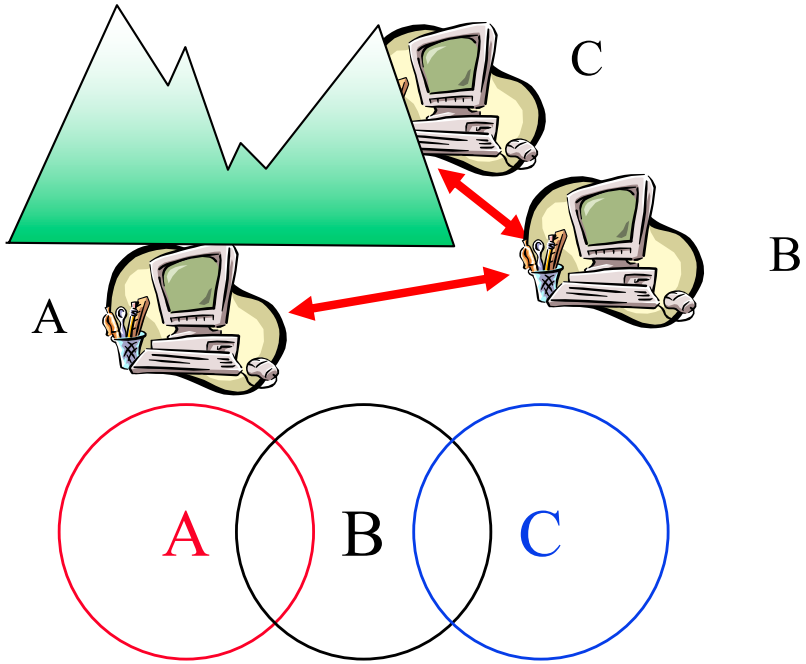
5GHz Channel Structure



Source: Wireless LAN Professionals

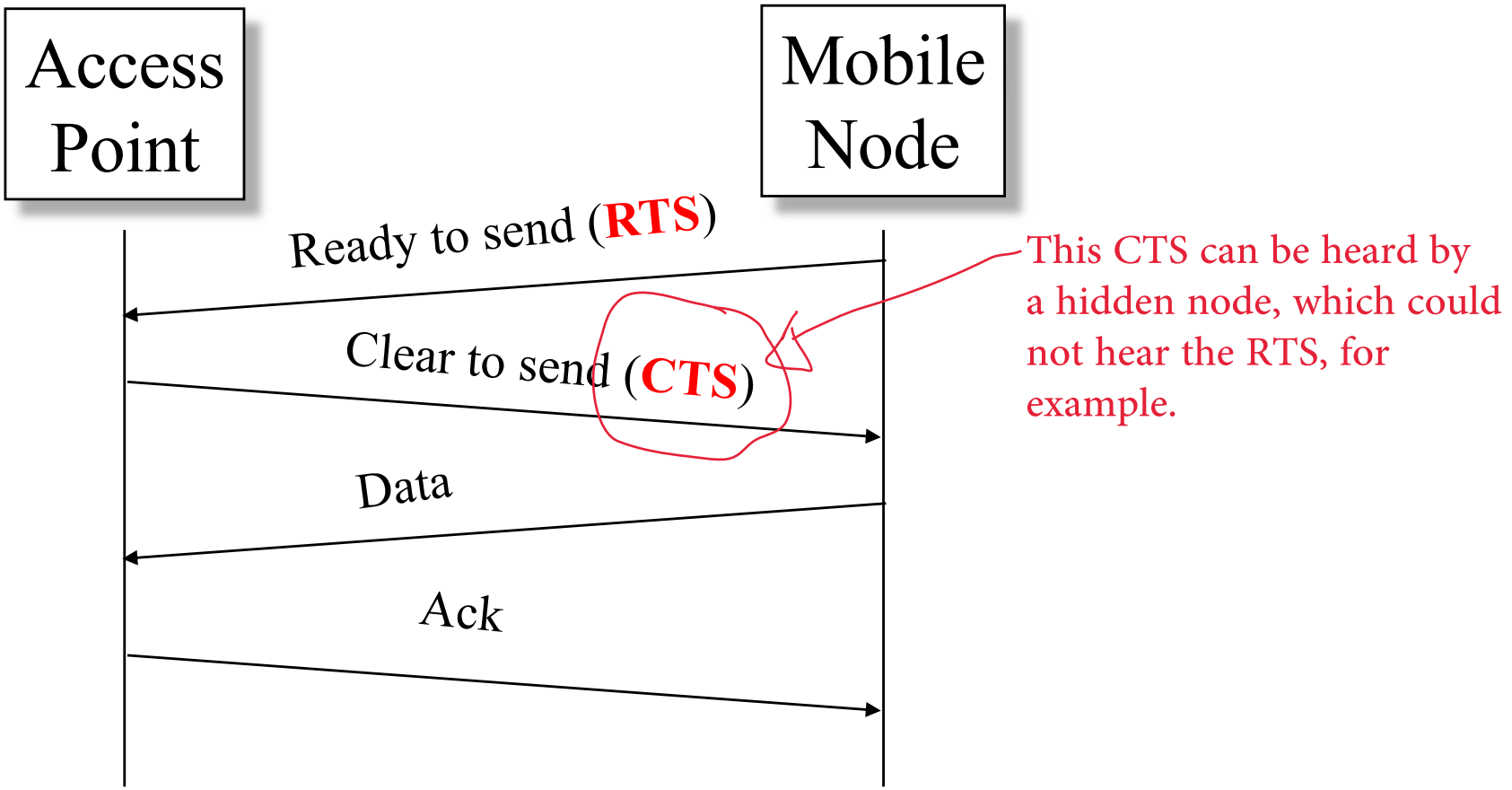
Source: https://www.ekahau.com/blog/channel-planning-best-practices-for-better-wi-fi/ (accessed 15 June 2020): this structure is probably for the US; radar channels may vary with countries

Hidden Node Problem



- A can hear B, B can hear C, but C cannot hear A (C and A are *hidden* from each other)
- C may start transmitting while A is also transmitting → collision at B!
  - A and C (wireless transmitters) can't detect collision (why?).
- CSMA/CD is not possible (CD = collision detection; CD used in Ethernet)
  → in WLAN, only the receiver can help *avoid* collisions
- 4-way handshake needed to implement CA (*collision avoidance*) in WLAN

4-Way Handshake

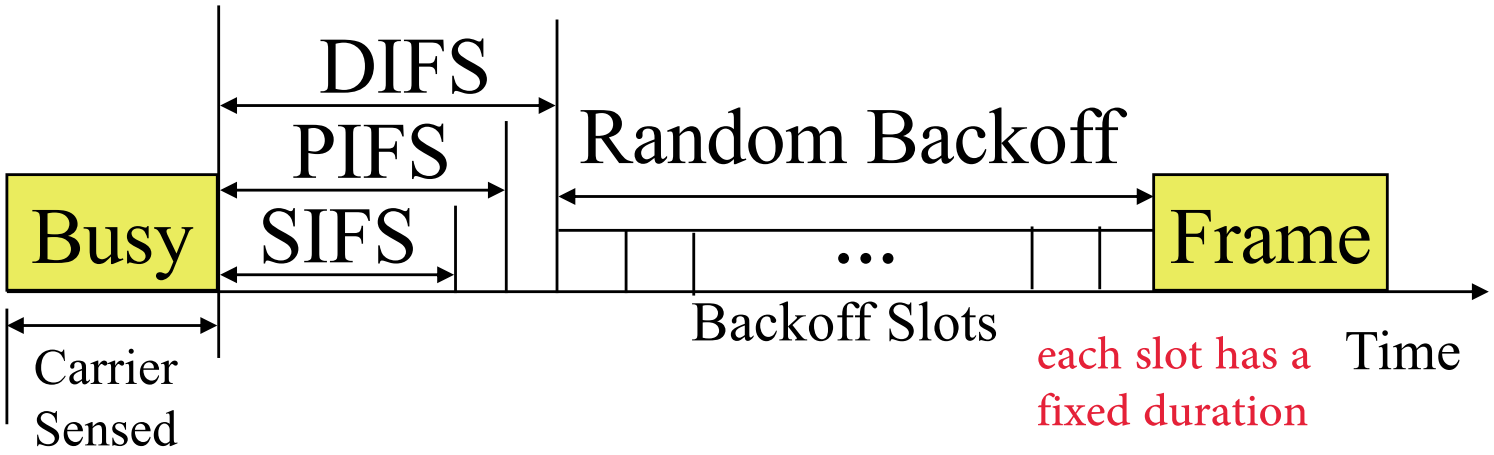


IEEE 802.11 MAC

- Carrier Sense Multiple Access with Collision Avoidance (**CSMA/CA**)
- Listen before you talk. If the medium is busy, the transmitter backs off for a random period.
- Avoids collision by sending a short message:
  Ready to send (**RTS**)
  RTS contains dest. address and duration of message.
  Tells everyone to backoff for the duration.
- Destination sends: Clear to send (**CTS**)
  Other stations set their network allocation vector (**NAV**) and wait for that duration
- Cannot detect collision, hence each packet is acked.
- MAC-level retransmission if not acked.

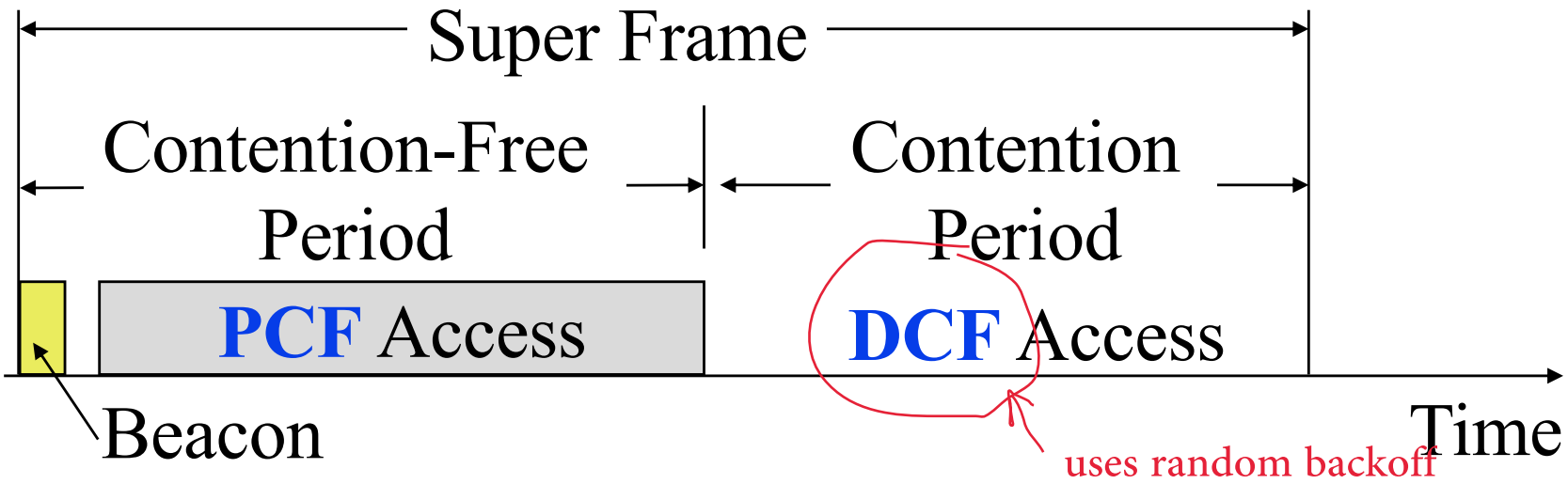
for the entire 4-way handshake, i.e., end of the ACK.

IEEE 802.11 Priorities with Inter-frame space



- 802.11 has different priorities for **control**, **data**, and **time-critical** packets
- Achieve priorities by using different amounts of interframe space (IFS)
- Highest priority frames, e.g., Acks, use short IFS (**SIFS)**
- Medium priority time-critical frames use "Point Coordination Function IFS" (**PIFS**)
- Asynchronous data frames use "Distributed coordination function IFS" (**DIFS**)

Time Critical Services



- Timer critical services use **Point Coordination Function**
- The point coordinator allows only one station to access
- Coordinator sends a beacon frame to all stations.
  Then uses a polling frame to allow a particular station to have contention-free access
- Contention Free Period (CFP) varies with the load.

IEEE 802.11 DCF Backoff

- MAC works with a single FIFO Queue
  - Focuses on transmitting the packet at the head of the queue
- Three variables:
  - Contention Window (CW)
  - Backoff count (BO)
  - Network Allocation Vector (NAV)
- If a frame (RTS, CTS, Data, Ack) is heard, NAV is set to the duration in that frame. Stations sense the media after NAV expires.
- If the medium is idle for DIFS, and backoff (BO) is not already active, the station draws a random BO in [0, CW] and sets the backoff timer.
  - CW is in units of *slot time* (slot time varies with 802.11 standards)
- If the medium becomes busy during backoff, the timer is paused and a new NAV is set. After NAV, back off continues.

IEEE 802.11 DCF Backoff (Cont)

- BO = *random*(0,CW)

if you increase CW, BO will choose a random number from a wider interval

- Initially and after each *successful* transmission:

$$CW = CW_{min}$$

- After each *unsuccessful* attempt

$$CW = \min\{2CW + 1, CW_{max}\}$$

Example

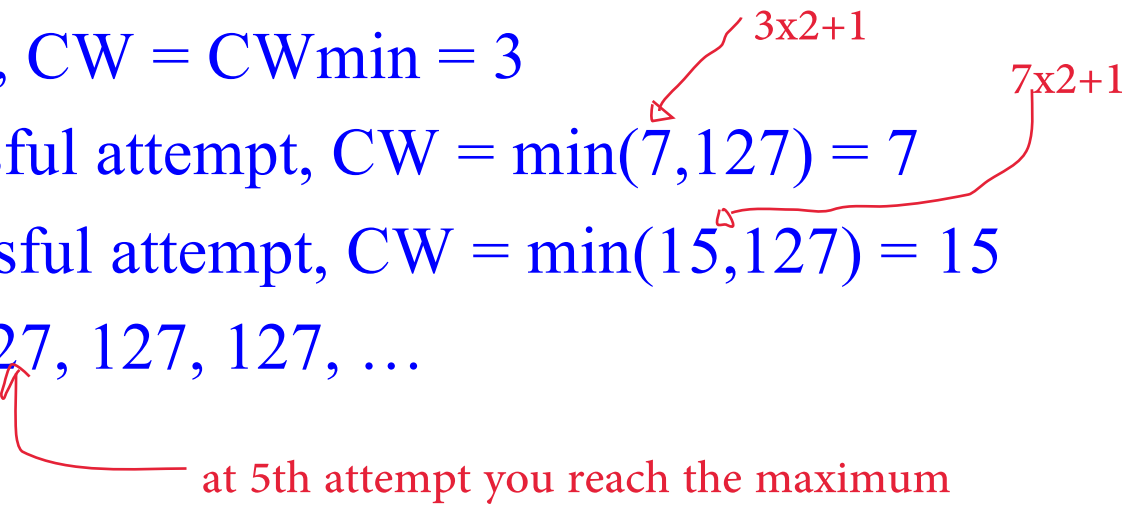
- Assume that we have CWmin=3 and CWmax=127 configured for a given WLAN. What would be the values of CW if there were 8 successive unsuccessful attempts after initalizing the network?

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, …



Parameter Values: interframe space and contention window

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

- PIFS = SIFS + 1 slot time
- DIFS = SIFS + 2 slot times = PIFS + 1 slot time

Slot time: basic unit of backoff algorithm

Example

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

Slot time = 20 μs

SIFS = 10 μs

PIFS = SIFS + slot time = 10+20 = 30 μs

DIFS = SIFS + 2 x slot time = 10 + 40 = 50 μs

Virtual Carrier Sense

does not consume battery (unlike physical)

- Every frame has a "Duration ID" which indicates how long the medium will be busy.
  - RTS has duration of RTS + SIF + CTS + SIF + Frame + SIF + Ack
  - CTS has duration of CTS + SIF + Frame + SIF + Ack
  - Frame has a duration of Frame + SIF + ACK
  - ACK has a duration of ACK
  - A station has to estimate the durations of RTS/CTS/ACK
- All stations keep a "**Network Allocation Vector (NAV)**" timer in which they record the duration of each frame they hear.
- Stations do not need to sense the channel until NAV becomes zero (conserve power)

Example

SIFS = 10 micro sec

- 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 ?

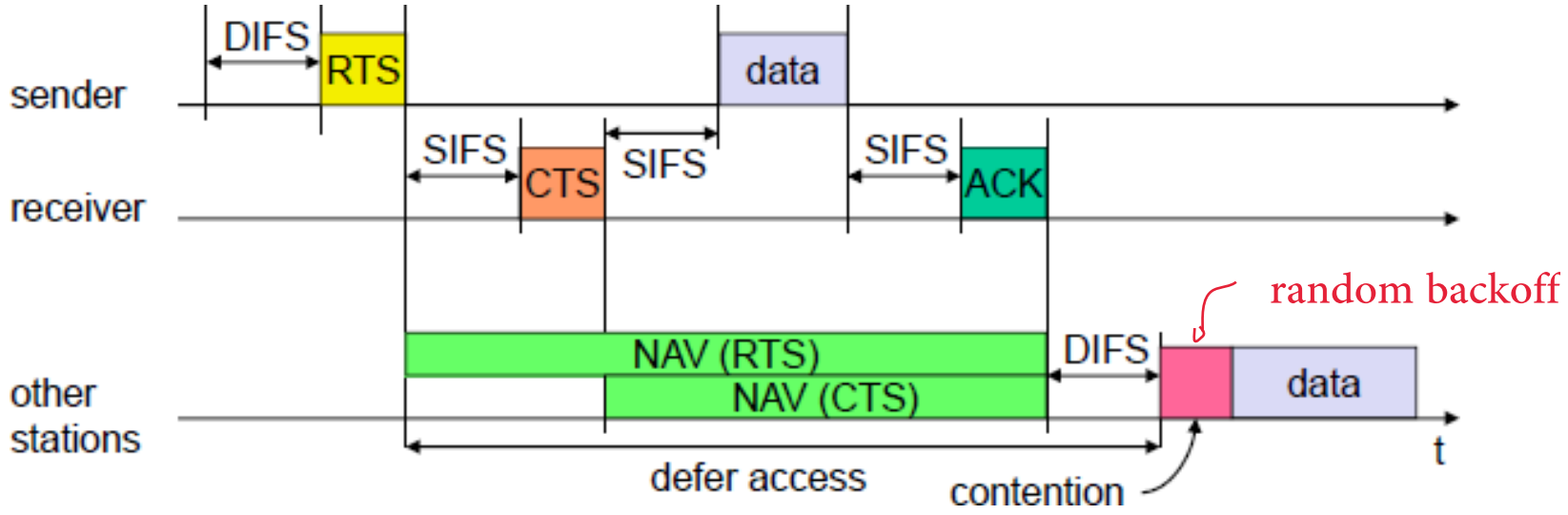
802.11b has a SIFS duration of 10 μs.

Duration field in RTS = RTS_time + CTS_time + ACK_time + data_time + 3xSIFS

= 10+10+25+250+3x10 = 325 μs

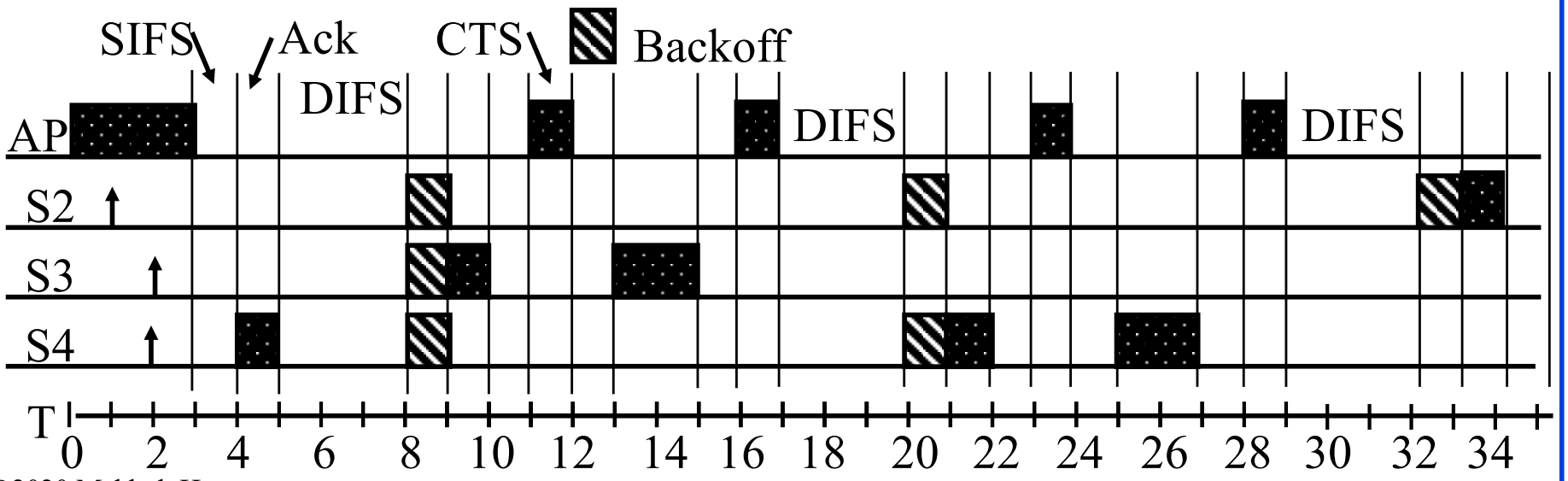
802.11 with RTS/CTS

When a node is sensing the channel, it must be free for DIFS period. SIFS is used as the wait time between the RTS, CTS, DATA and ACK frames. SIFS < DIFS means that another node cannot incorrectly determine that the channel is idle during the 4-way handshake between two other nodes.



DCF Example

- Example: Slot Time = 1, CWmin = 5, DIFS=3, PIFS=2, SIFS=1
- T=1 Station 2 wants to transmit but the media is busy
- T=2 Stations 3 and 4 want to transmit but the media is busy
- T=3 Station 1 finishes transmission.
- T=4 Station 1 receives ack for its transmission (SIFS=1)
  Stations 2, 3, 4 set their NAV to 1.
- T=5 Medium becomes free
- T=8 DIFS expires. Stations 2, 3, 4 draw backoff count between 0 and 5.
  The counts are 3, 1, 2



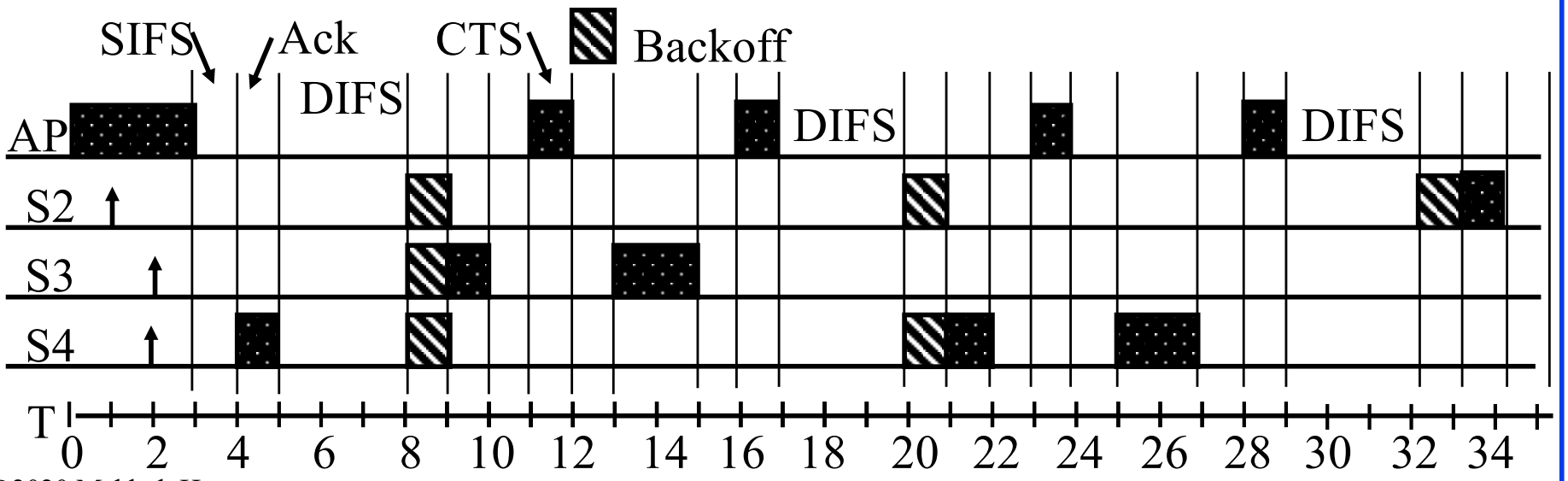
DCF Example (Cont)

- T=9 Station 3 starts transmitting. Announces a duration of 8 (RTS + SIFS + CTS + SIFS + DATA + SIFS + ACK). Station 2 and 4 pause backoff counter at 2 and 1 resp. and wait till T=17
- T=15 Station 3 finishes data transmission
- T=16 Station 3 receives Ack.
- T=17 Medium becomes free
- T=20 DIFS expires. Station 2 and 4 notice that there was no transmission for DIFS. Stations 2 and 4 start their backoff counter from 2 and 1, respectively.
- T=21 Station 4 starts transmitting RTS

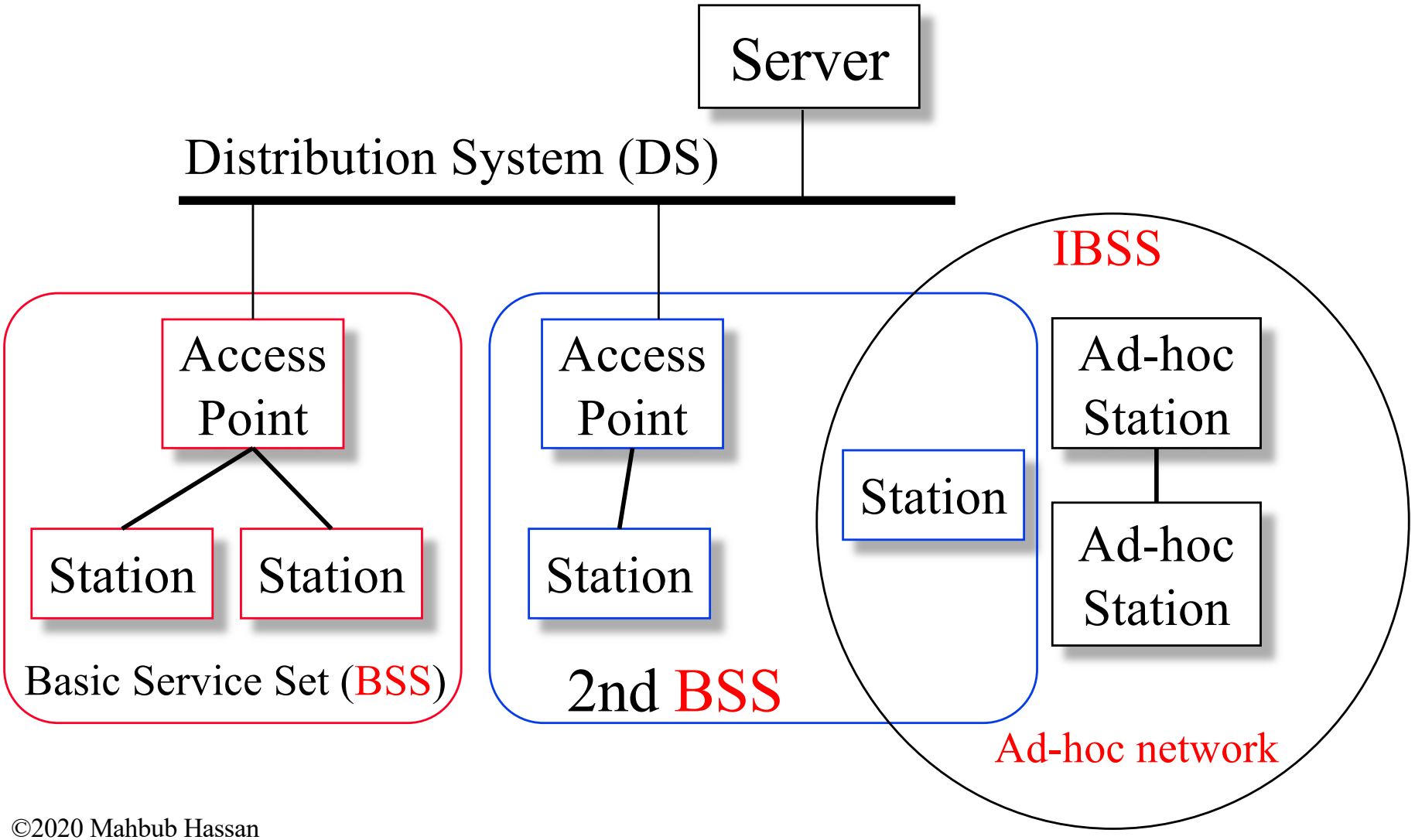
9+8 = 17

resume backoff with the remaining values

backoff ends for station 4



IEEE 802.11 Architecture



IEEE 802.11 Architecture (Cont)

- **Basic Service Set (BSS)**
  = Set of stations associated with one AP
- **Distribution System (DS)** - wired backbone
- **Independent Basic Service Set (IBSS)**: Set of computers in **ad-hoc mode**. May not be connected to wired backbone.
- Ad-hoc networks coexist and interoperate with infrastructure-based networks
- BSSID: 48-bit MAC address of the AP radio
- IBSSID: randomly generated address
  - 2 bits are fixed, 46 bits are generated randomly
- All-1s BSSID/IBSSID is used for broadcast

Frame Format

Frame Control	Duration/ ID	Adr 1	Adr 2	Adr 3	Seq Control	Adr 4	Info	CRC
16b	16b	48b	48b	48b	16b	48b		32b

Prot. Ver.	Type	Sub type	To DS	From DS	More Frag.	Retry	Power mgt	More Data	WEP	Order
2b	2b	4b	1b	1b	1b	1b	1b	1b	1b	1b

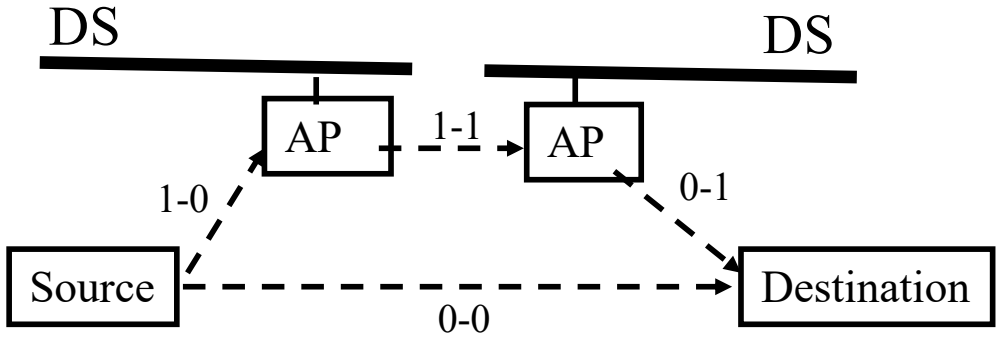
- Type: Control, management, or data
- Sub-Type: Association, disassociation, re-association, probe, authentication, de-authentication, CTS, RTS, Ack, Power-Save Poll (PS-POLL) …
- Retry/retransmission
- Power mgt: Going to Power Save mode
- More Data: More buffered data at AP for a station in power save mode
- WEP: Wireless Equivalent Privacy (Security) info in this frame
- Order: Strict ordering

MAC Frame Fields

- **Duration/Connection ID**:
  - If used as duration field, indicates time (in μs) channel will be allocated for successful transmission of MAC frame. Includes time until the end of Ack
  - In some control frames, contains association or connection identifier
- **Sequence Control**:
  - 4-bit fragment number subfield
    - For fragmentation and reassembly
  - 12-bit sequence number
  - Number frames between given transmitter and receiver

802.11 Frame Address Fields – data frames

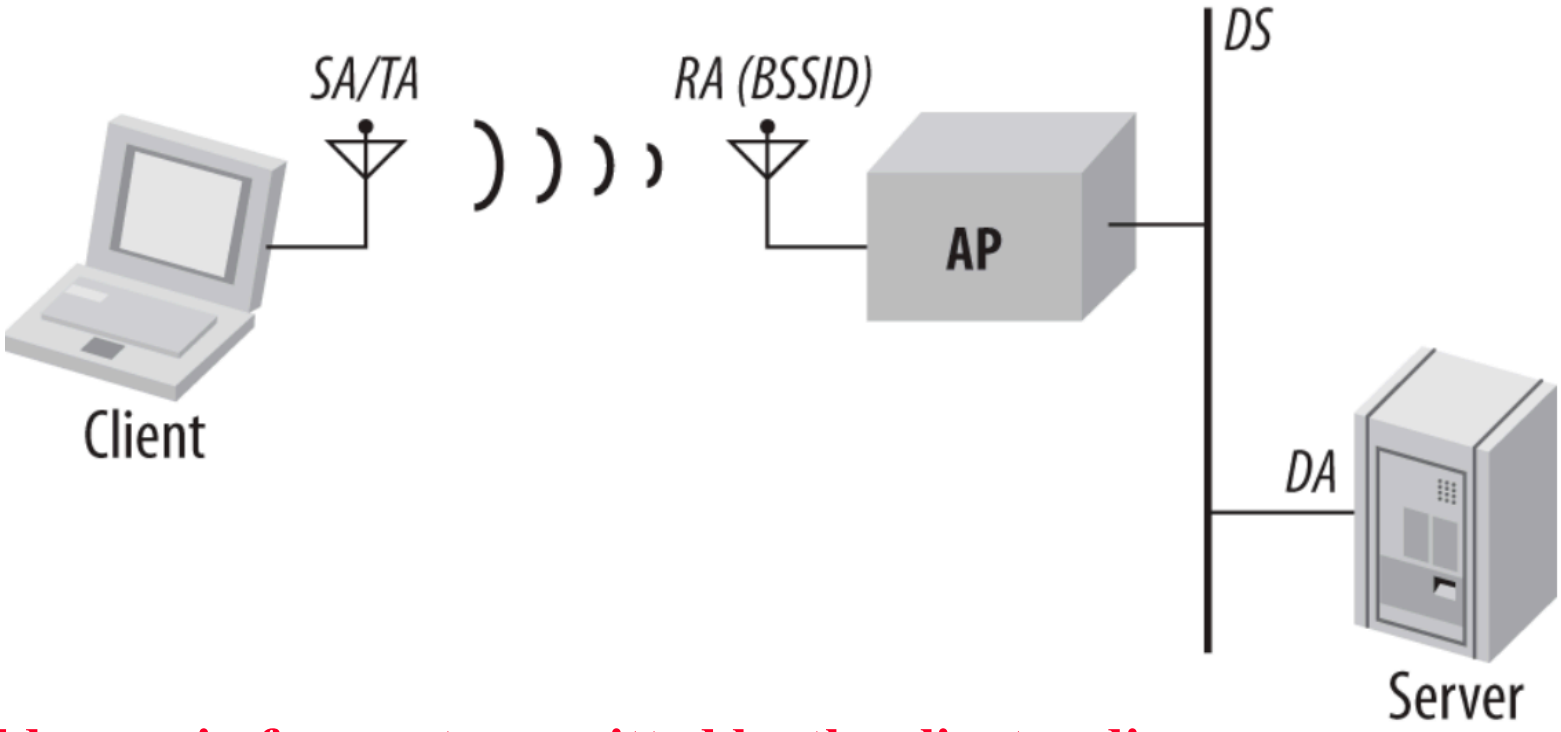
- Source/Destination: ultimate network devices that prepare and decode the frame for network layer
- Transmitter(Tx)/Receiver(Rx): Could be the source/destination, or intermediate radio devices, e.g., access point (AP)
- 4 address fields; defined by 2 DS bits



"WiFi Address Table"

Purpose	ToDS	FromDS	ADR1 (Rx)	ADR2 (Tx)	ADR3	ADR4
IBSS	0	0	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

Example 802.11 Addressing: Wireless Client to Server

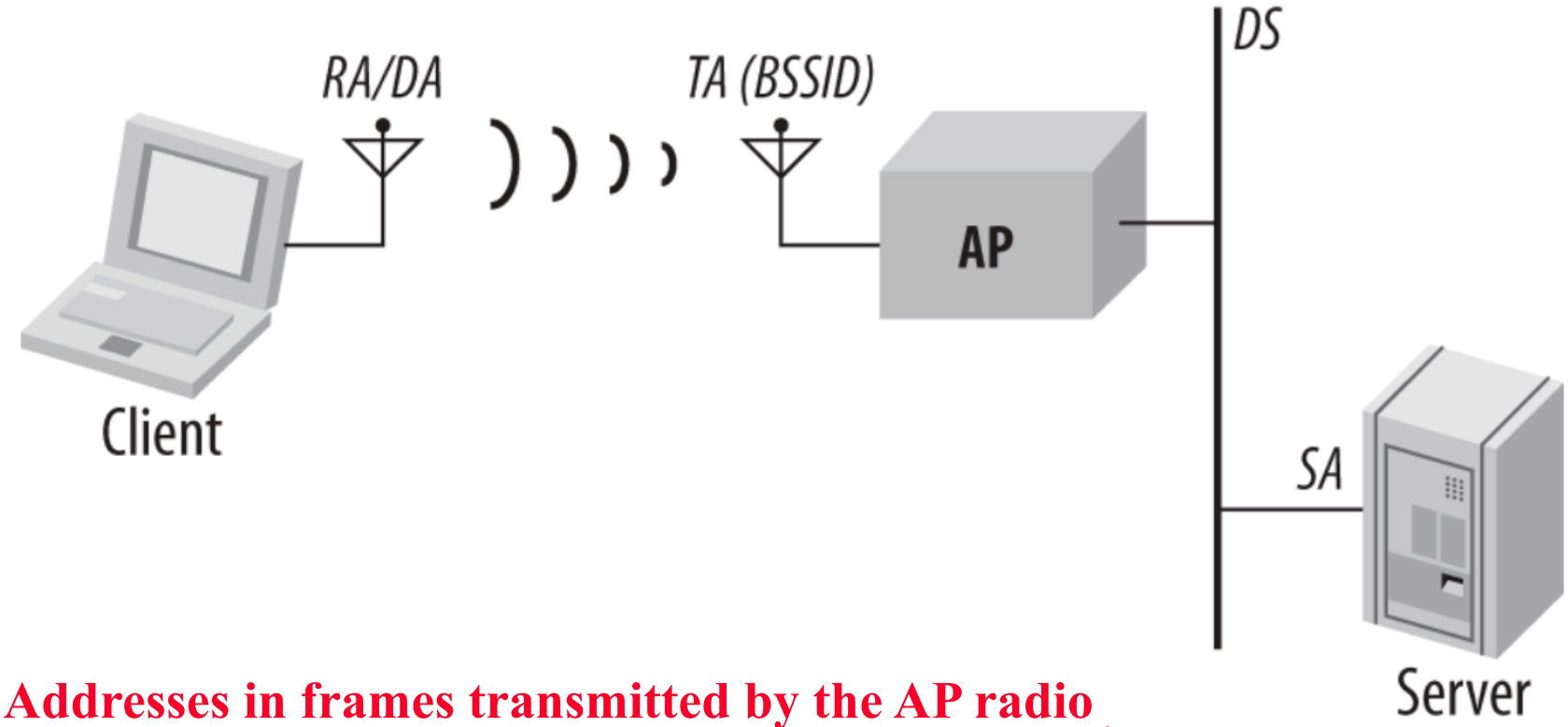


Addresses in frames transmitted by the client radio

ADR1: AP MAC address (BSSID)
ADR2: Client MAC address (source address)
ADR3: Server MAC address (destination address)
ADR4: Not applicable

From Row3 of "WiFi Address Table" shown in previous slide

Example 802.11 Addressing: Server to Wireless Client



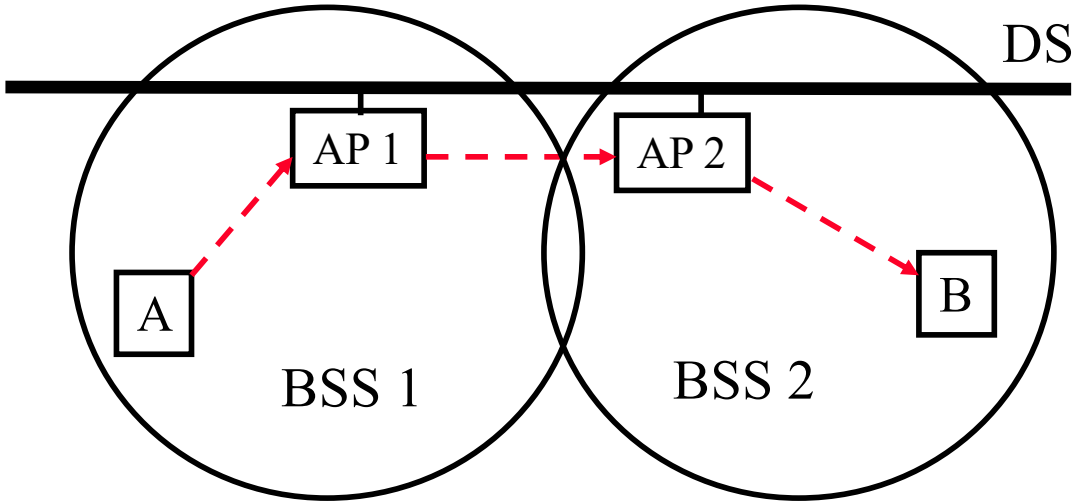
Addresses in frames transmitted by the AP radio

ADR1: Client MAC address (destination address)
ADR2: AP MAC address (BSSID)
ADR3: Server MAC address (source address)
ADR4: Not applicable

From Row2 of
"WiFi Address Table"

Example 802.11 addressing

- Consider the example WLAN in the figure 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?

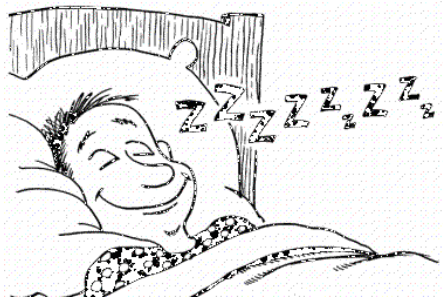


- In this case (To DS=1, From DS=0), Address 3 field should contain the address of the destination station. Therefore, it should be the address of B.

Power Saving

- Extending the battery life of portable devices is one of the main challenges of wireless networks.
- Mechanisms must be devised to let the device sleep as much as possible and wake up only when it needs to transmit or receive.
- If there are no packets to be received, a receiver could go to sleep and save battery power.
- To facilitate this kind of power saving, IEEE 802.11 has a power management function.

802.11 Power Management



- Station tells the base station its mode:
  Power saving (PS) or active
  - Mode changed by Power Mgmt bit in the frame control header.
- All packets destined to stations in PS mode are buffered (at AP)
- AP broadcasts list of stations with buffered packets in its beacon frames: Traffic Indication Map (TIM)
- When a station wakes up, it waits for the beacon; sends a PS-Poll message to AP if its bit is turned on in TIM; AP then sends one frame with buffered data and sets the More Data bit in the header if more data in the buffer (station does not go back to sleep after receiving one frame if More is set).

Traffic Indication Map (TIM)

- A bit map inside a beacon
- 2008 bits; each bit represents an Association ID (one associated client)
- If packets are buffered in the AP for a given Association ID, its corresponding bit is set to ‘1’, ‘0’ otherwise

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, but 5 GHz channels (20 MHz) are non-overlapped, but some are shared with the radar service
3. High speed applications can be supported by combining multiple adjacent channels into single channel with higher bandwidth
4. 802.11 uses SIFS, PIFS, DIFS for priority
5. WLAN frames have *four* address fields
6. 802.11 supports power saving mode

Acronyms

- Ack — Acknowledgement
- AP — Access Point
- APSD — Automatic Power Save Delivery
- BO — Backoff
- BSA — Basic Service Area
- BSS — Basic Service Set
- BSSID — Basic Service Set Identifier
- CA — Collision Avoidance
- CD — Collision Detection
- CDMA — Code Division Multiple Access
- CFP — Contention Free Period
- CRC — Cyclic Redundancy Check
- CSMA — Carrier Sense Multiple Access
- CTS — Clear to Send
- CW — Congestion Window
- CWmax — Maximum Congestion Window

Acronyms (Cont)

- CWmin — Minimum Congestion Window
- DA — Destination Address
- DCF — Distributed Coordination Function
- DIFS — DCF Inter-frame Spacing
- DS — Direct Sequence
- ESA — Extended Service Area
- ESS — Extended Service Set
- FH — Frequency Hopping
- FIFO — First In First Out
- GHz — Giga Hertz
- IBSS — Independent Basic Service Set
- ID — Identifier
- IEEE — Institution of Electrical and Electronics Engineers
- IFS — Inter-frame spacing
- ISM — Instrumentation, Scientific and Medical
- LAN — Local Area Network

Acronyms (Cont)

- MAC Media Access Control
- MHz Mega Hertz
- MIMO Multiple Input Multiple Output
- NAV Network Allocation Vector
- OFDM Orthogonal Frequency Division Multiplexing
- PCF Point Coordination Function
- PHY Physical Layer
- PIFS PCF inter-frame spacing
- PS Power saving
- QoS Quality of Service
- RA Receiver Address
- RTS Ready to Send
- SA Source Address
- SIFS Short Inter-frame Spacing

Acronyms (Cont)

- SS Subscriber Station
- TA Transmitter's Address
- TIM Traffic Indication Map
- WiFi Wireless Fidelity
- WLAN Wireless Local Area Network