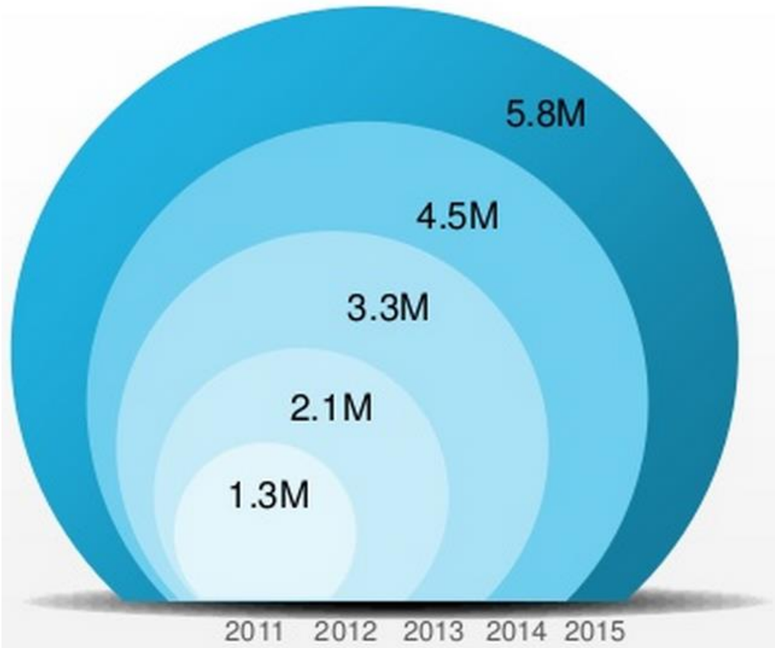
IEEE 802.11 WLANS
- Introduction to WiFi Networks -

Kyunghan Lee
Networked Computing Lab (NXC Lab)
Department of Electrical and Computer Engineering
Seoul National University
https://nxc.snu.ac.kr
kyunghanlee@snu.ac.kr

WiFi is Becoming Ubiquitous

Growing global deployment



Number of public hotspots worldwide

Source: Wireless Broadband Alliance (WBA) and Informa Telecoms & Media

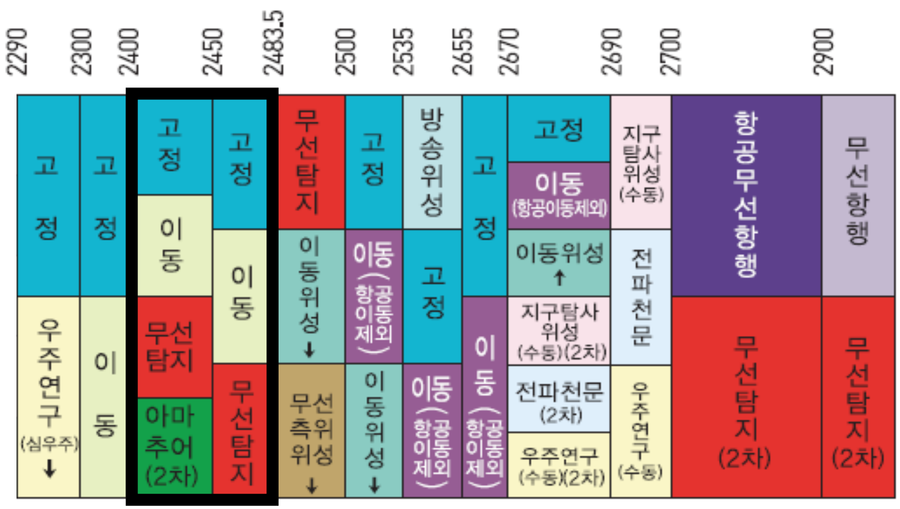
Expanding device support

Wi-Fi Enabled Devices Shipped	2012 MU	2015 MU
Phones/Accessories	685	1,459
Tablets, E-Readers, Media Players, etc	199	360
Laptops, Desktops, Peripherals, etc.	392	717
Connected Home	107	287
Others	39	338
TOTAL	1,422	3,161

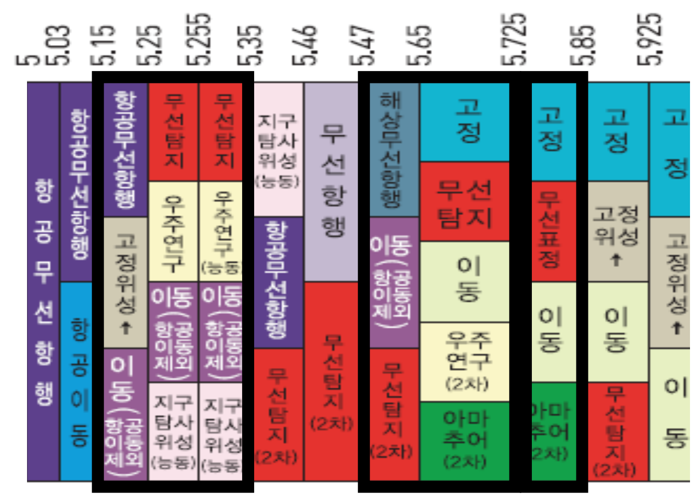
Source: ABI Research Forecast 2012

Unlicensed Spectrums

- Can be used without license as long as the regulatory requirements are met
  - Max transmit power level, spectrum mask, duty cycle, max tx time, etc.
- Availability depends on countries
- 2.4 GHz: Wi-Fi, Bluetooth, ZigBee, cordless telephone, and microwave oven
- 5 GHz: Wi-Fi, radars, (and potentially, LTE in unlicensed spectrum)



2.4GHz



5GHz

Wi-Fi based on IEEE 802.11

- IEEE 802.11 Working Group (WG)
  - Standardizes protocols for Wireless Local Area Network (WLAN)
  - Defines layer-1 PHY and layer-2 MAC protocols
- Wi-Fi Alliance (WFA)
  - Certifies products based on IEEE 802.11
  - Makes its own protocols on top of IEEE 802.11 now

- Provides (indoor) high-speed wireless connectivity
  - Using unlicensed spectrum @2.4, 5GHz, etc.
    - And 6GHz for WiFi 6E (approved by FCC, 2020/04) – upto 10Gbps
  - ~100 m range (actual range depends on tx power, antenna, environment, etc.)
  - Relatively simpler protocols (cf. LTE), low cost, plug-and-play

802.11 Baseline Protocols

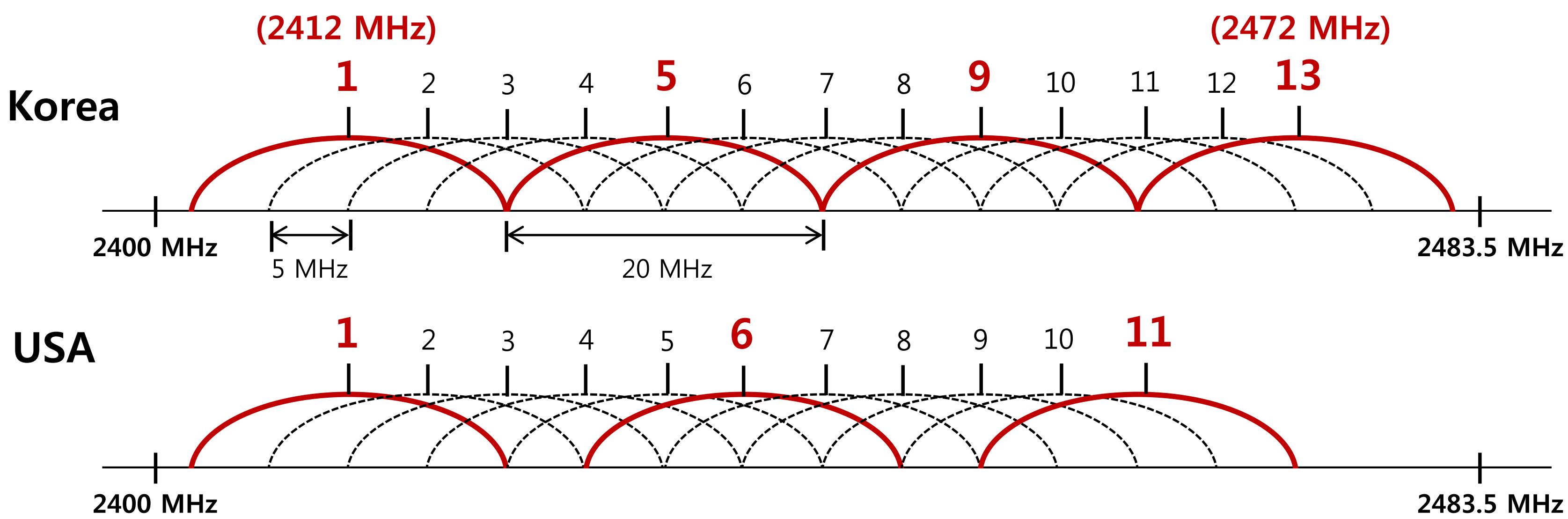
- Infrastructure WLAN with Access Points (APs)
  - Both AP and associated stations use the same frequency (kind of TDD system)
  - Default channel bandwidth = 20 MHz for 2.4 & 5 GHz versions
- Physical (PHY) layer
  - Multiple transmission rates with different combinations of modulation & coding schemes (MCSs)
- Medium Access Control (MAC) layer
  - Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
  - Transmit only if channel is idle → more friendly to other Wi-Fi as well as other types of unlicensed spectrum devices, e.g., Bluetooth

Various PHYs of IEEE 802.11

PHY	Tx Schemes	Frequency Bands	Supported Data Rates (Mbps)
Baseline	DSSS, FHSS, IR	DSSS & FHSS – 2.4 GHz IR – 850~950 nm wavelength	1, 2
802.11a	OFDM	5 GHz	6, 9, 12, 18, 24, 36, 48, 54
802.11b	CCK	2.4 GHz	5.5, 11 + DSSS rates
802.11g	OFDM	2.4 GHz	802.11a rates + 802.11b rates

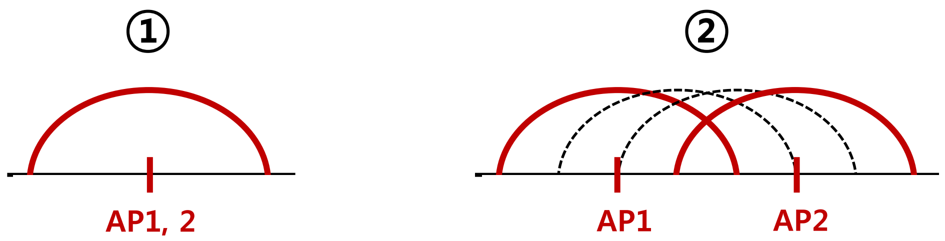
Channels @ 2.4GHz for 802.11b/g/n

- ISM bands (2400~2483.5 MHz)
  - 13 (in case of Korea) or 11 (in case of Taiwan and USA) channels with 5 MHz gap
- Channel bandwidth of 22 MHz (for .11b DSSS/CCK) or 20 MHz (for .11g/n OFDM)
- Only 3~4 non-overlapping channels



Channels @ 2.4GHz for 802.11b/g/n

- Channel use cases in two-cell network

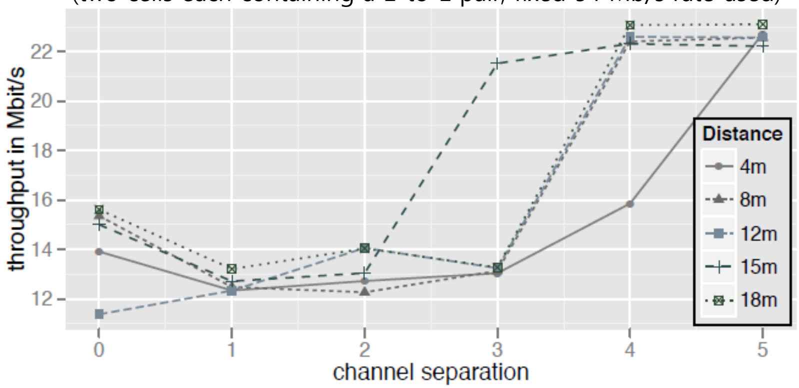


Same channel (fully overlapping) **Adjacent channels (partially overlapping)** **Orthogonal channels (non-overlapping)**

- Which is better in terms of network throughput?

  It will depend on
  - Topology (e.g., distances)
  - Rate adaptation
  - Hardware's Rx performance
  - External influences (interference)

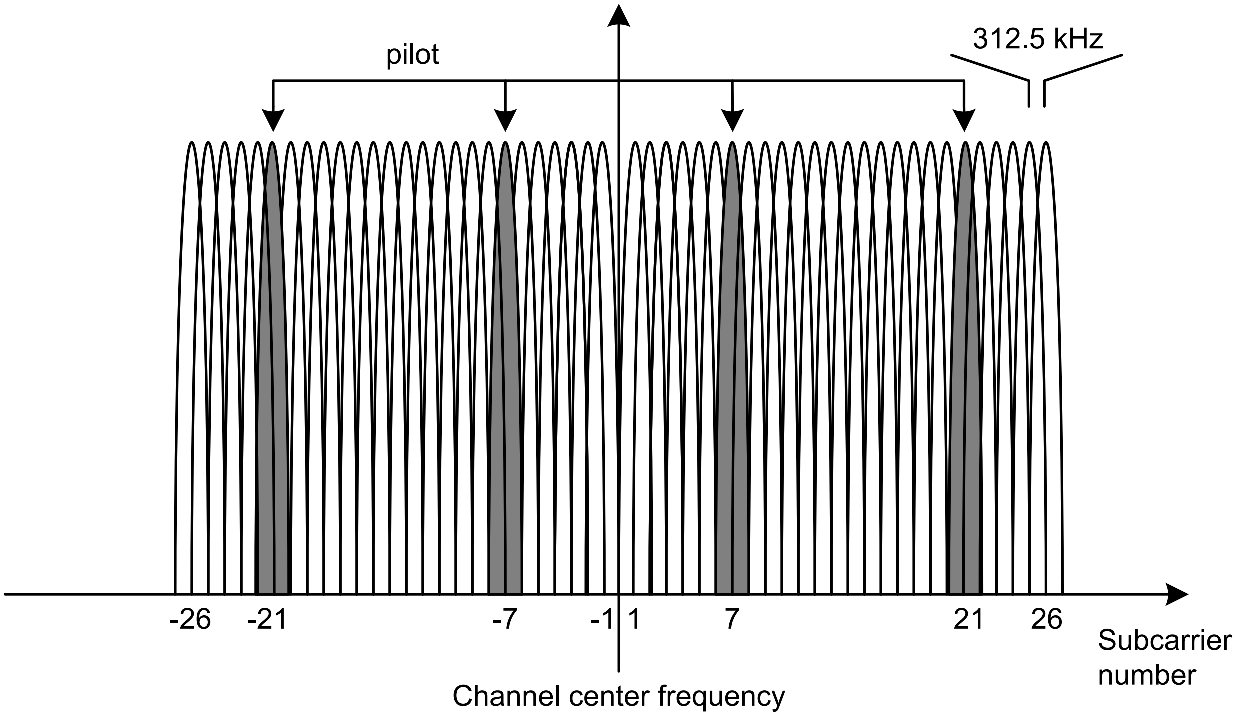
A measurement example*
(two cells each containing a 1-to-1 pair, fixed 54 Mb/s rate used)



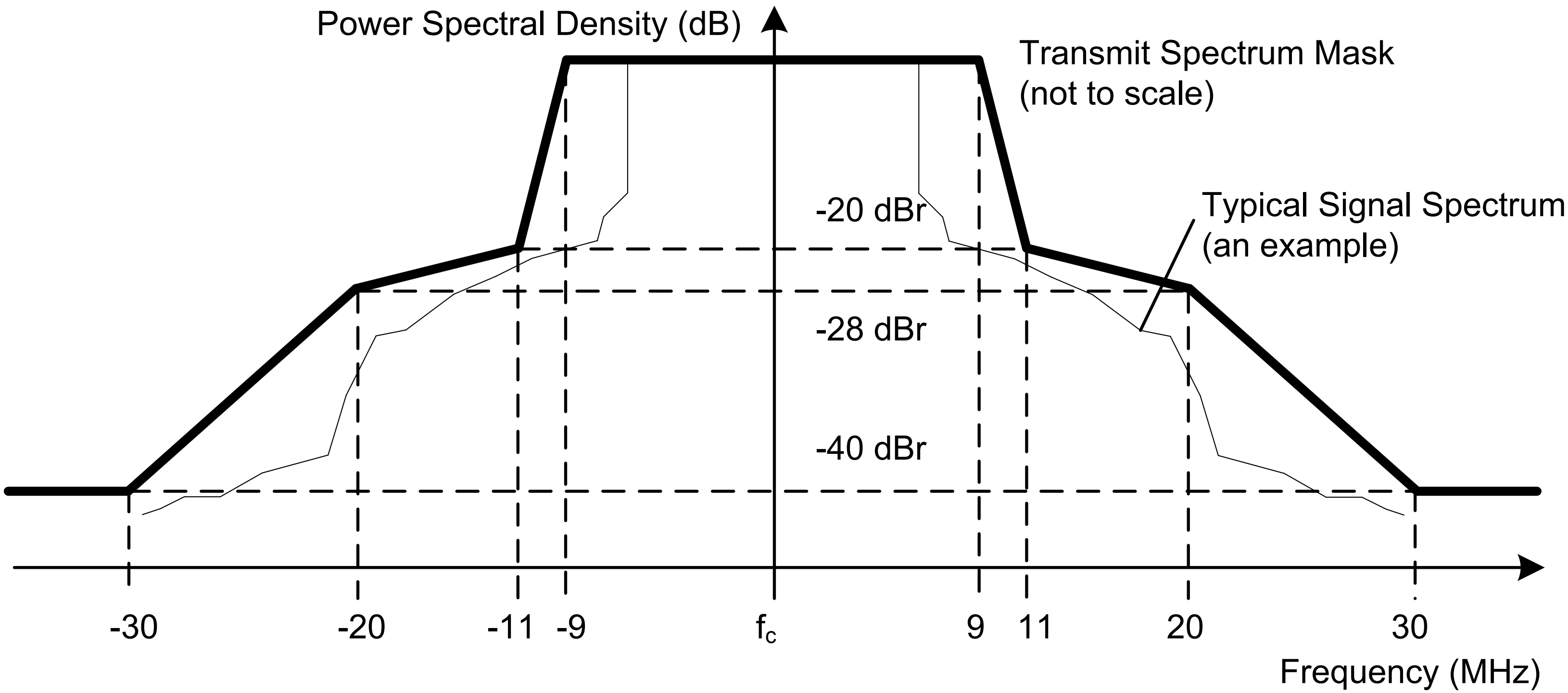
Michael Doering, Łukasz Budzisz, Daniel Willkomm and Adam Wolisz, "About the practicality of using partially overlapping channels in IEEE 802.11 b/g networks," in Proc. IEEE ICC 2013 - Wireless Communications Symposium, June, 2013.

OFDM Modulation in 802.11a/g

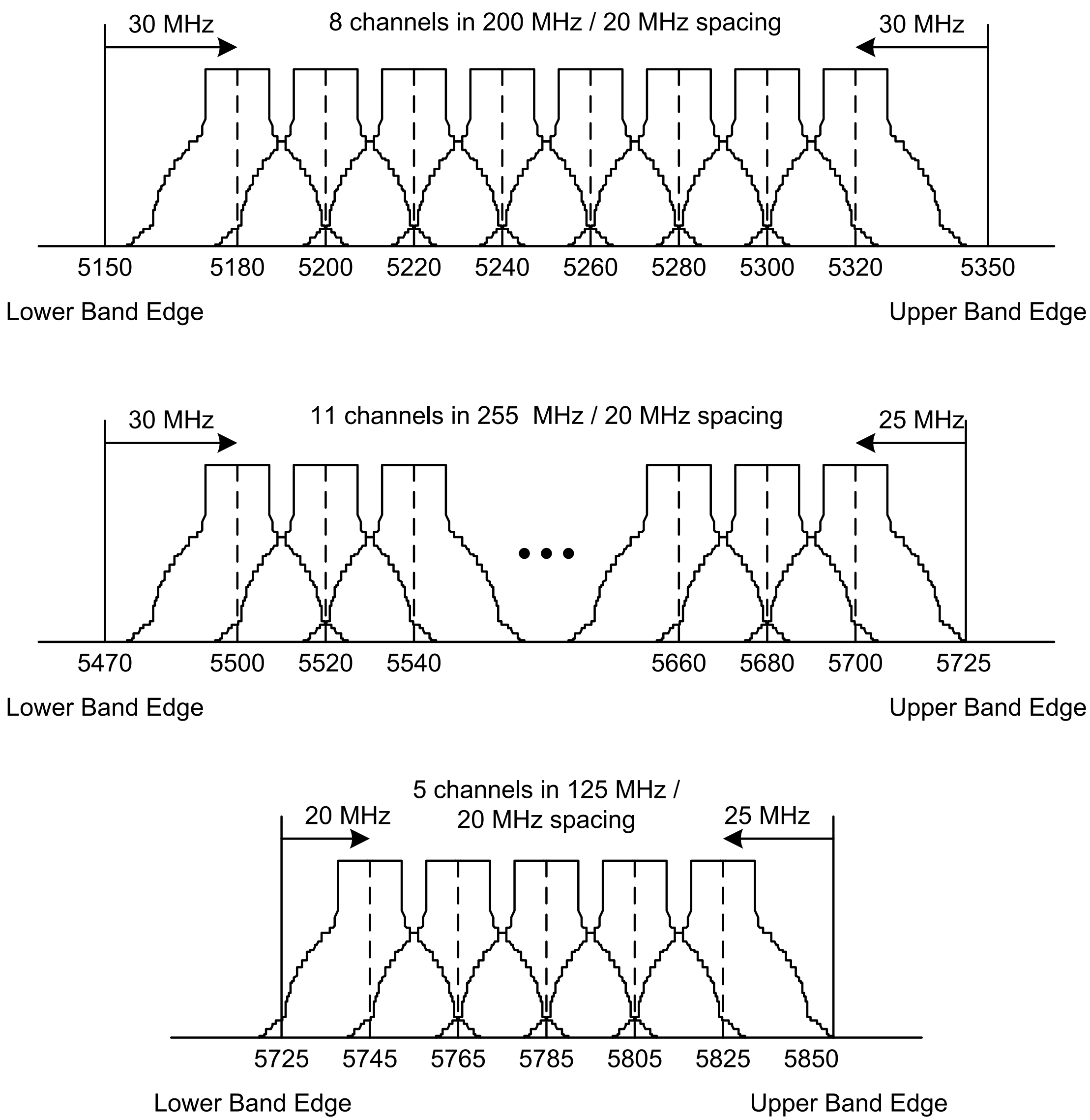
- OFDM with 52 used subcarriers (64 in total)
- 48 data + 4 pilot (plus 12 virtual subcarriers)
- 312.5 kHz spacing



802.11a Transmit Spectrum Mask



Channels @ 5GHz for 802.11a/n

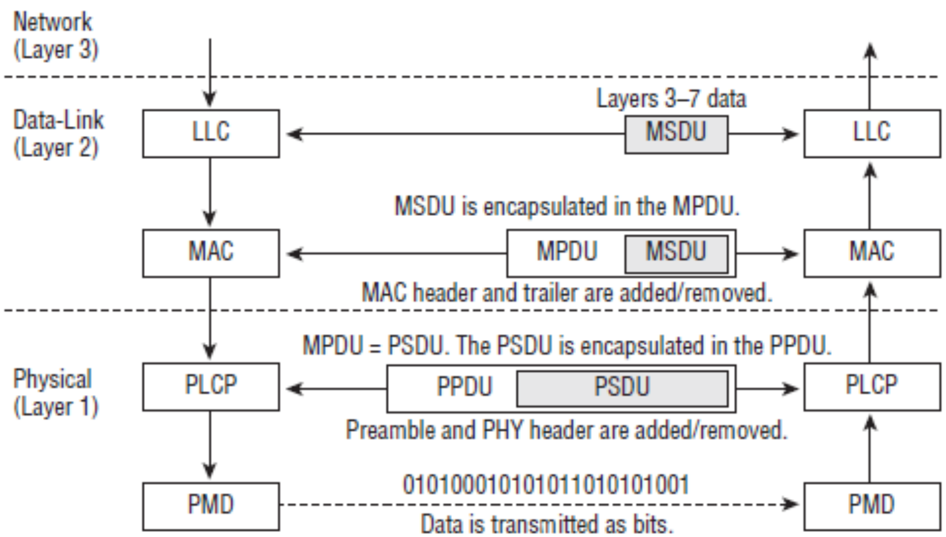


Channels @ 5GHz for 802.11a/n

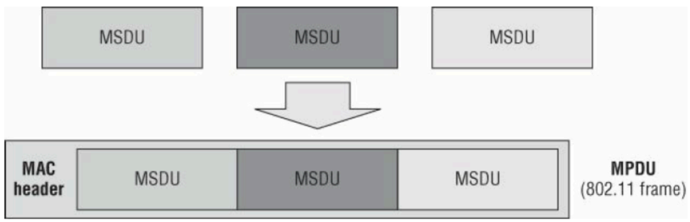
Frequency sub-Band (GHz)	Channel number	Center frequency (GHz)	Regulatory domain
5.15~5.25	36 40 44 48	5.180 5.200 5.220 5.240	Europe, US, Korea
5.25~5.35	52 56 60 64	5.260 5.280 5.300 5.320	Europe, US, Korea
5.47~5.725	100 104 108 112 116 120 124	5.500 5.520 5.540 5.560 5.580 5.600 5.620	Europe, US, Korea
	128 132 136 140	5.640 5.660 5.680 5.700	Europe, US, (Korea)
	144	5.720	US, (Korea)
5.725~5.850	149 153 157 161	5.745 5.765 5.785 5.805	Europe, US, Korea
	165	5.825	Europe, US, (Korea)

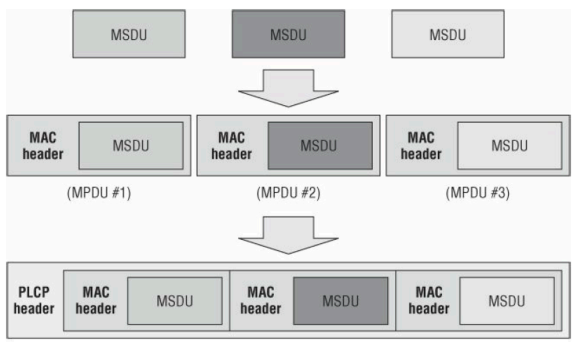
802.11a PHY/MAC Protocol Overview

- 802.11 Physical (PHY) layer is divided into two sublayers
  - PLCP (Physical Layer Convergence Procedure) sublayer
  - PMD (Physical Medium Dependent) sublayer



MSDU (MAC Service Data Unit)
A-MPDU (Aggregated MAC Protocol Data Unit)

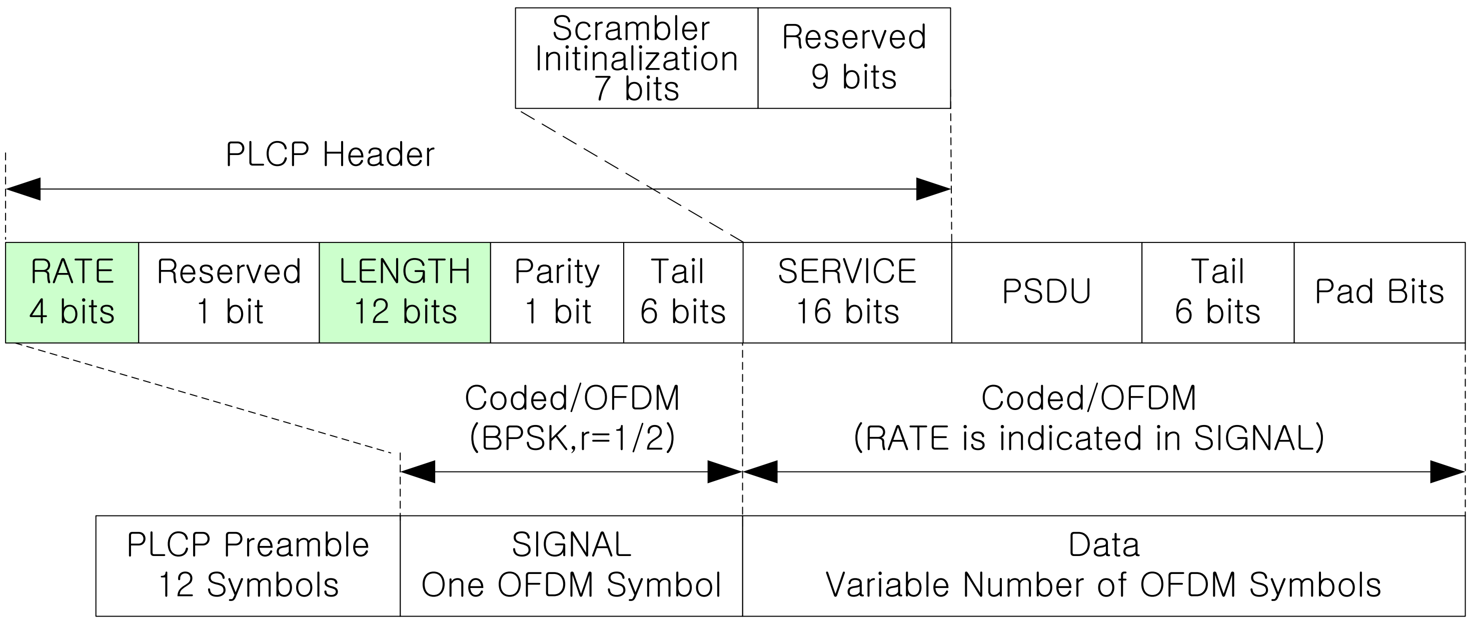




NXC LAB

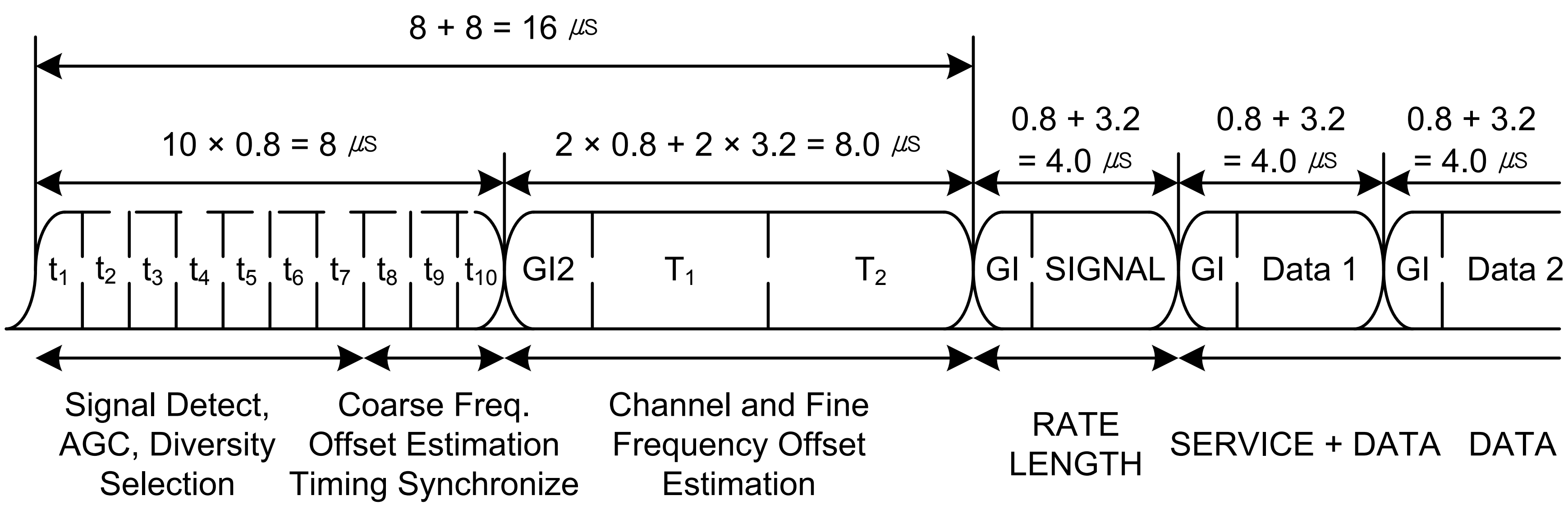
802.11a PHY Protocol Data Unit (PPDU)

- RATE: the transmission rate used for the PSDU (PHY Service Data Unit)
- LENGTH: length of the PSDU contained in the PPDU
- PSDU = MAC Protocol Data Unit (MPDU)



802.11a OFDM Training Structure

- More detailed view of PLCP preamble
- Short OFDM training symbol of 0.8 μsec using 12 subcarriers
- Long OFDM training symbol 3.2 μsec using 53 subcarriers (including a zero value at DC)



802.11a Modulation & Coding Schemes (MCSs)

Mandatory rates

MCS index	Modulation	Code Rate	Coded bits per subcarrier	Coded bits per OFDM symbol	Data bits per OFDM symbol	OFDM symbol duration (us)	Data rates (Mb/s)
0	BPSK	1/2	1	48	24	4	*6*
1	BPSK	3/4	1	48	36	4	*9*
2	QPSK	1/2	2	96	48	4	*12*
3	QPSK	3/4	2	96	72	4	*18*
4	16-QAM	1/2	4	192	96	4	*24*
5	16-QAM	3/4	4	192	144	4	*36*
6	64-QAM	2/3	6	288	192	4	*48*
7	64-QAM	3/4	6	288	216	4	*54*

Data rate = Data bits per OFDM symbol/OFDM symbol duration

How to Determine Data Rate

- Nsym = M × R × NSC
  - Nsym = # bits / OFDM symbol
  - M = # bits / mod. symbol = 1, 2, 4 or 6
    - (for BPSK, QPSK, 16-QAM, or 64-QAM)
  - R = code rate = 1/2, 2/3, or 3/4
  - NSC = # data subcarriers = 48

- Rate = Nsym / TOFDM
  - TOFDM = OFDM symbol duration = 4 μsec

- Example for 54 Mbps
  - (6 × 3/4 × 48) / 4 = 54 Mbps (for 64-QAM, 3/4 rate, 20 MHz)

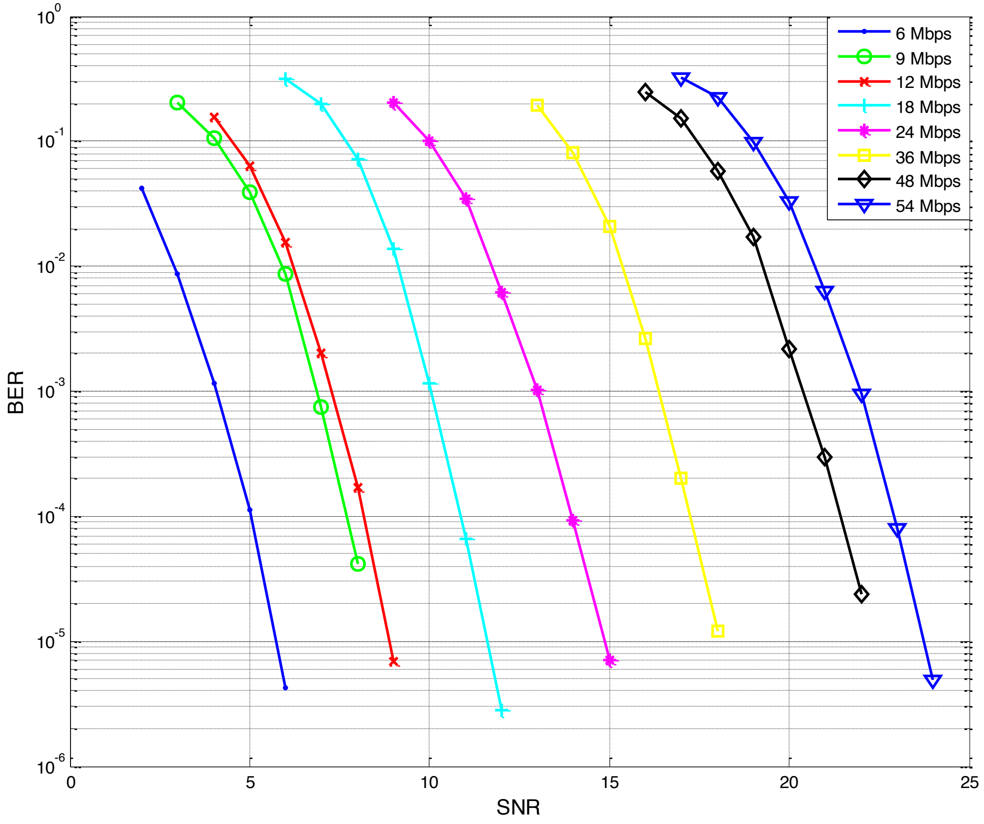
Receiver Minimum Input Sensitivity

- Frame error rate (FER) for a PSDU length of 1000 octets should be under 10% with the minimum sensitivity.

Rate (Mbps)	Modulation	Code Rate (*R*)	Minimum sensitivity (dBm)
6	BPSK	1/2	−82
9	BPSK	3/4	−81
12	QPSK	1/2	−79
18	QPSK	3/4	−77
24	16-QAM	1/2	−74
36	16-QAM	3/4	−70
48	64-QAM	2/3	−66
54	64-QAM	3/4	−65

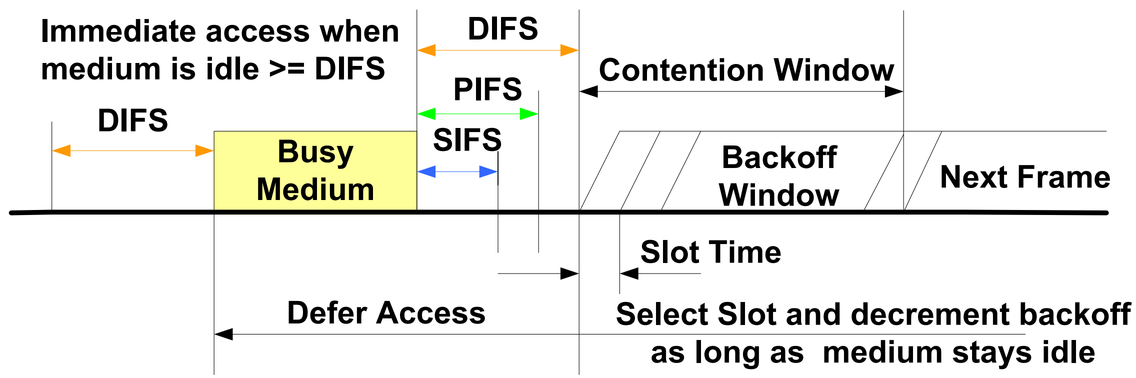
802.11a PHY: BER vs. SNR

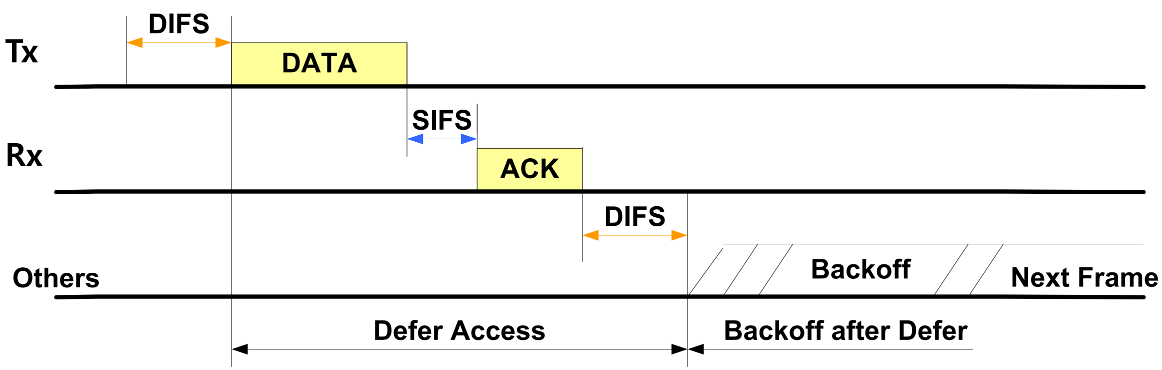
- Higher data rate requires higher SNR
- Transmitter should choose the best rate for a given channel



Distributed Coordination Function (DCF)

- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
  - Attempts to "avoid collision" using random backoff before transmission
  - ACK transmission upon successful data reception at the same channel





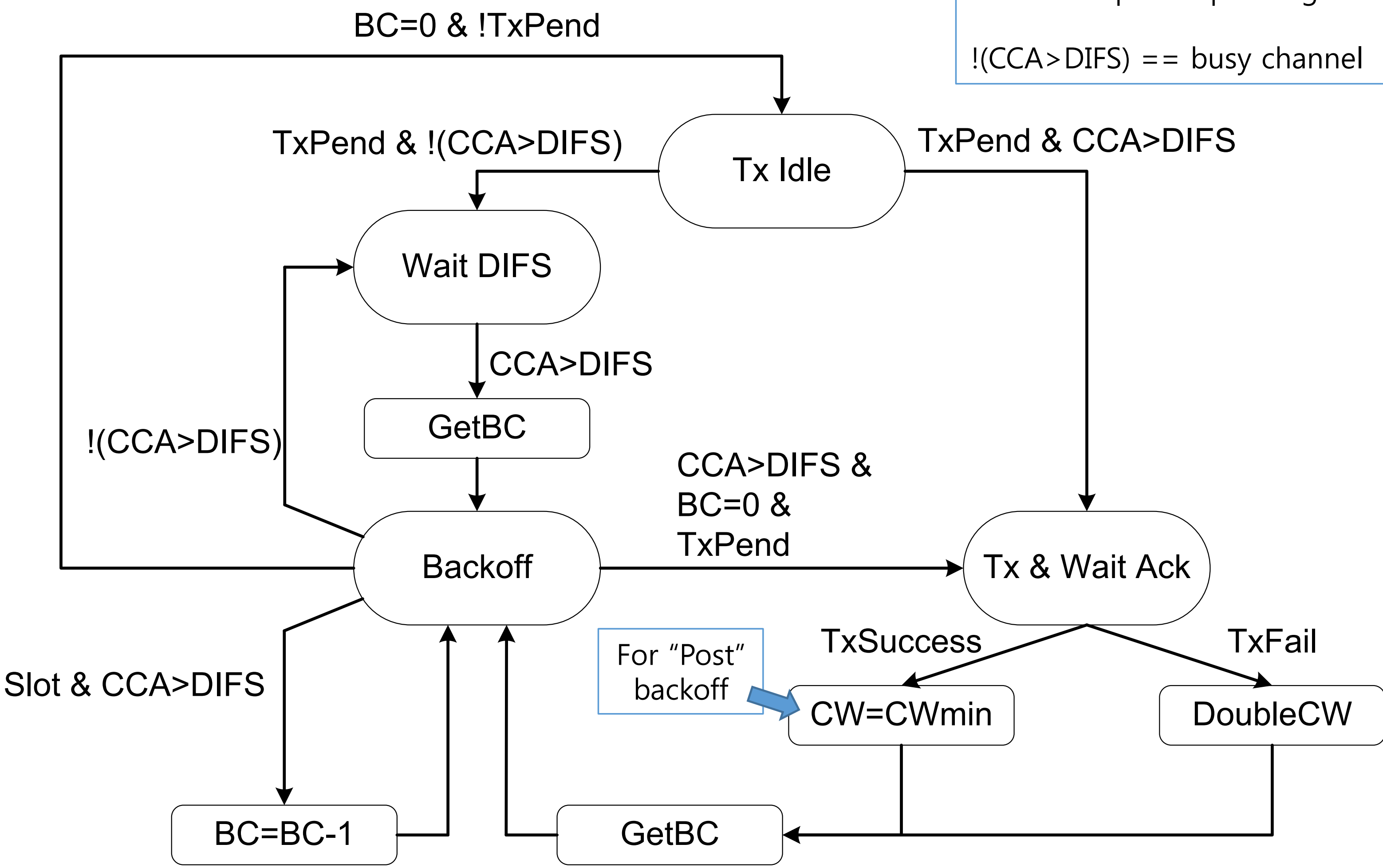
Binary Exponential Backoff

- Backoff Counter is randomly selected from [0,CW], where CW is contention window
- For each unsuccessful frame transmission, CW doubles (from CWmin to CWmax)
  - CW → 2 (CW+1)-1
  - e.g., CW: 15 → 31 → 63 → 127 → 255
- Reduces the collision probability

DCF State Diagram

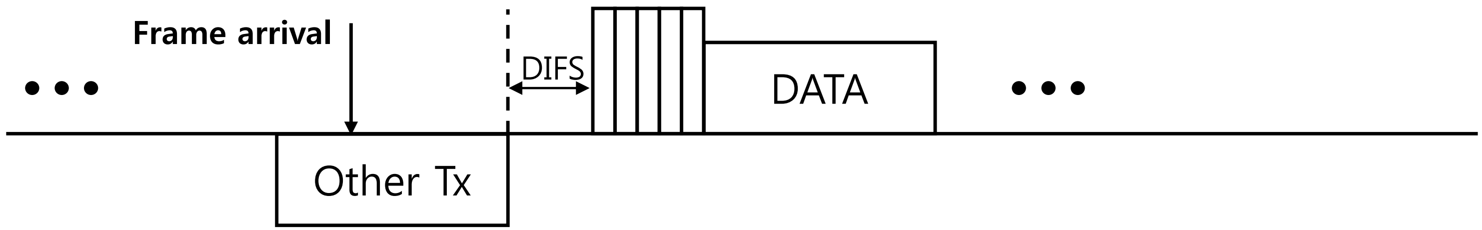
CCA: Clear Channel Assessment
BC: Backoff Counter
TxPend: Tx packet pending

!(CCA>DIFS) == busy channel

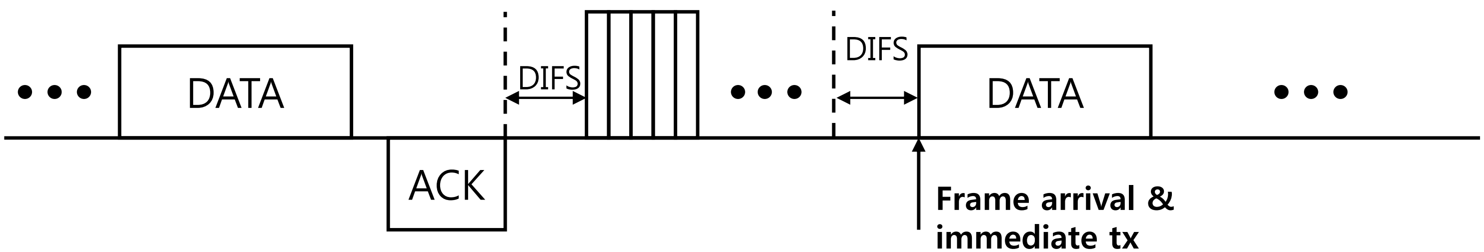


Post Backoff

- Normal backoff



- Post backoff



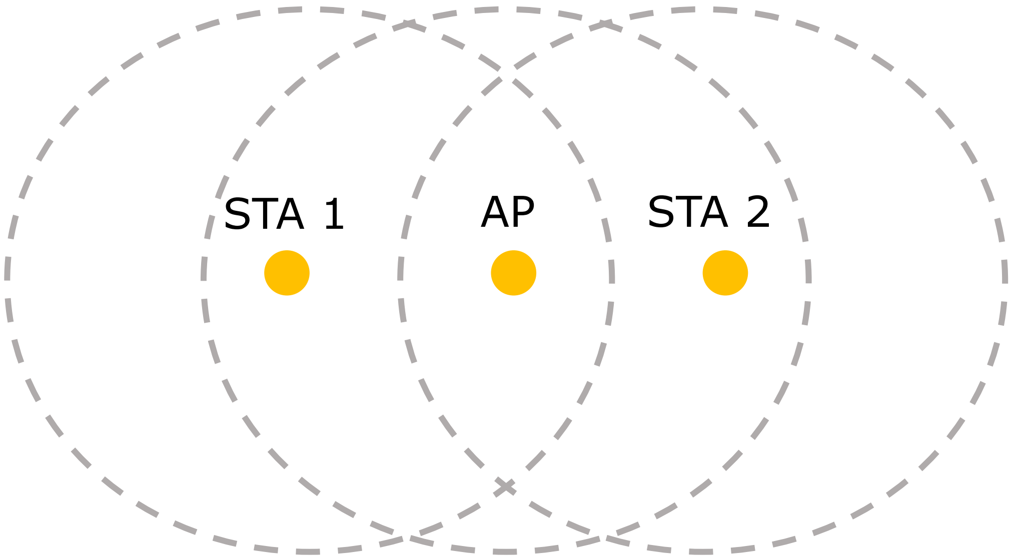
- After a successful transmission, STA performs a "post" backoff even if it has no queued data frame in buffer
- Post backoff becomes normal backoff if packet arrives during backoff

Carrier-Sense Mechanisms

- Needed as part of CSMA/CA operation
- Physical carrier-sense
  - Provided by PHY, and depends on PHY
  - Clear Channel Assessment (CCA) by PHY
  - ED (Energy Detection, -62 dBm), CS (Carrier Sensing, -82 dBm)
- Virtual carrier-sense
  - Provided by MAC via Network Allocation Vector (NAV) counter
  - Each frame carries Duration value in the MAC header
  - Any correctly received frame updates NAV if the new NAV is larger
  - Assumes busy channel if non-zero NAV irrespective of CCA!

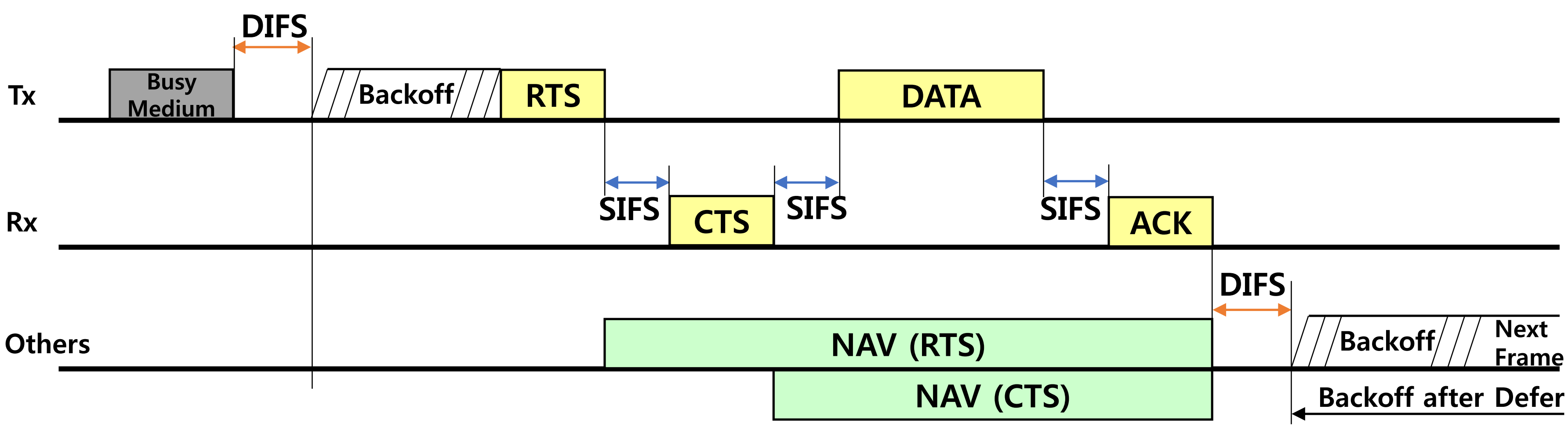
Hidden Terminal

- STA 1 and STA 2 can see AP, but they do not see each other
- May result in more collisions due to the failure of carrier-sensing!



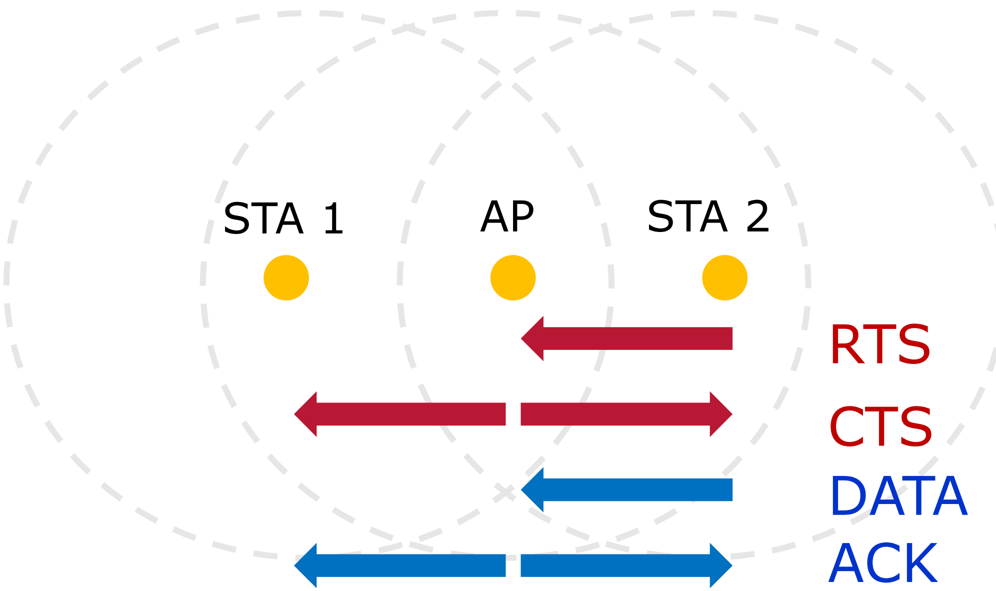
RTS/CTS Exchange

- A way to handle hidden terminals!
  - Request-To-Send / Clear-To-Send (RTS/CTS) exchange to reserve medium
  - Works with virtual carrier-sense



RTS/CTS at Work!

- Upon reception of RTS from STA 2, AP transmits CTS
- By receiving CTS, STA 1 is informed of the upcoming DATA/ACK transaction



Exposed Terminal

- AP2 decides CCA channel “BUSY” after sensing AP1’s transmission, while STA2 is not affected by AP1 at all
- There could be better performance by spatial reuse, but carrier-sensing may suppress the possibility