WLANpedia

for Wi-Fi engineers

Rev2208_00

Jay Ahn

WLANpedia for Wi-Fi engineers

WLANpedia for Wi-Fi engineers is …

Open book : free to share

Wiki book : needs your participations

As Wi-Fi technology evolves, this book will be updated in a random manner and you can find and download the latest version from www.wlanpedia.com. As Wi-Fi covers a wide range of new engineering, there may be mistakes or out-of-date contents in this book, which is not easy to be handled by one person. If you find anything wrong or have anything to add or any comment to make, you are welcome to contact me. (ahnjoohyun@gmail.com) Update will be applied in the following version and contributors are listed in the book, if you have no concerns.

For Engineering technology and information only : No vendor-specific contents

This book deals only with general Wi-Fi engineering technologies on IEEE PHY/MAC standards and HW/RF/SW that are related in WLAN. There will be no vendor specific contents that might be a commercial or confidential information.

Written in Picture and in English

I prefer explaining with one big picture to having a long talk by words. One or more pictures at every page is not an additional explanation, but the main description for the topic minimizing my writing. I feel sorry if the letters in the pictures in some pages are too small to read. Along with the pictures, descriptions are written in English hoping that it can be shared with more engineers and students, as IEEE standards and terminologies are also in English. I am not a native speaker and I am afraid there are many awkward expressions. Along with your participation updating the engineering stuff, I would appreciate if anyone corrects my weird English in this book.

Publishing WLANpedia …

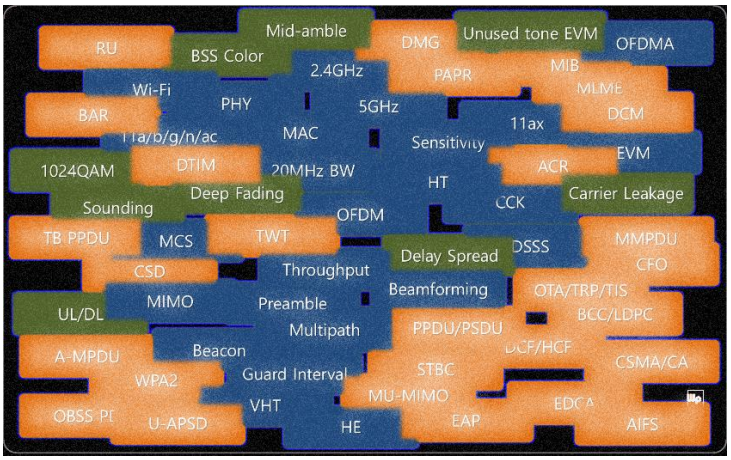
Wireless LAN (WLAN) must be the most democratic and open wireless communication technology ever. Every station in a WLAN service set has a fair opportunity to occupy the media and there is no big controlling base station like in cellular network. The standard itself is based on the individual participation and WLAN keeps embracing the technologies ever used before; the old-fashioned 11b network published 25 years ago is not disclaimed and still in use. WLAN moves fast in the full-scale deployment of new technologies like OFDM and MIMO without much hesitation bringing the new technologies into the world.

It was simple, when WLAN first started 30 years ago, and I was lucky to be there at the beginning. But, meanwhile, WLAN has become more and more complicated, as it has been embracing all the previous technologies and polishing itself. Engineers who just start in the area or students who want to take a look at WLAN technology could be easily intimidated with many unfamiliar concept and abbreviated terminologies. Field engineers may also have trouble to catch up with the fast changing standards. IEEE standard document is too much in detail and not appropriate to grasp the overall idea or to learn the concept from.

I have been an enthusiastic fan of WLAN for more than twenty years of my career in WLAN chipset, module, AP and tester vendors as a HW/RF and software engineer attending IEEE conferences. As a field engineer, a lecturer and an advocate of WLAN, I have been keeping tracking on WLAN technologies and the standard spending a long time taking notes and contemplating how to effectively deliver the engineering stuff to WLAN engineers and students. This book is the result of my effort meanwhile.

This book is not for the hobbyist who just have the questions; why is my Wi-Fi at home not working well? Which AP should I buy? This book deals with the detailed engineering stuff ranging PHY, RF, MAC and the new technology of 11ax and 11be and it is for the engineers who are working or start working in WLAN field. At the same time, I hope this can be a good source for the student learning a wireless communication system and WLAN.

Jay Ahn Aug. 2022



Revision history, author and contributors

- Rev2208_00 : First edition by Jay Ahn

Table of Contents

WLAN Overview

Wireless Communication

Benefits on Wireless

- Mobility
  - Enables users to physically move, while using an appliance
- Networking Cost Reduction
  - Installation in Difficult-to-Wire area : river, road, obstacles, and historic building
- Increased reliability
  - From accidental cutting from cable fault or by water intrusion
- Long-term cost saving
  - The case of re-cabling the network with company reorganization

Concerns on Wireless

- Radio signal interference
  - Harmonics or noise from internal system
  - Interference from other wireless signals
- High battery consumption
- Network security
- Connection problem
  - Susceptible to losing connection in wireless border
  - Propagation pattern is irregular and unpredictable
- Possible health risks

Wireless Network by Area

Most common way to classify wireless network is by “area”, which means the range of use. Standard is generally led by SIG (Special Interest Group) in PAN or Organization in WAN, while it is led by IEEE in WLAN. Wi-Fi, known as a technology brand name of WLAN, is the alliance of companies and contributes to promoting with interoperability based on WLAN standard.

When you are using tablet PC with Bluetooth keyboard tethering by smartphone

Wireless

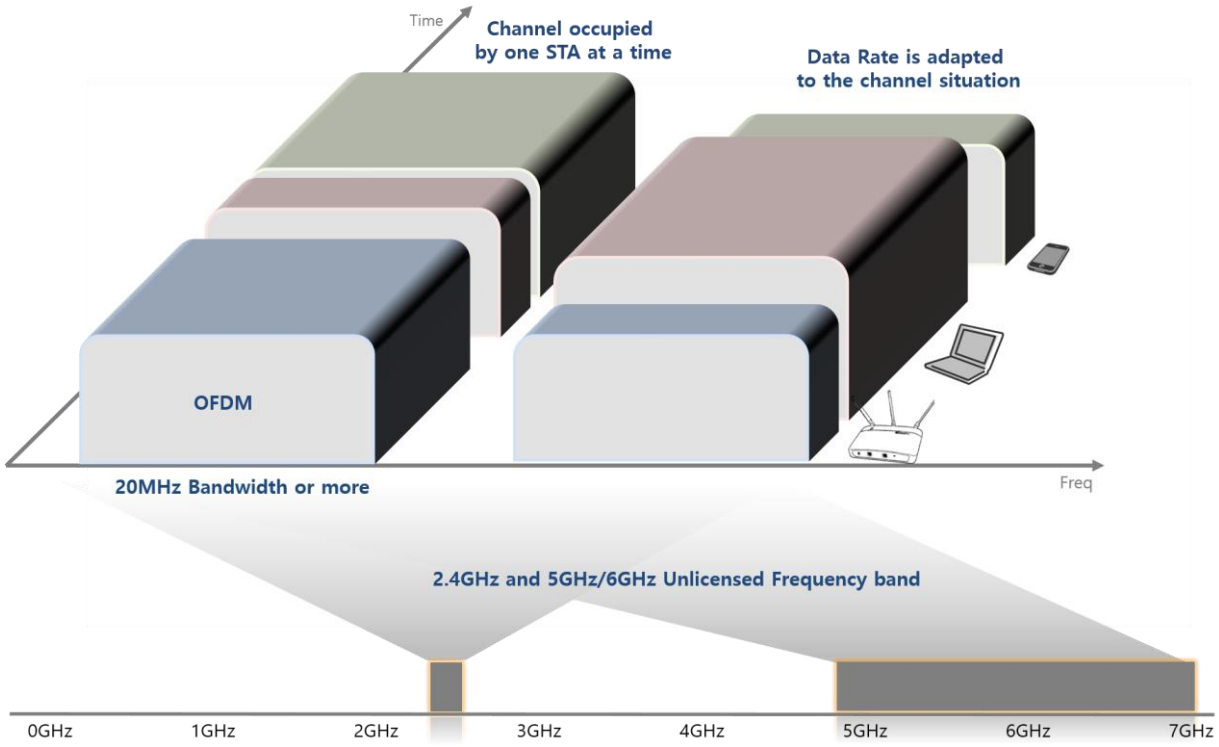
PAN : Bluetooth	→	IEEE802.15 (Bluetooth SIG)
LAN : 802.11a/b/g/n/ac/ax	→	IEEE802.11 (Wi-Fi Alliance)
MAN : WiBro, WiMax	→	IEEE802.16 (WiMAX)
WAN : Cellular(GSM,CDMA,LTE), LPWA	→	3GPP/3GPP2, LoRa, SigFox

Nanoscale, Near-field (NFC), Body(BAN), Personal(PAN), Near-me(NAN), Local(LAN), Home(HAN), Storage(SAN), Campus(CAN), Car(CAN), Metropolitan(MAN), Wide(WAN), Cloud(IAN), Internet

WLAN Overview

PHY Overview

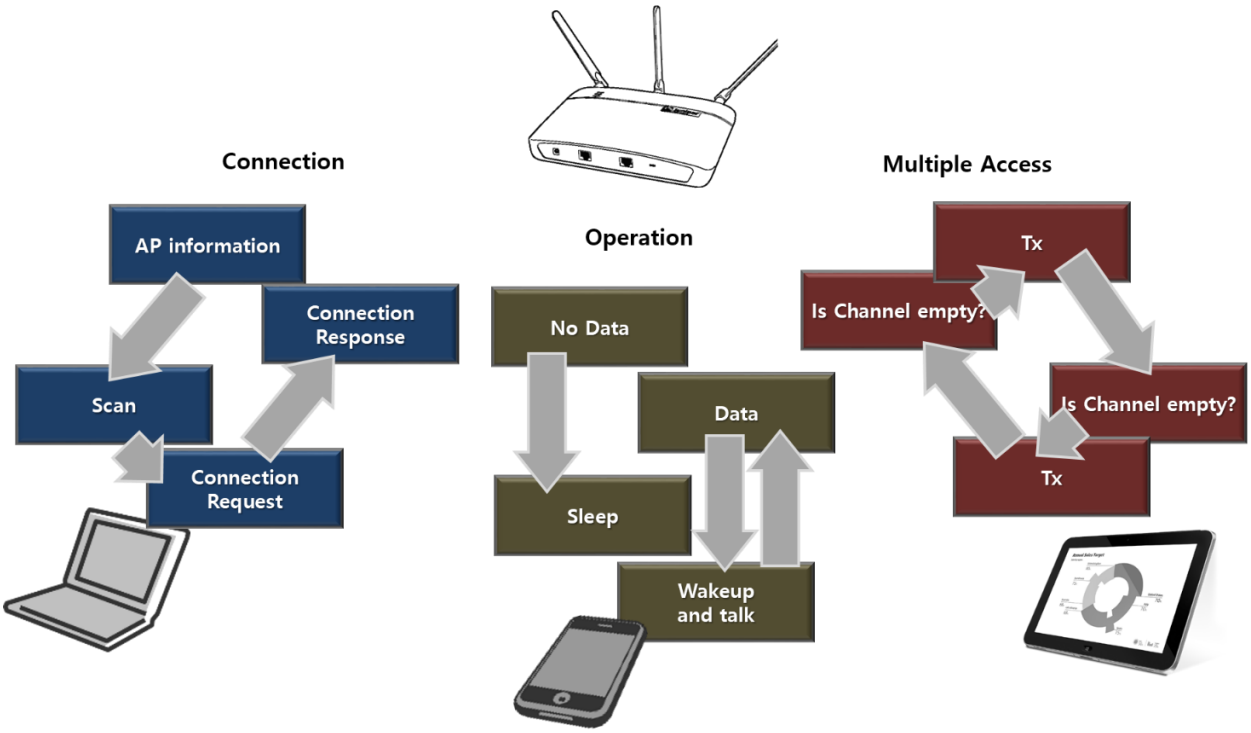
- WLAN utilizes “unlicensed frequency band” of 2.4GHz, 5GHz (and 6GHz from Wi-Fi 6E)
- WLAN signal occupies bandwidth of 20MHz or higher (40MHz, 80MHz, 160MHz, 320MHz)
- OFDM is the basic modulation scheme in WLAN (Spread spectrum in 11b)
- If a channel situation is good, a station(STA) sets the data rate to high, while it adapts down with bad channel situation
- Every station, Access Point (AP) or non-AP station associated to AP, has “equal footing” in PHY layer. They physically operate in the same way. (this equality changes from 11ax)



WLAN PHY Overview

MAC Overview

- Basic access control and multiple access are applied equally to AP and non-AP STA, while AP has additional roles managing network
- STA requests connection to Service Set with AP and AP approves or rejects.
- Non-AP STA generally goes to power save mode to reduce battery consumption, while AP is always powered on. STA wakes up to exchange data.
- If channel is occupied, STA waits until channel is available, which is a basic multiple access control in WLAN. It is applied both AP and STA.



WLAN MAC Overview

WLAN Standard

IEEE802.11 and Wi-Fi

IEEE (Institute of Electrical and Electronics Engineers) is the technical professional organization for academic activities and it also handles standardization for US (ANSI/IEEE) to International Standard (IEC/ISO)

- IEEE802 : LAN and MAN standard including WLAN, Ethernet, etc.
- IEEE802.11 : Wireless LAN standard for MAC and PHY layer
  - 802.11 Working Group page : http://grouper.ieee.org/groups/802/11

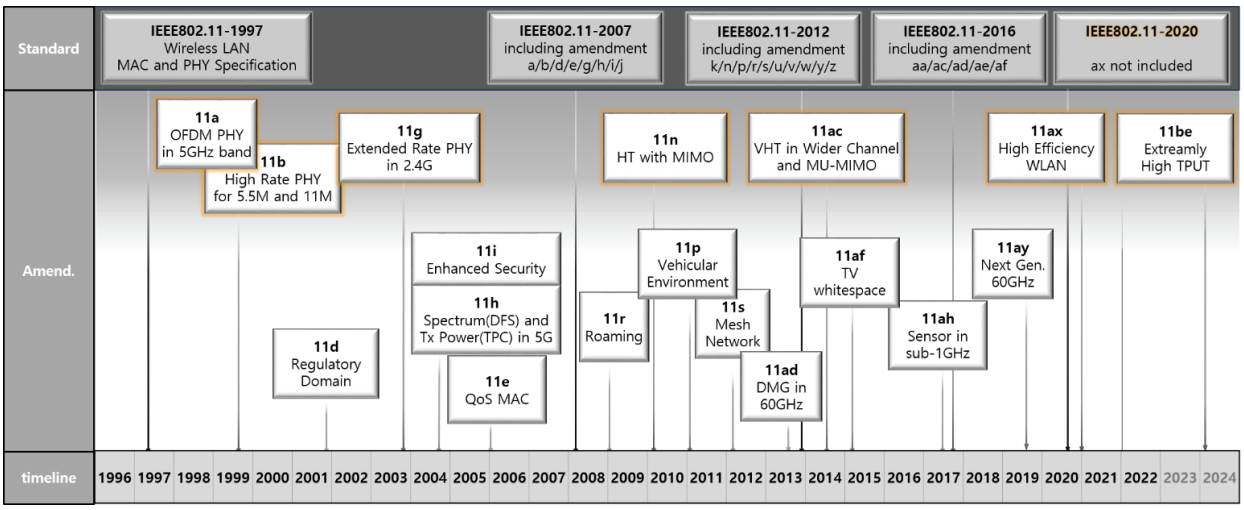
Wi-Fi Alliance is a global non-profit industry association to certify interoperability of WLAN mostly based on IEEE802.11 standard

- Wi-Fi Alliance homepage : https://wi-fi.org

IEEE802.11 Standard

Two major output from IEEE802.11 are “standard” and “amendment”. After the first standard (IEEE802.11-1997) was released, many Task Groups (TG) accomplished their work of “amendment”. TG naming starts from “a”,”b”,”c”,”f”,,.. ,”z”,”aa”,”ab”,”ac”,…, which we call as 11a, 11e, and the like. IEEE has edited the updated standard reflecting the successful amendment. Currently, IEEE802.11-2020 is the latest WLAN standard where 11ax is not included yet.

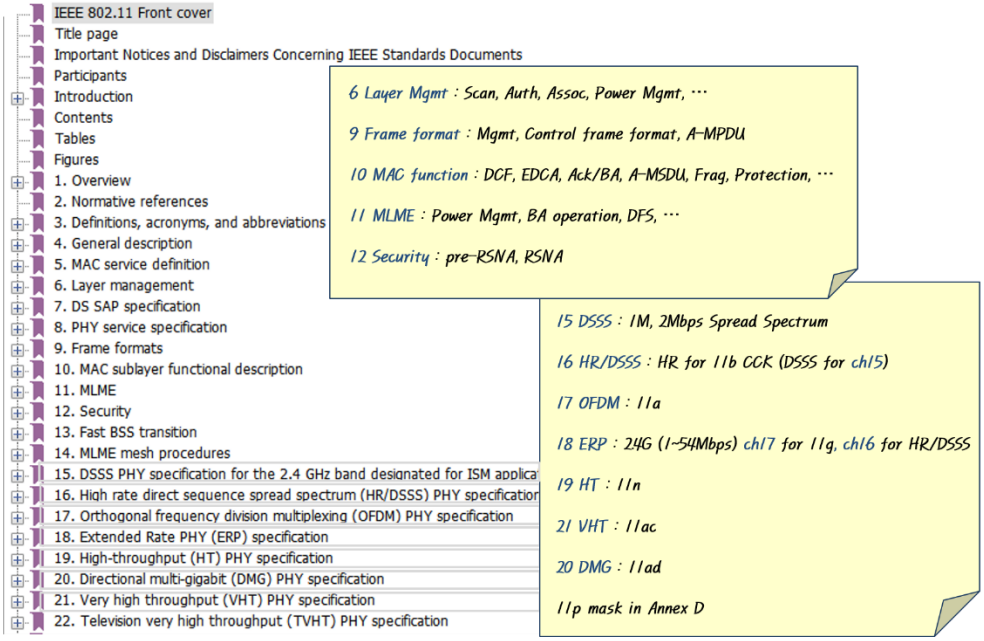
11a/b/g/n/ac/ax are the major amendment, which names are widely used by WLAN world. Recently, Wi-Fi alliance changed the naming of WLAN generation like Wi-Fi 6 for 11ax



IEEE802.11 Standard and Amendment in timeline

Inside IEEE802.11 Standard

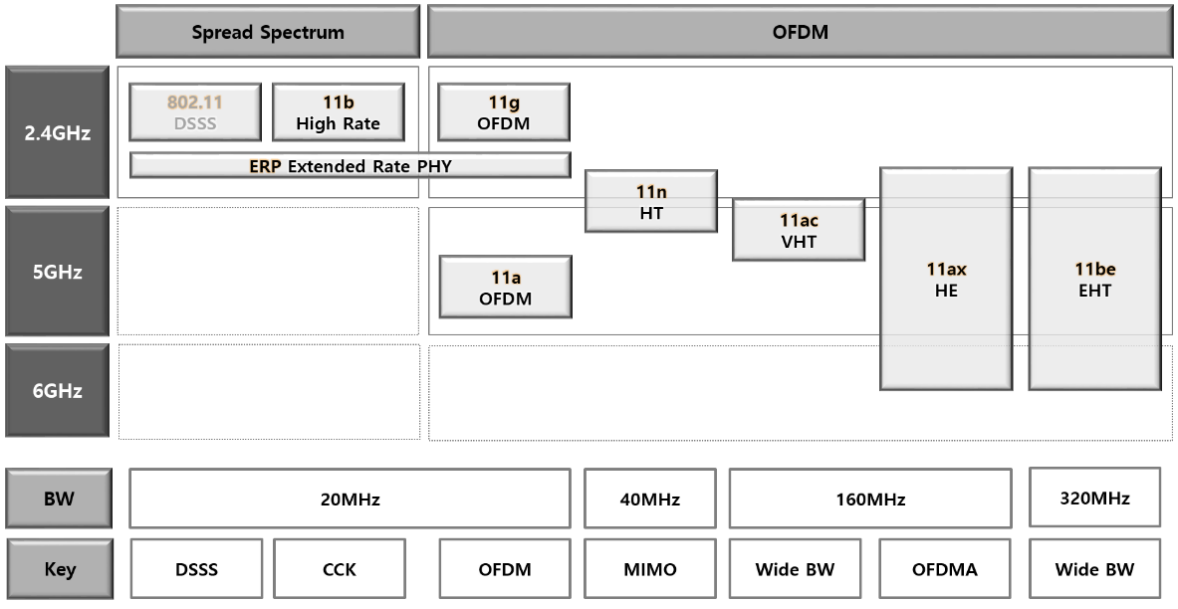
Former parts describes MAC layer protocol and latter for PHY layer. As 11a/b/g/n/ac is the name of Task Group, it does not appear in the standard. Instead, keywords (like High Throughput, HT for 11n) are used.



IEEE802.11 Standard Table of Contents

Major Amendment

Almost every four years, there has been a big change in WLAN. Physical layer adopted the modulation scheme (from Spread Spectrum to OFDM), the expansion in bandwidth (20MHz to 40/80/160MHz) and the multiple antenna techniques. MAC layer introduced QoS, BlockAck (11e), security (11i) and MPDU aggregation (11n).



	2000	2004	2008	2012	2016	2020	2024
Standard (amendment)	11b	11a/g	11n	11ac (wave1)	11ac (wave2)	11ax	11be
Frequency	2.4GHz	2.4GHz 5GHz				2.4GHz 5GHz 6GHz	
Bandwidth	20MHz	20MHz	+40MHz	+80MHz	+160MHz		+320MHz
Modulation	Spread Spectrum	OFDM (312.5KHz subcarrier space)				OFDM (78.126KHz subcarrier space)	
MCS	DSSS CCK	54Mbps	MCS7	MCS9 256 QAM		MCS11 1024 QAM	MCS13 4K-QAM
Max datarate	11Mbps	54Mbps	600Mbps (40M,4SS)	1.7Gbps (80M,4SS)	6.7Gbps (160M,8SS)	9.6GHz (160M,8SS)	46GHz (320M,16SS)
Multi-Ant			MIMO (4SS) Beamforming	MIMO (8SS) MU-MIMO (explicit)			MIMO (16SS) MU-MIMO (implicit)
Coding		BCC	BCC LDPC (optional)			BCC LDPC	
Multi-User	CSMA/CA			CSMA/CA MU-MIMO (DL)		CSMA/CA OFDMA (DL/UL) MU-MIMO (DL/UL)	
MAC	CSMA/CA in DCF	Security QoS	Aggregation			BSS Management	MLO HARQ
Security	WEP	WPA	WPA2			WPA3	

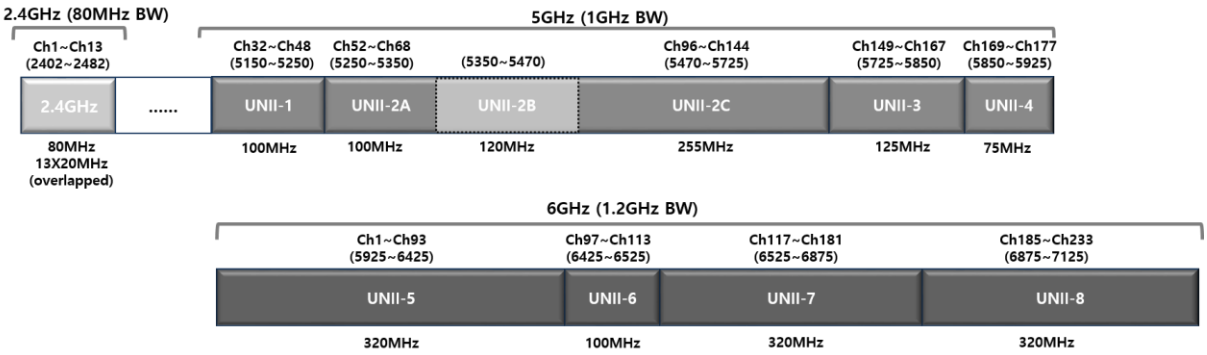
WLAN Mainstream

WLAN Frequency

WLAN Frequency

WLAN uses the unlicensed band of 2.4GHz and 5GHz. IEEE cannot regulate the frequency band, as it is the valuable resources for each regulatory (country) and managed accordingly. Policies and restrictions are different by regulatory domain. After ISM (Industrial, Scientific and Medial) bands were established by ITU (International Telecommunication Conference), many regulatory domains has made it unlicensed following FCC in 1985.

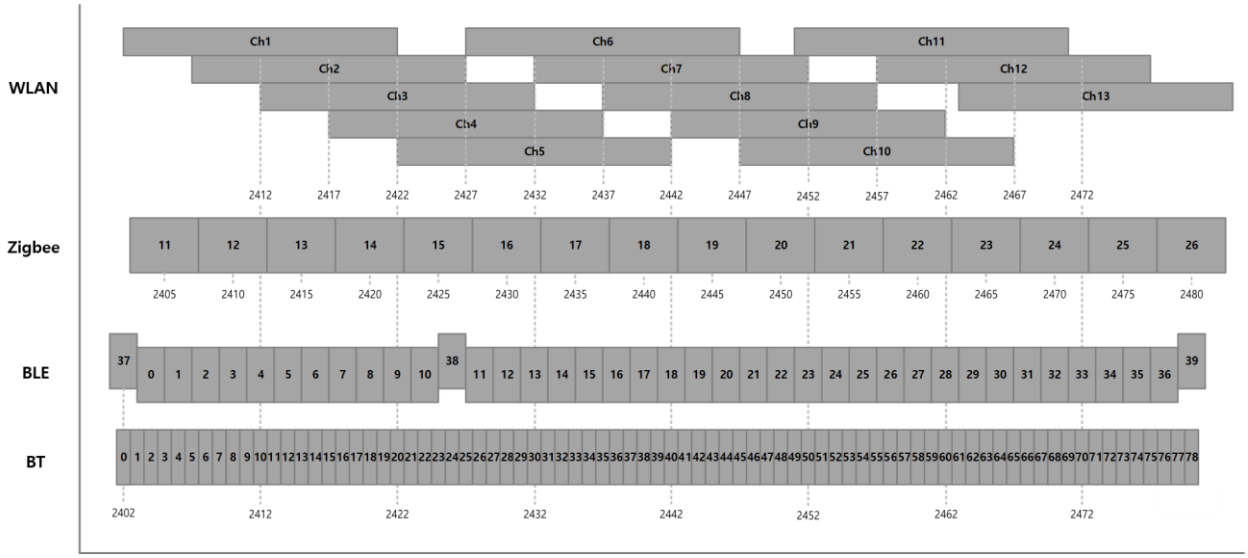
- 2.4GHz : WLAN channel of 20MHz BW is overlapped and it is not easy to utilize even 40MHz BW. Most of countries are using up to Ch13, while FCC limited it to Ch11 for WLAN. As many other wireless technologies like Bluetooth, Zigbee are using this bands as well, this band is very congested.
- 5GHz : Wider BW up to 160MHz can be utilized in 5GHz. However, many channels are limited with TPC (Transmit Power Control), DFS (Dynamic Frequency Selection) or SRD (Short Range Device) according to regulatory with the existence of RLAN.
- 6GHz : Regulatory domain starts to open 6GHz as unlicensed bands (FCC 5935~7125MHz end of 2018, ETSI ~7.1GHz 2019) and Wi-Fi 6E (11ax) is ready for it. Wider BW like 320MHz is expected in 6GHz. For more about 6GHz, please find *6GHz operation* in 11ax chapter.



WLAN Frequency and Channel overview

2.4GHz channel

Channel Center Frequency (MHz) = Channel starting frequency(2407) + 5 × Channel Number (1~13)



WLAN Frequency : 2.4GHz

5GHz channel

Channel Center Frequency (MHz) = Channel starting frequency (5000) + 5 × Channel Number (1~200)

	20M		40M		80M		160M		US	EU	KR
	Ch	MHz	Ch	MHz	Ch	MHz	Ch	MHz			
UNII-1	32	5160	34	5170	42	5210	50	5250		Indoor /TPC	Indoor
	36	5180	38	5190							
	40	5200									
	44	5220	46	5230							
	48	5240									
UNII-2A	52	5260	54	5270	58	5290			DFS /TPC	Indoor /DFS /TPC	DFS /TPC
	56	5280									
	60	5300	62	5310							
	64	5320									
	68	5340									
UNII-2B	72	5360									
	76	5380									
	80	5400									
	84	5420									
	88	5440									
	92	5460									
UNII-2C	96	5480									
	100	5500	102	5510	106	5530	114	5570	DFS /TPC	DFS /TPC	DFS /TPC
	104	5520									
	108	5540	110	5550							
	112	5560									
	116	5580	118	5590	122	5610					
	120	5600									
	124	5620	126	5630							
	128	5640									
	132	5660	134	5670	138	5690				DFS/SRD	
	136	5680									
	140	5700	142	5710							
	144	5720									
UNII-3	149	5745	151	5755	153	5765	163	5815		SRD	
	153	5765									
	157	5785	159	5795							
	161	5805									
	165	5825	167	5835	171	5855					
UNII-4	169	5845							Indoor	SRD	
	173	5865	175	5875							
	177	5885									

TPC and DFS are explained in detail in the chapter *Channel Management* of MAC

6GHz channel

Channel Center Frequency (MHz) = Channel starting frequency (5950) + 5 × Channel Number (1~233)

	20M		40M		80M		160M		US	EU	KR
	Ch	MHz	Ch	MHz	Ch	MHz	Ch	MHz			
UNII-5	1	5955	3	5965	7	5985	15	6025	STD /LPI	LPI /VLP	
	5	5975									
	9	5995	11	6005							
	13	6015									
	17	6035	19	6045	23	6065					
	21	6055									
	25	6075	27	6085							
	29	6095									
	33	6115	35	6125	39	6145	47	6185			
	37	6135									
	41	6155	43	6165							
	45	6175									
	49	6195	51	6205	55	6225					
	53	6215									
	57	6235	59	6245							
	61	6255									
	65	6275	67	6285	71	6305	79	6345			
	69	6295									
	73	6315	75	6325							
	77	6335									
	81	6355	83	6365	87	6385					
	85	6375									
	89	6395	91	6405							
	93	6415									
UNII-6	97	6435	99	6445	103	6465	111	6505	LPI		
	101	6455									
	105	6475	107	6485							
	109	6495									
	113	6515	115	6525	119	6545					
UNII-7	117	6535							STD /LPI		
	121	6555	123	6565							
	125	6575									
	129	6595	131	6605	135	6625	143	6665			
	133	6615									
	137	6635	139	6645							
	141	6655									
	145	6675	147	6685	151	6705					
	149	6695									
	153	6715	155	6725							
	157	6735									
	161	6755	163	6765	167	6785	175	6825			
	165	6775									
	169	6795	171	6805							
	173	6815									
	177	6835	179	6845	183	6865					
	181	6855									
	185	6875	187	6885							
UNII-8	189	6895							LPI		
	193	6915	195	6925	199	6945	207	6985			
	197	6935									
	201	6955	203	6965							
	205	6975									
	209	6995	211	7005	215	7025					
	213	7015									
	217	7035	219	7045							
	221	7055									
	225	7075	227	7085							
	229	7095									
	233	7115									

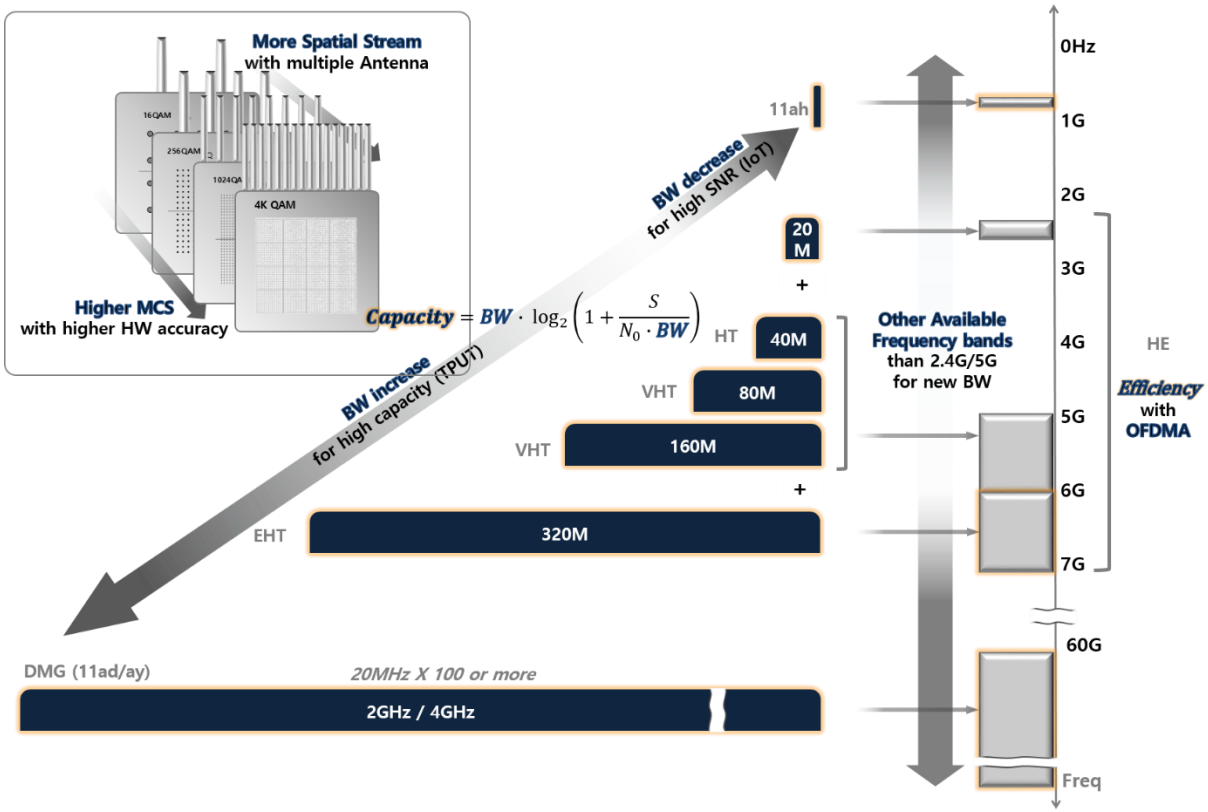
AP has three classes; Standard, LPI (Low Power Indoor), VLP (Very Low Power), which are handled in *6GHz operation* in 11ax chapter,

WLAN trends

Higher Capacity and Higher Efficiency

WLAN standard has focused on high capacity (speed) and started considering high efficiency from 11ax.

- Higher Capacity
  - Wider BW is required for higher capacity (Shannon formula). 6GHz and 60GHz are being explored for the available wider BW
  - MIMO was adopted and the number of MIMO stream gets higher : ~ 8 stream (16SS in 11be)
  - Modulation scheme is getting higher : ~1024QAM (4K QAM in 11be)
  - On the contrary, narrow BW is being utilized for IoT application, which does not need high capacity. Narrow BW is better for IoT application in terms of SNR
- High Efficiency
  - In 11ax, OFDMA and spectrum reusing technologies are adopted for higher spectral efficiency



WLAN trends

Item	WLAN main stream		Multi-gigabit	IoT
Standard	11a/b/g/n/ac and be	11ax	11ad/ay	11ah
Target	High TPUT	High Efficiency	DMG	IoT
Frequency	2.4GHz, 5GHz and 6GHz		60GHz~70GHz	Sub 1GHz
BW	20M/40M/80M/160MHz and 320M		2G, 4GHz	1~16MHz
MIMO	~8SS and 16SS		~4SS(11ay)	~4SS

WLAN trends

Wi-Fi 6 and Wi-Fi 7

Wi-Fi alliance announced the new naming system for Wi-Fi generation by a numerical sequence

- Wi-Fi 7 for devices that will support 802.11be technology
- Wi-Fi 6 for devices that support 802.11ax technology. Wi-Fi 6 includes Wi-Fi 6E for 6GHz extension.
- Wi-Fi 5 and Wi-Fi 4 support 802.11ac and 802.11n technologies each.

Generation name	Technology	Sample user interface
Wi-Fi 7	802.11be	
Wi-Fi 6	802.11ax	
Wi-Fi 5	802.11ac	
Wi-Fi 4	802.11n	

Wi-Fi 6 includes Wi-Fi 6E for 6GHz extension
Wi-Fi 7 in development (as of 2022)

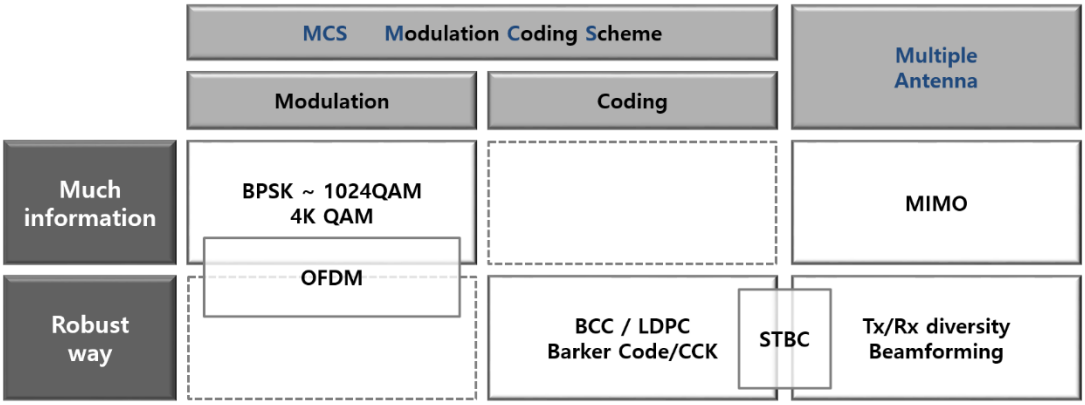
Wi-Fi generation

PHY

PHY Layer Overview

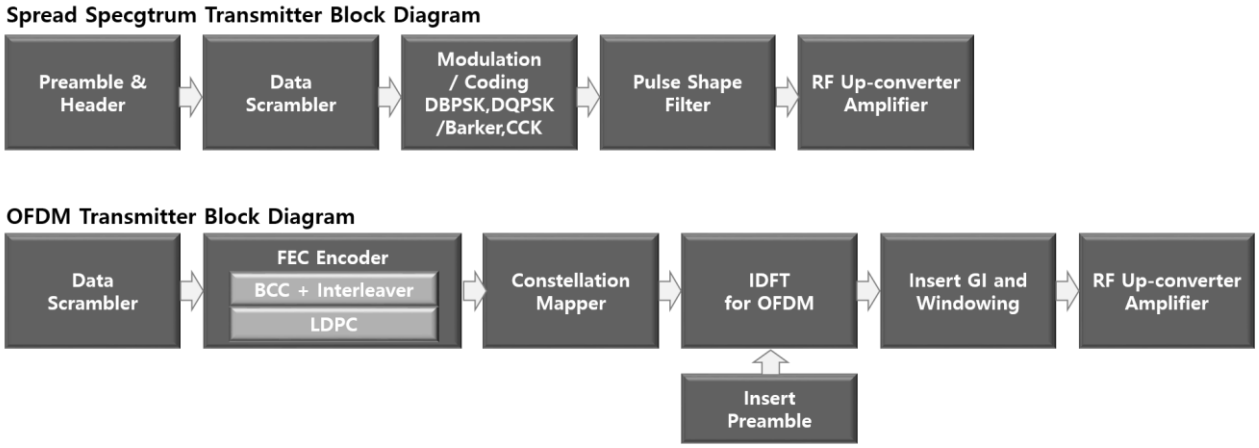
In layer-wise, PHY has PLCP (PHY Layer Convergence Procedure) and PMD (Physical Medium Dependent) sub-layer. PHY packet is composed with preamble, header and tailer in PLCP and modulation and coding is done in PMD.

For function-wise, PHY layer helps to exchange more information and in robust way in a wireless media.



PHY Layer Overview

WLAN Transmitter Block

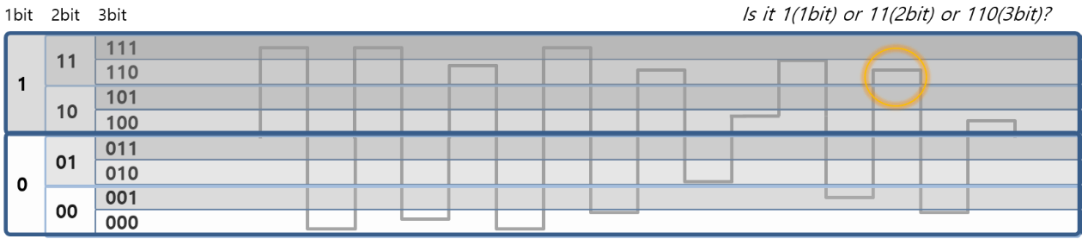


Transmitter Block Diagram

Modulation and constellation

Modulation is based on "accuracy" and "mutual agreement"

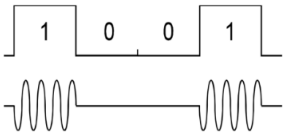
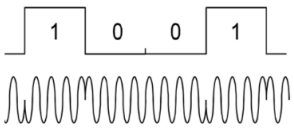
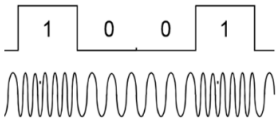
Both Transmitter and Receiver should share the information with which modulation the symbol is being sent. The transmitter should meet accuracy according to the modulation scheme. WLAN transmitter specifies MCS (modulation) information in Packet header (SIG field) and needs to meet EVM (accuracy) requirement.



Is the symbol in the yellow circle indicating one bit or two bit or three bit?

Amplitude, Phase and Frequency as the information source in modulation

Signal can be expressed with amplitude, phase and frequency and the information is delivered subdividing these factors, which is called as "modulation" or "keying". Frequency modulation is relatively easy to implement, while hard to deliver many information and it is widely used in low rate communication like voice. In WLAN, a combination of amplitude and phase modulation is used like BPSK, QPSK, 16QAM, and so on.

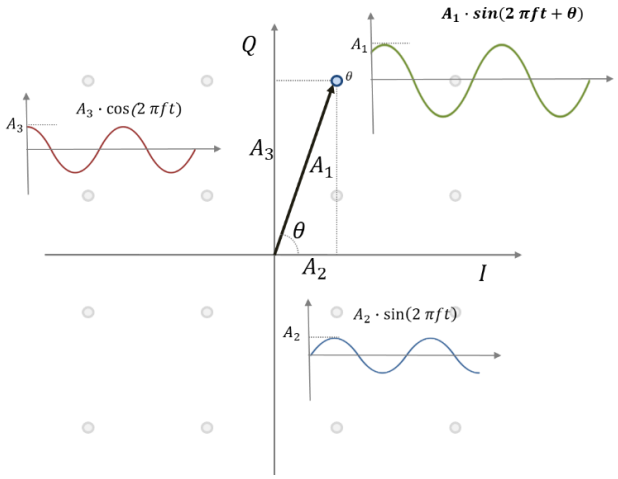
	ASK : Amplitude	PSK : Phase	FSK : Frequency
Baseband → Modulated			
Expression	$A \cdot \sin(2\pi f t + \theta)$		
	A	θ	f
Feature	Easy to implement Weak to noise/interference	Easy for M-ary bandwidth efficient	Easy to implement For low speed like voice
Example	**Quadrature Amplitude Modulation (Amplitude + Phase)** **BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM, 4K QAM (WLAN)**		GMSK = (0.5BT) GBFSK (BT 1M BDR)
		BPSK, QPSK (WLAN)	
		Offset QPSK (Zigbee) pi/4 DQPSK (BT 2M EDR) 8DPSK (BT 3M EDR)	

Amplitude, Phase and Frequency Modulation

Modulation and Constellation

A sinusoidal signal with an amplitude and a phase can be expressed with the combination of two sinusoidal signals with 90 degree phase shift (sine and cosine). This signal is graphically expressed in “constellation” with in-phase (sine) and quadrature phase (cosine), which is widely used in communication system to see the modulation accuracy (EVM)

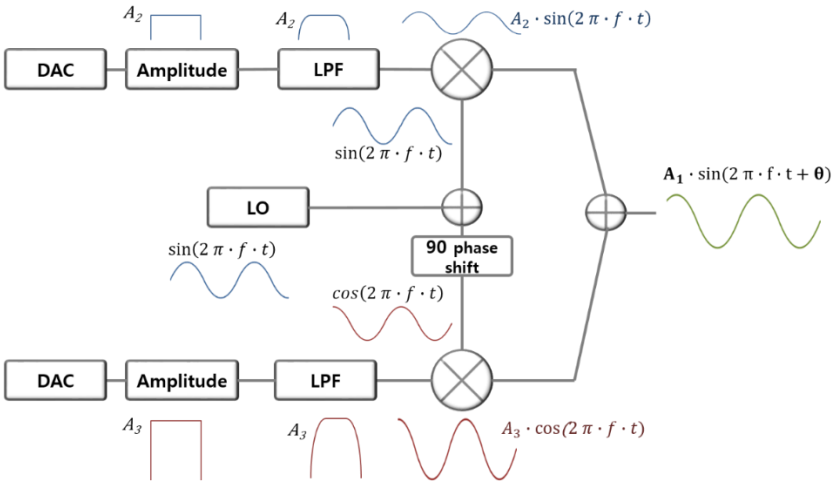
$$A_1 \cdot \sin(2\pi ft + \theta)$$
$$= A_1 \cdot \cos(\theta) \cdot \sin(2\pi ft) \cdot + A_1 \cdot \sin(\theta) \cdot \cos(2\pi ft)$$
$$= A_2 \cdot \sin(2\pi ft) + A_3 \cdot \cos(2\pi ft)$$



Constellation and Modulation information of Amplitude, Phase

Implementation of QAM

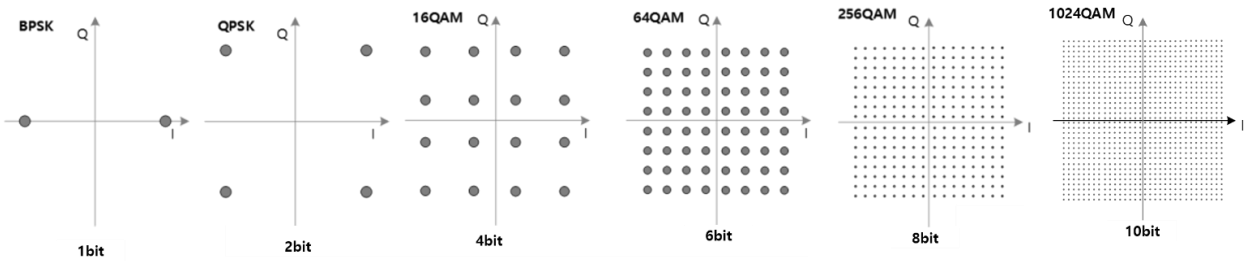
One sinusoidal signal from Local Oscillator (LO) can be divided into in-phase and quadrature-phase signal. When the different amplitudes are multiplied with LO, various QAM modulation is implemented.



How is QPSK implemented?

Modulation in WLAN

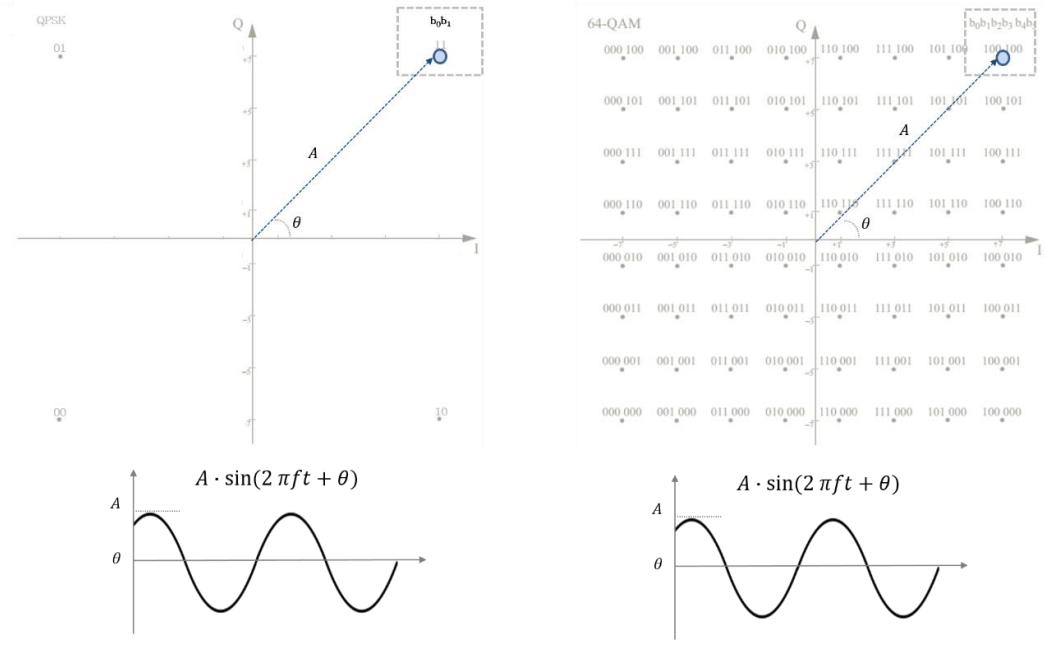
BPSK signal has two different phases for 1 bit (0 or 1) information. If a signal has 16 different points in constellation, it is 16 QAM with 4 bit information (2^4). In WLAN, up to 64 QAM is used for 11a/g/n, 256 QAM for 11ac and 1024 QAM for 11ax.



Modulation in WLAN

Modulation is "accuracy", again!

The signals itself in QPSK and 64 QAM can be identical, if they have the same amplitude and phase. With same amount of error in constellation in the picture below, QPSK indicates the same information, while 64 QAM tells it as a different information. Again, modulation is accuracy.



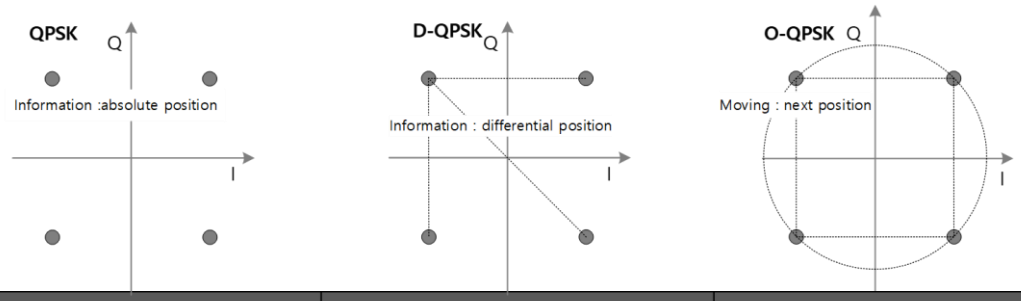
Modulation example : QPSK vs 64QAM

Modulation	QPSK	64QAM
Information	2bit (11)	6bit (100100)
Same Error	Correct decision	Wrong decision
	Robust in channel	higher information

Modulation is "accuracy"

QPSK? DQPSK? OQPSK?

When a signal experiences a wireless channel, the amplitude and the phase are subject to a serious change (distortion). In (coherent) QPSK, a receiver interprets symbols with the same position transmitter sent at. For these purpose, QPSK requires the reference signal which is Pilot subcarrier in WLAN OFDM. Differential QPSK (DQPSK) interprets signal with the relative position between the previous and the current symbol. Even if accuracy is lower than coherent QPSK (both error of the previous and the current symbol can be added), it does not require the additional reference like Pilot. Offset QPSK (OQPSK) is operating like DQPSK except that the signal does not change both of in-phase and quadrature-phase at the same time, which prevents zero-crossing that may demands wider linear amp.



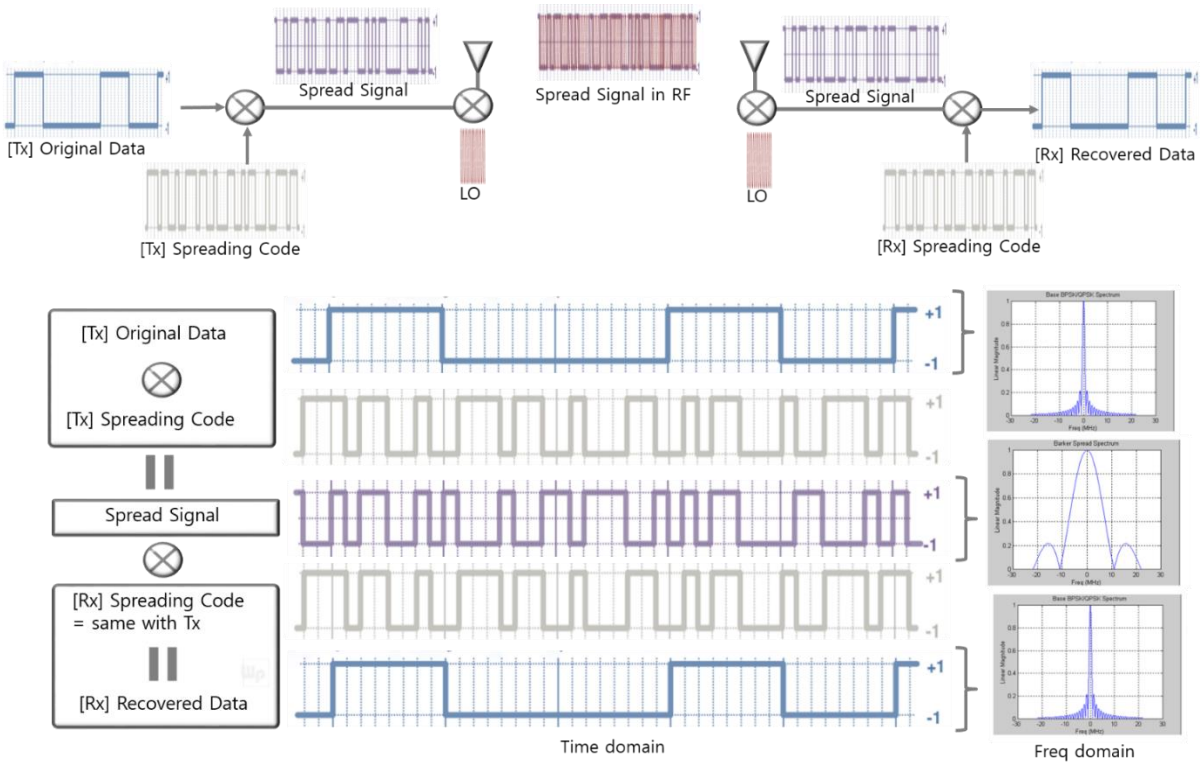
	(Coherent) QPSK	(Non-coherent) Differential QPSK	Offset QPSK
Detection	Absolute Position	Difference in Position	Moving I or Q at one time
Pro	3dB more accurate than Differential PSK Faster than Offset PSK	Easier to implement with relative position	Non/low linear amp
Contra	Complex receiver (D-PSK) Higher Amp Linearity (O-PSK) BW inefficient Needs reference (Pilot subcarrier, WLAN)	3dB inaccurate Coherent PSK with error from previous position	Slow
Application	**WLAN (OFDM)**	**WLAN (DSSS/CCK)**, BT (EDR)	Zigbee

Various QPSK types (DQPSK, OQPSK)

Spread spectrum

Operation of Spread Spectrum

When a symbol is multiplied with a faster symbol (code or chip), the bandwidth of original symbol gets wider according to the chip rate. If this spread signal is multiplied with the same code, the original signal is recovered.



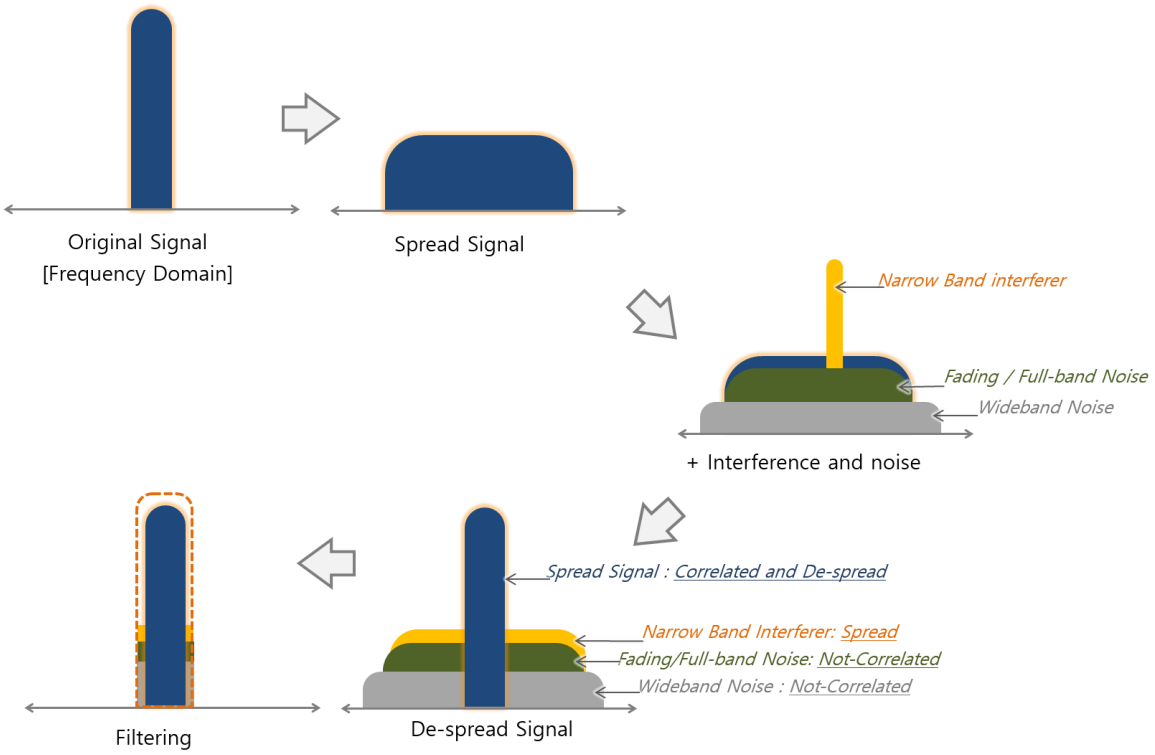
Operation of Spread Spectrum

Spread Spectrum and processing gain

The spread signal is de-spread to the original signal at receiver, as it is multiplied with same spread code. While in this process, the spread signal from the other users remains the same (not de-spread) without correlation and a narrow band interferer in wireless channel is spread and filtered. Ruling out the interference in spread spectrum system is the processing gain.

Processing Gain is the ratio of the spreading bandwidth to the un-spread (original) signal bandwidth

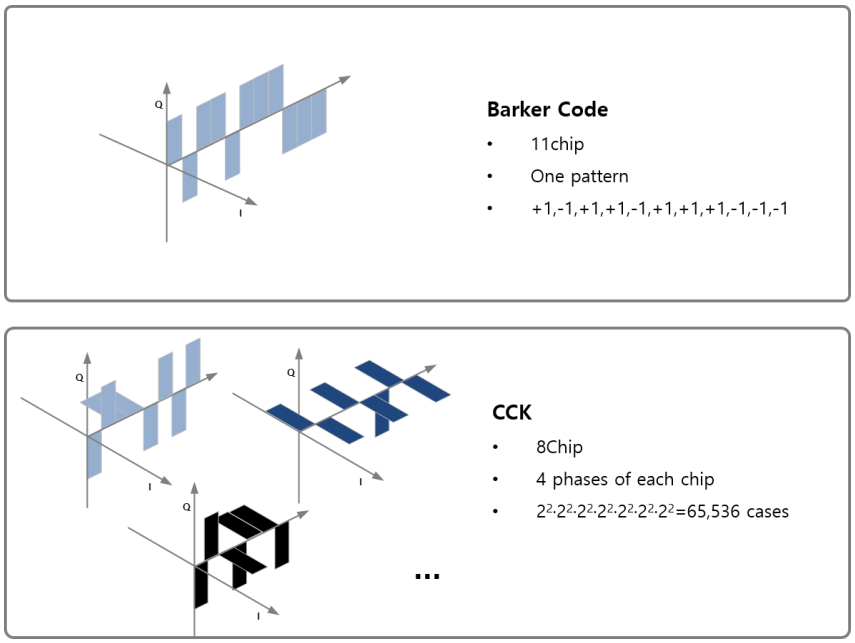
- 1 kHz signal is spread to 100 kHz, the processing gain is 100,000/1,000 = 100. (10*log100 = 20dB)
- If PN sequence is 11 chip; 10*log11 = 10.4dB



Spread Spectrum and Processing Gain

Barker Code and CCK in WLAN

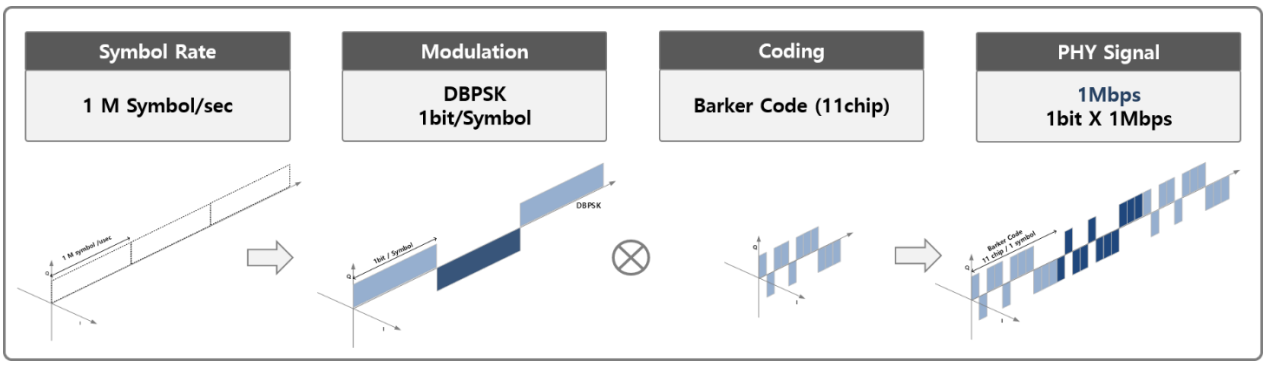
11 chip Barker code is used for 1Mbps and 2Mbps in WLAN and 8 chip CCK (Complimentary Code Keying) is used for 5.5Mbps and 11Mbps of 11b. Barker code is used with one pattern (combination of +1 and -1) and CCK is used to deliver information with the selection among about 64K cases.



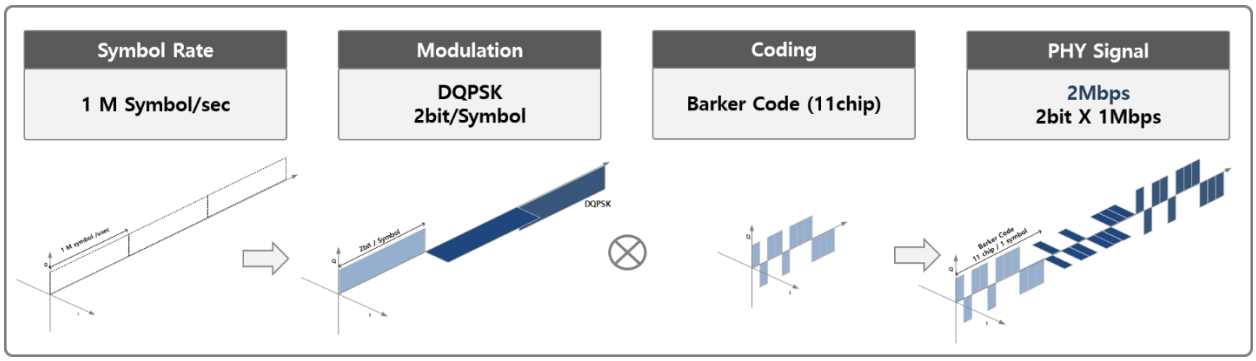
Barker Code and CCK in WLAN Spread Spectrum

11b data rate

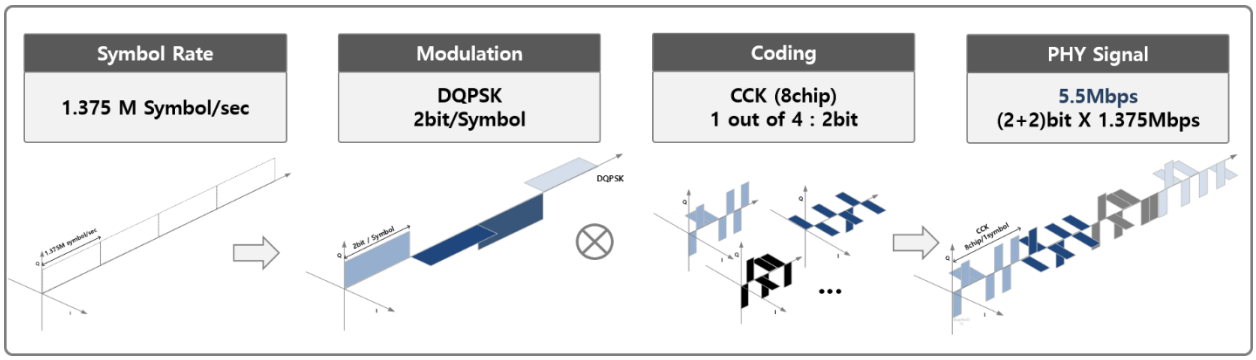
Originally 1M and 2Mbps with Barker code is 802.11 standard and 11b expands to 5.5M and 11Mbps, even if all of them are conventionally called as 11b. Symbol rate of 1Mbps and 2Mbps is 1M symbol/sec and signal after Barker code is expressed in 11M chip/sec. Symbol rate of 5.5M and 11M is 1.25M symbol/sec and they become 11M chip/sec with 8bit CCK. They all have same BW of 20MHz (11M chips/sec)



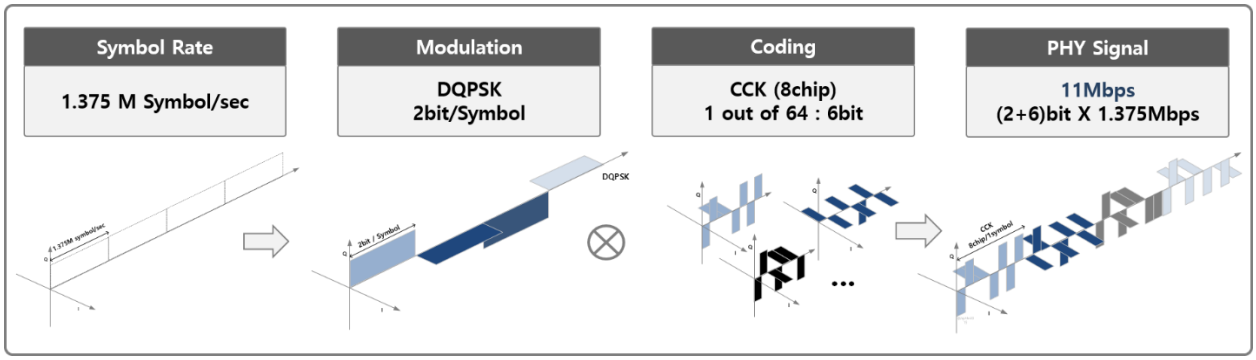
1Mbps with DSSS



2Mbps with DSSS



5.5Mbps with CCK



11Mbps with CCK

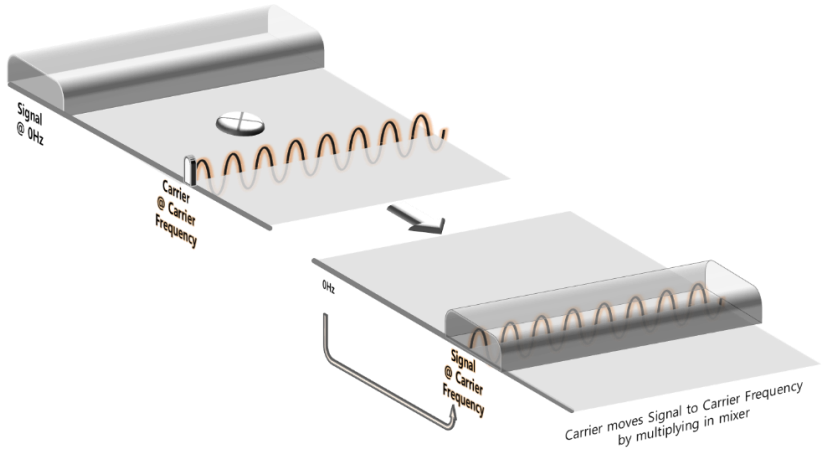
Data Rate	Symbol Rate	Modulation	Coding	Bit/Symbol	Rate	Code Length	Chip Rate
1Mbps	1M symbol/sec	DBPSK (1bit)	1 barker (1bit)	1X1 : 1	(1X1)Mbps	11chip (Barker)	11chipX1M
2Mbps	1M symbol/sec	DQPSK (2bit)	1 barker (1bit)	1X2 : 2	(1X2)Mbps	11chip (Barker)	11chipX1M
5.5Mbps	1.375M symbol/sec	DQPSK (2bit)	1 of 4 CCK (2^2: 2bit)	2+2 : 4	(1.375X4)Mbps	8chip (CCK)	8chipX1.375M
11Mbps	1.375M symbol/sec	DQPSK (2bit)	1 of 64 CCK (2^6: 6bit)	6+2: 8	(1.375X8)Mbps	8chip (CCK)	8chipX1.375M

11b data rate summary

OFDM

Carrier

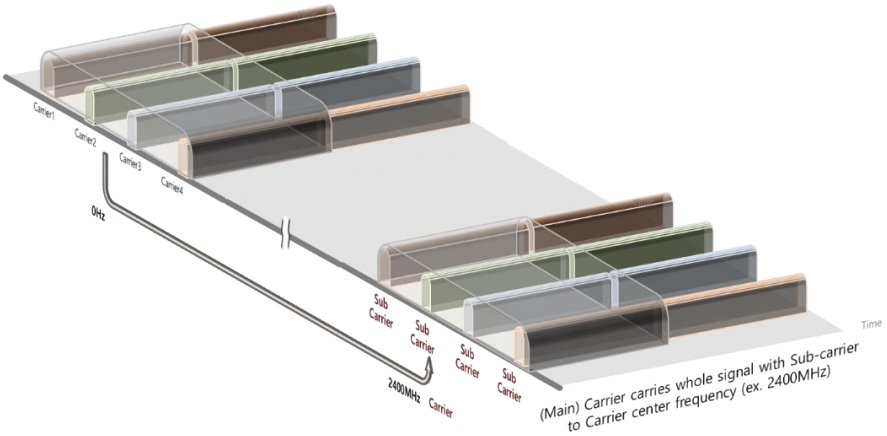
When a signal in base band (BB) is multiplied with “carrier” signal with a higher frequency (LO), the carrier frequency becomes the center frequency of the original signal. Carrier carries the signal in radio frequency.



“Carrier” carries signal to its frequency

Multi-carrier

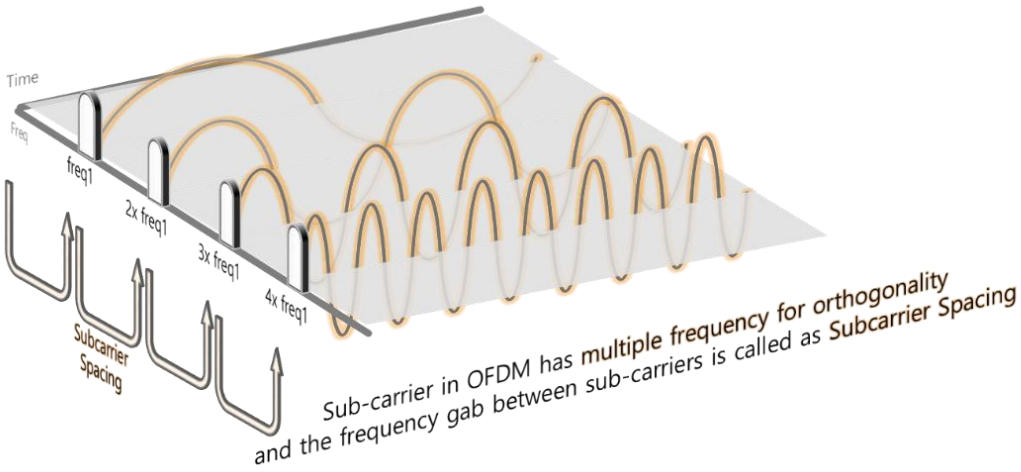
If the signal is composed of multi-carriers, each carrier is called as “subcarrier”. Multi-carrier signal sends information in each subcarrier and this parallel communication system allows symbol duration relatively longer than single carrier system. (Sending 10 symbol together for 10sec and sending 1 symbol in 1sec 10 times. Each case takes the same time of 10sec). Based on one symbol, a symbol in single carrier system changes faster than a symbol in multi-carrier and it takes up wider bandwidth. In multi-carrier system, information is delivered in parallel and the bandwidth is of the total signal (symbol) is combined one of all the subcarriers.



Sub-carrier in Multi-carrier signal

Subcarrier in OFDM

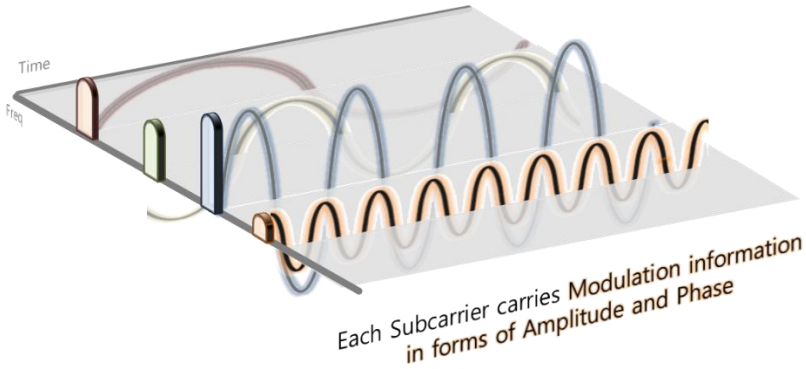
Subcarriers in OFDM have multiple frequency to have orthogonality each other. They have same frequency gab which is called as “subcarrier spacing”.



Orthogonal sub-carrier allocation in OFDM

Modulation information on subcarrier

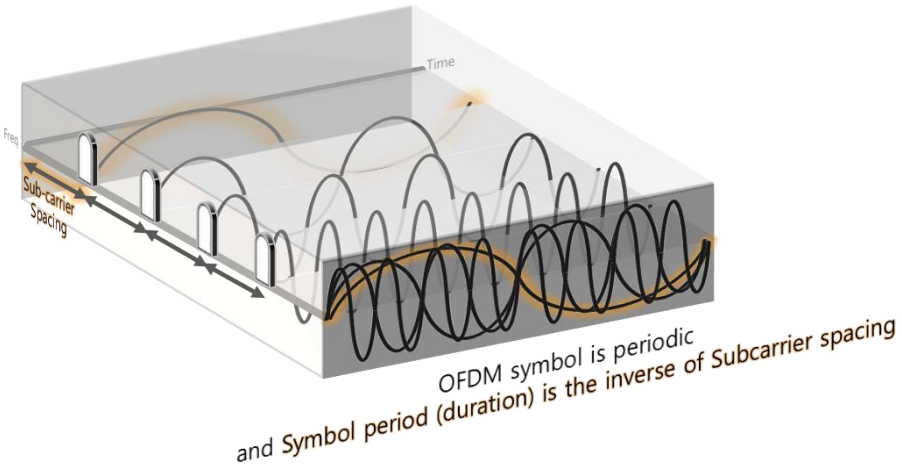
Each subcarrier (sinusoidal wave) carries the information in form of a specific amplitude and a phase.



Amplitude/phase information on sub-carrier

Subcarrier spacing and symbol duration

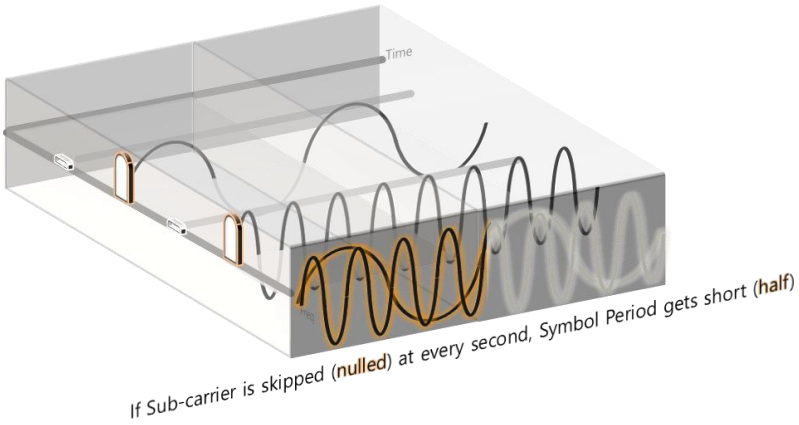
OFDM symbol is summation of all subcarriers. The symbol itself is periodic and its duration depends on lowest subcarrier frequency (the longest duration) which is same with the subcarrier spacing.



Sub-carrier spacing and symbol duration

Short symbol duration

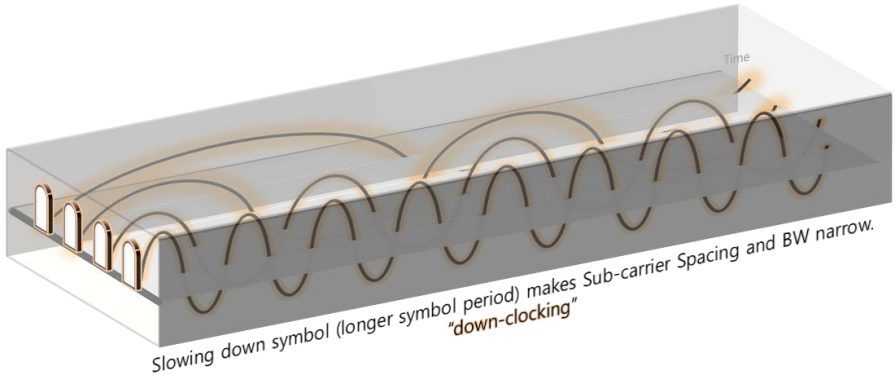
If subcarrier is skipped (nulled) at every second, symbol period gets short (half), as subcarrier spacing gets double and symbol period is inverse of subcarrier spacing. Sub-carrier is assigned this way in some OFDMA symbols like Short Training field in preamble of WLAN. Short training symbol has sub-carrier at every 4th and one symbol duration is 0.8usec which is 1/4 of original WLAN OFDM symbol duration of 3.2usec.



How to make symbol duration short

Down-clocking

Slowing down symbol (longer symbol period) makes subcarrier spacing and overall BW to be narrower. This “down-clocking” technique is applied widely in WLAN (11p/11h/11ax). For example, 2MHz BW of 11h is implemented with 1/10 down clocking of 20MHz OFDM symbol.

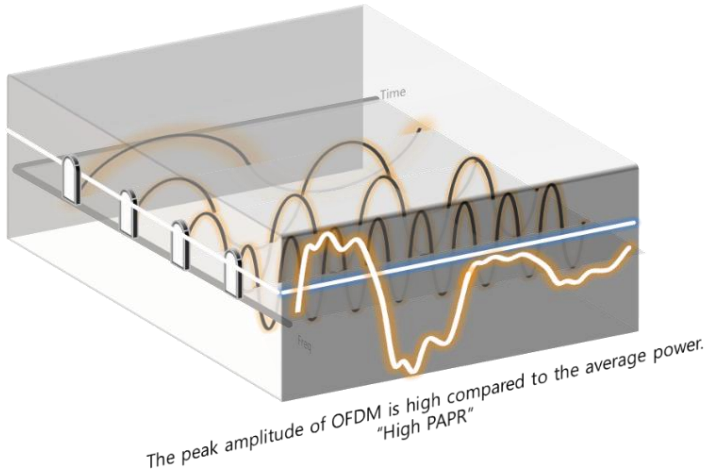


Down clocking : How to make overall bandwidth narrow

High PAPR (Peak to Average Power Ratio)

OFDM Symbol is the summation of each subcarrier’s component, and peak amplitude can get high compared to average power (High PAPR). Stochastically, PAPR increases, as the number of sub-carrier increases. High PAPR is the major drawback of OFDM, as it requires Power Amplifier with wide linearity.

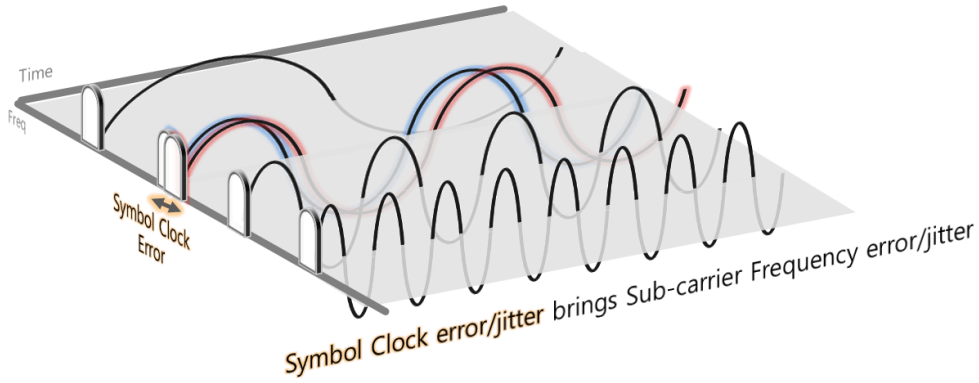
- PAPR [dB] = 10 log (N) , N = # of sub-carrier
- (Ex) 11n : N=58, PAPR = 10 log (58) = 17.6 dB for all phase aligned up
- 2~3dB decrease in Modem Design : PAPR =~ 15dB
- Rare situation for in-phase of all subcarriers : PAPR =~ 10dB



High PAPR in OFDM

Symbol Clock error

If symbol clock has frequency error, it results in frequency error and jitter in OFDM. If it has phase noise (short term jittering), it also results in error with the same reason



Symbol clock error

OFDM Summary

OFDM is adopted in most of the modern high speed communication system like WLAN, LTE, DOCSIS3.1. It is efficient in allocating subcarriers with flexibility and robust in multipath fading, while its high PAPR demands high system cost.

Pro	Contra
➔ Long Symbol + GI : multipath fading ➔ Simple implementation with IFFT ➔ High Expandability ➔ Efficient freq utilization with sub-carrier allocation	➔ High PAPR (average to peak power ratio) : High system cost ➔ Sub-carrier spacing : Sensitive to frequency offset and phase noise

Pros and Cons of OFDM

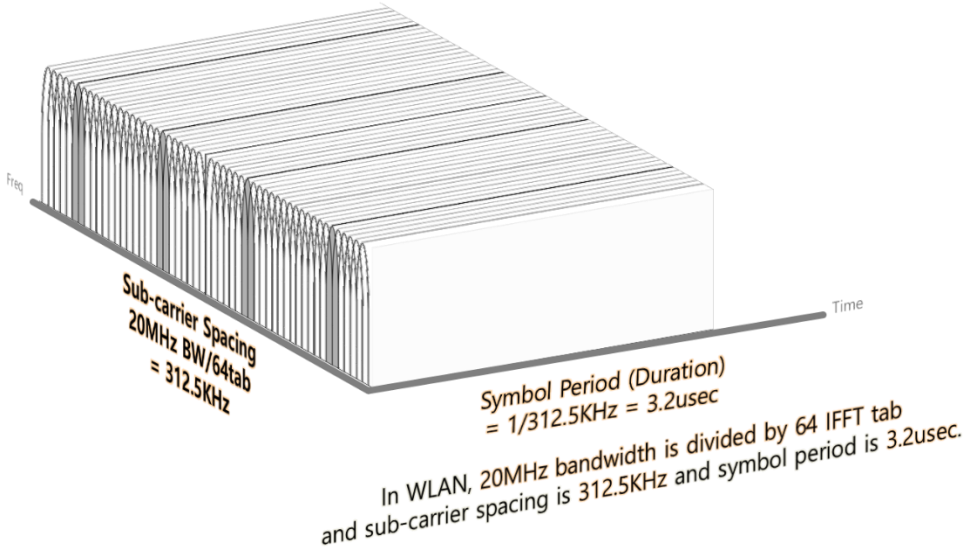
OFDM in WLAN

OFDM symbol in WLAN

In WLAN, 20MHz BW is divided by 64 for each subcarrier. (This scheme changes from 11ax)

- Subcarrier spacing : 20MHz/64 = 312.5KHz
- Symbol period : 1/312.5KHz = 3.2usec

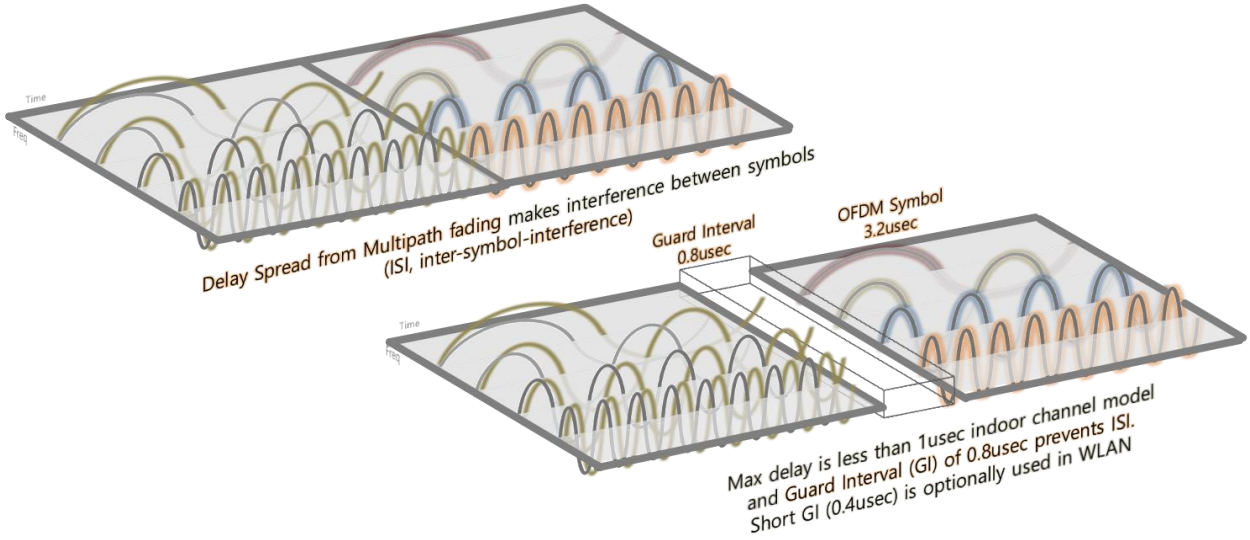
Among 64 subcarrier position in 20MHz, most of sub-carriers are used for data, while the center and guard (edge) subcarriers are nulled and some carriers are assigned for Pilots.



Sub-carrier spacing and symbol duration in WLAN OFDM

Guard Interval

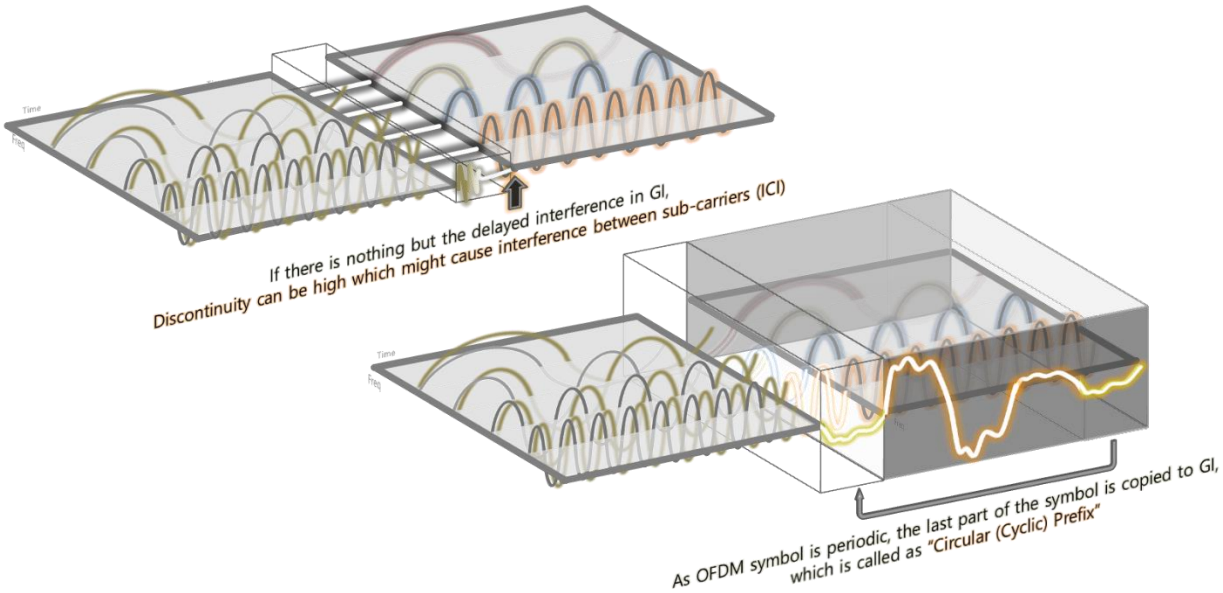
Multipath fading in wireless channel results in delay spread of original signal, which situation causes interference between two consecutive symbols. (Inter-symbol interference, ISI). The channel model show max indoor delay spread is less than about 1usec and in WLAN, Guard Interval (GI) of 0.8usec (Long GI) or of 0.4usec (Short GI) is inserted between symbols to prevents ISI. For more information on channel, find *Wireless Channel* chapter.



ISI from multi-path fading and Guard Interval

Circular (Cyclic) Prefix

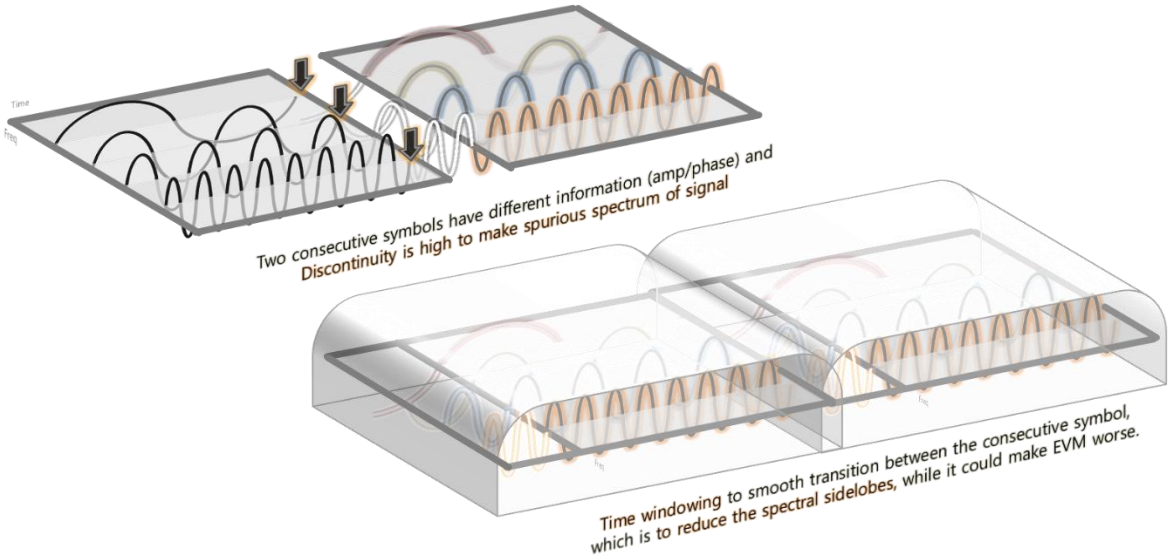
Discontinuity between (empty) GI and symbol may result in the interference between subcarriers. As OFDM symbol is periodic, the last portion (0.8usec or 0.4usec) of OFDM symbol is copied to GI, which is called as "Circular Prefix" or "Cyclic Prefix".



Circular Prefix (Cyclic Prefix)

(Time) Windowing

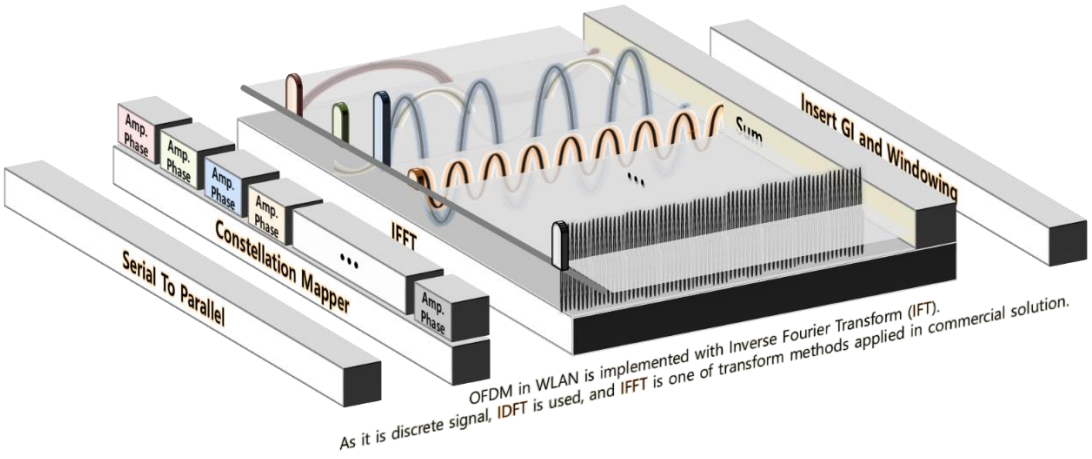
With Circular Prefix, discontinuity at the point between symbols may be high to make spurious spectrum of signal. Time windowing is applied to mitigate this situation.



Windowing

OFDM implementation in WLAN transmitter

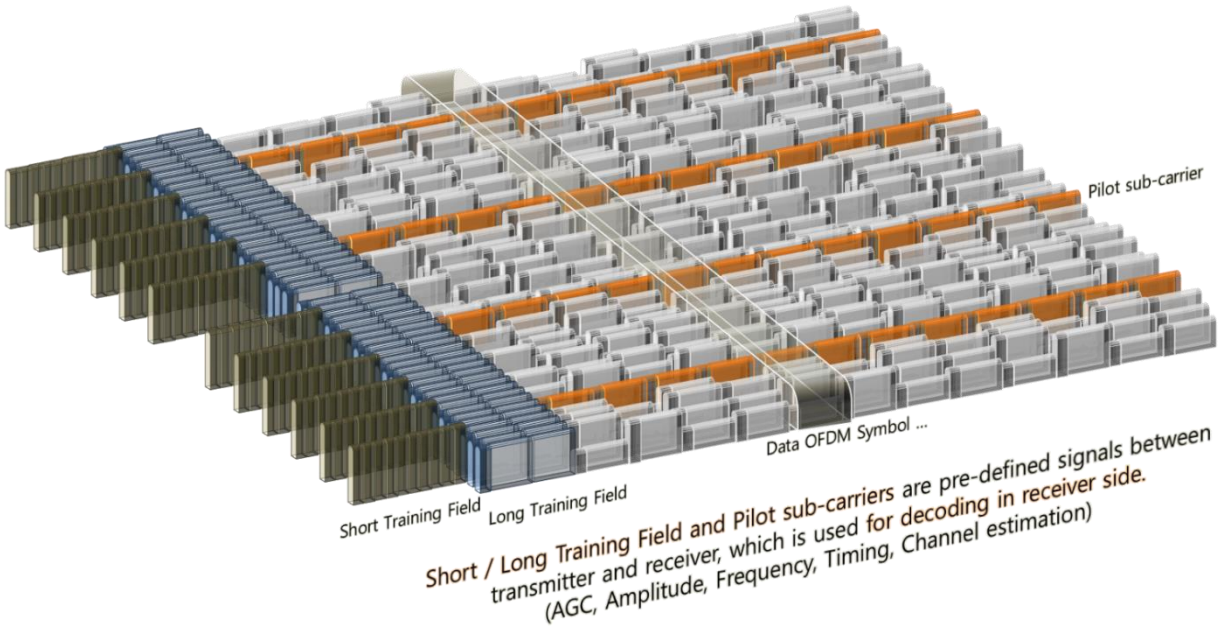
OFDM is the summation of the frequency components (the information assigned at every sub-carrier). To convert this frequency domain operation to time domain, Inverse Fourier Transform (IFT) is used. As it is discrete signal, IDFT is used, and IFFT is one of transform methods applied in commercial solutions.



How to implement OFDM in WLAN Tx block

OFDM packet

The image below is the conceptual WLAN OFDM packet expressed with the same number of subcarrier in 11a/g. The first parts are “Short Training” and “Long Training” field (preamble) to support receiver’s decoding along with pilot subcarriers lying inside data symbols.

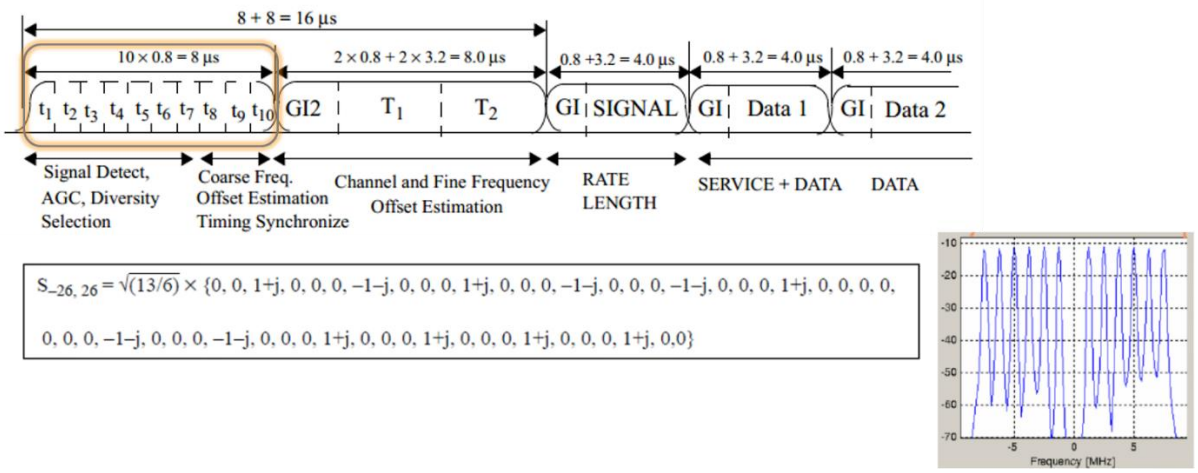


WLAN OFDM Packet

Short Training Field (STF)

As the first symbol in OFDM packet, STF helps the receiver for the reference level convergence of the received signal AGC (Auto Gain Control), coarse frequency acquisition and timing synchronization. It consists of 10 symbols of 0.8usec duration.

It has 12 tone only among 64 tone in 20MHz. Subcarrier spacing is 1.25MHz (= 312.5KHz X 4) and symbol duration is 0.8usec (=1/1.250MHz)

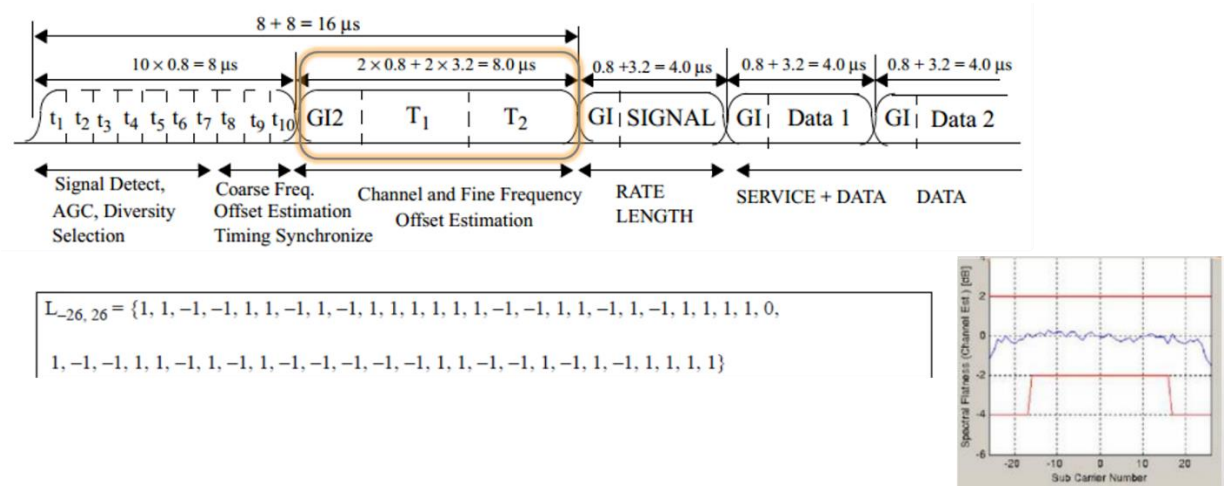


OFDM Training Sequence (Preamble) : Short Training (legacy)

Long Training Field (LTF)

Long training field is “flat” in frequency distribution and consists of subcarriers with amplitude of “1” (1 or -1). From this field, wireless channel can be estimated. Along with it, it is used for fine frequency acquisition.

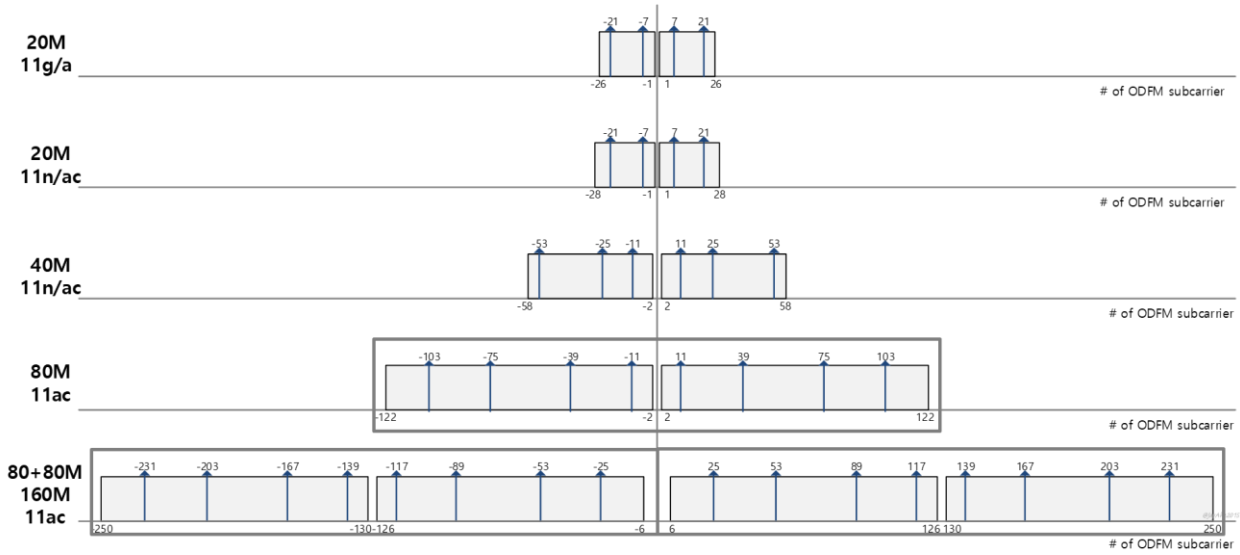
LTF is used for frequency flatness measurement of RF test



OFDM Training Sequence (Preamble) : Long Training (legacy)

Subcarrier and pilot in 20MHz, 40MHz, 80MHz and 160MHz BW

Number of subcarrier and pilot allocation is different from 11a/g and 11n/ac, which is the reason why HT/VHT data rate is slightly higher than 11a/g data rate with the same modulation and coding rate. Compared to 20MHz, the number of data subcarrier of 80MHz is about 5 time high, not 4 times, as the data subcarrier allocation scheme is different.



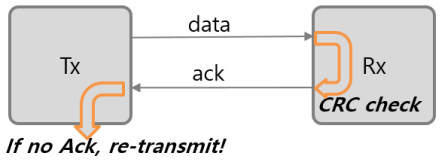
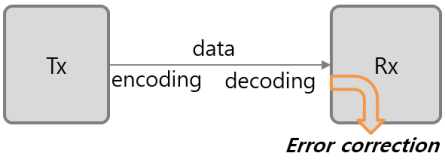
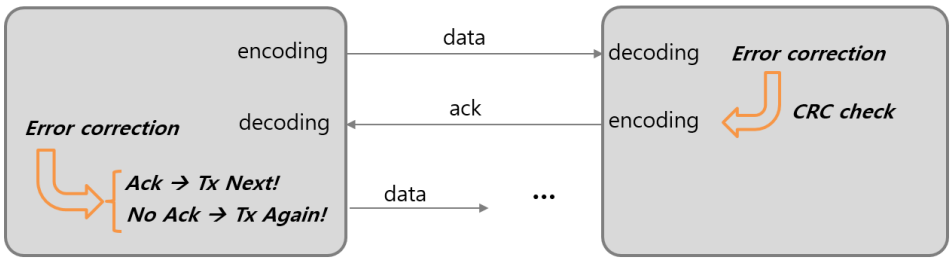
BW	IEEE	# Subcarrier	# data	# pilot	% pilot	Relative BW	Relative capacity
20M	11g/a	52	48	4	8%	**base**	**base**
20M	HT/VHT	56	52	4	7%	**1**	**1.1**
40M	HT/VHT	114	108	6	5%	**2**	**2.3**
80M	VHT	242	234	8	3%	**4**	**4.9**
160M	VHT	484	468	16	3%	**8**	**9.75**

Bandwidth and OFDM subcarrier

FEC Coding

How to deal with error in the communication system

There are two ways to handle error in communication system, (1) retransmission (ARQ) and (2) forward error correction (FEC). In retransmission scheme, there is acknowledge (Ack) from receiver, as the transmitter needs to know if data has been delivered or not properly. This scheme is applied in MAC layer in WLAN. For FEC, the transmitter sends data after coding and the receiver tries to correct error with decoding, if any and if possible.

	Re-transmission	FEC (Forward Error Correction)
Layer	**MAC** (mostly)	**PHY**
Direction	Two way	One way (*forward*)
Method	Acknowledge (CRC)	**Coding**
		
FEC + Retransmission		

How to deal with error in communication system

Brief history on Error Coding

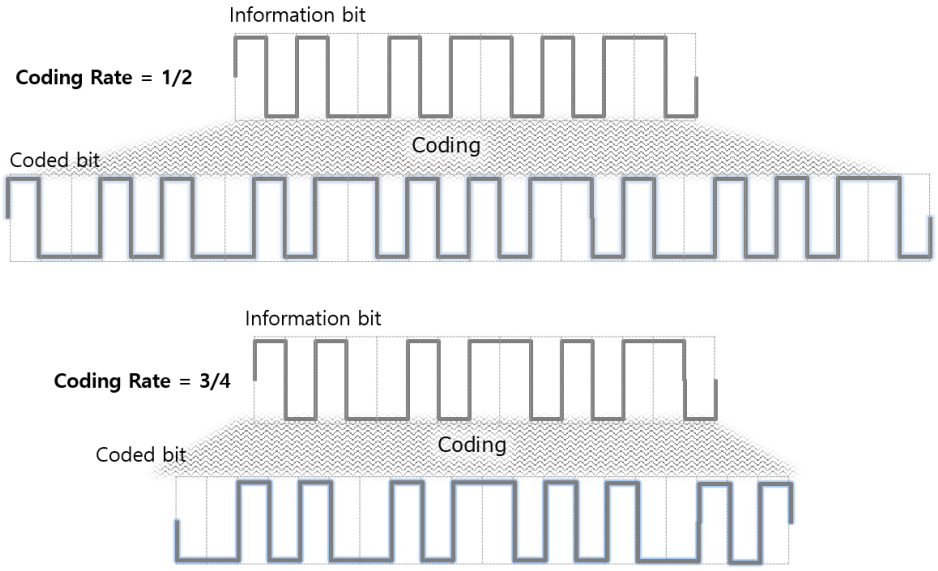
There are two types of coding, (1) Convolutional Coding (CC) and (2) Block Coding. The convolutional code is state-machine based, while block code is an algebraic approach. Regardless of type, it is known that FEC performance can be close to Shannon limit, if the iterative decoder can be applied as in Turbo Code or LDPC. In WLAN, BCC (Binary CC) has been mandatory coding method. In performance-wise, LDPC is known to be better than BCC, while its complexity is much higher. LDPC is widely used from 11ax as a mandatory feature.

Type	Item	Application	Feature
Convolutional (State Machine base)	**BCC** (1960')	**WLAN** (11a/g)	Simple and widely used coding method in communication Viterbi decoder
	Turbo (1993)	3G, 4G	Two parallel convolutional encoder (like Turbo Engine machine) Iterative decoder (close to Shannon limit)
Block Code (Algebra base)	Hamming (1950)	Computer memory	Simple. Detect up to 2 simultaneous bit error and can correct 1 bit
	Reed-Solomon (1960)	CD/MP3, Satellite, DVB	Widely used in digital storage and communication
	LDPC (1962/1996)	**WLAN(11n~)** 5G NR	Low density and complexity proportional to coding length Iterative decoder (close to Shannon limit)
	Polar (2009)	5G NR	When block code size is large in discrete memory-less channel, it can achieve Shannon capacity

Brief history on Error Coding in Communication System

Coding Rate

Coding rate is the ratio of the information bit and the coded bit. If 10 information bits are coded to 20 bit, coding rate is 1/2. Low coding rate like 1/2 has high error correcting performance, while it has high data rate drop.



$$Coding\ Rate = \frac{Information\_bit}{Coded\ bit}$$

*(generally) related to encoding/decoding **speed** and system **complexity***

*related to **data rate** and error correction **performance** (Low rate : high performance, high data rate drop)*

Coding and Coding Rate

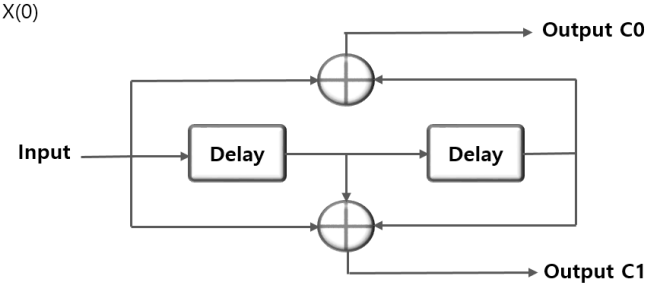
BCC

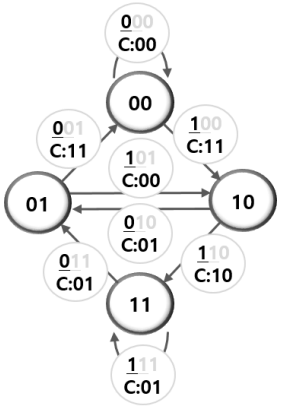
Simple example of BCC

In BCC, encoding is done with the previous bits along with the current one, which is called as a constraint field. With the encoder, state machine can be drawn where it can be found to which state to go with the received bit. In decoder, error can be corrected finding out the best way with the received bit.

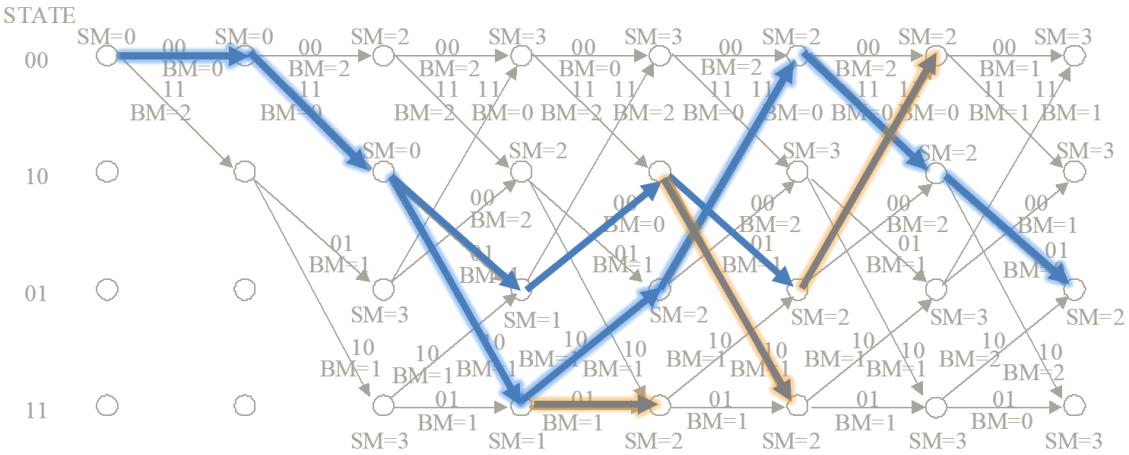
[BCC Example]
Coding Rate = 1/2
Constraint field = 3 : coding with (1) current, (2) previous and (3) previous-previous information

[Encoding]
C0 = X(-2) ⊕ X(0)
C1 = X(-2) ⊕ X(-1) ⊕ X(0)





[Decoding]
Viterbi algorithm

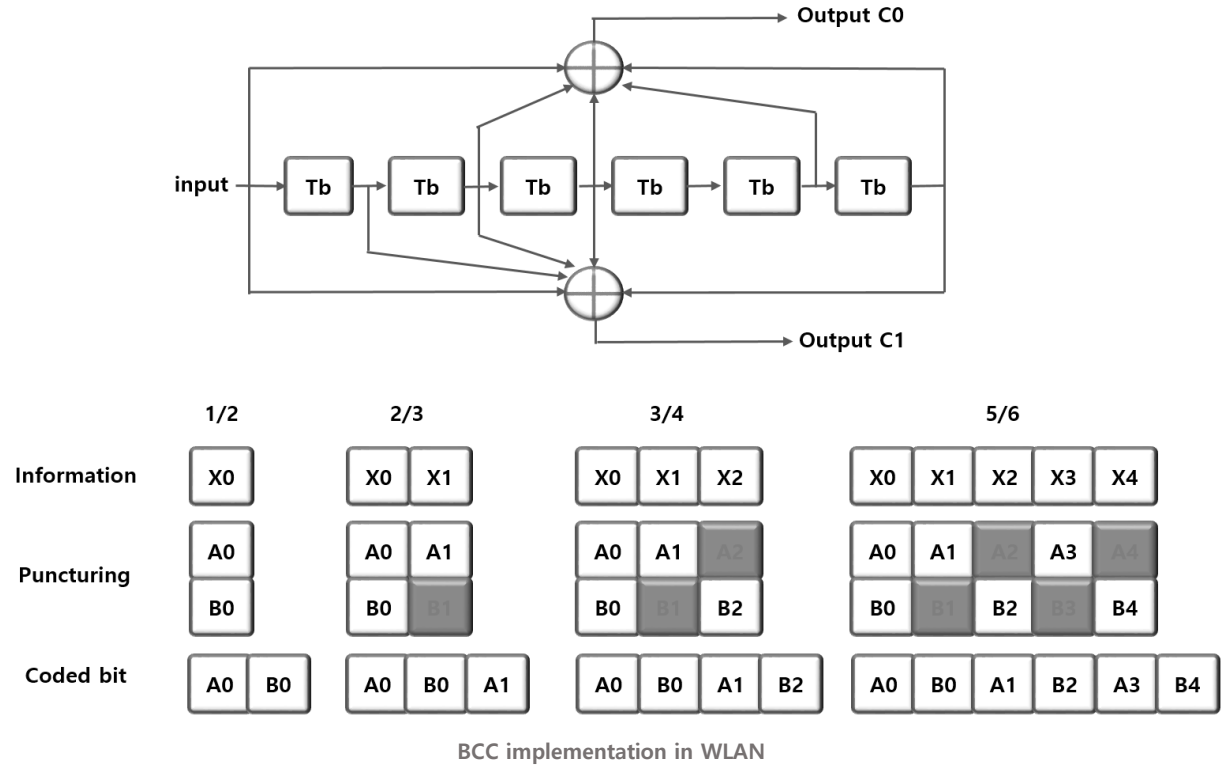


Received	00	11	11 (?)	00 (?)	11 (?)	11 (?)	01
Survived	00	11	10	10	11	11	01

BCC encoding/decoding example

BCC in WLAN

1/2 encoder with the constraint field of 7 is used in WLAN. WLAN uses 4 coding rate (1/2, 2/3, 3/4 and 5/6) and 1/2 encoder is used with puncturing to make lower coding rates.



BCC implementation in WLAN

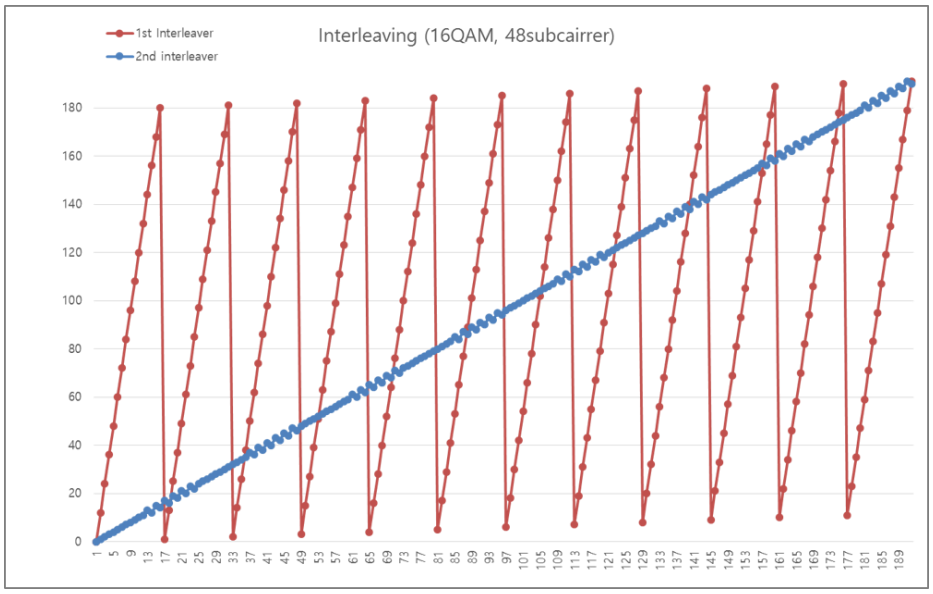
BCC Interleaver

Interleaver improves the performance applied along with BCC. In case of burst error, if the number of errors exceeds the error-correcting capability, it fails to recover the original code and interleaver distributes data mitigating it to create a more uniform distribution of error.

In WLAN, 2 stage interleaver follows BCC encoder.

- 1st permutation : adjacent coded bit to be mapped onto non-adjacent subcarriers
- 2nd permutation : adjacent coded bits to be mapped alternately onto less and more significant bit of the constellation.

Scrambler is different from interleaver. It is rather randomizer eliminating long sequence of '0' or '1' and eliminating concentration of power in a narrow frequency band.

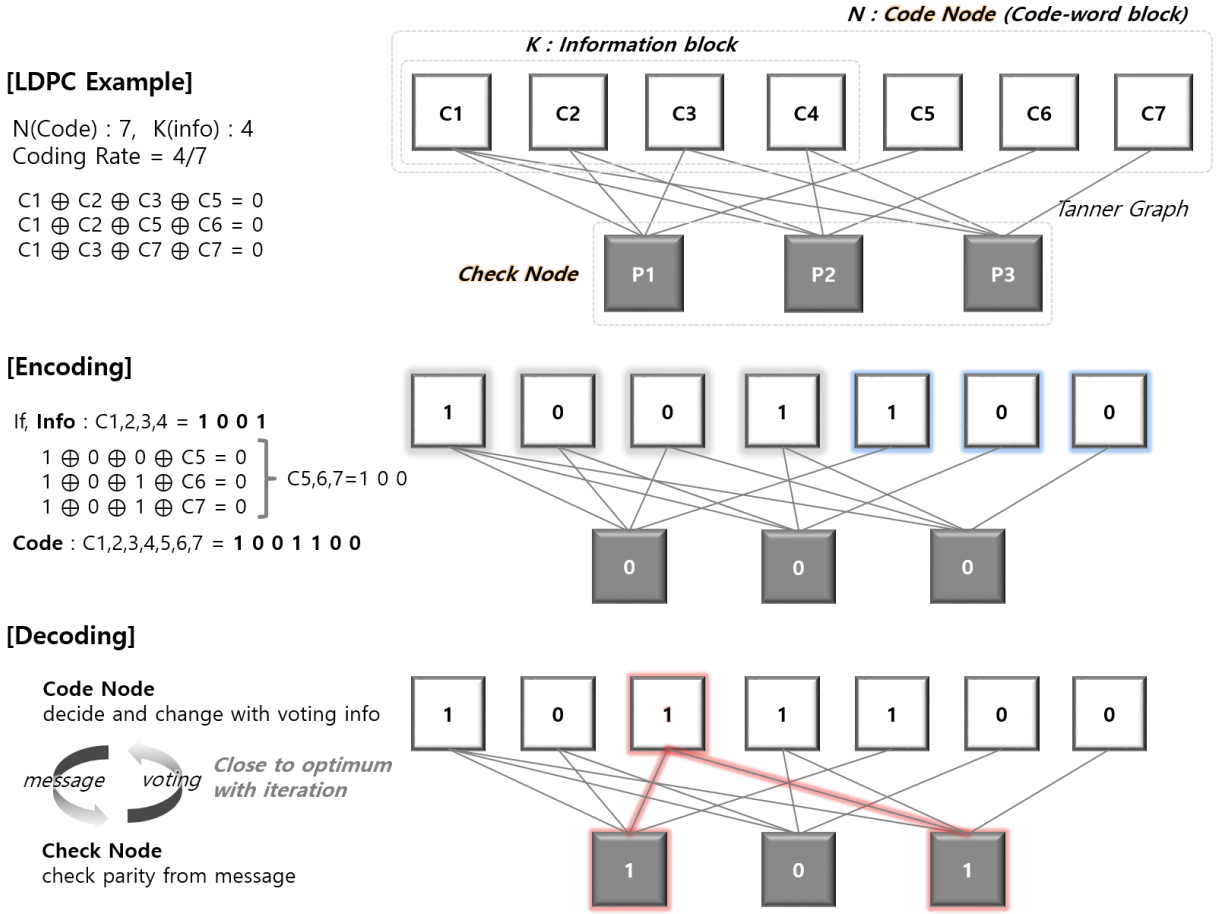


Interleaver with BCC in WLAN

LDPC

Simple example of LDPC

Codeword block is made with the combination of the information bits and other bits to make the defined checksum to be zero. For receiver to decode, Code node sends message and Check node checks parity and votes back. The process is iterated correcting error, until the output is optimal.

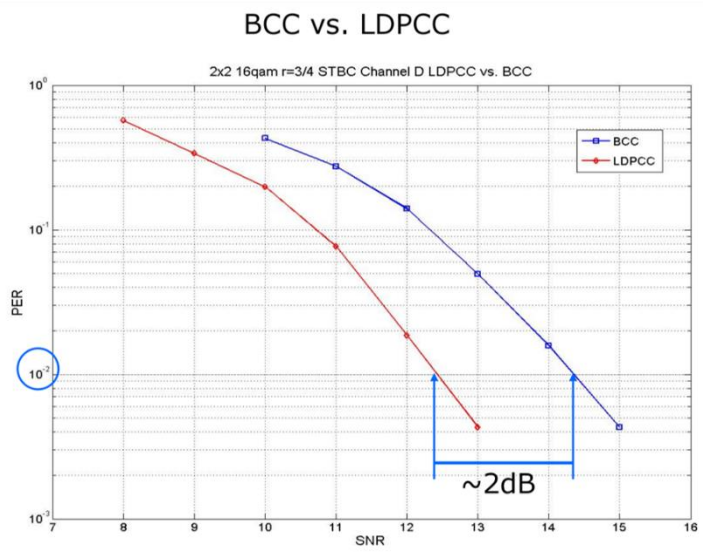


LDPC encoding/decoding example

LDPC Performance

This high performing block code is first introduced to WLAN in 11n. With its complexity, it has not been widely used, until it gets regularized from 11ax. In WLAN, 648, 1296, and 1944 codeword block length are used with coding rate of 1/2, 2/3, 3/4, 5/6.

Generally, the performance is known to be better than BCC by about 2~3dB. For example, if a station can receive the signal coded in BCC at the minimum level of -70dBm, it may decode LDPC waveform up to about -72dBm or -73dBm.



BCC vs. LDPC (Reference : https://kr.mathworks.com)

Data Rates

What consists of data rate?

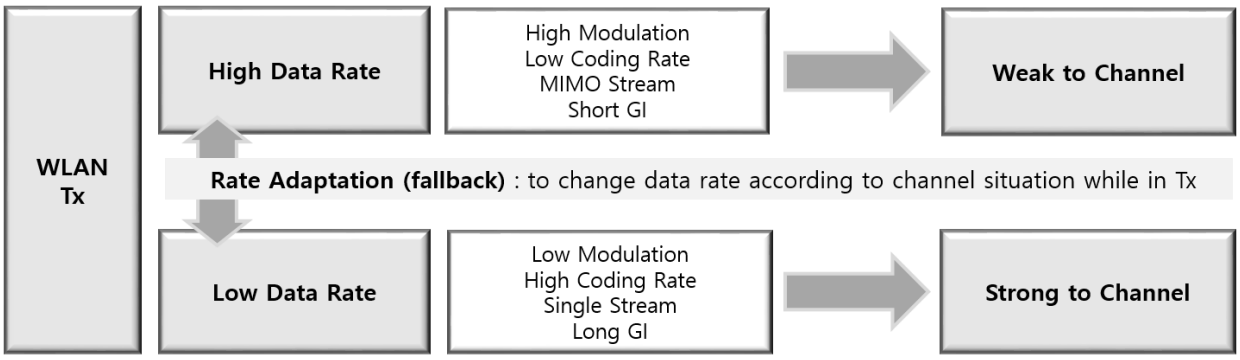
Modulation, coding rate, guard interval, bandwidth, and the number of MIMO stream are all the factors to consist of data rate in WLAN.

Data Rate	
Modulation	BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM, 4K QAM
Coding Rate	1/2, 3/4, 5/6
Guard Interval	Long GI, Short GI, Quadruple GI, Double GI, Normal GI
Bandwidth # of data sub-carrier	20MHz, 40MHz, 80MHz, 160MHz, 320MHz
MIMO Stream #	1SS ~ 8SS, 16SS

What consists of data rate in WLAN

Rate Adaptation

Transmitter decides in which data rate to send the data considering the channel situation and others. IEEE802.11 talks only about “multi-rate support”, while it does not specify rate adaptation algorithm. This decision is based on various factors like re-transmission, RSSI, etc., which is vendor-specific.



Rate Adaptation

Data Rate for HT and VHT

Sing stream case. Multiplying the number of MIMO stream with the values in the table will be MIMO data rate.

Modulation	C/R	11a/g	MCS	HT/VHT20		HT/VHT40		VHT80		VHT160, 80+80	
				800n GI	400n GI	800n	400n	800n	400n	800n	400n
BPSK	1/2	6	MCS0 (HT/VHT)	6.5	7.2	13.5	15.0	29.3	32.5	58.5	65.0
BPSK	3/4	9	-	-	-	-	-	-	-	-	-
QPSK	1/2	12	MCS1 (HT/VHT)	13.0	14.4	27.0	30.0	58.5	65.0	117.0	130.0
QPSK	3/4	18	MCS2 (HT/VHT)	19.5	21.7	40.5	45.0	87.8	97.5	175.5	195.0
16QAM	1/2	24	MCS3 (HT/VHT)	26.0	28.9	54.0	60.0	117.0	130.0	234.0	260.0
16QAM	3/4	36	MCS4 (HT/VHT)	39.0	43.3	81.0	90.0	175.5	195.0	351.0	390.0
64QAM	2/3	48	MCS5 (HT/VHT)	52.0	57.8	108.0	120.0	234.0	260.0	468.0	520.0
64QAM	3/4	54	MCS6 (HT/VHT)	58.0	65.0	121.5	135.0	263.3	292.5	526.5	585.0
64QAM	5/6	-	MCS7 (HT/VHT)	65.0	72.2	135.0	150.0	292.5	325.0	585.0	650.0
256QAM	3/4	-	MCS8 (VHT)	78.0	86.7	162.0	180.0	351.0	390.0	702.0	780.0
256QAM	5/6	-	MCS9 (VHT)	invalid	invalid	180.0	200.0	390.0	433.3	780.0	866.7

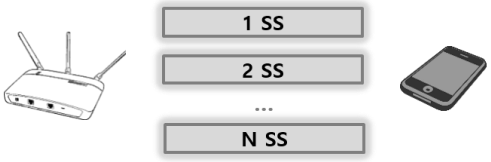
Invalid data rate in VHT
- MCS9 : 20MHz (1,2,4,5,7,8 SS), 80MHz (6 SS), 160MHz (3 SS)
- MCS6 : 80M (3,7 SS)

(Unit : Mbps) based on 1SS

Data Rate in WLAN (Legacy/HT/VHT)

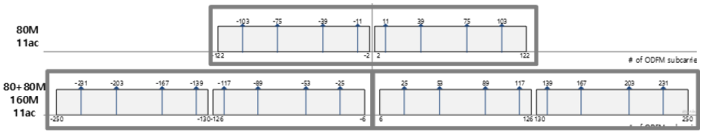
Data rate with MIMO, 160MHz BW and short GI

MIMO data rate
- (data rate of 1SS) X (# of SS)
- (ex) VHT80 MCS9 2SS (Short GI)
  : 866.7Mbps (=433.3 X 2)



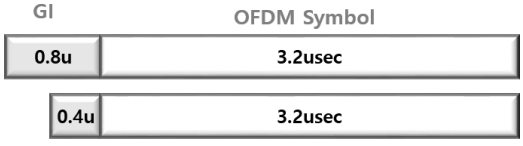
Data rate is doubled, tripled, ... according to SS

VHT160(80+80) data rate
- 2 times of VHT80 data Rate
- VHT160(80+80) 1SS= VHT80 2SS
- VHT160(80+80) is exactly double copy of VHT80



VHT160 1SS and VHT80 2SS have the same rate

Long GI vs. Short GI
- Data rate of Short GI is higher by 10%
- Symbol Duration : 3.6usec/4.0usec = 0.9

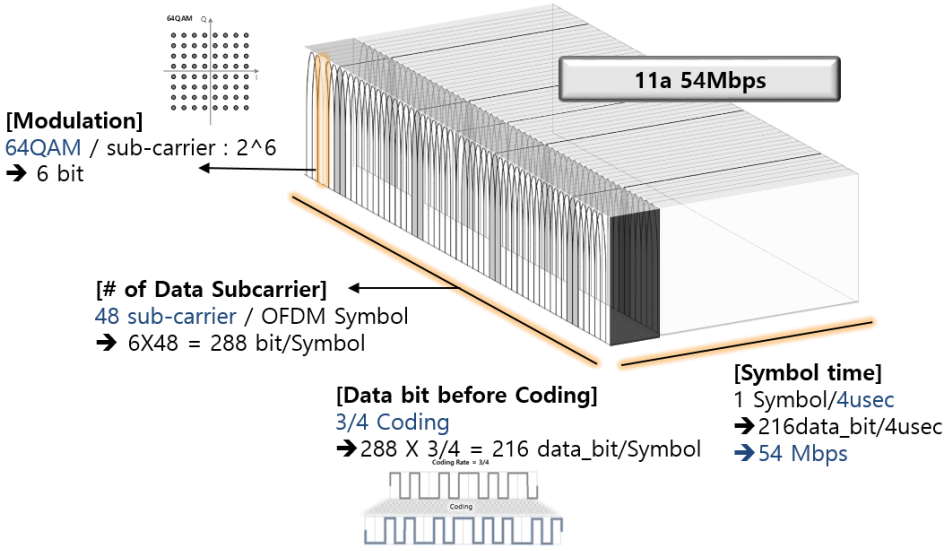


Short GI is faster than Long GI by 10%

Data Rate with MIMO, 160M and Short GI

Data Rate calculation example

With the modulation and coding rate information from MCS, data rate can be calculated, if the number of subcarrier and GI option are defined.

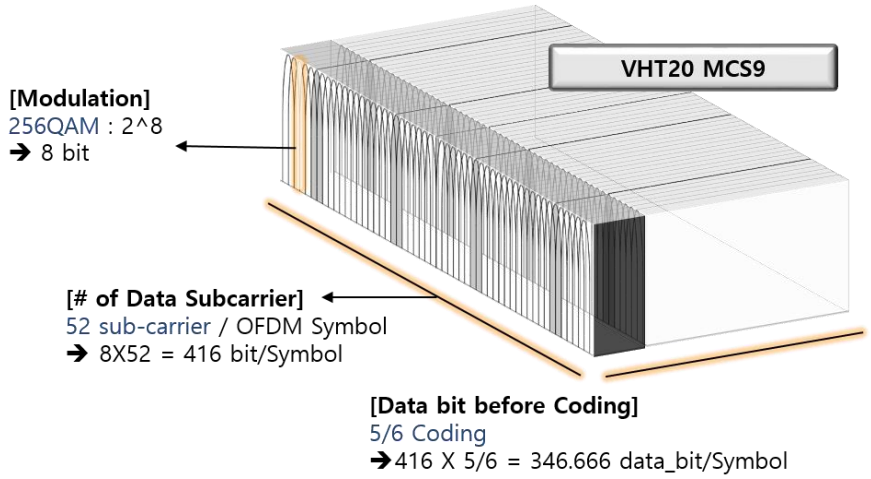


216 data bit is assigned to one symbol (6bit X 48 sub-carrier X 3/4) for one symbol time

Data Rates example : 54Mbps in 11a

Why there is No MCS9 in VHT20?

To make MCS9 in VHT20, 346.666 data bits are needed. There is no 0.666 bit.



346.666 data bit for VHT20 MCS9 one symbol. <u>There is no 0.666bit</u>!

Why there is no MCS9 in VHT20

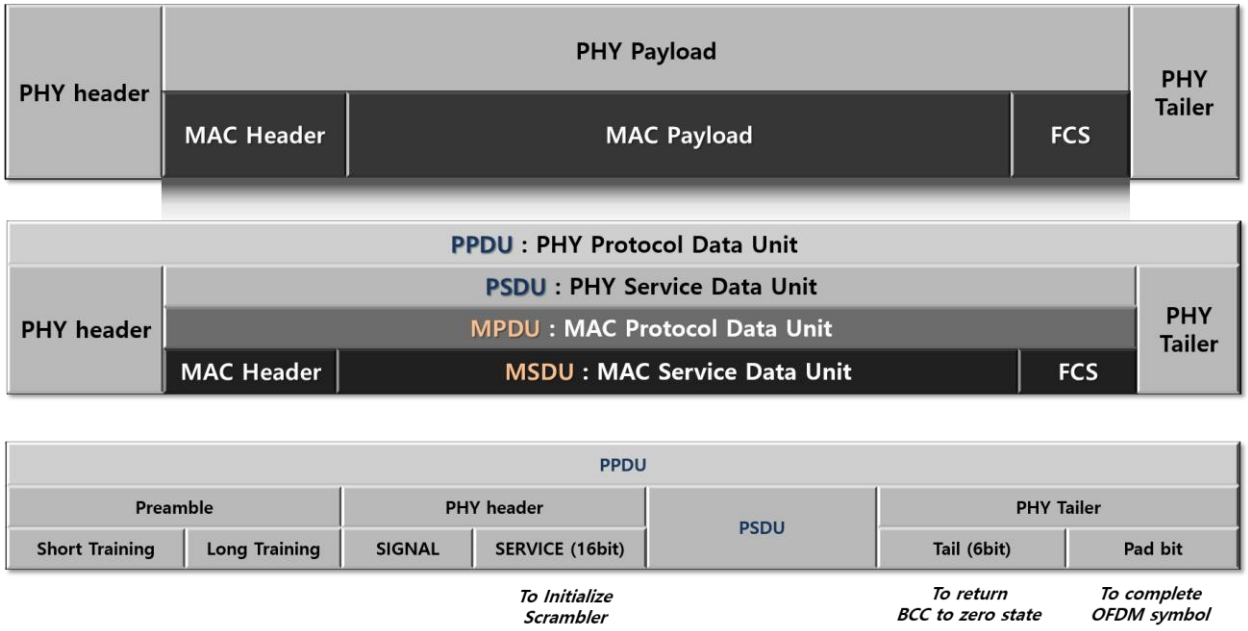
PHY Packet

PPDU and PSDU

To deliver payload (PSDU), PHY header and tailer are added in PHY packet (PPDU). PPDU and PHY frame is the official name of data exchanged between PHY entity in IEEE, while PHY frame is often called as PHY packet in this document.

Preamble and SIG (Signal) field are explained later of this chapter.

- SERVICE : Scrambler Initialization (7 bit) + Reserved (9 bit)
- Tail : Non scrambled zero bits are required to return the convolutional encoder to zero state
- Pad bits (PAD) : To fill data bit per OFDM symbol. Zero are appended and scrambled

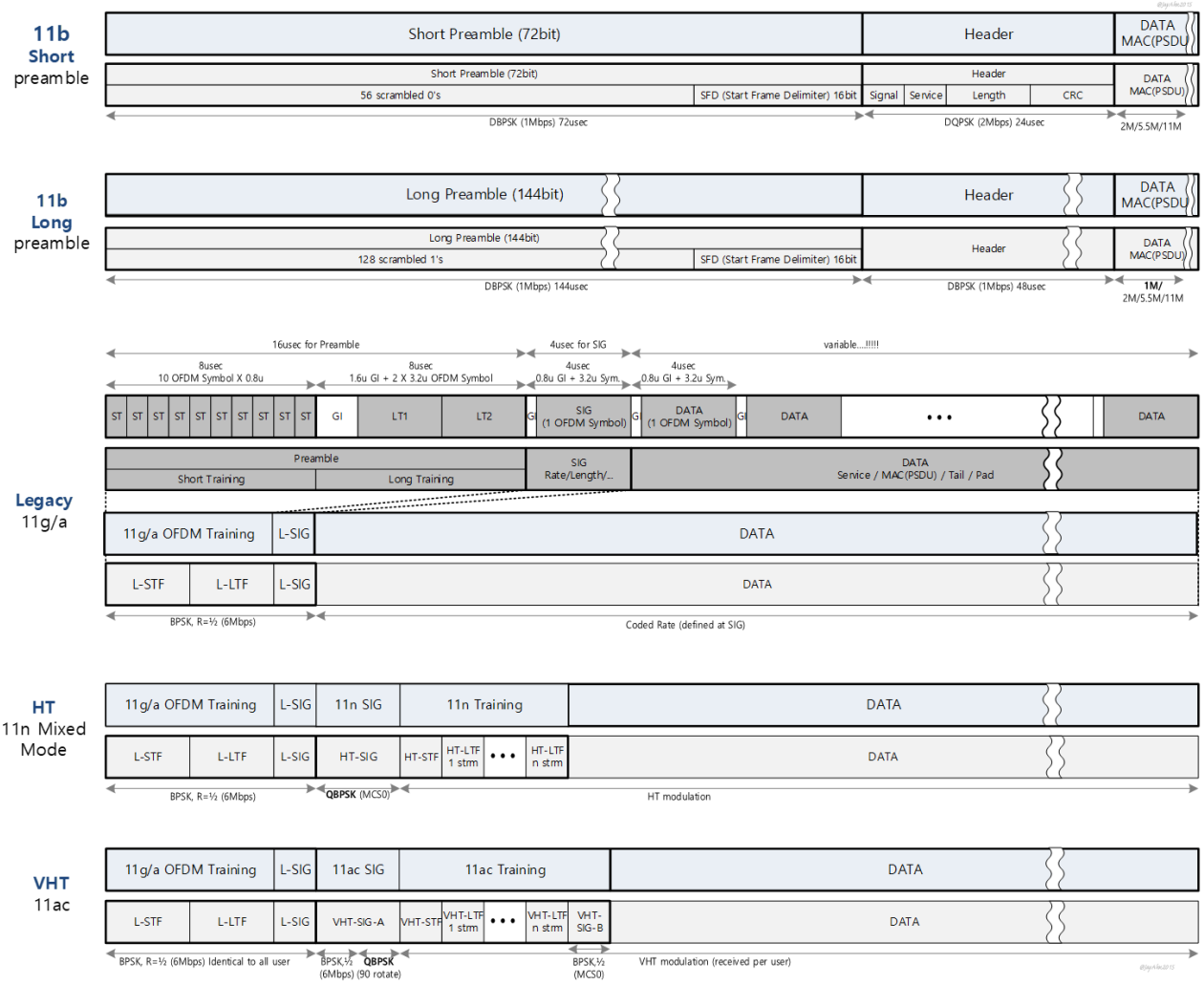


PHY Packet

PHY Packet

11b original preamble (Long preamble) takes too much time (144usec) and 11b introduced “Short Preamble” mode (half time), which supports 2Mbps, 5.5Mbps and 11Mbps, which does not support 1Mbps. OFDM has Short training field (STF) and Long training field (LTF), while 11b has short preamble or long preamble.

For backward compatibility, every OFDM PHY (11a/g/n/ac/ax) starts with Legacy (11a/g) preamble and SIG. SIG and Training fields of HT and VHT follows this legacy field.

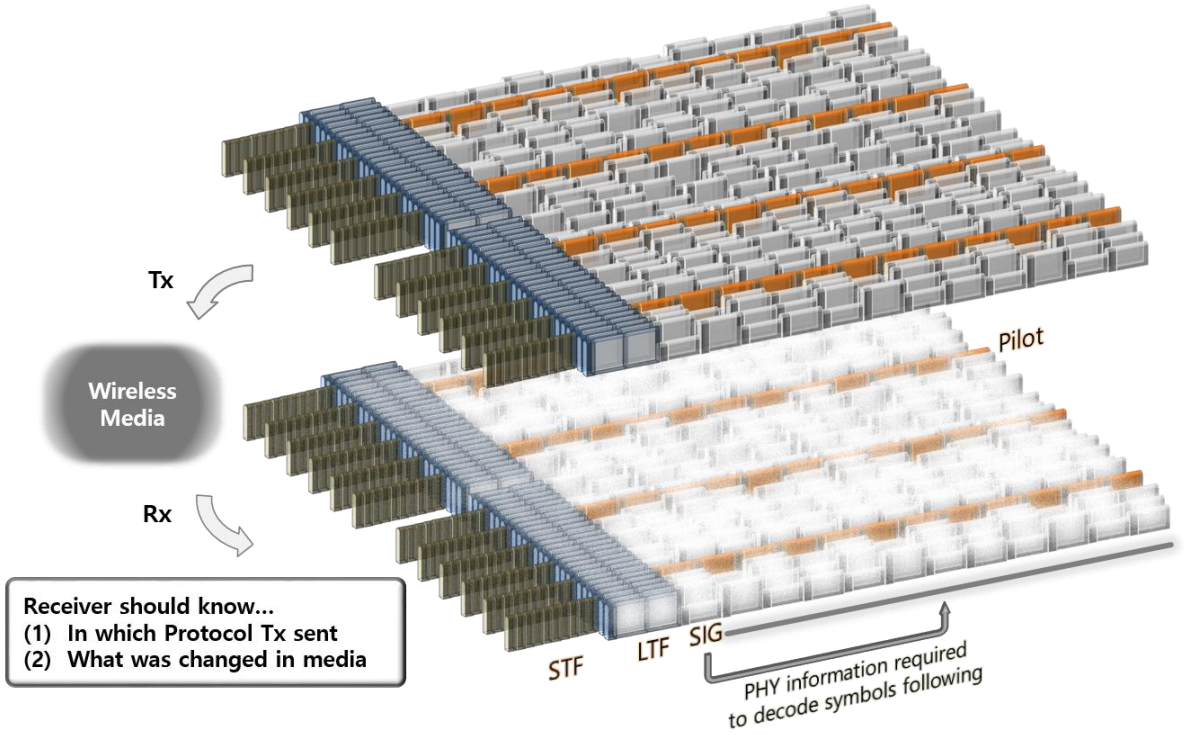


PHY Packet Structure

For Receiver to decode…

To decode the received packet, a receiver should have information on (1) with which physical protocol transmitter sent packet (2) what has been physically changed in wireless channel.

- SIG field has information on MCS, Length for decoder to interpret the packet
- Training (STF/LTF) field and Pilot subcarriers are physically pre-defined signal to estimate the change in wireless media

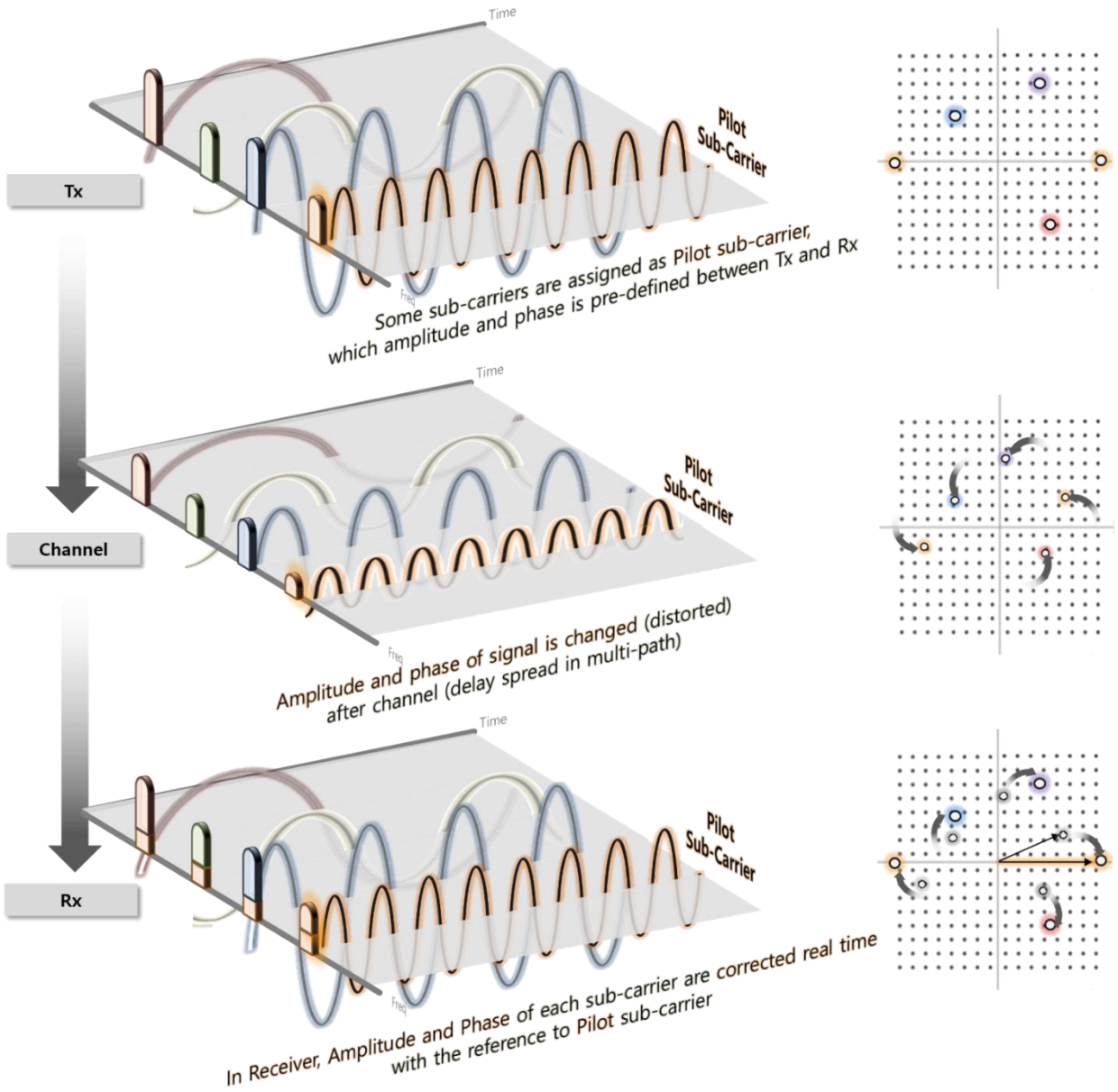


Field	Contents	For Rx to
SIGNAL	**[Protocol Information]** MCS, Length GI, BW, SS, STBC support, etc	**Decode & Interpret**
STF/LTF/Pilot	**[Physical Information]** Amplitude, Phase, Frequency, Timing	**Estimate & Correct**

Role of SIG, Training Field and Pilot

Pilot

One subcarrier can deliver up to 8 bit of information (256QAM in case of VHT) and a portion of subcarriers is assigned as Pilot subcarriers. This can be considered to be costly. (3~8% of subcarriers in OFDM are for Pilot) Every symbol experiences the change in amplitude and phase via fading channel and Pilot is used for the reference correcting the change.



Pilot in OFDM

Preamble and SIG in Legacy OFDM

SIG field has data rate and length information.

Field	Role	11a/g packet header
L-STF	AGC convergence, Coarse Frequency acquisition, Timing Sync	- 10 symbol of 0.8usec each - Utilizing 12 tones only. Every 4th tone
L-LTF	Channel Estimation, Fine Freq Acquisition	- 2 symbol of 3.2usec each
L-SIG	PSDU information on Data Rate, Length(Byte)	- Modulated : 6Mbps - Data Rate subfield (4b) : 6Mbps ~ 54Mbps - Length subfield (12b) : Byte in PSDU. Used by PHY to determine the # of byte transfers between MAC and PHY

OFDM Training and SIG field

Preamble and SIG in HT

L-SIG : Data rate and Length is described based on 6Mbps to spoof legacy device. STA not supporting HT can defer transmission for this period for CSMA/CA.

Field	Role	HT header
L-STF	AGC convergence, Coarse Frequency acquisition, Timing Sync	- HT20 : Same with 11a/g STF - HT40 : 90° rotation *(refer to Tone Rotation)*
L-LTF	Channel Estimation, Fine Freq Acquisition	- HT20 : Same with 11a/g LTF - HT40 : 90° rotation *(refer to Tone Rotation)*
L-SIG	Used to spoof legacy devices to defer transmission for a period	- Modulated : 6Mbps - Data Rate subfield : 6Mbps (L_DATARATE) - Length subfield: Byte in L-SIG data rate (6Mbps).
HT-SIG	PSDU information on MCS, BW, HT Length, Aggregation, STBC, Coding, Short GI, etc	- BPSK, ½, 90° rotation relative to L-SIG to accommodate detection of the start of HT-SIG - QBPSK (Quadrature BPSK),
HT-STF	To improve AGC estimation in MIMO system	- HT20 : same allocation with L-STF - HT40 : 90° rotation *(refer to Tone Rotation)*
HT-LTF (1~5)	for the receiver to estimate the MIMO channel between the set of QAM mapper outputs	- HT-LTF = HT-DLTF (data portion) + HT-ELTF (to sound Extra spatial dimension of MIMO chan. Optional) - # HT-LTF < 6 - HT-DLTF : 1,2 or 4 according to STBC and MIMO SS # - HT-ELTF : 0,1,2,or 4 according to extension MIMO SS #

HT Training and SIG field

Preamble and SIG in VHT

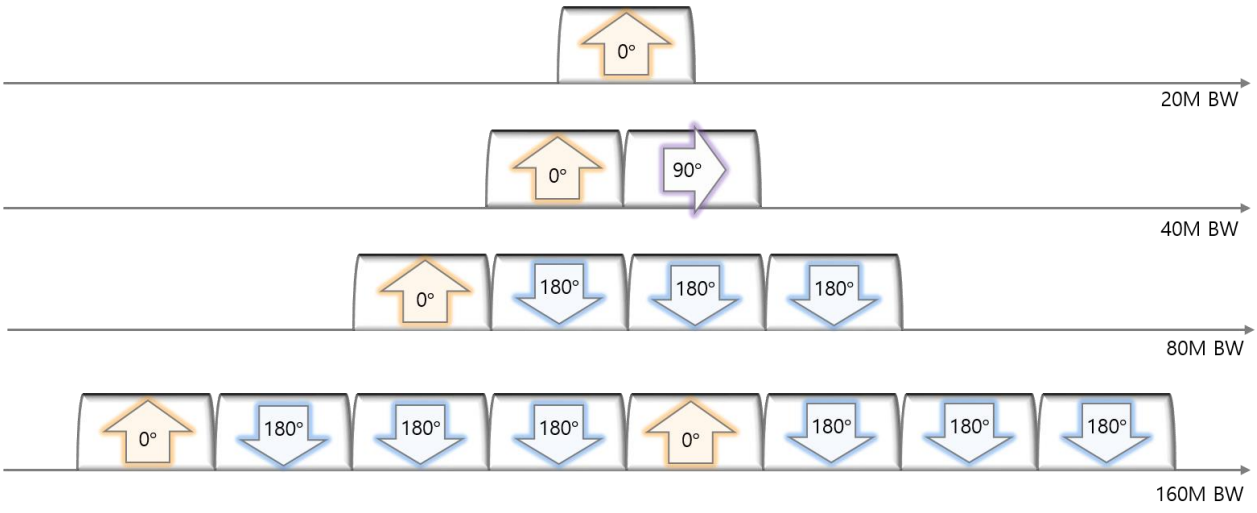
VHT-SIG-B : MU (MIMO) information per-user base

Field	Role	VHT header
L-STF	AGC convergence, Coarse Frequency acquisition, Timing Sync	- VHT20/40 : Same with HT20/40 - VHT80/160 : refer to Tone Rotation
L-LTF	Channel Estimation, Fine Freq Acquisition	- VHT20/40 : Same with HT20/40 LTF - VHT80/160 : refer to Tone Rotation
L-SIG	Used to spoof legacy devices to defer transmission for a period	- Modulated : 6Mbps - Data Rate subfield : 6Mbps - Length subfield: Byte in L-SIG data rate (6Mbps).
VHT-SIG-A	PSDU information on MCS, BW, HT Length, Aggregation, STBC, Coding, Short GI, etc (SU / MU-MIMO)	- Modulated in BPSK, ½ - Consists of VHT-SIG-A1 and VHT-SIG-A2 - VHT-SIG-A2 : 90° rotation relative to VHT-SIG-A1 (VHT-SIG-A1 phase same with L-SIG)
VHT-STF	To improve AGC estimation in MIMO / beamforming	- VHT20/40 : Same with HT20/40 - VHT80/160 : refer to Tone Rotation
VHT-LTF	Provides a means for receiver to estimate MIMO channel.	- VHT20/40 : Same with HT20/40 - VHT80/160 : refer to Tone Rotation
VHT-SIG-B	MCS (MU-MIMO) and Length	- Modulated in VHT MCS0 (BPSK, ½)

VHT Training and SIG field

Tone rotation in HT and VHT

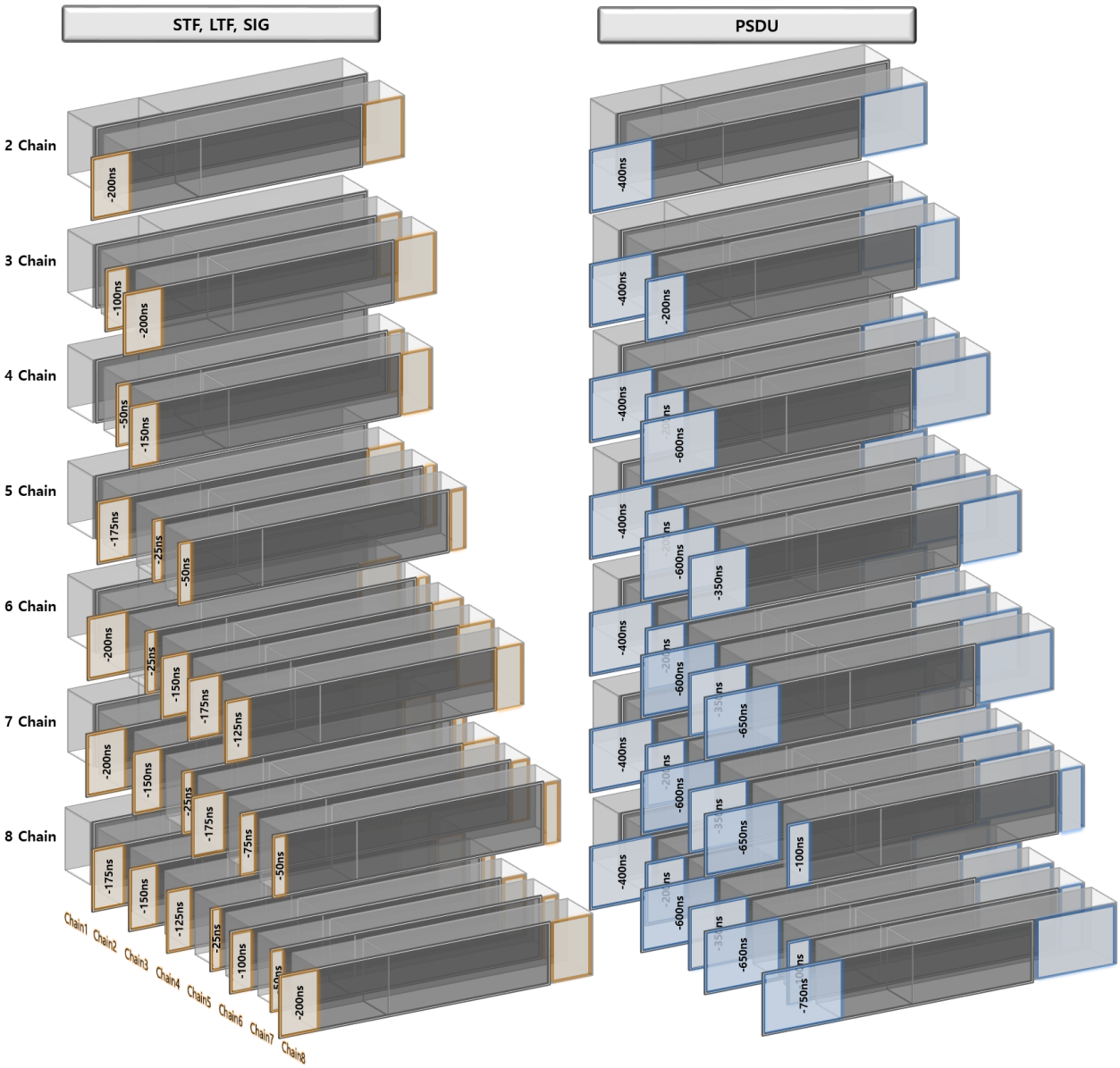
To reduce PAPR, HT/VHT40 and VHT80/160 have tone rotation by 20MHz. This is not applied in legacy portion (L-STF, L-LTF, L-SIG)



Tone Rotation in HT/VHT

CSD by Chain

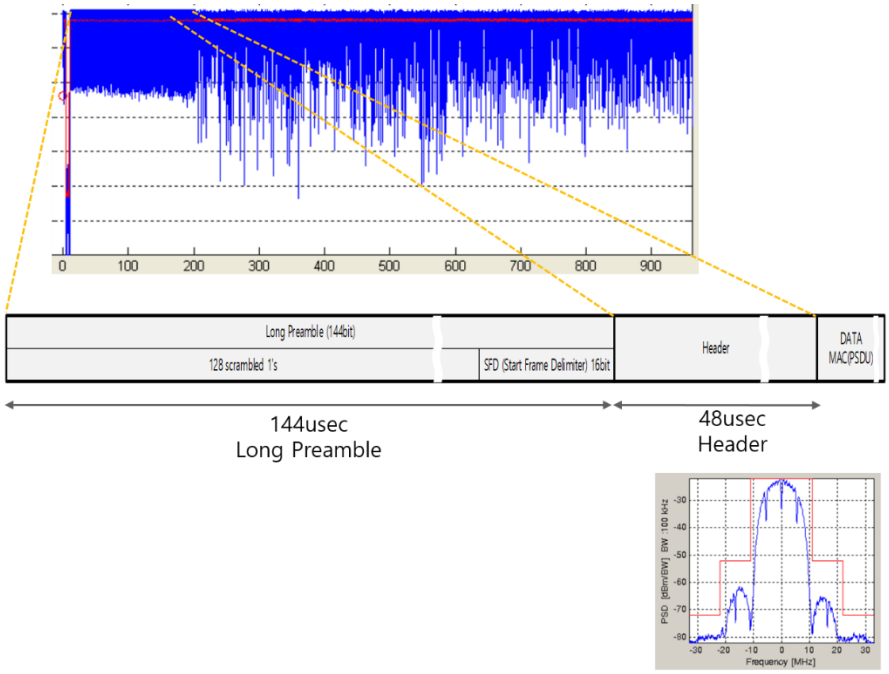
Delay value of each chain for CSD is as below. Find *Tx Diversity : CSD* for more information.



CSD by chain

The real 11b Packet measured

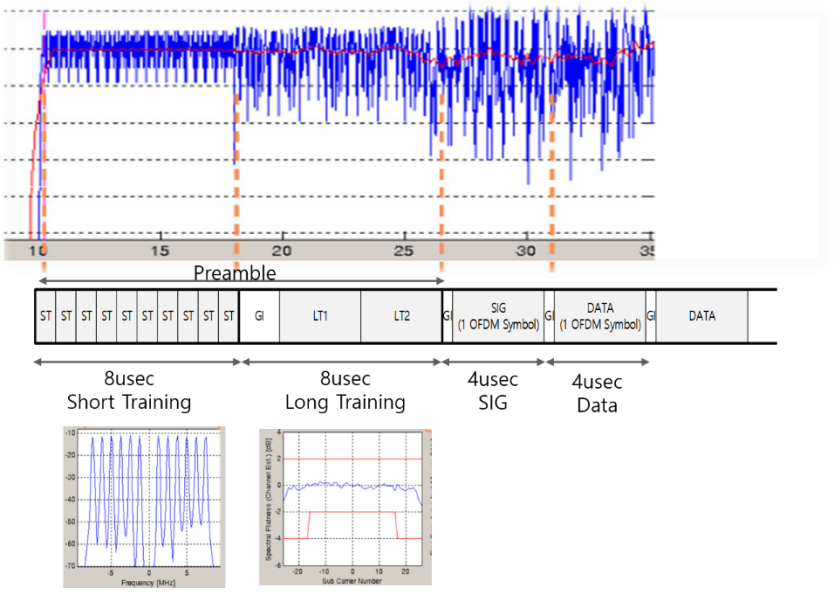
Waveform in time and frequency domain



11b Packet in real

The real OFDM Packet measured

Waveform in time and frequency domain



OFDM Packet in real

Simple Calculation on Packet Length

Legacy preamble and header takes 20 usec and HT/VHT 36 usec. Payload bit divided by data rate is packet length in time. (Padding is not Considered)

	Preamble	SIG/Header	Data	Packet Length for 1000Byte		
11b Long-preamble	144usec	48usec	ByteX8 / DataRate (Mbps)	1Mbps	192+8000/1	8192usec
11b Short-preamble	72usec	24usec	ByteX8 / DataRate (Mbps)	11Mbps	96+8000/11	823usec
11a/g	16usec	4usec	ByteX8 / DataRate (Mbps)	54Mbps	20+8000/54	168usec
HT	16usec	20usec	ByteX8 / DataRate (Mbps)	HT20 MCS7 L-GI	36+8000/65	159usec
VHT	16usec	20usec	ByteX8 / DataRate (Mbps)	VHT80 MCS9 S-GI	36+8000/433	54usec

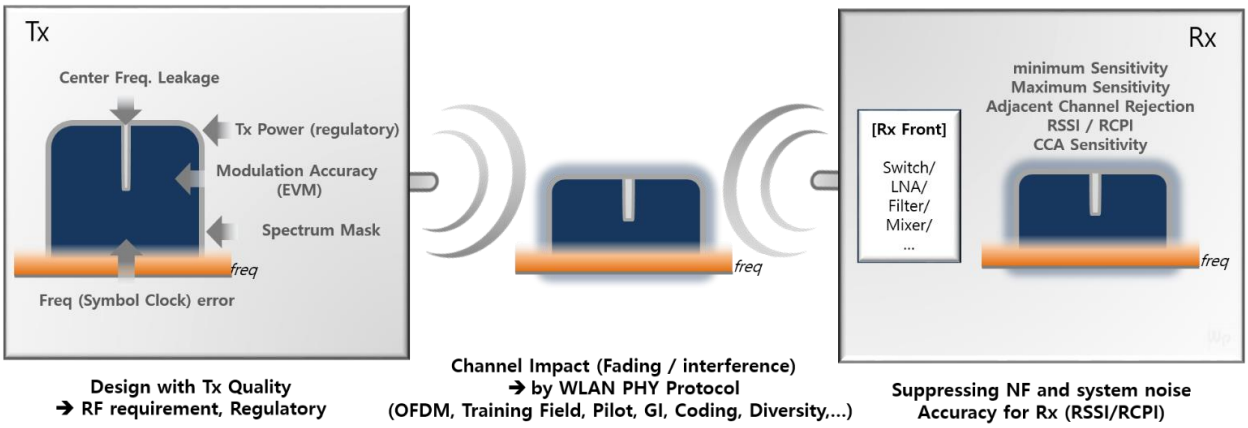
PHY Packet Length (Simple Calculation)

RF

RF requirement on Transmitter and Receiver

Reducing the change and the impact from channel is a job by WLAN PHY protocol, mostly. IEEE defines minimum requirements on transmitter and receiver side and the regulatory domains have its own requirement for regulating frequency usage.

- Tx requirement : transmit power, modulation accuracy (EVM), spectral mask, frequency and symbol error, center frequency leakage
- Rx requirement : minimum and maximum sensitivity, adjacent channel rejection, RSSI/RCPI, CCA sensitivity.



RF requirement in WLAN overview

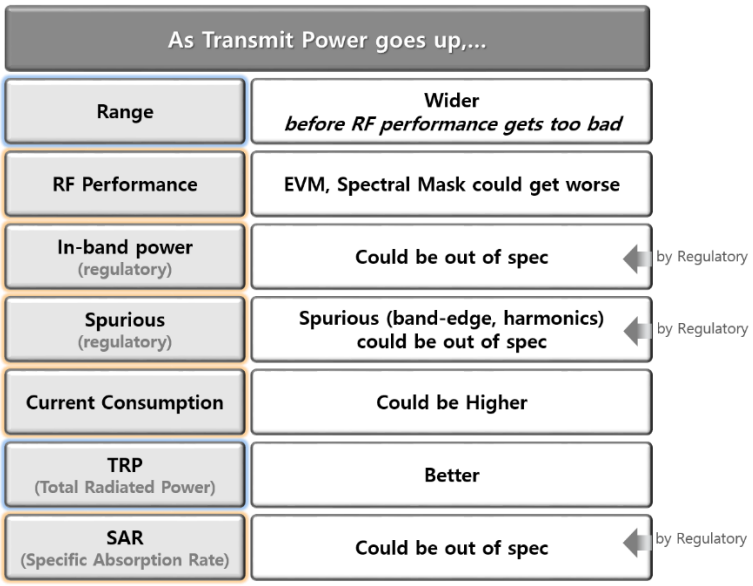
Not only just mentioning the meaning and the criteria of IEEE requirement, this chapter tries to explain the fundamentals and some basic knowledge of WLAN RF and the causes and basic solutions for some situations.

Power

Transmit Power

Transmit power is the most important factor in transmitter's performance, even if IEEE802.11 describes little.

With the change of transmit power, many related factors change accordingly. As the power goes high, Wi-Fi coverage and TRP go high, while some performance like EVM and spectral mask are affected. Regulatory requirement (in-band, out-band spurious, SAR) also need to be considered. Generally power level in Wi-Fi devices before antenna is between 15dBm and 20dBm and the values are defined by data rate. The transmit power level depends on end-customer's requirement, as far as it meets other WLAN RF requirement and regulatory requirement. For transmit power accuracy, power may have to be calibrated depending on HW situation and the requirement from vendors or end-customers.



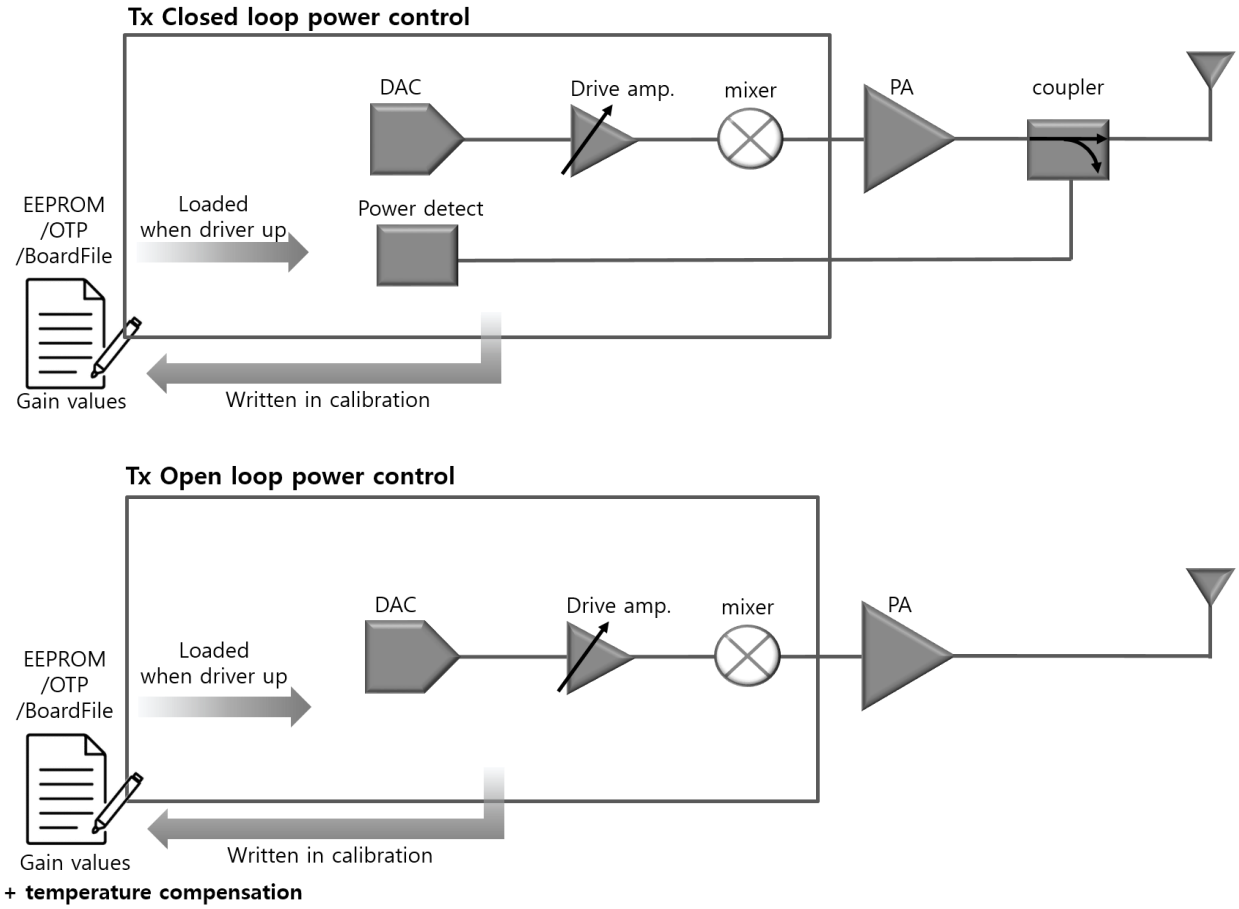
Effects on Transmit Power

Transmit Power Control (TPC)

Generally, WLAN does not perform power control considering the distance between stations. Every data rate (MCS and MIMO) has its own gain information or target power. They are saved somewhere in WLAN product (EEPROM, OTP, board file, etc) and loaded when WLAN driver is up. In some cases, Tx power are backed off (reducing power) to meet regulatory and the conditions and values are also saved along with target power values.

WLAN devices runs power control to push the designated amount of value (target power) and for this purpose, the closed loop power control and the open loop power control are open used. Closed loop power control system has the coupler at output of PA and the feedback values are used for controlling power. It can cope with the changes outside, while open loop power control cannot using pre-defined gain values. One

of the condition for this changes is the temperature and many open loop power control system manages offset values for the temperature change. The drawback of closed loop system can be seen, when there is a sudden change in the system like device gripping situation.



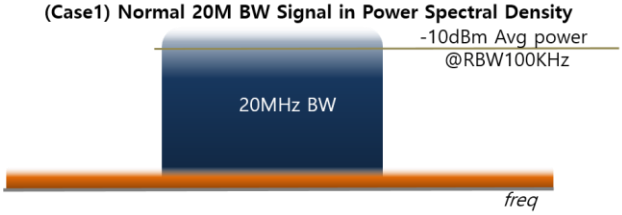
Tx Power control (TPC)

How to read power in spectrum

Waveform (Spectrum) in frequency domain is mostly Power Spectral Density (PSD) and the power in spectrum needs to be approached by the power density concept. If 20MHz BW signal has 10dBm in one portion (10MHz) and 10dBm in another portion (10MHz), the total power is 13dBm (10dBm + 10dBm)

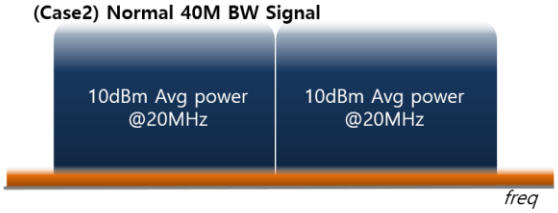
In frequency domain, a signal is expressed by unit of a narrow bandwidth (resolution), which is called as Resolution Bandwidth (RBW). Originally, RBW concept came from the analog spectrum analyzer which is the frequency span of filter for input signal. In WLAN, RBW is 100KHz mostly used setting and level in spectrum reads the value by 100KHz.

(Case1) Normal 20M BW Signal in Power Spectral Density



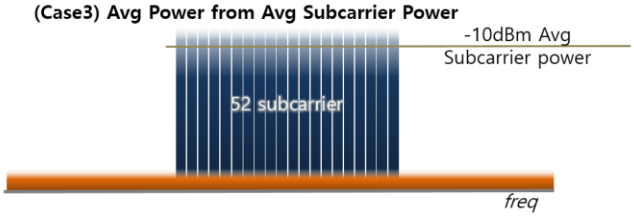
Avg Signal Power (20MHz)
= -10dBm/100KHz X 20MHz
= -10dBm X 200
= -10dBm + 10Xlog(200)dB
= -10dBm + 23dB
= 13dBm

(Case2) Normal 40M BW Signal



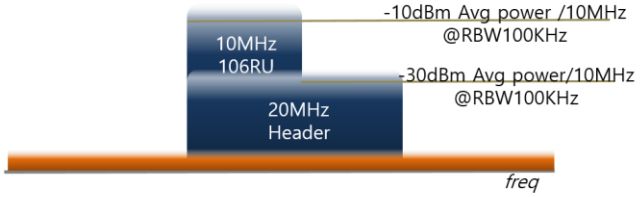
Avg Signal Power (40MHz)
= 10dBm X 2
= 10dBm X 10log(2)dB
= 10dBm + 3dB
= 13dBm

(Case3) Avg Power from Avg Subcarrier Power



Avg Signal Power (20MHz)
= -10dBm X 52
= -10dBm + 10Xlog(52)dB
= -10dBm + 17dB
= 7dBm

(Case4) HE20 106RU OFDMA MU



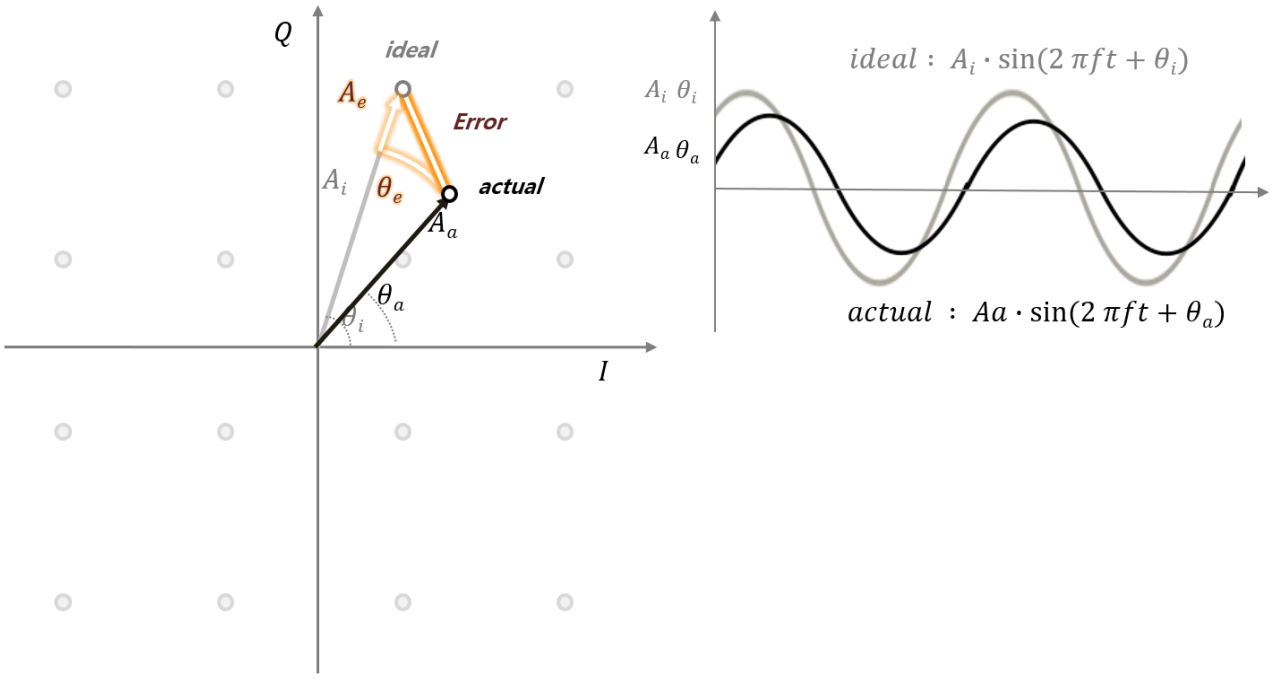
Avg Signal Power (20MHz)
= -10dBm/100KHz X 10MHz + -30dBm/100KHz X 10MHz
= -10dBmX100 + -30dBmX100
= -10dBm+10Xlog(100) + -30dBm+10Xlog(100)
= 10dBm + -10dBm
= 10mW + 0.1mW
= 10.1mW
= 10.043dBm ≈ 10dBm

How to read Signal Power in Spectrum

EVM

Tx Accuracy and Error

A sinusoidal signal can be expressed with an amplitude and a phase and it can have error in the amplitude and/or the phase, which is EVM (Error Vector Magnitude). It represents Tx accuracy and is graphically expressed in constellation with in-phase (I) and quadruple (Q) channel. More information can be found in *Modulation and Constellation*.



Tx Accuracy and EVM

IEEE EVM requirement

The table below is IEEE EVM requirements. 11ax TB PPDU has minimum and maximum power range, as it is under power control from AP and it has a different EVM requirement in case that Tx power is over or the case that it is under the maximum power of MCS7.

Data Rate				EVM (dB)						
Modulation	C/R	11a/g	MCS	11a/g	BW20 HT/VHT/HE	BW40 HT/VHT/HE	BW80 VHT/HE	BW160 VHT/HE	HE TB PPDU >MCS7 PWR	HE TB PPDU < MCS7 PWR
BPSK	1/2	6	MCS0	-5					-13	-27
BPSK	3/4	9	-	-8						
QPSK	1/2	12	MCS1	-10						
QPSK	3/4	18	MCS2	-13						
16QAM	1/2	24	MCS3	-16						
16QAM	3/4	36	MCS4	-19						
64QAM	2/3	48	MCS5	-22						
64QAM	3/4	54	MCS6	-25						
64QAM	5/6	-	MCS7	-27						
256QAM	3/4	-	MCS8 (VHT)	-30						
256QAM	5/6	-	MCS9 (VHT)	-32						
1024QAM	3/4	-	MCS10 (HE)	-35 (-32, amplitude tracking off)						
1024QAM	5/6	-	MCS11 (HE)	-35 (-32, amplitude tracking off)						

11b (DSSS/CCK) : 35% peak

Packet shall be 16OFDM symbol at least and 20 frames at least

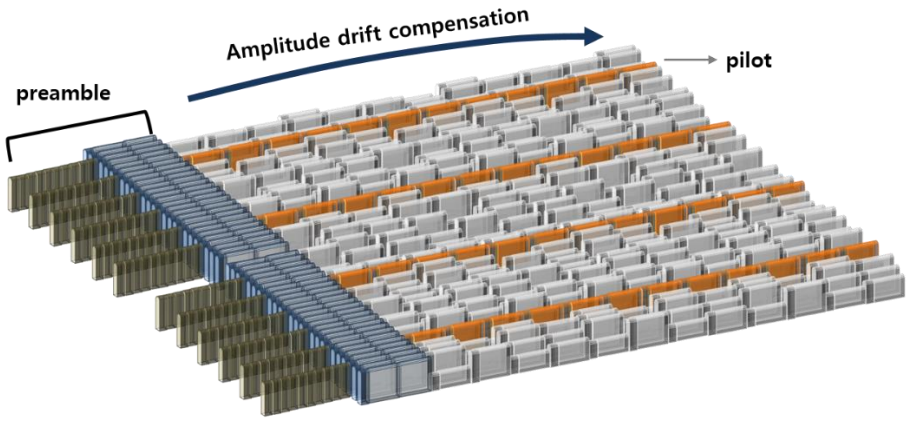
IEEE802.11 Tx requirement : EVM

EVM measurement

WLAN receiver makes use of preambles (STF, LTF) and pilot subcarriers of OFDM frame for the frequency, the amplitude and the phase correction in decoding. For more information, please find *For Receiver to decode…*. Instead of measuring the raw signal from device, EVM tester is also required by IEEE to correct the error in the frequency, the phase and the amplitude using preamble and pilot like the receiver of the real world devices.

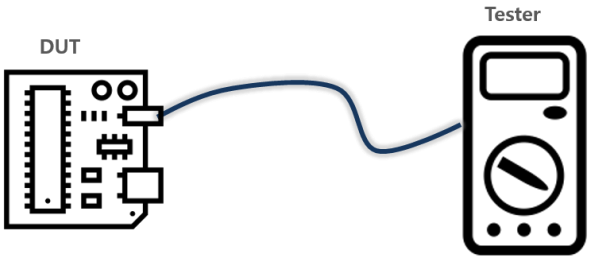
As WLAN packet length gets longer with an aggregation (A-MPDU) and PA degrades easily with this long transmission, WLAN receiver can track the amplitude along with the whole packet and IEEE standard introduced the amplitude drift compensation (amplitude tracking) for the optional test setup for 1024QAM. EVM requirement is different enabling or disabling this feature in the tester.

Channel estimation is supposed to be done in preamble (LTF), while many WLAN testers have the capability to track (previous) data signals which is called as Full Packet Channel Estimation or Data Estimation (contrary to preamble estimation). As it is not specified in IEEE standard and the performance differs from tester performance, I recommend not to enable it for mutual understanding and analysis of the test result.



- Frequency, Phase, Amplitude correction/estimation with preamble/pilot : IEEE required
- Amplitude drift compensation : IEEE optional
- Data tracking/estimation : tester vendor optional

EVM measured by a tester is EVM of DUT (Device under Test) with tester's EVM floor. If tester's EVM floor is relatively high compared to the EVM of DUT, the accuracy of measured EVM value may get worse. As EVM floor of the tester and DUT may not be correlated, the values in the table will be regarded as the worst case.



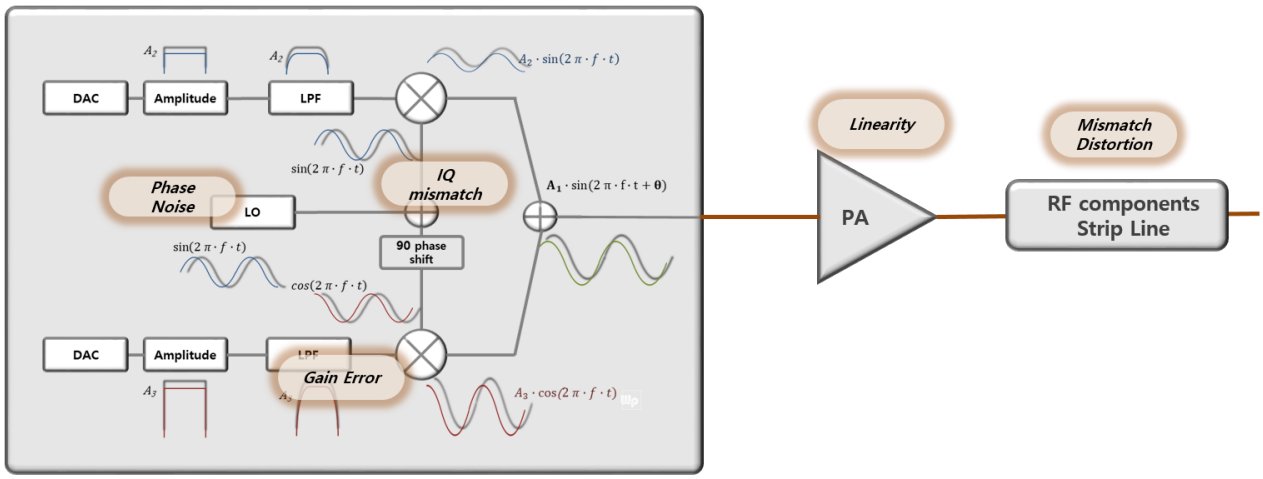
$$\mathrm{EVM}_{measure} = \sqrt{\mathrm{EVM}_{DUT}^2 + \mathrm{EVM}_{tester}^2}$$

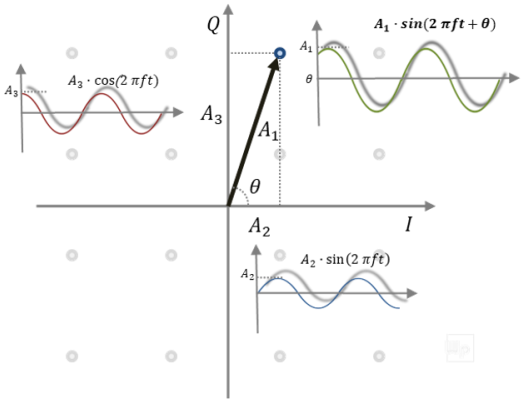
	EVM_{TESTER}	EVM_{DUT}	$\mathrm{EVM}_{Measure}$	Error
Case 1	-40 dB	**-30 dB**	**-29.59 dB**	0.41 dB
Case 2	-40 dB	**-34 dB**	**-33.01 dB**	0.99 dB
Case 3	-40 dB	**-38 dB**	**-35.88 dB**	2.12 dB

Tester EVM floor impacts on DUT's EVM performance

Where is the error from

- Inside chipset : phase noise of LO, IQ gain and phase mismatch, Gain imbalance
- Inside board : PA linearity and compression, RF mismatch





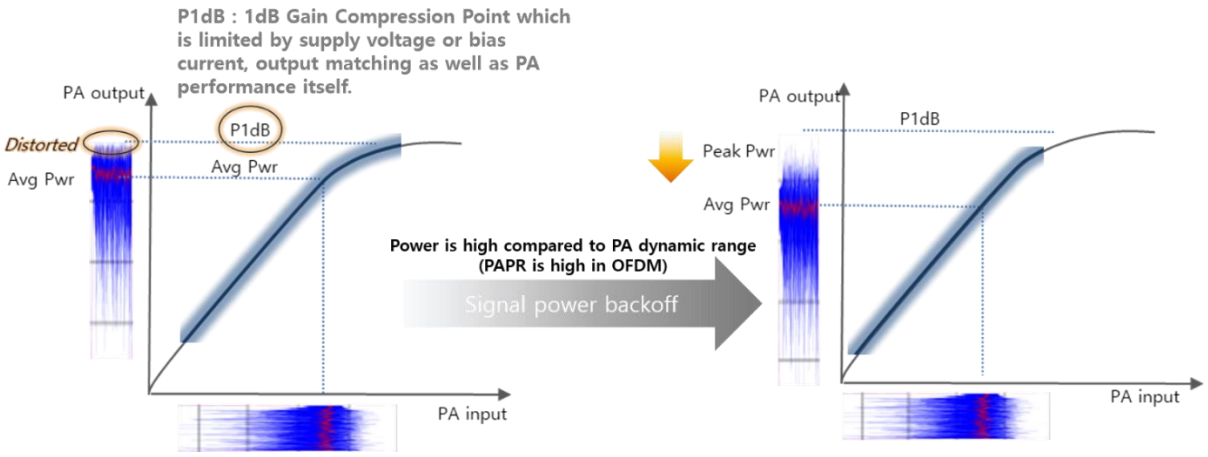
Effects on EVM performance in WLAN System

EVM and PA

EVM can be improved by correct IQ phase and amplitude matching (IQ calibration), frequency correction and reducing the phase noise especially from LO. As high impact is from PA's linearity and compression, let's take a close look at it.

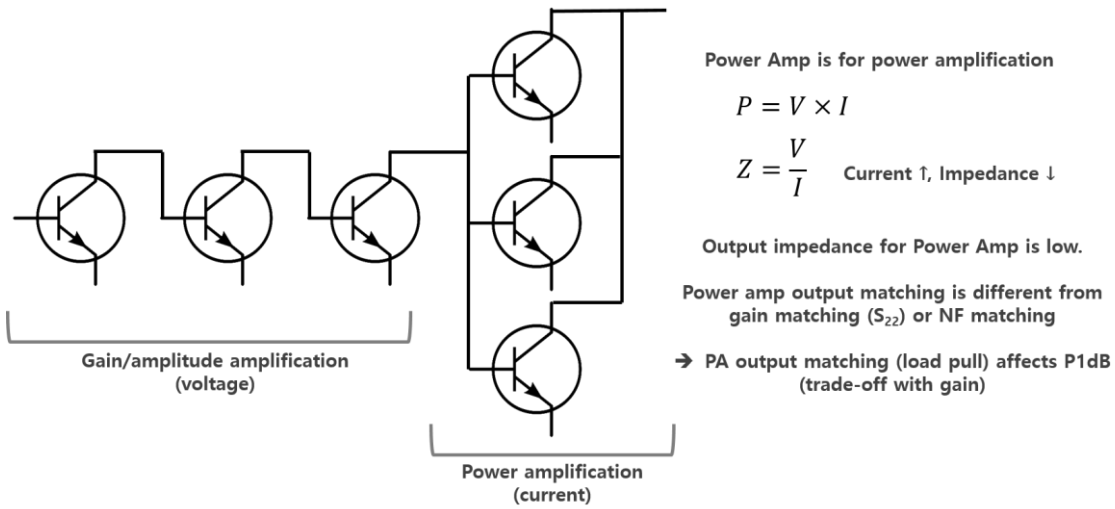
High PAPR and power back-off

High PAPR of OFDM makes signal vulnerable to distortion, when the target power is set high, the peak portion of signal can be easily around or over P1dB (high limit of linearity) of amplifier. You can see this situation with the change of EVM with power back off. (Setting target power low)



Power amplifier and output matching

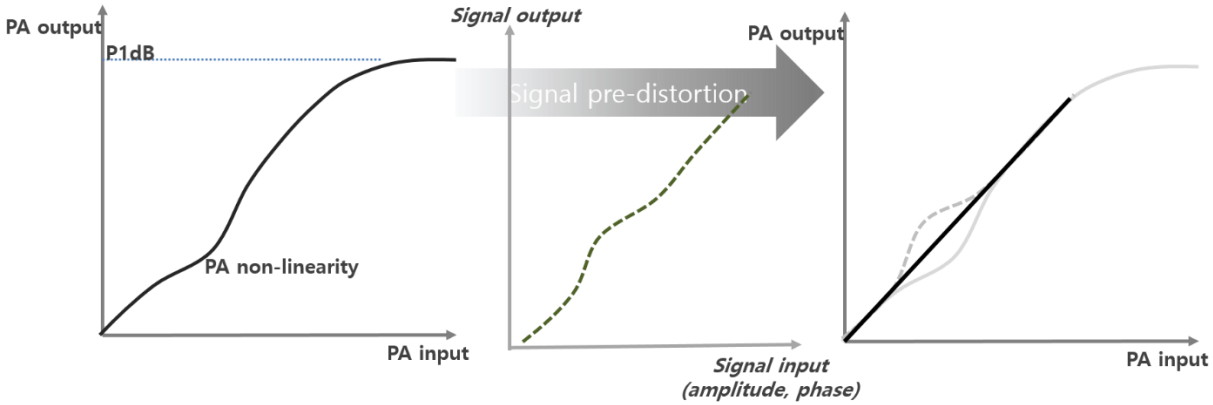
Proper PA output matching can secure wider dynamic range. Different from normal gain amplifier, power (current) amplifier has low output impedance. Output matching point is different by gain matching, noise figure matching and power matching and the method like load pull test is run for PA matching.

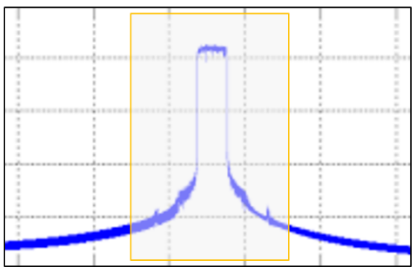


Pre-distortion

Unlike a gain amplifier, high current/power amplifier can be non-linear even in dynamic range below P1dB. Various techniques are applied like feedforward, pre-distortion and post-distortion. When pre-distortion is implemented in baseband, it is called as digital pre-distortion (DPD), which is widely used in WLAN solutions.

Considering the non-linearity of amplifier (discussed in the following chapter, Spectral mask), all the side lobes are the signal itself (even if it is distorted) and to analyze or calibrate the signal (amplitude and phase) for DPD, 3 or 5 times of signal bandwidth needs to be sampled.





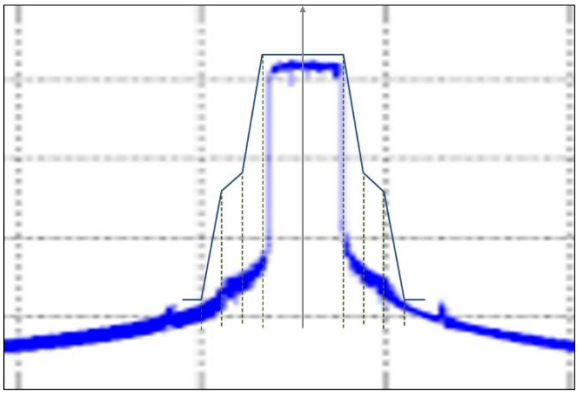
When pre-distortion is done in modem : DPD (digital pre-distortion)

In DPD, signal of 3 or 5time wider bandwidth needs to be sampled for calculation

Spectral mask

Spectral Mask

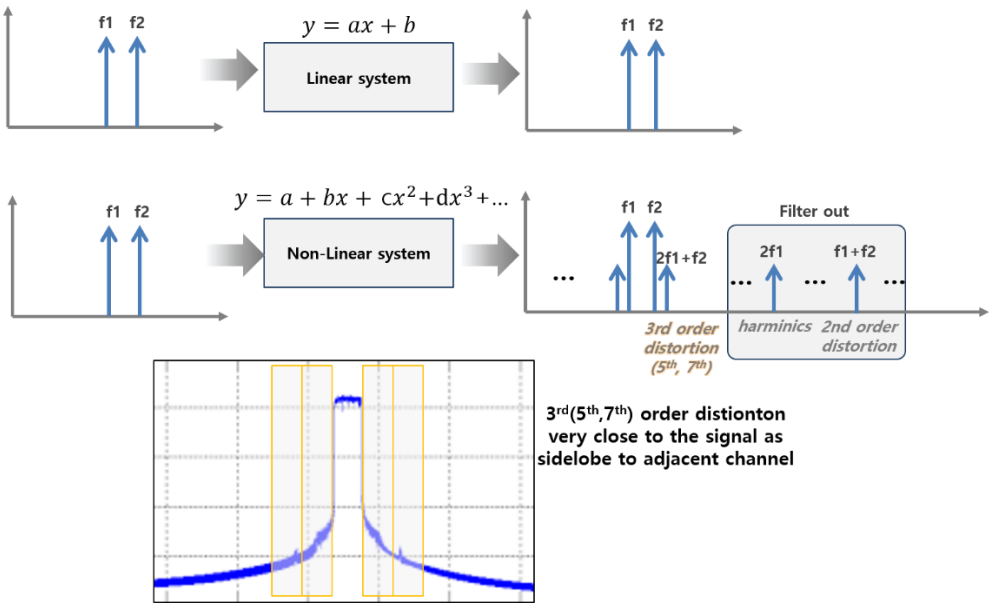
Spectral mask requirement is to see if the transmitted signal intrudes the adjacent channel affecting the other users. It has something to do with ACPR (adjacent channel power ratio) or ACLR (adjacent channel leakage ratio) which concept is used in other communication systems. Just to check the mask to meet IEEE requirement is one thing. However, the signal shape in frequency domain tells us a lot of information on transmitter's performance like PA linearity, LO phase noise and improving mask is closely related to the overall Tx signal quality.



Spectral mask requirement is for ACLR (adjacent channel leakage ratio) in WLAN,
,while it also gives much information on Tx signal quality from spectral domain (PA linearity, LO phase noise, etc)

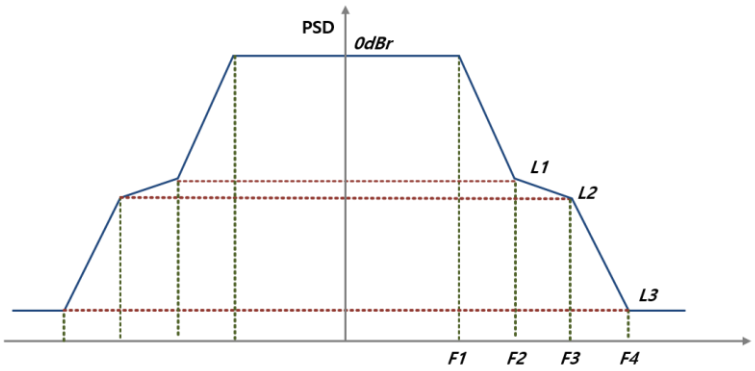
Non-linearity of Power Amplifier

Let's first find the characteristics of linear and non-linear system (PA) to see how linearity of PA affects mask.



IEEE requirement

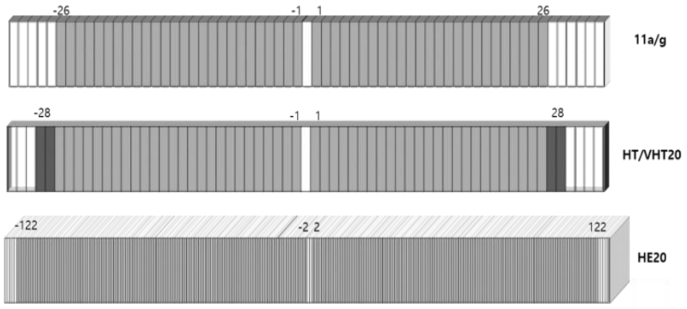
IEEE specifies HT20/40 in 2.4GHz spectral mask requirement different from other band. It is supposed to reduce the interference to other devices, as 2.4GHz is already congested. Measurement is based on 100KHz RBW. Regardless of IEEE requirement, the mask should not be higher than regulatory requirement, if any.



BW	Frequency Offset (MHz)				Level (dBr)		
	F0	F1	F2	F3	L1	L2	L3
11b	11		22		-30		-50
11a/g	9	11	20	30	-20	-28	-40
VHT20, HT20_5G	9	11	20	30			
VHT40, HT40_5G	19	21	40	60			
VHT80	39	41	80	120			
VHT160	79	81	160	240			
HT20_2.4G	9	11	20	30	-20	-28	-45
HT40_2.4G	19	21	40	60			
HE20	9.75	10.5	20	30	-20	-28	-40
HE40	19.5	20.5	40	60			
HE80	39.5	40.5	80	120			
HE160	79.5	80.5	160	240			

WLAN Spectral Mask

11ax has different frequency offset for spectral mask requirement, as it has different subcarrier scheme and allocation.



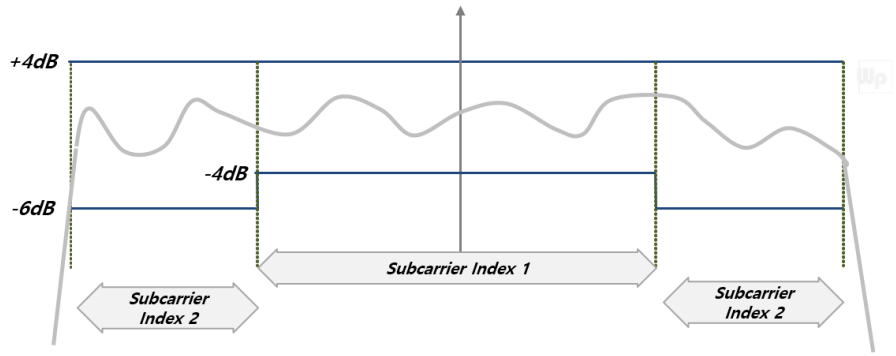
Subcarrier allocation in 20MHz bandwidth

Spectral flatness

Spectral Flatness

LTF consists of subcarriers with the amplitude of “1” and the main role of LTF in preamble is to help channel estimation. If the amplitude imbalance between subcarriers (spectral flatness) is too high, there could be an issue decoding the signal at the receiver and IEEE specifies spectral flatness.

Based on the averaged value among subcarriers in “subcarrier index 1”, the maximum deviation of the subcarrier should be within +/4dB for subcarrier index 1 and +4dB ~ -6dB for subcarrier index 2. IEEE specifies it can be measured using the designated subcarrier values or the magnitude of the channel estimation. Practically, spectral flatness is measured with the magnitude of the channel estimation, which is LTF. To measure it with data payload, BPSK shall be used.



BW	Frequency Offset	
	Subcarrier index 1	Subcarrier index 2
11a/g	±1 ~ ±16	±17 ~ ±26
HT/VHT20	±1 ~ ±16	±17 ~ ±28
HT/VHT40	±2 ~ ±42	±43 ~ ±58
VHT80	±2 ~ ±84	±85 ~ ±122
VHT160	±44 ~ ±126, ±130 ~ ±172	±6 ~ ±43, ±173 ~ ±250
HE20	±2 ~ ±84	±85 ~ ±122
HE40	±3 ~ ±168	±169 ~ ±244
HE80	±3 ~ ±344	±345 ~ ±500
HE160	±166 ~ ±509, ±515 ~ ±696	±12 ~ ±165, ±697 ~ ±1012

WLAN Spectral Flatness

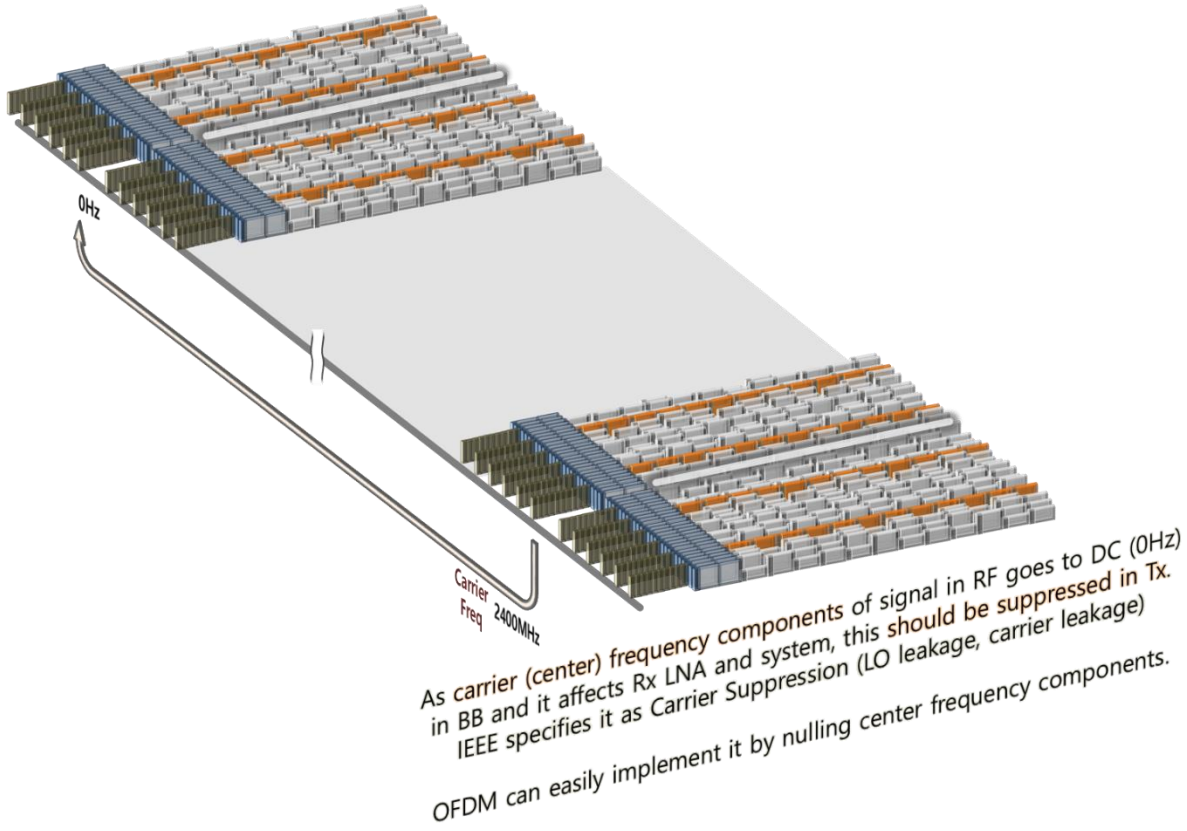
LO leakage

Leakage at Center frequency components

If RF signal is multiplied with carrier at receiver (down-converting), just as it is done in RF up-converting at transmitter, it goes back to baseband. While in this process, the center frequency components in RF go to DC (0 Hz) at BB, which may saturate LNA or affect receiver components, if the level is high.

This can be referred as other terminologies.

- Carrier Suppression
- LO (Local Oscillator) leakage
- DC leakage
- Center Frequency leakage



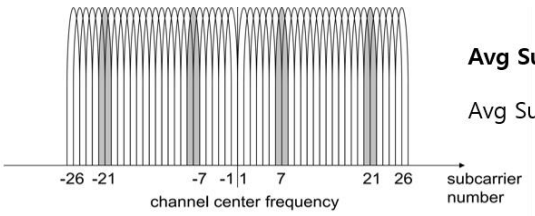
What is carrier leakage?

IEEE requirement

It is one of the most confusing RF requirements to read in IEEE. OFDM and Spread Spectrum have totally different way of measuring. 11b compares center frequency component with peak power spectrum, while OFDM compares with power. In addition, IEEE specifies OFDM power in two ways, the total power and the average subcarrier power. These two number does not always match exactly.

STD	BW	Center Frequency Leakage (dB)	
		Signal Power based	Avg subcarrier Power based
11b	20M	**-15dB** below to **peak power spectrum** *11b is spectrum based measurement*	
11a/g	20M	**-15dB** below overall Tx power	+2dB below compared with [average sub-carrier power] [P – 10*log(52)] = [P - **17.1dB**] + **2dB**
11n	20M	Same with 11a/g. Generally -17.5dB below	
	20M in 40M	**-17dB** below overall Tx power	+0dB below compared with [average sub-carrier power] [P – 10*log(56)] = [P - **17.5dB**] + 0dB
	40M	**-20dB** below overall Tx power	+0dB below compared with [average sub-carrier power] [P – 10*log(114)] = [P - **20.6dB**] + 0dB
11ac	20M		[P - 10*log(56)] = [P **- 17.5dB**] + 0dB
	40M		[P - 10*log(114)] = [P **- 20.6dB**] + 0dB
	80M		[P - 10*log(242)] = [P **- 23.8dB**] + 0dB
	160M		[P - 10*log(484)] = [P **- 26.8dB**] + 0dB
11ax	-	Max(P**-32**, -20)	

Average subcarrier power can be derived from signal power as below. It is just signal power divided by number for OFDM subcarrier expressed in “dB”



Avg Sub-carrier Power (dBm) = Signal Power – 10xlog(# of Sub-carrier)

Avg Sub-carrier Power = Signal Power (mW) / 52 sub-carrier
= Signal Power (dBm) – 10xlog(52)

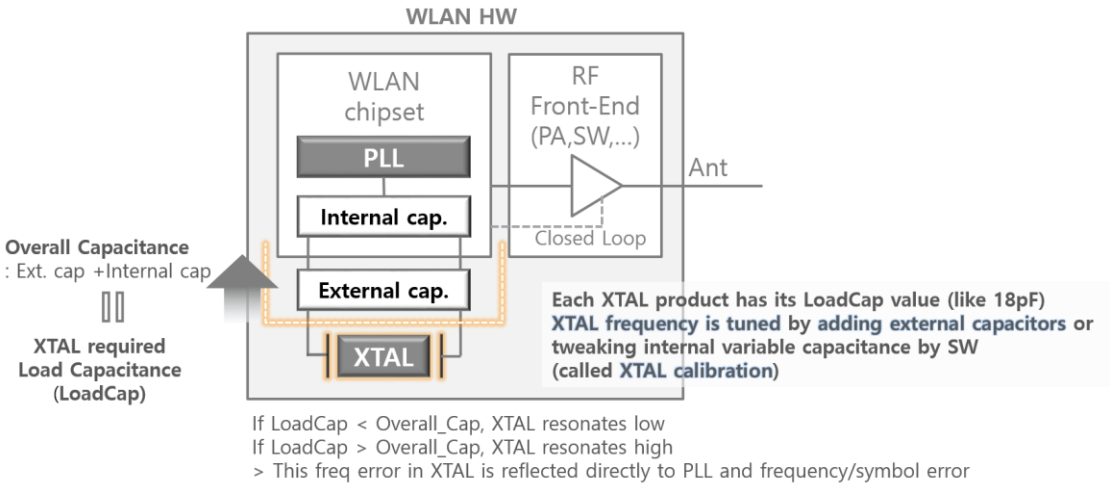
IEEE802.11 Tx requirement : Center Frequency Leakage

Frequency Error

Frequency Error and XTAL

RF frequency is from LO (local oscillator) and PLL based frequency synthesizer is generally used to generate LO in communication system. PLL frequency synthesizer has input clock from outside XTAL and various frequencies generated by PLL are used inside the chipset like processor, memory as well as RF parts.

For the deep understanding of frequency generation and error, let's take a look inside PLL and XTAL setting.

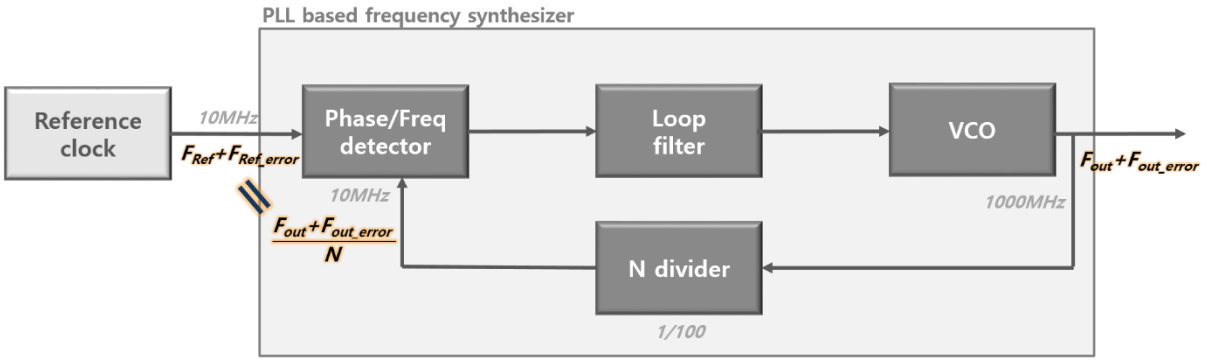


Frequency and Clock error and XTAL

Frequency error and PLL based frequency synthesizer

If there is a frequency error at frequency from XTAL, it is reflected to other frequencies like center frequency and symbol clock. If there is frequency error in XTAL (ppm), there mostly is the same portion of frequency/symbol error (ppm) in RF.

Here is how PLL synthesizer operates and how XTAL error is reflected to LO..



Phase is locked
Freq is differenciation of phase

$$\phi_{in} - \frac{\phi_{out}}{N} = constant$$

$$F_{out} = N \cdot F_{ref}$$

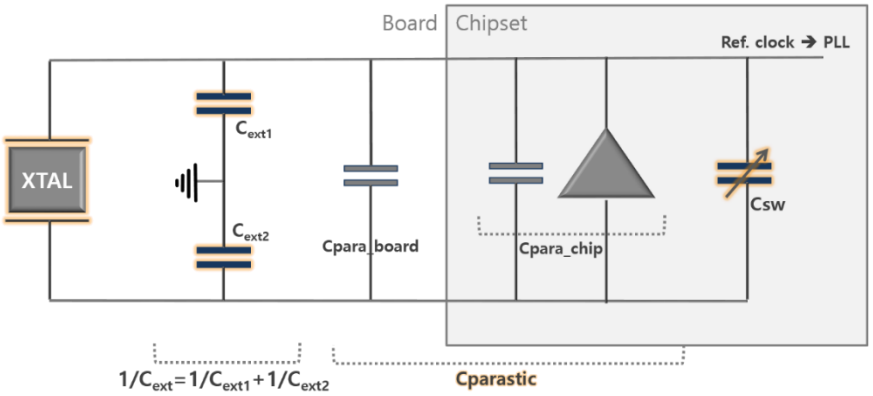
$$F_{out\_error} = N \cdot F_{ref\_error}$$

$$\frac{F_{ref\_error}}{F_{ref}}(ppm) = \frac{F_{out\_error}}{F_{out}}(ppm)$$

Freq error in reference clock (ppm) is the same with frequency error in PLL output (ppm)

How to tune XTAL frequency

Most of the current WLAN HW solutions apply XTAL (crystal oscillator) as an external clock source. Oscillated signal from XTAL is injected to PLL to make higher frequencies needed like digital, memory and RF parts. XTAL is a localized component and the system-level designer may not be able to choose exactly the same vendor's part recommended by the chipset vendors. Choosing XTAL, the load capacitance value of XTAL should be carefully checked, as the frequency changes based on it. XTAL can be tuned by HW components (external load capacitors) and by SW (internal tune-able capacitors), which is called as XTAL calibration.



$$C_{L\_total} = \frac{C_{ext1} \cdot C_{ext2}}{C_{ext1} + C_{ext2}} + C_{parastic} + C_{SW}$$

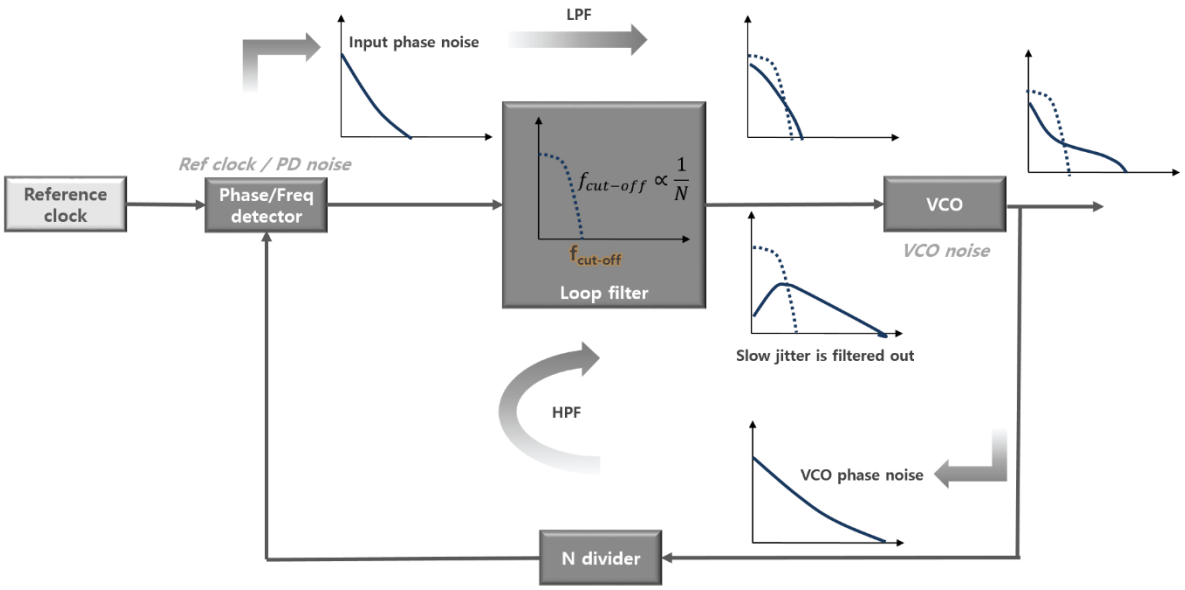
When, Xtal load cap. is 20pF and two 20pF external cap. are applied and the total parasitic cap. is 5pF

$$20p = \frac{20p \cdot 20p}{20p+20p} + 5p + C_{SW} = 10p + 5p + C_{SW}$$

Phase noise in PLL

The phase noise is short term frequency jittering and the phase noise in PLL frequency synthesizer (LO) is one of the main reason to degrade RF performance both in Tx and Rx. Phase noise is little thing to do with frequency error itself. However, frequency generating PLL synthesizer is the major source for system phase noise and let's check it briefly here.

The major sources for phase noise in PLL are classified into two. Input phase noise from reference clock (XTA) or/and phase detector and VCO's phase noise. The phase noise from reference clock and PD is filtered out outside the cut-off frequency in loop filter and VCO phase noise operates as if it is through HPF. Tuning loop filter is important, but it has to be dealt with different manners according to the noise source in PLL.



Input phase noise is reduced, when fcut-off is low
VCO phase noise is reduced, when fcut-off is high

IEEE requirement

IEEE requirement on center frequency tolerance and symbol clock tolerance is usually same, as they are normally considered to be from the same source.

Band	STD	Center Frequency / Symbol Clock Tolerance (ppm)
2.4G	11b	±25
	11g/n/ac/ax	±25
5G	11a/n/ac/ax	±20

IEEE802.11 Tx requirement : Center Frequency / Symbol Clock tolerance

RSSI and RCPI

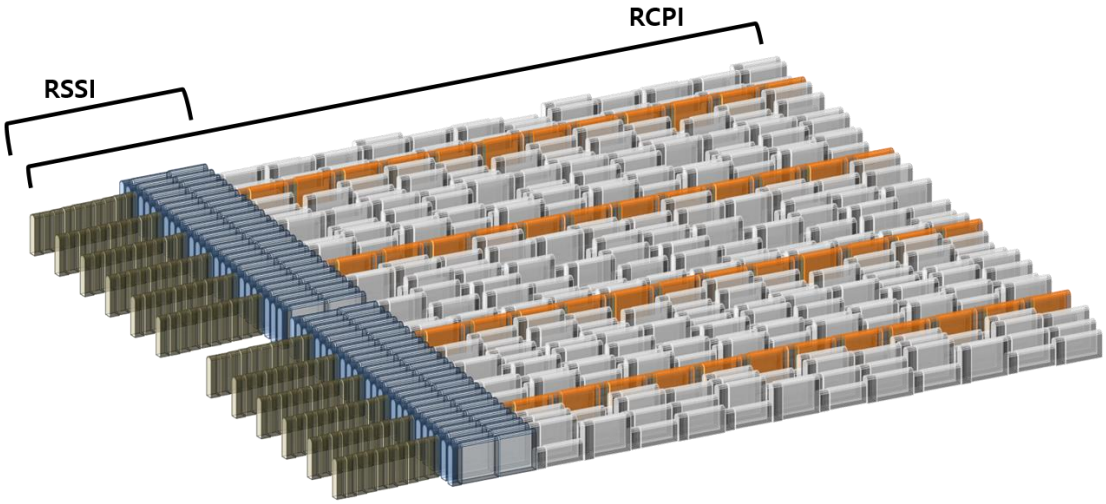
Dealing with the receiver performance of WLAN, terminologies and items like RSSI, RCPI, sensitivity, maximum input level and ACR (adjacent channel ratio, different from ACPR/ACLR which is Tx quality) are mentioned. Contrary to the popular knowledge, RSSI is not indicating the power of the received frame and it is not an absolute value in dBm as well.

RSSI : Receive Signal Strength Indicator

- Measured during the reception of preamble
- RSSI is relative value (8bit, 0~255) managed by the each vendors.
- However, 802.11 implies RSSI to be translated to the absolute value (dBm) as in cases below
  - Beacon RSSI : signal strength of Beacon frame. Reported in dBm (with +/-5dB accuracy)
  - CCA/CS(carrier sense) : -82dBm/20MHz
  - In 11ax, RSSI measurement accuracy is required for Power pre-correction.
- An absolute value can be derived from noise power or from RSSI calibration

RCPI : Receive Channel Power Indicator

- Received RF power of a frame. Averaged over all the Rx chains
- RF power is determined assuming a noise with bandwidth multiplied by 1.1
- With accuracy +/-5dB



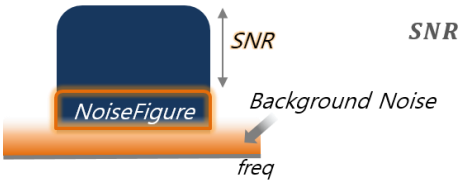
Sensitivity

A (minimum) sensitivity normally represents the overall receiver performance in WLAN system. But, for analyzing the receiver system and debugging the performance, we need to have understanding on SNR more than the sensitivity or RSSI.

Basic Concept on SNR

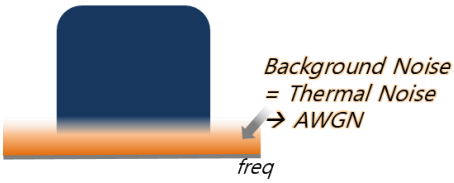
SNR (Signal to Noise Ratio) is a key factor to interpret receiver's performance. To understand it, the characteristics of the noise (the thermal background noise and the noise figure) needs to be seen.

Noise is the very broad concept that includes all the unwanted signals. But by the narrow meaning, noise is different from the interference that is usually generated by others. The interference can be categorized into two; the interference from other RF in the wireless channel and the interference from outside RF parts in the HW system. The first one is handled mostly by PHY protocol and the latter by system/RF engineers as it highly depends on the situations. Only noise along with signal is talked here instead of the interference.

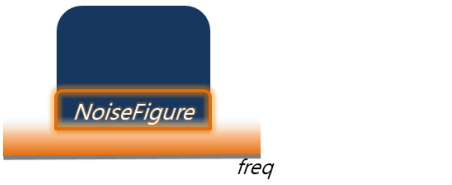


$$SNR = \frac{Signal\ Power}{Noise\ Power} = \frac{Signal\ Power}{Background\ Noise + System\ Noise\ figure}$$

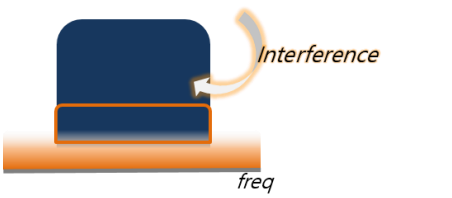
- SNR is dominant factor in analyzing receiver.
- At every stage, signal as well as background noise is amplied or attenuated by the system parameter and the noise is added by noise figure.



- Background noise is all the noise at input of the each stage.
- Background noise is regarded as thermal noise at the first stage.
- Thermal noise resides in every electronic devices with thermal agitation of electrons
- Factor of temperature and bandwidth. Flat in freq
- Added to signal. but not added by itself
  - ✓ AWGN+AWGN = AWGN (correlation is 0)
  - ✓ Adding two signal : 2 X SNR (only signal power added)



- Noise Figure (NF) is added by every stage (component)
- NF is independent of gain or input signal
- NF of Passive component is Attenuation
  - ✓ If attenuation is 1 (ideal), no noise is added



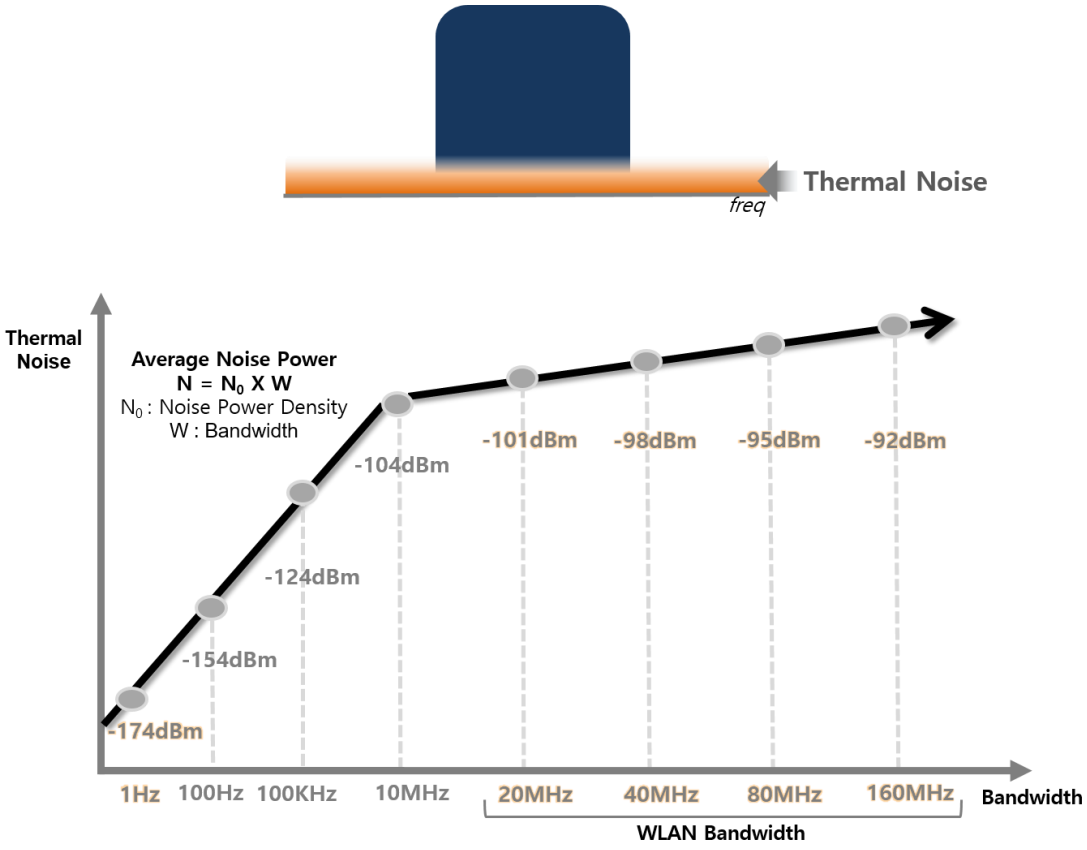
- Interference from other RF or noise in channel
  - ✓ SINR. Mostly, protocol level situation
- Interference from other parts in device
  - ✓ System level situation.

Basic Concept on SNR in receiver

Thermal noise in WLAN

Background noise floor is all the noise at the input of the system and basically it is the thermal noise generated by a random thermal agitation of electrons that exists in all electron devices. It cannot be avoided or removed. It is the function of temperature and bandwidth with AWGN characteristics.

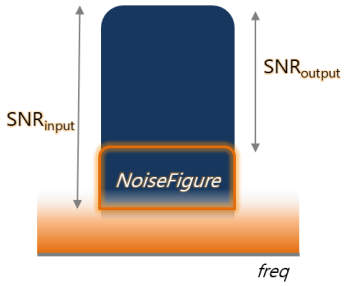
Power density of the thermal noise is -173.9dBm/Hz at 300K degree. For WLAN bandwidth of 20 MHz, the noise power is about -101 dBm. As BW goes wider, the thermal noise power gets higher. Compared to 20MHz, noise power is doubled in 40MHz (3dB higher)



Thermal Noise in WLAN

Noise Figure

Noise Figure (NF) is the noise of the system inside (a stage or a component) generated by itself and it is expressed by the degree how much SNR is degraded between input and output of the system. NF is the ratio of input SNR to output SNR. At every stage and block in receiver, NF is added making the overall system SNR worse.



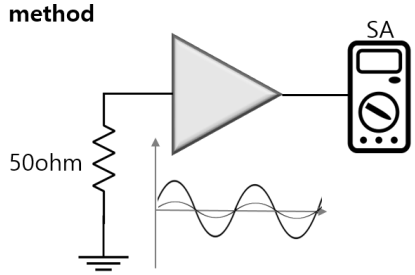
$$NF = \frac{SNR_{input}}{SNR_{output}}$$

Noise figure is the ratio of input SNR and output SNR
To see how much noise is added through the system

There are a couple of ways to measure NF. Modern method (Y-factor) gives more accurate result, while it needs a calibrated noise source. Gain method is a generic way of NF measurement.

How to measure NF

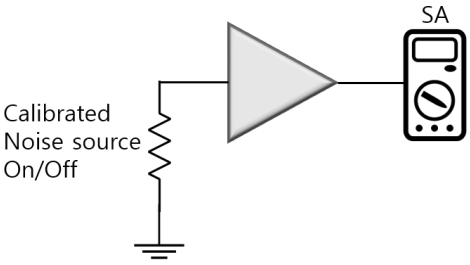
Gain method



$$NF = \frac{S_i/N_i}{S_o/N_o}$$
$$= N_o - Gain - N_i$$

Measure output noise power
Measure signal gain
Thermal noise (-174dBm/Hz)

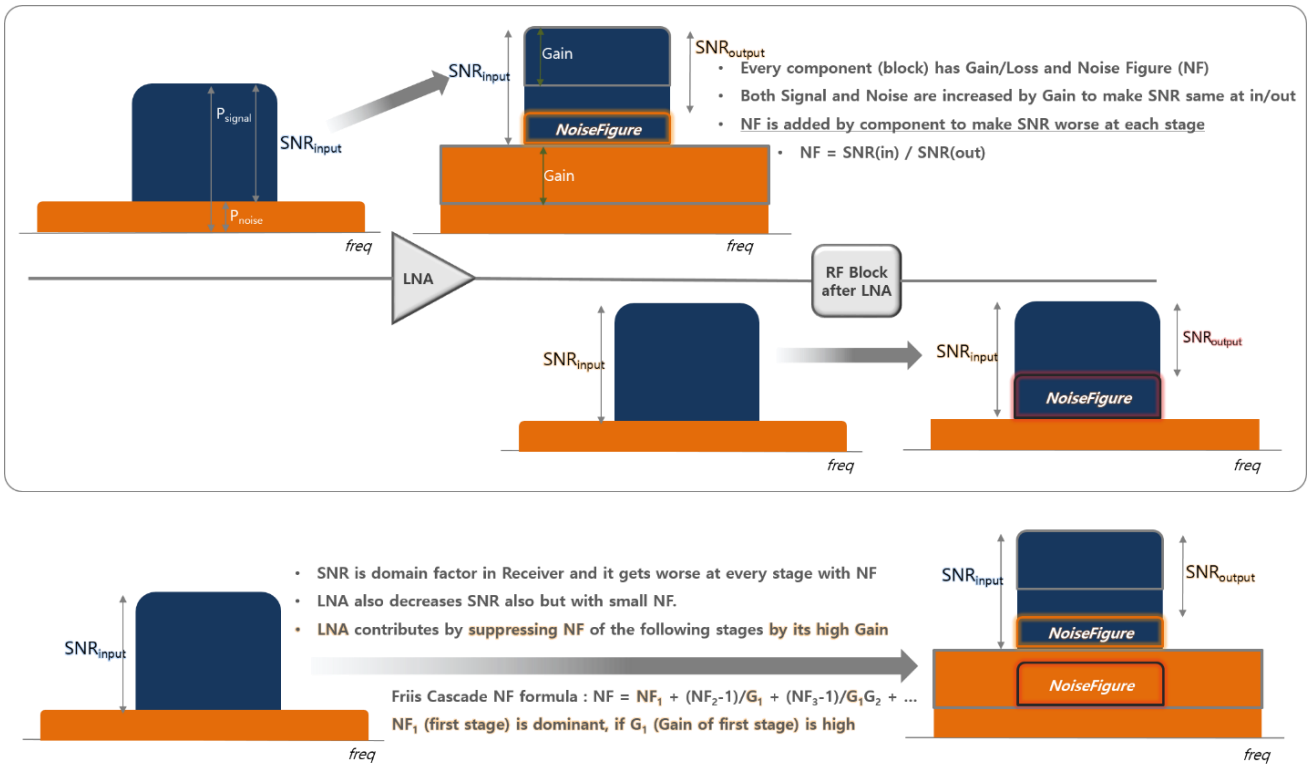
Y-factor method



$$NF = 10 \cdot \log_{10}\left(\frac{ENR}{Y-1}\right)$$

ENR : power level difference between hot and cold
Y : ration of measured noise power between hot and cold

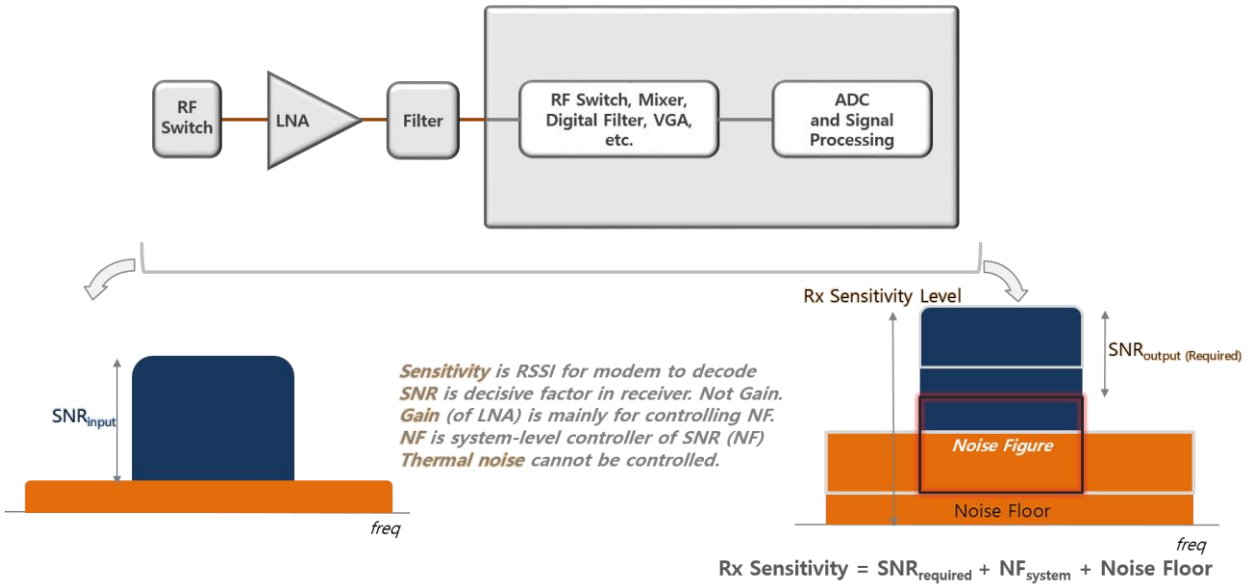
Every component adds NF figure and LNA (low noise amplfier) also does, which meas SNR goes worse after LNA. Then why LNA is used in the system? By the Friis formula, NF is suppressed by the gains of the preceding stages and the high gain of LNA plays a role of supressing the overall system NF. So, LNA should be placed at the very front of receiver chain.



Noise Figure and LNA

Link budget and Sensitivity Level

If the system (ADC for example) requires 10dB SNR and NF is expected to be 15dB for 20MHz BW in a system. The Noise floor for 20MHz is -101dBm and a minimum sensitivity level is calculated to -76dBm. (-101dBm + 15dB + 10dB). In other words, the difference between the signal (-76dBm) and the noise (-101dBm+15dB) makes 10dB gain for ADC.



IEEE Requirement

Commercial WLAN solution may have higher performance than the values in the table. IEEE requirement can be regarded as the minimum level of system performance, which can be applied to pass/fail criteria in mass production.

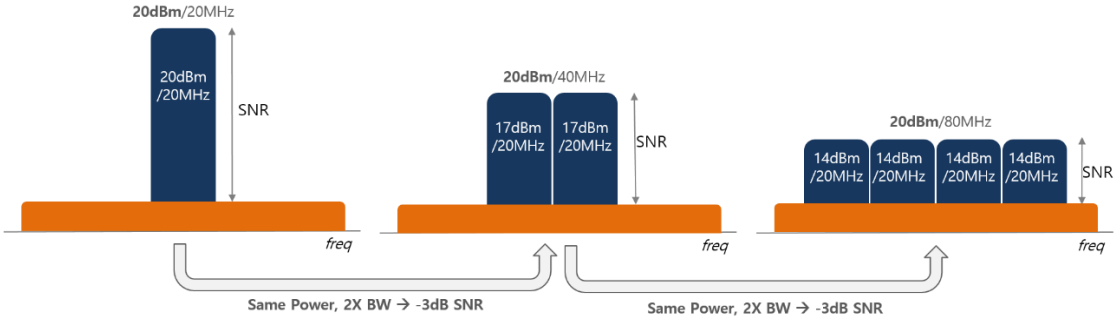
Data Rate				Minimum Sensitivity (dBm)				
Modulation	C/R	11a/g	MCS	11a/g	BW20 HT/VHT/HE	BW40 HT/VHT/HE	BW80 VHT/HE	BW160 VHT/HE
BPSK	1/2	6	MCS0		-82	-79	-76	-73
BPSK	3/4	9	-		-81			
QPSK	1/2	12	MCS1		-79	-76	-73	-70
QPSK	3/4	18	MCS2		-77	-74	-71	-68
16QAM	1/2	24	MCS3		-74	-71	-68	-65
16QAM	3/4	36	MCS4		-70	-67	-64	-61
64QAM	2/3	48	MCS5		-66	-63	-60	-57
64QAM	3/4	54	MCS6		-65	-62	-59	-56
64QAM	5/6	-	MCS7		-64	-61	-58	-55
256QAM	3/4	-	MCS8 (VHT)		-59	-56	-53	-50
256QAM	5/6	-	MCS9 (VHT)		-57	-54	-51	-48
1024QAM	3/4		MCS10 (HE)		-54	-51	-48	-45
1024QAM	5/6		MCS11 (HE)		-52	-49	-46	-43

11a/g : PER < 10% for PSDU of 1000 octets at ant. Connector
11n/ac : PER < 10% for PSDU of 4096 octets, Non-STBC, 800nsec GI, BCC
11ax : PER < 10% for PSDU of 4096 octets, Non-STBC, 800nsec GI, BCC (20MHz, ~MCS9) and LDPC (40/80/160MHz and 20MHz with MCS10, 11)

IEEE802.11 Rx requirement : minimum Sensitivity

SNR and Bandwidth

If the received signal power is same in 20MHz, 40MHz and 80MHz, SNR has 3 dB difference between them because of the noise power, which is the reason why IEEE requirement has exactly 3 dB difference between BW.



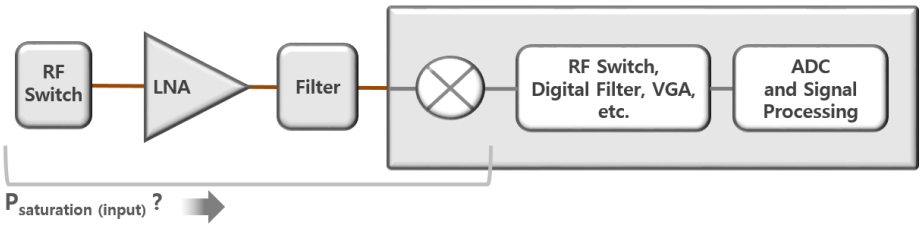
SNR and Bandwidth

Max input level

Max Input Level

It can be called as a maximum sensitivity. Normally, RF distance between AP and mobile devices is far and there has not been much concerns this requirement. However, considering Wi-Fi Direct or Smartphone tethering, there will be more and more situations that WLAN device could capture high power from its counterpart in close distance.

Every component in receiver has a dynamic range or a linear range with a maximum input as well as minimum input level. Here is the simple example to figure out at which power level each components is saturated, which results in the maximum input level of system.



Stage	Component	Gain	P_{1dB}	$P_{sat(input)}$	Calculation
1	RF Switch	-2dB	Inf.	Inf.	If linear
2	LNA	20dB	10dBm (output)	-8dBm	$P_{sat} = P_{1dB(in)} - G_1 = P_{1dB(out)} - G_1 - G_2 = 10-(-2)-20$
3	Filter	-1dB	Inf.	Inf.	If linear
4	Mixer	-6dB	0dBm (input)	-17dBm	$P_{sat} = P_{1dB(in)} - G_1 - G_2 - G_3 = 0-(-2)-20-(-1)$

Rx maximum input level (simple example)

IEEE requirement

Band	STD	Maximum Sensitivity (dBm)
2.4G	11b	-10
	11g/n/ac/ax	-20
5G	11a/n/ac/ax	-30

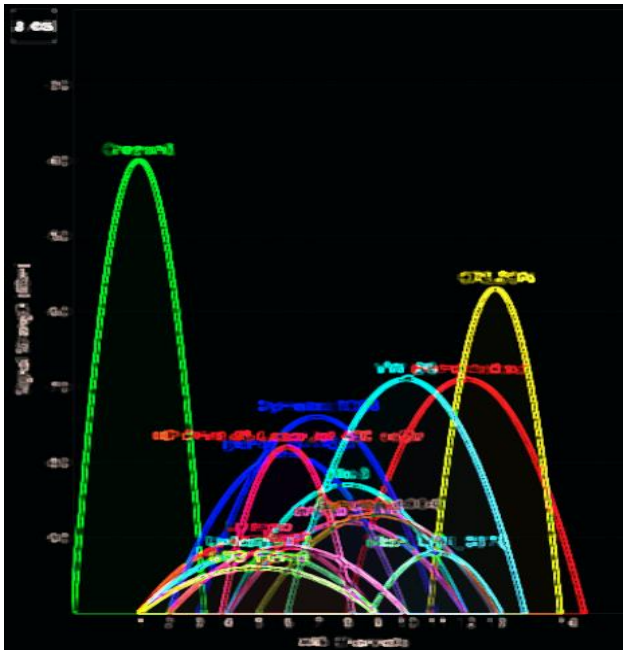
IEEE802.11 Rx requirement : maximum Sensitivity

ACR

Why is ACR getting important

As a consequence of an increasing amount of in-band and adjacent band interference from many WLAN devices, the design of radio and digital filtering has become critical with the demand of evaluation.

Adjacent Channel Reject (ACR) is not handling the in-band (signal band) interference. (ACR is totally different concept with ACLR or ACPR of Tx) In-band interference can be regarded as the signal that occupies the channel and CCA takes the role in CSMA/CA. ACR is the only IEEE requirement to see the Rx performance with the interference at the channel around.



IEEE Requirement

The interferer level of IEEE requirement is defined by each data rate which value is relative to sensitivity level. However, the level is simply calculated to be a constant one as in the table below. Interferer signal does not need to be synchronized with the wanted signal with the minimum duty cycle of 50%

		Wanted Signal	Adjacent Interferer		Non-adjacent Interferer	
		Level (dBm)	Level	Spacing	Level	Spacing
2.4G	DSSS	-74dBm	-39dBm	±30MHz		
	CCK	-70dBm	-35dBm	±25MHz		
	11g	Min Sensitivity + 3dB	-63dBm	±25MHz		
5G	11a, HT/VHT20	Min Sensitivity + 3dB	-63dBm	±20MHz	-47dBm	±40MHz
	HT/VHT40		-60dBm	±40MHz	-44dBm	±80MHz
	HT/VHT80		-57dBm	±80MHz	-41dBm	±160MHz

IEEE802.11 Rx requirement : ACR

ACR example

ACR is measuring the sensitivity of the wanted (desired) signal while the interference at adjacent channel (ACR) or non-adjacent channel at specific level is transmitted.

5480MHz (5500 – 20 MHz)
MCS7 20MHz

➔ Interferer at **-63dBm**
(-61dBm – 2 dB)

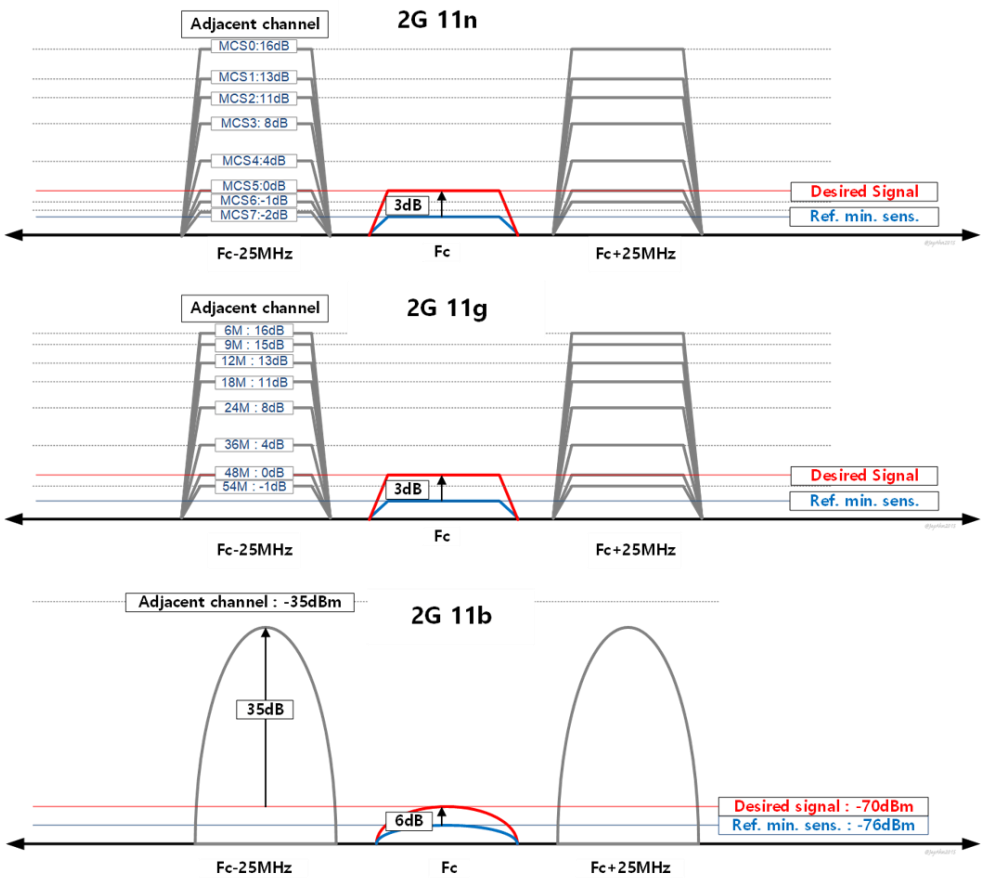
5500MHz (**CH100**)
MCS7 20MHz (min Sensitivity : **-64dBm**)

➔ Check PER at **-61dBm**
(-64dBm + 3dB)

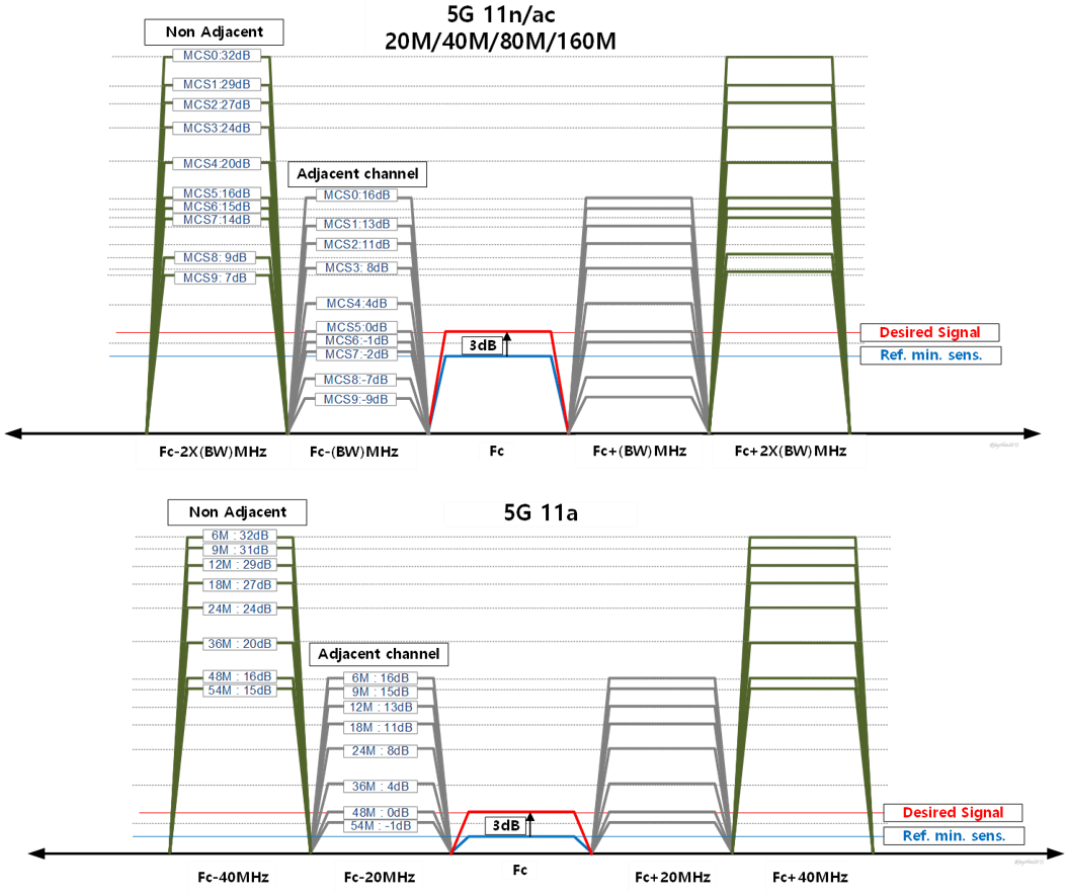
Simple example : How to test ACR

Interferer Level

IEEE describes interferer level as the relative value based on each MCS's sensitivity level and it look complicated.



IEEE802.11 ACR level for 2.4G



IEEE802.11 ACR level for 5GHz

Recalculating the interferer level from IEEE requirement, the level is simply -63dBm for the adjacent and -47dBm for the non-adjacent channel based on 20MHz as in the table below.

ACR

11b	Sens	Adj Sens	Adj Int	Adj Int lev	
1M	-80	-74	41	-39	
2M	-80	-74	41	-39	30MHz
5.5M	-76	-70	41	-35	
11M	-76	-70	41	-35	25MHz

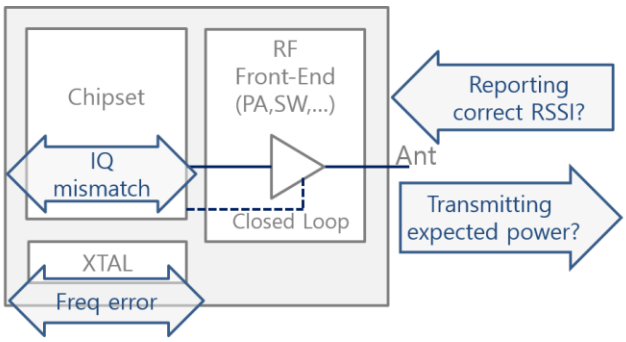
				1st		2nd
11a/g	Sens	Adj Sens	Adj Int	Adj Int lev	Alt. Adj. Int	Alt. Int lev
6M	-82	-79	16	-63	32	-47
9M	-81	-78	15	-63	31	-47
12M	-79	-76	13	-63	29	-47
18M	-77	-74	11	-63	27	-47
24M	-74	-71	8	-63	24	-47
36M	-70	-67	4	-63	20	-47
48M	-66	-63	0	-63	16	-47
54M	-65	-62	-1	-63	15	-47

	20M	40M	80M	20MHz		1st		2nd	40MHz		1st		2nd	80MHz		1st		2nd
11n/ac	Sens	Sens	Sens	Adj Sens	Adj Int	Adj Int lev	Alt. Adj. Int	Alt. Int lev	Adj Sens	Adj Int	Adj Int lev	Alt. Adj. In	Alt. Int lev	Adj Sens	Adj Int	Adj Int lev	Alt. Adj. In	Alt. Int lev
MCS0	-82	-79	-76	-79	16	-63	32	-47	-76	16	-60	32	-44	-73	16	-57	32	-41
MCS1	-79	-76	-73	-76	13	-63	29	-47	-73	13	-60	29	-44	-70	13	-57	29	-41
MCS2	-77	-74	-71	-74	11	-63	27	-47	-71	11	-60	27	-44	-68	11	-57	27	-41
MCS3	-74	-71	-68	-71	8	-63	24	-47	-68	8	-60	24	-44	-65	8	-57	24	-41
MCS4	-70	-67	-64	-67	4	-63	20	-47	-64	4	-60	20	-44	-61	4	-57	20	-41
MCS5	-66	-63	-60	-63	0	-63	16	-47	-60	0	-60	16	-44	-57	0	-57	16	-41
MCS6	-65	-62	-59	-62	-1	-63	15	-47	-59	-1	-60	15	-44	-56	-1	-57	15	-41
MCS7	-64	-61	-58	-61	-2	-63	14	-47	-58	-2	-60	14	-44	-55	-2	-57	14	-41
MCS8	-59	-56	-53	-56	-7	-63	9	-47	-53	-7	-60	9	-44	-50	-7	-57	9	-41
MCS9	-57	-54	-51	-54	-9	-63	7	-47	-51	-9	-60	7	-44	-48	-9	-57	7	-41

Calibration

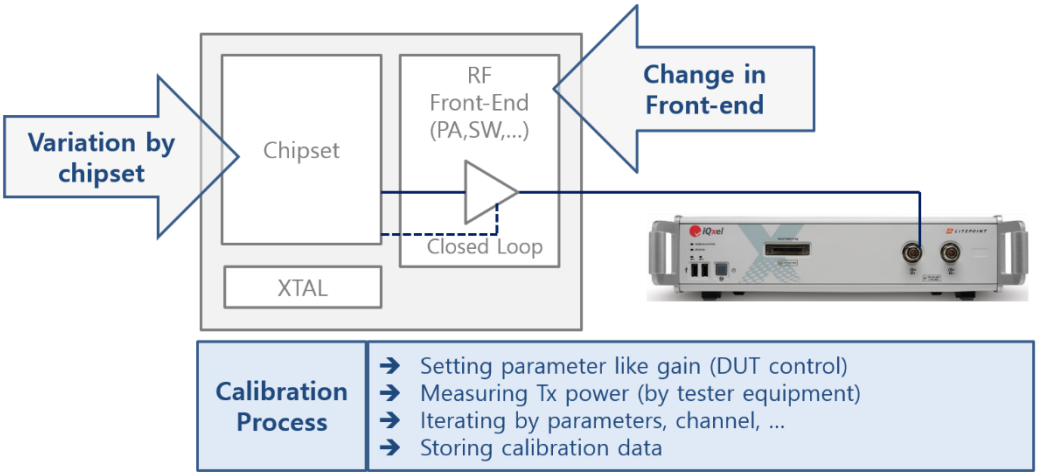
The frequency, phase and the amplitude of the system need to be calibrated in case that there happens the changes while implementing system or there are deviations between chipsets or components. In WLAN, Tx power, XTAL frequency, RSSI and I/Q mismatch are candidates for the calibration.

HW Calibrations in WLAN



- **Tx power Calibration**
  - Gain setting → Tx → measure with tester → writing values to EEPROM/OTP/BoardFile
- **XTAL Calibration**
  - XTAL frequency error is reflected to LO frequency error. It can be fine-tuned by SW tunable capacitor inside chipset.
- **RSSI(RCPI) Calibration**
  - Transmit a frame with a specific power from tester → read signal power value in chipset
- **IQ Calibration**
  - IQ mismatch brings amplitude and phase imbalance between in-phase and quadrature path to impact Tx and Rx performance.

Calibrating transmitting power

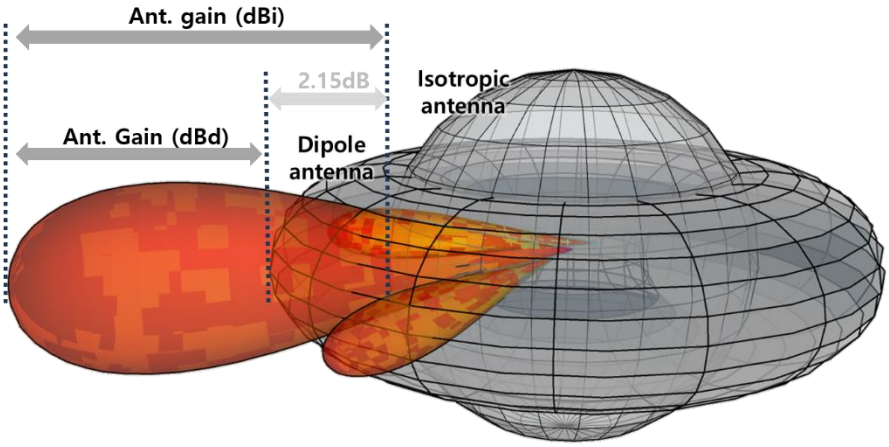


- **Conditions**
  - (1) High variation by chipset ➔ Each DUT calibration
  - (2) Change in front-end or PCB design ➔ Tx power may not be the same as chipset expects
    - High variation by board ➔ Each DUT calibration
    - Low variation by board ➔ Golden DUT calibration
- **Where to store calibration information**
  - (1) Memory in WLAN HW (EEPROM, OTP)
    - Every DUT can have a different calibration information ➔ Each DUT calibration
  - (2) File in CPU
    - Difficult to store different calibration information for each DUT ➔ Golden DUT calibration

Antenna and OTA test

Antenna gain and ERP

Antenna is a passive device (mostly) to transform electric signal to electromagnetic wave and vise versa. Antenna gain is not the kind of gain that the active device has, but it is how much the peak value of antenna main lobe is there compared to the isotropic antenna (dBi) or dipole antenna (dBd). As defined, the antenna gain indicates antenna's directivity and efficiency and the high gain antenna means the narrow bandwidth with strong directivity.



Antenna gain indicates antenna's directivity and efficiency comparing with isotropic antenna (dBi) or dipole antenna (dBd)

ERP (effective radiated power) is a radiated Tx power based on dipole antenna and EIRP (effective isotropic radiated power) is a radiated Tx power based on isotropic antenna

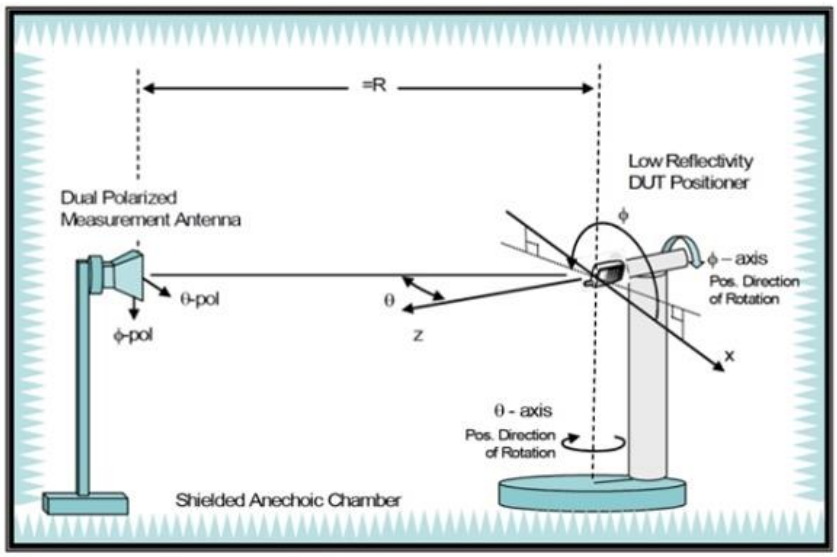
- ERP = Tx_Power(dBm) + Antenna_Gain(dBd) = EIRP – 2.15dB
- EIRP = Tx_Power(dBm) + Antenna_Gain(dBi)

Radiated Tx power is expressed with ERP (effective radiated power) or EIRP (effective isotropic radiated power), which are the conducted Tx power value multiplied by the antenna gain. The unit of ERP or EIRP is dBm (not dBi or dBd), as they are the real radiated value and not a gain.

OTA test

Over The Air (OTA) test is to find out DUT's radiated Tx (TRP : Total Radiated Power) and Rx (TIS : Total Isotropic Sensitivity) performance, which shows 3 dimensional radiation performance including antenna. The guideline is from collaboration between CTIA and Wi-Fi alliance and the pass/fail criteria is vendor or carrier's decision.

- Test Condition
  - Disable Scan, Power Save
  - Actively re-associate, when losing association
  - Disable other RF like Bluetooth and Cellular (there is cellular enabled de-sense test, instead)
- Tx test
  - Ack base : 100 packet, 60 Byte payload
  - PING base : 10 packet, 1K Byte payload
- Rx test
  - PER : 10%, 1dB resolution
  - Ack base : 1000 packet, 1K Byte payload

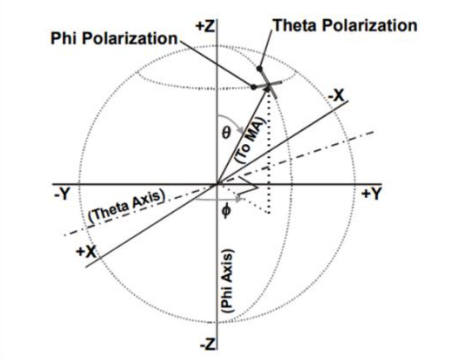


Item	Method	Rate	Channel
Conducted Tx	**ACK base or Ping base**	11b : 11M 11a/g : 6M 11n : MCS0	2.4GHz : Low/mid/high 5GHz : Low/mid/high of each sub-band
Radiated Tx (TRP)		11b : 11Mbps 11a/g : 6M **11n : MCS0**	2.4G : Ch6 5G : (table)
Conducted Rx	FRR (frame reception ratio) #ACK received/ # DataFrame sent	11b : 11Mbps 11a/g : 6M,54M 11n : MCS0, MCS7	2.4GHz : Low/mid/high 5GHz : Low/mid/high of each sub-band
Radiated Rx (TIS)		11b : 11Mbps 11a/g : 54M **11n : MCS7**	2.4G : Ch6 5G : (table)

	Channel Range	TRP/TIS Channel
UNII Low Band	36~48	44
UNII Middle Band	52~64	60
ETSI European Band	100~140	120
UNII Upper Band	149~161	157
USA	165	165

TRP has 15 degree for each Theta and Phi rotation, while TIS has 30 degree. TRP is one point measurement for each Theta and Phi. However, TIS takes far more time than TRP, as it has to find out PER 10% level searching for several levels at each Theta and Phi.

The formula has "sine" weighting and the values at Theta degree of 0 and 180 are zero and does not need to measure. "Sine" weighting is a kind of normalization.



$$TRP \cong \frac{\pi}{2NM}\sum_{i=1}^{N-1}\sum_{j=0}^{M-1}\left[E_i RP_\theta(\theta_i,\emptyset_j)+E_i RP_\emptyset(\theta_i,\emptyset_j)\right]\sin(\theta_i)$$

Theta, Phi 15
N:12, M:24

$$TIS \cong \frac{2NM}{\pi\sum_{i=1}^{N-1}\sum_{j=0}^{M-1}\left[\frac{1}{EIS_\theta(\theta_i,\emptyset_j)}+\frac{1}{EIS_\emptyset(\theta_i,\emptyset_j)}\right]\sin(\theta_i)}$$

Theta, Phi 30
N:6, M:12

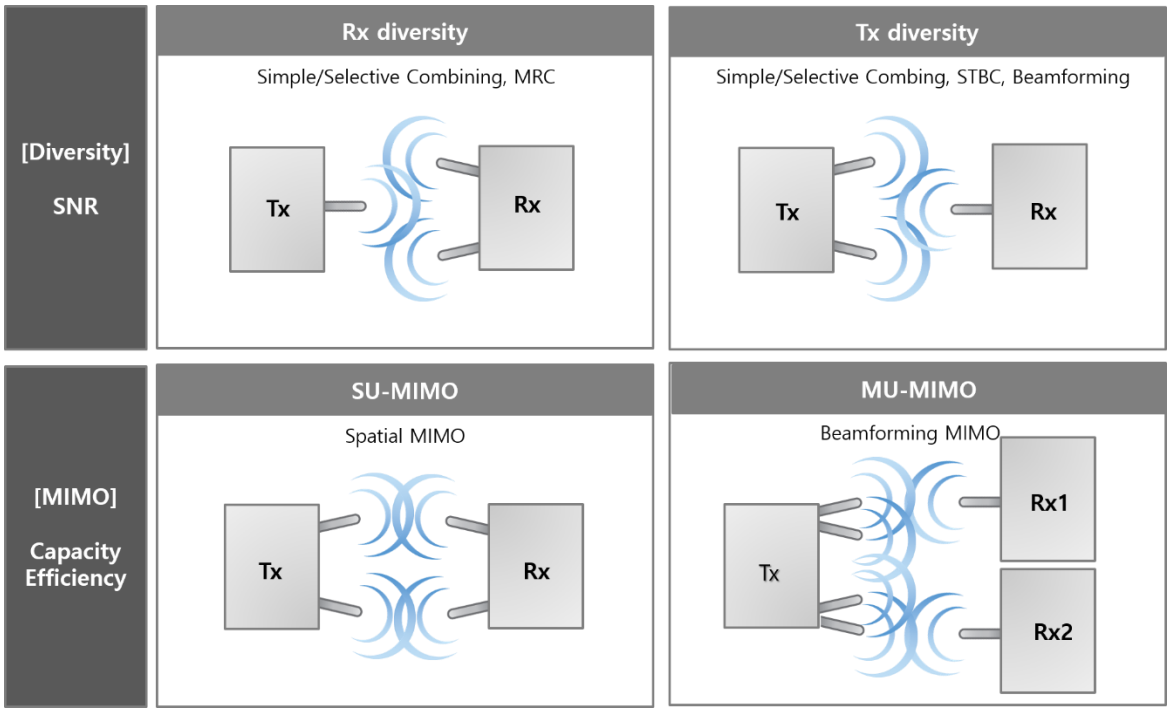
Multiple Antenna

What to do with multiple antenna?

Multiple antenna brings utilization of diverse space, timing and stream in RF to enhance SNR (Tx and Rx diversity) and capacity/efficiency (MIMO). Diversity can be used in Tx and/or Rx and the multiple stream can be used for one user (SU-MIMO) and/or for multi-user (MU-MIMO).

Considering the link-budget between transmitter and receiver, to improve SNR with multiple antenna at transmitter is very costly way from the view point of the implementation cost (Tx chain with PA) and the operation cost (the current consumption). Rx diversity is much effective way of SNR improvement and has been used widely in wireless communication systems. In WLAN, multiple antenna for Tx diversity techniques are introduced and implemented not just for diversity. For higher capacity, multiple Tx is required for MIMO and Tx diversity is a way of utilizing already-built multiple antenna in transmitter.

Transmitting and receiving multiple streams can be used between single users or between single user and multiple users. SU-MIMO utilizes multi-path wireless channel and is called as spatial MIMO and MU-MIMO uses beamforming and is called as beamforming MIMO.



How to utilize multiple antenna in WLAN?

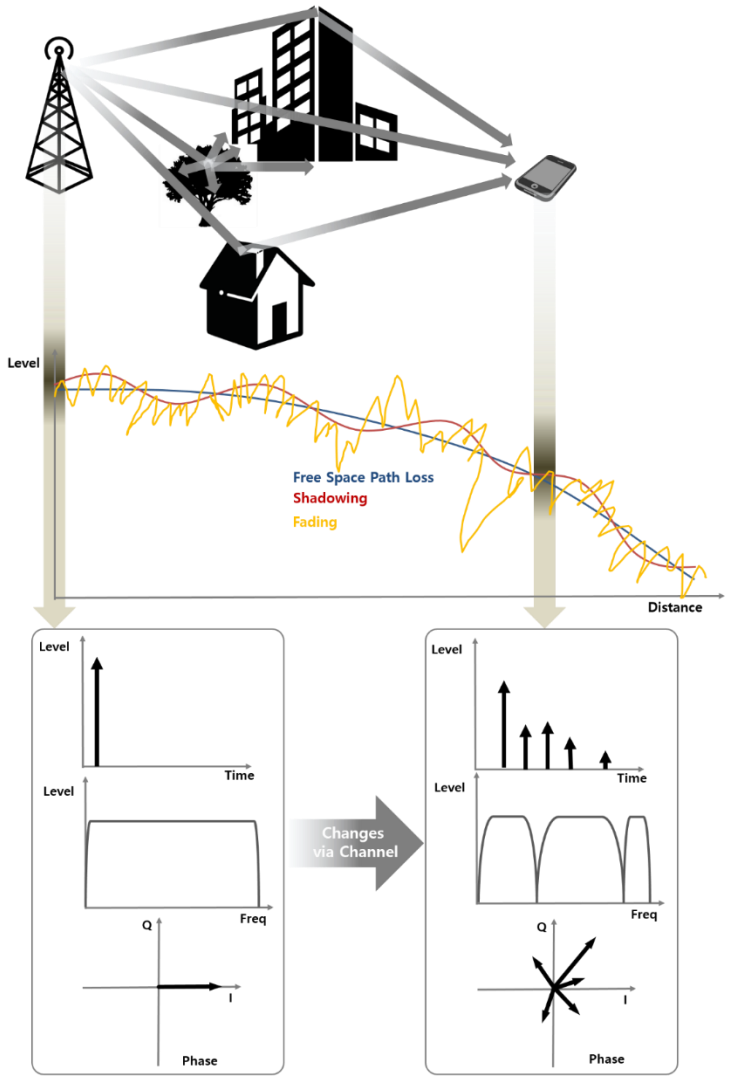
	Type	Goal
Rx Diversity	Simple (Equal Gain)/Selective combining, MRC	More than 2 Rx to improve effective **SNR**
Tx Diversity	Simple/Selective Tx, STBC, Beamforming	Diversity(CSD), **SNR** (STBC, Beamforming)
SU-MIMO	2 Spatial Stream, ~	**High capacity** using multiple stream
MU-MIMO	Multi-user beamforming MIMO	To Send to (receive from) multiple User simultaneously

Wireless channel

What happens to radio signal in wireless channel?

The amplitude and phase of signal changes in wireless channel and in time domain, the signal is delayed and spread.

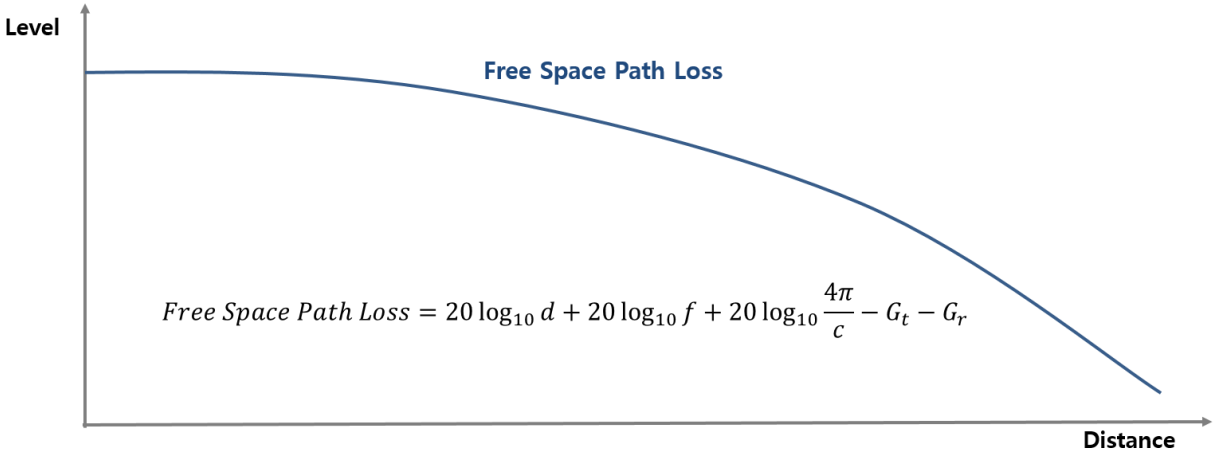
- Reflection : Object with smooth (very) large dimension to wavelength
- Refraction / diffraction : Object with dense large dimension to wavelength. Reason for Shadowing
- Scattering : Object with small dimension or its surface irregular
- Spreading : Multiple Object to make multipath



Signal in Wireless Channel

Free Space Path Loss

Diffusion of energy to three dimensional space from antenna is the main reason of the free space path loss. This loss can be calculated with the formula below. (Gt, Gr is gain of Tx and Rx each).



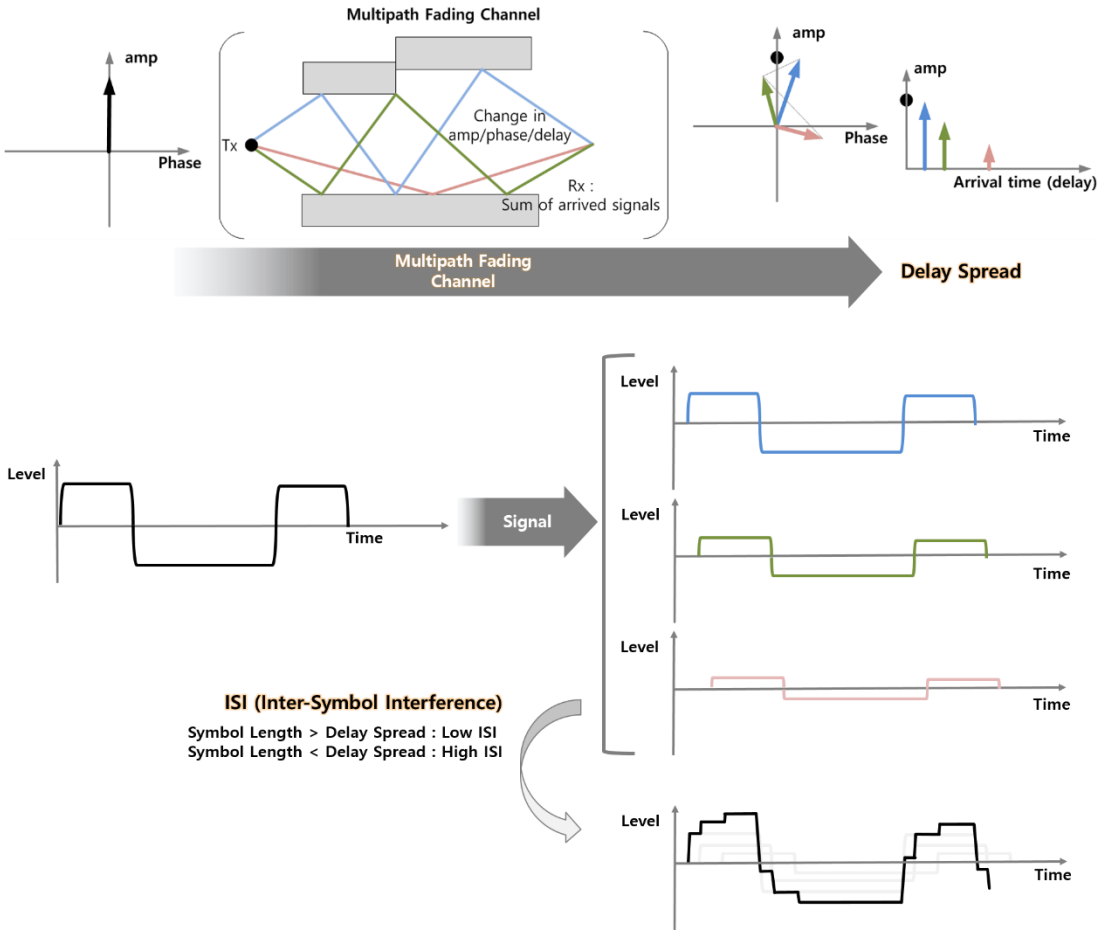
Path loss	20m	50m	100m	200m	400m
2.4GHz	66dB	74dB	80dB	86dB	92dB
5.5GHz	73dB	81dB	87dB	93dB	99dB

Free Space Path Loss of WLAN frequency band

Multipath Fading

Overall reduction of signal energy from free space path loss or shadowing can be managed with amplifier. However, the most common and problematic situation is multipath fading, as the transmitted signal is received via many paths between them. Signal at each path experiences different amount of delay (phase change) along with the change in amplitude and the summed signals from many paths look spread compared to the original signal, which is called as “delay spread”

This multipath has both good and bad aspects. It causes fading and at the same time, it is utilized as spatial diversity for multiple stream as in MIMO.

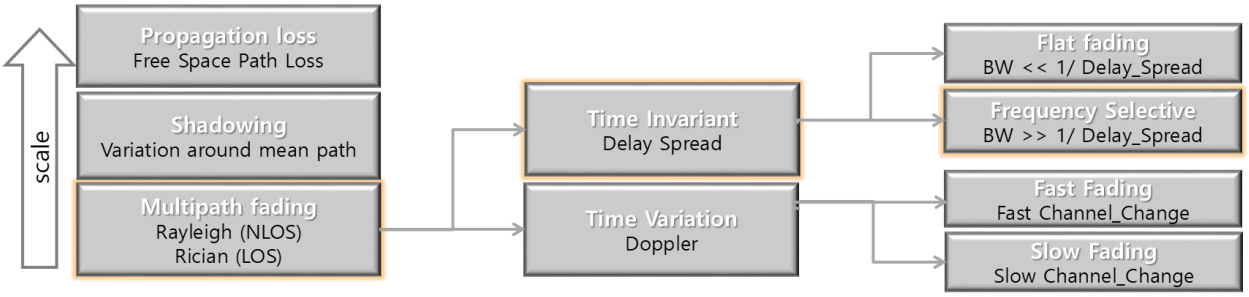


Multipath Fading

Fading Channel

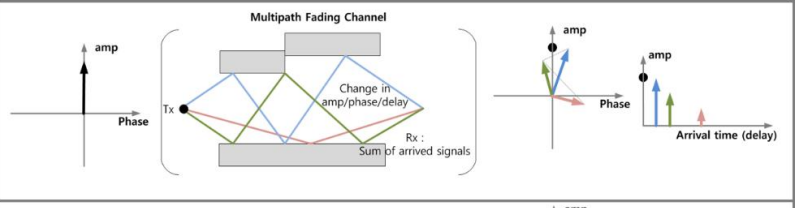
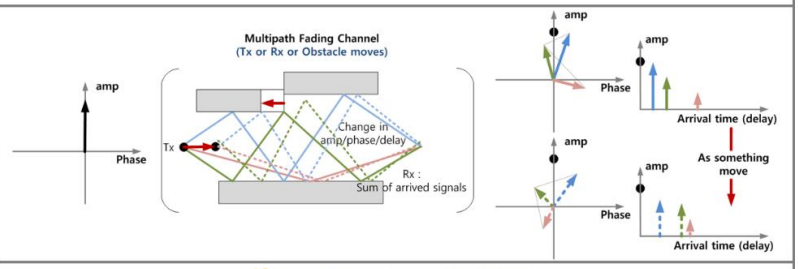
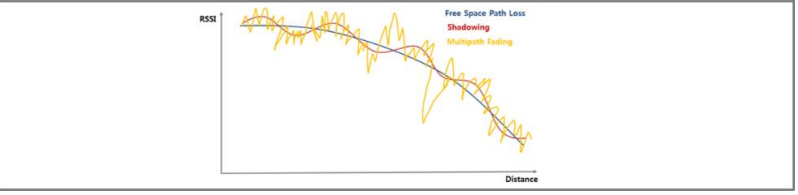
Fading channel can be categorized to “time invariant channel” and “time variant channel”. Time variant channel is to make the received signal vary by time, as reflectors/transmitter/receiver move. WLAN devices do not usually run fast and the time variant channel has not been the main topic in WLAN and IEEE starts dealing with it from 11ax with Midamble.

Time invariant channel can be divided into “flat fading channel” and “frequency selective channel” according to the signal (symbol) speed and amount of delay spread.



Time	Type		Impact
Invariant	Flat Fading	[Delay Spread] - Un-simultaneous arrival of signal in multipath causes the spread of original signal in time domain [Multipath] - This multipath richness of channel can be utilized in MIMO	SNR loss Generally not serious except deep fading
	Freq. Selective Fading		Long delay spread causes Inter-Symbol interference
Variant	Fast Fading	[Doppler spread] - Not big topic in WLAN indoor channel model . 1.2km/h : 3Hz (2.4G), 6Hz (5G) . 40 km/h : 80Hz (2.4G), 190Hz (5G)	[Time Selective Fading] - Channel change dramatically in time - Distortion, Sync error, SNR loss
	Slow Fading		[Shadowing] - Channel does not change much compared to symbol duration - Loss in SNR

Fading Channel Summary

Scale perspective	Channel perspective (time)	Signal perspective (Frequency)	Signal perspective
[small scale] Multipath fading Rayleigh(NLOS) / Rician (LOS)	Time spreading Delay Spreading	Flat fading Delay spreading < Symbol period	
		Frequency Selective delay spreading > Symbol period	
	Time variant Doppler Spreading	Fast Fading Channel change > Symbol change	
		Slow Fading Channel change < Symbol change	
[mid scale] Shadow fading Variation around avg			
[large scale] Propagation loss path distance			

Fading Channel Summary with Signal

Indoor Channel Model

This channel model has been discussed in 11n and there are 6 types according to the size of indoor environment. As the signal experiences the relatively short delay indoor, the amount of max delay is less than 1usec.

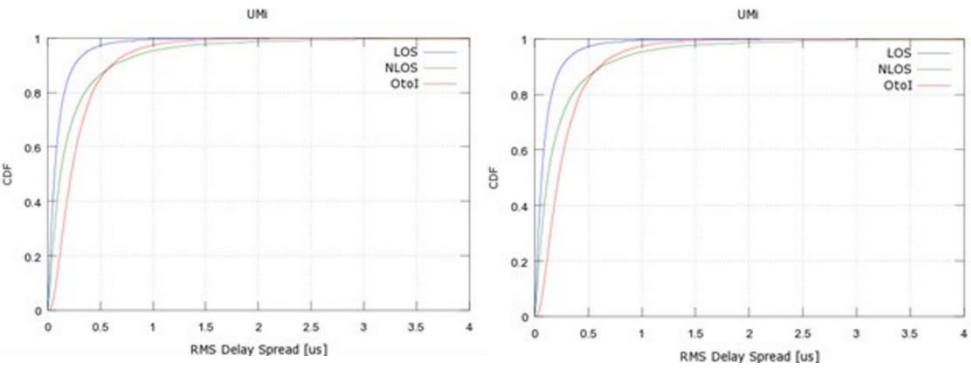
Model	Environment	1st break point	RMS Spreading delay	Max delay	# tap	#cluster	Doppler
A	Test (optional)	-	0nsec	0nsec	1	-	1.2km/h all tap
B	Residential	5m	15nsec	80nsec	9	2	1.2km/h all tap
C	Small office	5m	30nsec	200nsec	14	2	1.2km/h all tap
D	Typical office	10m	50nsec	390nsec	18	3	1.2km/h all tap
E	Indoor hotspot	20m	100nsec	730nsec	18	4	1.2km/h all tap
F	Large Indoor hotspot	30m	150nsec	1050nsec	18	6	40km/h for tap3

WLAN Indoor Channel Model

Outdoor Channel Model

Before 11ax, outdoor channel has not been in a big interest. The discussion on outdoor model (adopted from 3GPP/3GPP2) started in full-scale from 11ax. The amount of delay is relatively long compared to indoor model.

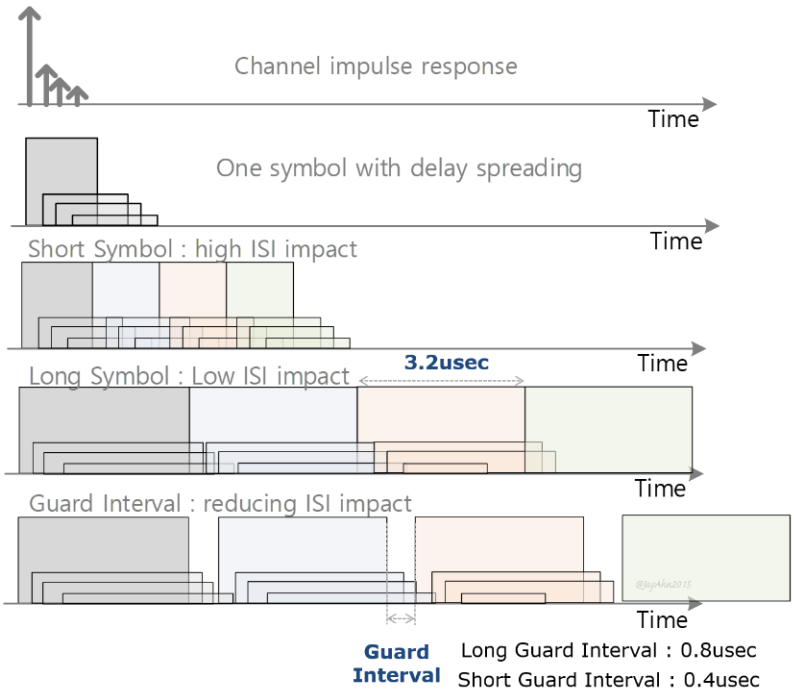
Channel Model	Scenario	Delay Spread (ns)
Urban Micro Channel (UMi)	LOS	65
	NLOS	129
	O-to-I	240
Urban Macro Channel (UMa)	LOS	93
	NLOS	363



WLAN Outdoor Channel Model

Impact on Multipath (ISI) and Guard Interval In WLAN

Multipath fading brings delay spread of the signal and this situation results in interference between symbols. In WLAN, guard interval is applied to prevent ISI (Inter-symbol interference)

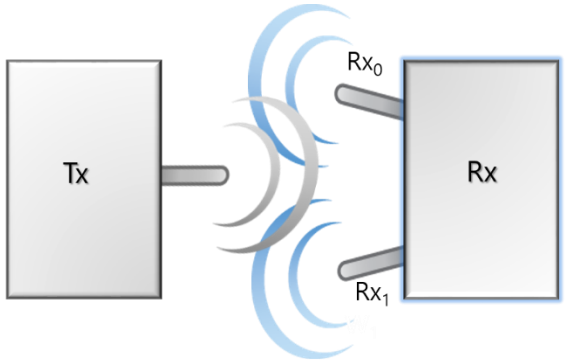


Impact from multipath (ISI) and Guard Interval in WLAN

Rx Diversity

Rx diversity overview

For Rx diversity, number of antenna in receiver should be two or more regardless of the number of antenna in transmitter to make use of space diversity (different position and direction of antenna) to get SNR gain. This is the traditional way of diversity in RF, as it demands the minimum cost and complexity compared to Tx diversity



For Rx diversity, Rx antenna should be 2 or more regardless of # of Tx antenna

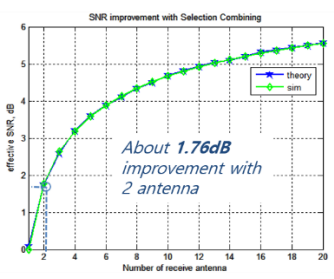
Type	Operation	Comparison
Selective Combining	Rx_0 **OR** Rx_1	Receiving both chains, while taking signal from one of antenna that has better SNR. About 1.76dB SNR gain with 2 ant BPSK in Fading/AWGN channel
Simple/Equal-Gain Combining	Rx_0 **AND** Rx_1	Simply combining signals from both antenna with equal gain About 2.5dB SNR gain with 2 ant BPSK in Fading/AWGN channel
MRC (maximum ratio combining)	Rx_0 (w_0) **AND** Rx_1 (w_1)	Combining signal with "weighting" according to signal status. Complex but Optimal. About 3dB SNR with 2 ant BPSK in Fading/AWGN channel

Rx Diversity overview

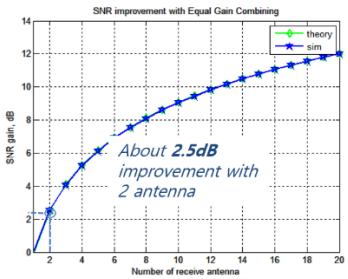
Selective, Equal-gain and MRC

Maximum Ratio Combining (MRC) is the optimum solution for Rx diversity, while selective and equal-gain (simple) combining are in use together in WLAN solutions.

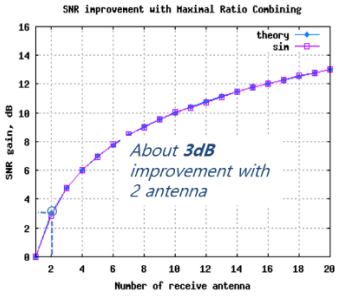
Selective Combining



Equal-Gain Combining



MRC

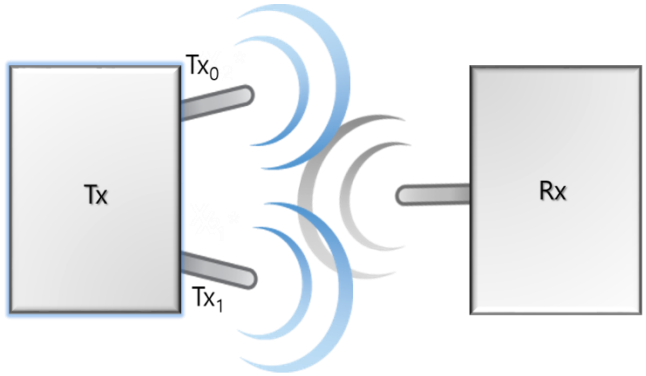


Rx Diversity Gain for BPSK in AWGN and Fading Channel (reference : www.dsplog.com)

Tx Diversity : Selective Tx

Tx diversity overview

For Tx diversity, the number of antenna in transmitter should be two or more regardless of the number of receiver antenna. In most of the cases, the purpose is to get SNR gain.



For Tx diversity, Tx antenna should be 2 or more regardless of # of Rx antenna

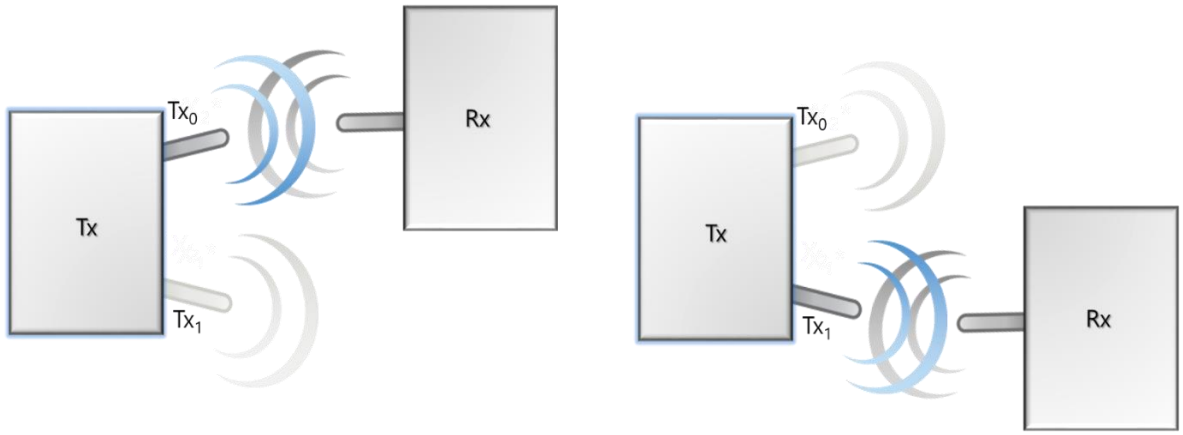
Type	Operation	Comparison
Selective Combining	Tx_0 **OR** Tx_1	Based on decision from Rx signal on each antenna, signal is transmitted only from one better antenna
Simple Combining	Tx_0 **AND** Tx_1	Same signal is transmitted from two antenna. CSD (Cyclic Shift Diversity) can be applied.
STBC	Alamouti Coding	SNR gain without data rate drop (Coding Rate = 1)
Beamforming	Implicit Beamforming Explicit Beamforming	SNR gain with steering angles (amplitude and phase) of each antenna

Tx Diversity overview

Selective Tx

Selective Tx is to transmit the signal from one of the multiple antenna not using both antenna at the same time.

- Operations
  - Each antenna has its own pattern and direction, and one of two antenna is supposed to be better than another according to the relative situation with the receiver
  - Transmitter chooses one better antenna. Decision for antenna choice can be made based on the received signal; if Rx signal is better in one antenna, Tx might be better, as RF is reciprocal
- Pros
  - Device's TRP (Total Radiated Power) can be increased with the improvement of overall antenna pattern of a deivce.
  - One PA (Power Amp) consumes hundreds of currents which is about 10 times of Rx current. No need to turn on both PAs like in simultaneous Tx or CSD.
  - If symbol duration is very short like 11b (90nsec), CSD cannot be applied and the selective Tx is good solution utilizing multiple antenna
- Cons
  - Device requires two Tx chains; chipset-support, PA, RF components. It will be costly to have it only for the selective Tx. When the device has two or more Tx chains for MIMO support, it can utilize it in legacy mode or when MIMO is not in use.



Selective Tx

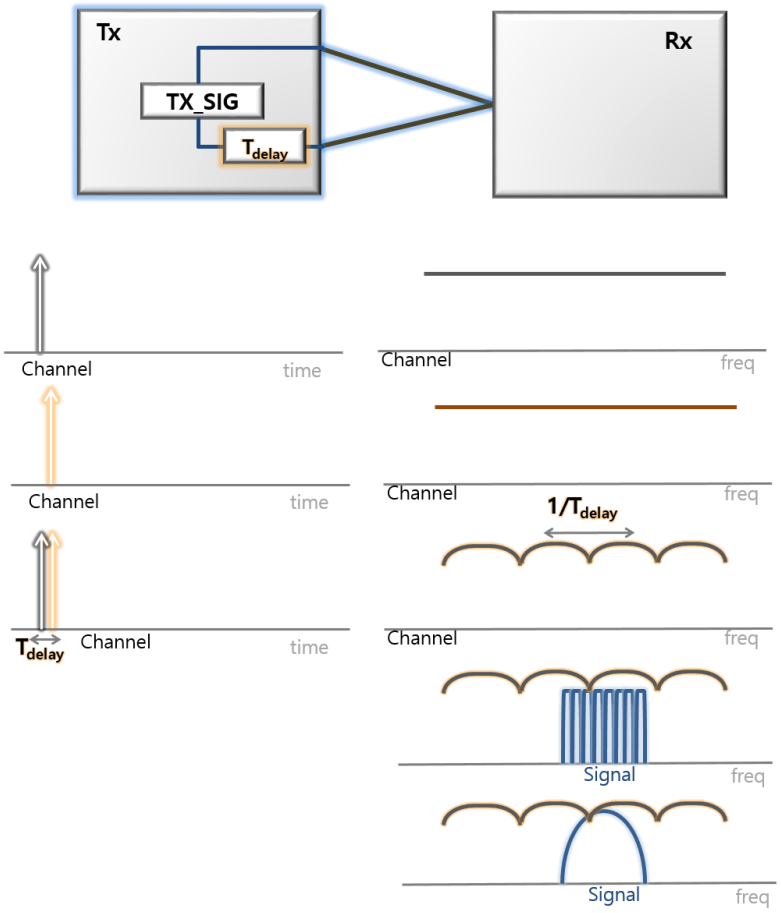
Tx Diversity : CSD

CSD is a complicated process to analyze. Let's check one by one with the various situations to see how CSD is working in WLAN.

When an identical signal from two chains are combined with the conductive cable

Combining the signals is the complicated process. If two signals are exactly same in shape and timing, it is perfectly correlated and the power of the combined signal gets double and SNR to be double. (Background thermal noise has no correlation between them and cannot be added each other)

OFDM symbols combined from two chain might be OK, as it has long symbol duration, while the fast changing 11b symbol might be distorted or be fluctuating

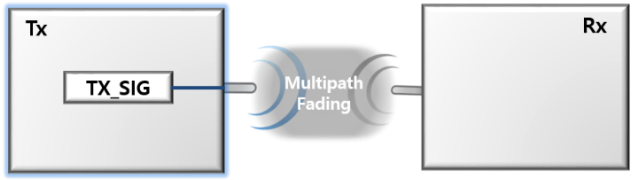


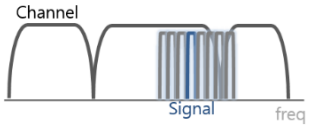
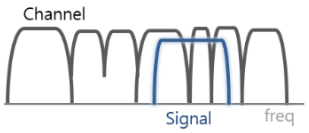
Path		Result
Exactly Same (ideal) Path_1 and Path_2 are same conductive cable and PCB line inside device is exactly same		Received signal is 2x Tx_Sig
Path_1 and Path_2 is conductive (like cable) and the difference between two cable is little. PCB line inside device is almost same.	**Tx Signal with Long Symbol duration like OFDM**	Received signal is 2x Tx_Sig. Sub-carrier (symbol) does not experience frequency selective fading
	Tx Signal with Short Symbol duration like 11b	Wide bandwidth signal experience frequency selective fading. Combined signal can fluctuating

WLAN Signal with cabled setup

Single Stream signal in multipath fading

When the fast changing signal experiences long delay spread (Delay Spread > Symbol Duration), it is under the frequency selective fading (frequency domain) and there can be the interference between the symbols (time domain). If the symbol duration is long as OFDM, the signal is under flat fading and generally it only has an impact on SNR.

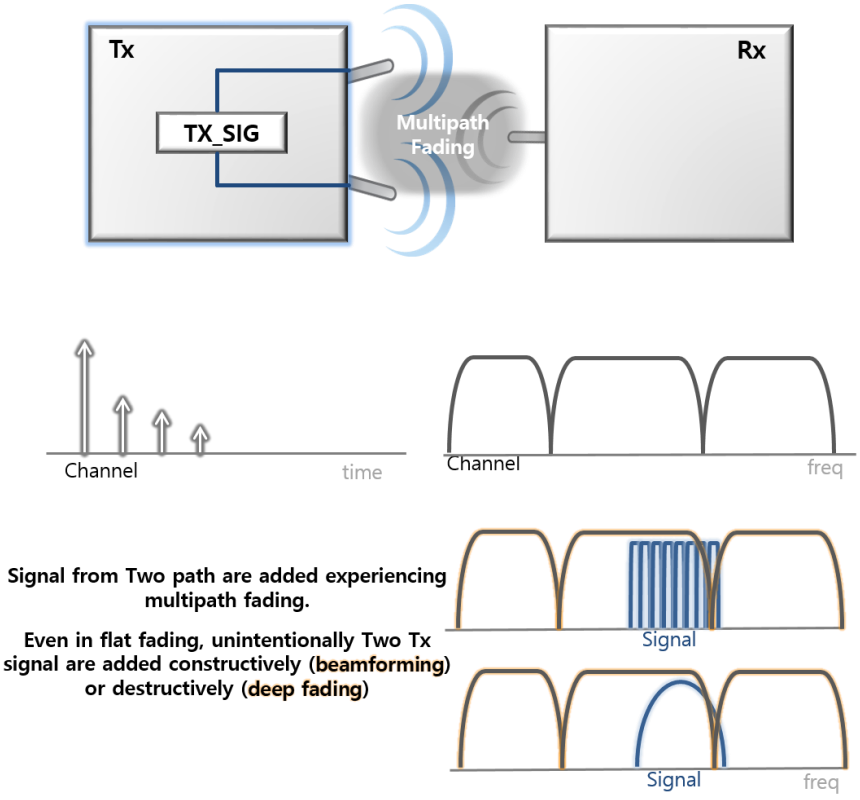


Condition	Result	Freq Response
Delay Spread < Symbol duration	Considered to be flat fading channel generally with the impact on SNR. *OFDM is assembly of subcarriers with long period*	
Delay Spread > symbol duration	Time perspective : Signal is delay-spread and two consecutive symbols interferes each other (ISI) Frequency perspective : Frequency selective fading. Some frequency component in signal experiences deep fading	

Single Stream Signal in multipath fading

Two identical Signals transmitted from multiple antenna in multipath fading

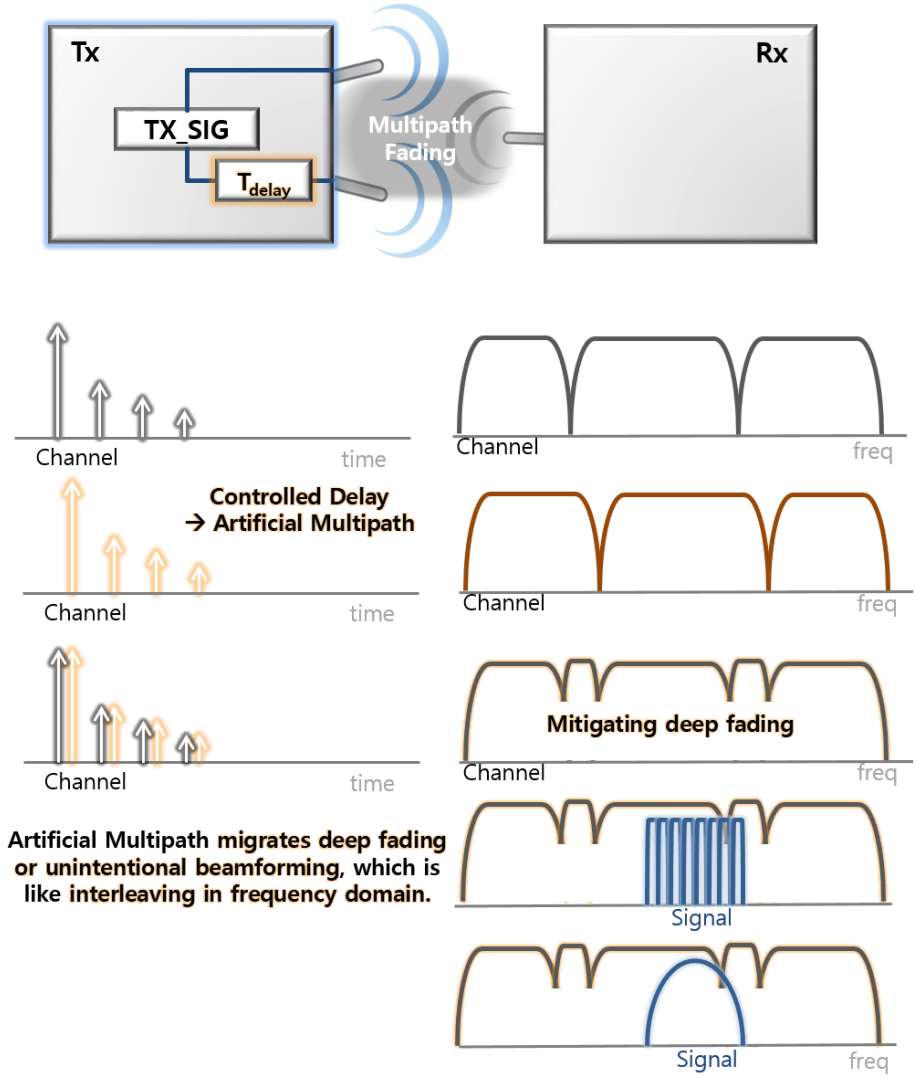
Multi-Antenna signals in multipath both experience fading and added at the receiver. Even in flat fading, they are unintentionally added constructively or destructively.



Multi-Signals in multipath fading

Delay Diversity (DD)

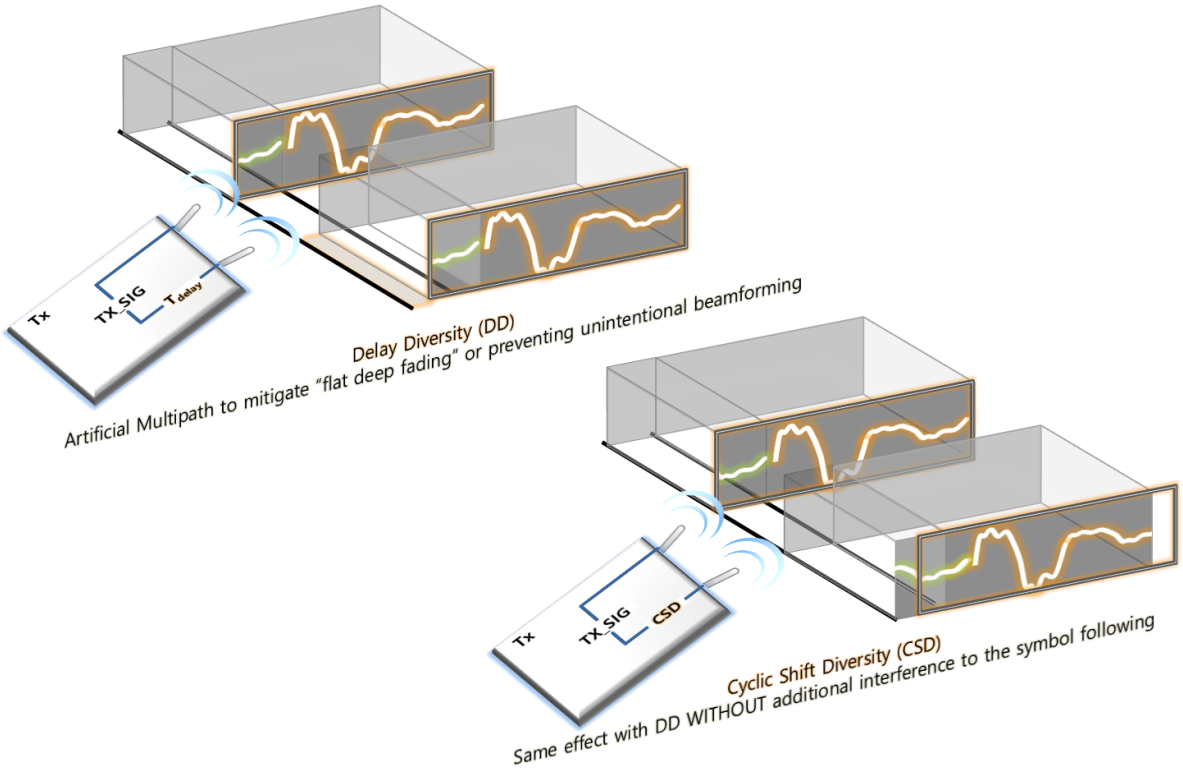
If a signal of one chain has a controlled delay to another chain, it will make an artificial delay that mitigates unintentional beamforming or deep fading, which scheme is called as delay diversity (DD)



Delay Diversity (DD) in multipath fading

Cyclic Shift Diversity (CSD)

Cyclic Delay Diversity (CDD) is called as CSD in WLAN to have a same effect on DD and an artificial delay in DD makes a kind of frequency interleaving situation. In WLAN, as OFDM symbol is periodic, the last part of the symbol in one chain is copied to the first to have delay diversity effect.



Delay Diversity (DD) and Cyclic Shift Delay (CSD)

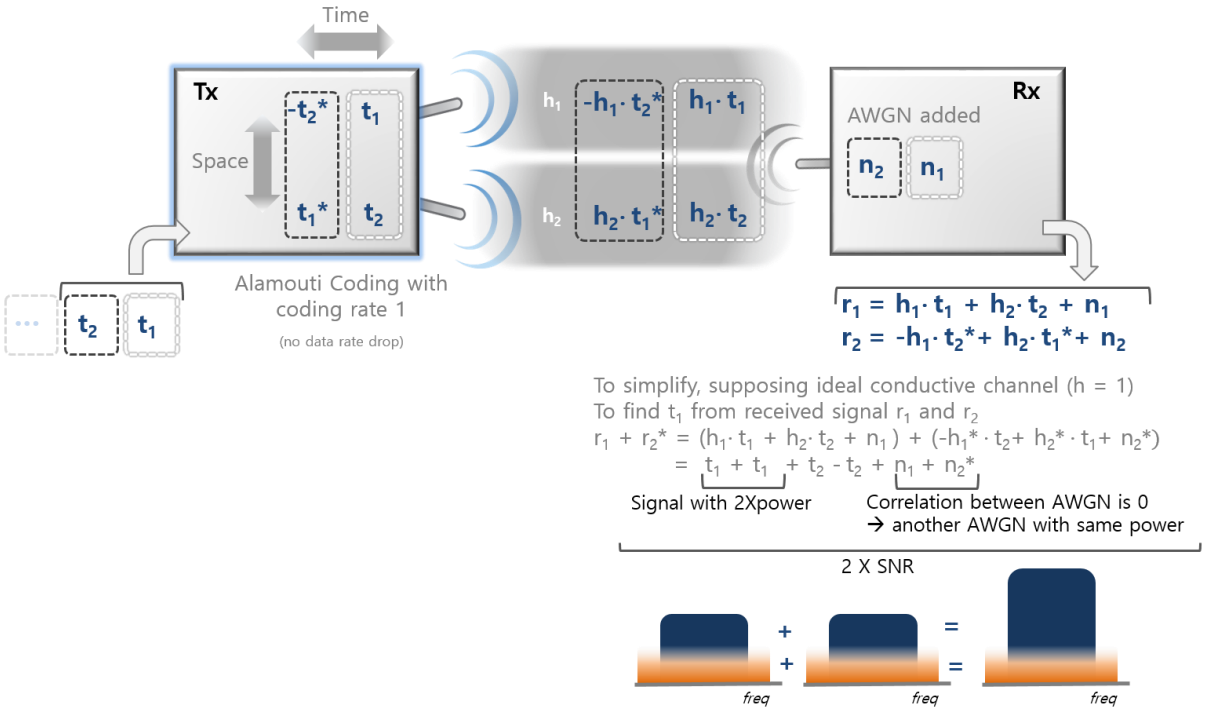
Tx Diversity : STBC

STBC

Space Time Block Coding is a kind of block coding scheme to enhance SNR. It is Tx diversity scheme with multiple antenna in transmitter and works regardless of the number of receiver antenna.

From two antenna (Space) at two times (Time), two symbols (Block) are transmitted. and it is the only coding scheme (Alamouti code) with coding rate “1”, which means there is no data rate drop with coding.

To understand STBC concept in a simple way, suppose that two paths are combined with ideal cable. The transmitted signal can be found with the amplitude of two, while noise power is the same, as the power of commbined AWGN is same.

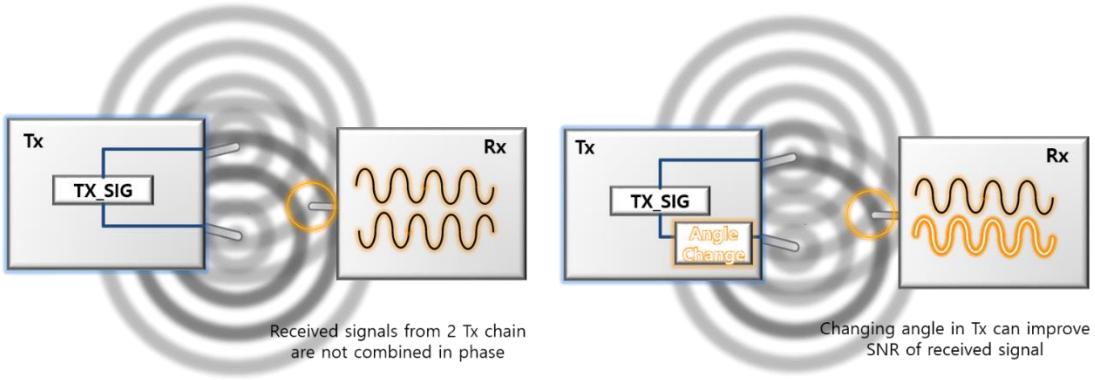


STBC

Tx Diversity : Beamforming

Beamforming Concept

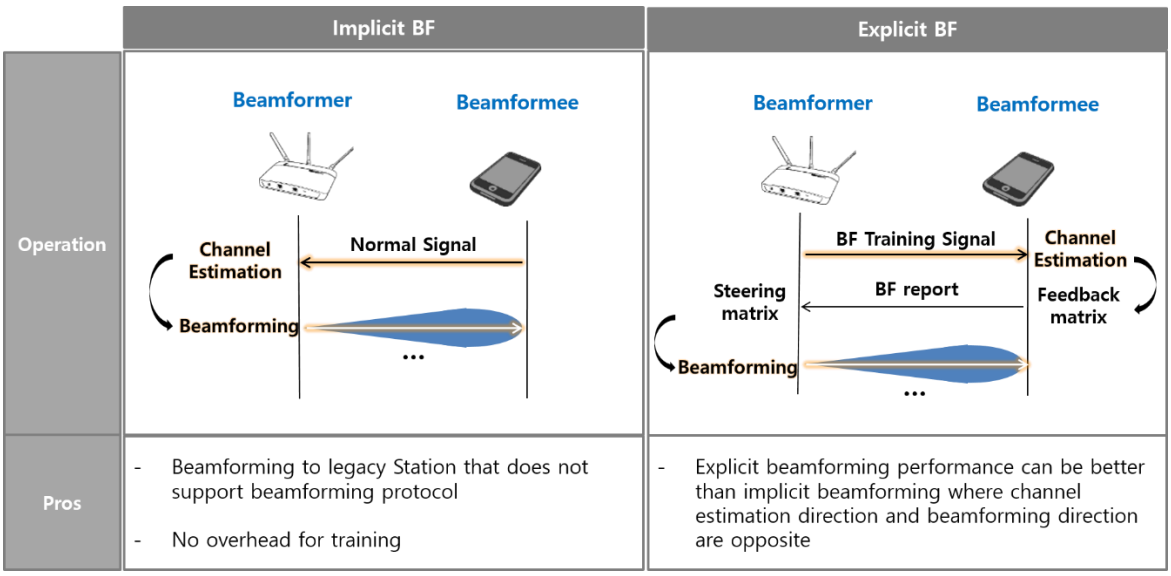
At receiver side, the one signals transmitted from two transmitter's antenna can be added constructively or destructively according to the position. The way to control this situation and to make the signals to be added to have SNR gain is by tuning an angle (phase and amplitude) from each Tx antenna, as far as the transmitter can figure out the changes that happen in the channel between the transmitter and the receiver. (Channel Status Information. CSI)



Basic Concept on Beamforming

Explicit and Implicit Beamforming

Depending on the method how to get the channel status information, there are two kinds of beamforming; Implicit and Explicit, which both are used in WLAN. Implicit beamforming gets channel information from the received signal, as RF is supposed to be reciprocal, while explicit beamforming runs "Sounding process" to get the channel information.

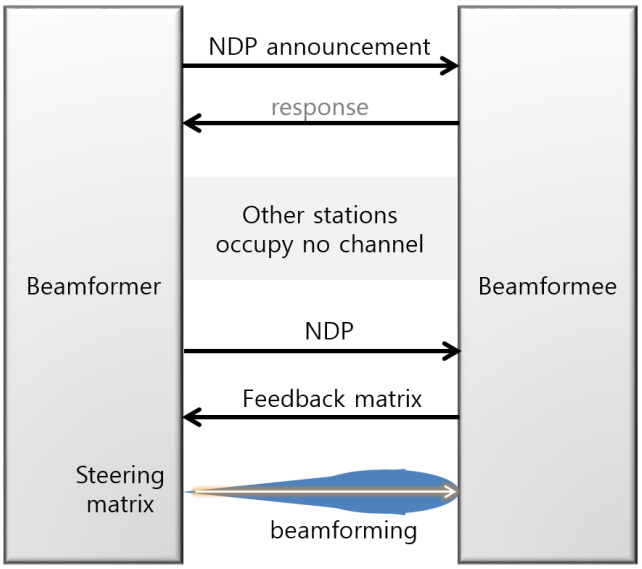


Sounding Process in Explicit Beamforming

Beamformer (STA who is beamforming) sends Null-Data packet (NDP) which only have PHY header, and beamformee (STA who is beamformed) gives back a feedback matrix after calculation. Beamformer steers beamforming with the information.

The sounding process requires time depending on the size of feedback matrix. The size of Feedback matrix increases, as the number of subcarriers increase and beamforming demands a lot of calculation. At the same time, as all the stations need to be in silence mode while in sounding process, the network overhead from the explicit beamforming is high.

- Example of Single-user 2×2 MIMO @ 20 MHz, low resolution
- 52 subcarriers x 2 angles/subcarrier x 6 bits/angle = 624 bits or 78 bytes.



Explicit Beamforming Sounding Process

MIMO

MIMO Concept

If two pairs of stations can exchange each stream (picture left) in one channel, one pair of stations can exchange two streams (picture right), which is MIMO (Multi-Input Multi-Output).

Different from Tx or Rx diversity, the number of antenna of both transmitter and receiver side should be same of higher than the number of stream. For example of 2 stream MIMO, transmitter should have more than two antenna and receiver also needs more than two.

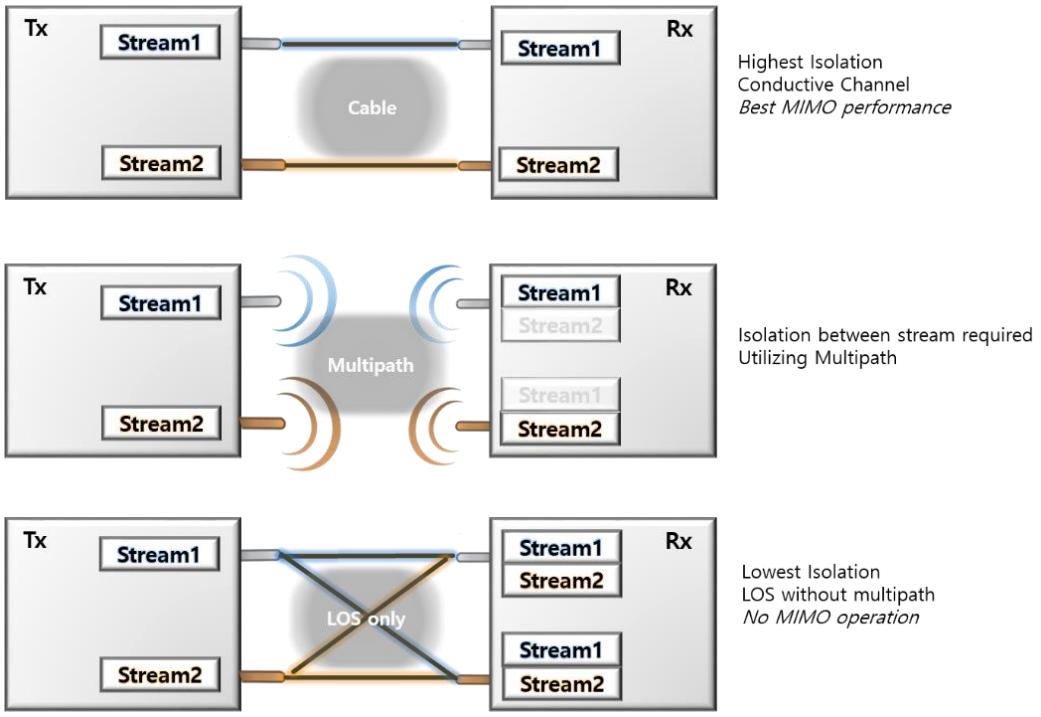
MIMO can be called as “Spatial MIMO”, as it uses spatial (multipath) diversity and it is also called as SU-MIMO (Single-user MIMO) compared to MU-MIMO (Multi-user MIMO)

Basic Concept of Spatial MIMO

Three Cases on MIMO Channel

To get a sense of how MIMO operates in a channel, comparing three different channel conditions below will be helpful.

- MIMO performance is the best, when the isolation between streams is highest. Cabling setup is the case and it can be used to find out the best throughput ruling out antenna isolation or wireless channel issue.
- MIMO utilized the richness of multipath. Antenna isolation should be secured to guarantee MIMO performance testing in the wireless channel.
- When one receiver antenna gets both stream with the same amount, MIMO cannot work properly. LOS (Line of Sight) situation without multipath is this case.



3 Cases of MIMO channel situation

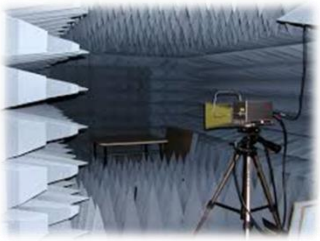
Three Cases on MIMO test environment

MIMO performance (throughput) test requires multipath along with high antenna isolation

- Reverberation chamber (shield room) has too many reflected signals and stable MIMO throughput can be hardly measured. Measured performance could be too sensitive and changing by position
- Anechoic chamber has only LOS signal without multipath. No MIMO performance is expected.
- Real office might be rather a good situation to measure MIMO, while it is hard to find out real value because of uncontrollable interferences from other Wi-Fi devices.

Shield Room(Reverberation chamber)

Too many & strong reflected signals
Too sensitive by position



Anechoic Chamber

Line Of Sight only
without multipath

Office

Real multipath environment,
but uncontrollable interference

No MIMO TPUT performance !
Not repeatable result !
➔ MIMO TPUT test requires multipath as well as shielding from interference

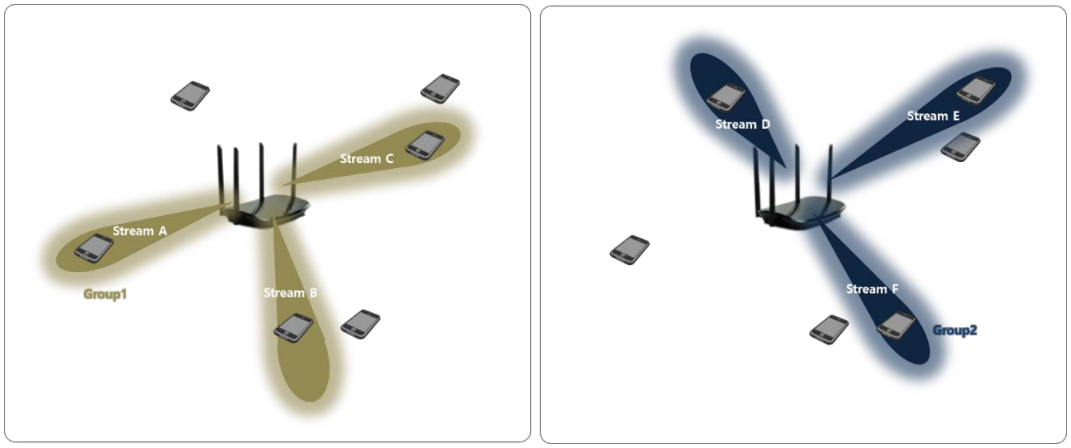
Challenge on wireless Channel in MIMO TPUT test

To get a reasonable MIMO test result, both multi-path and shielding are required. Blocking the interference with shield room or box and the proper amount of absorber on the wall inside might be one of the test condition.

MU-MIMO

MU-MIMO

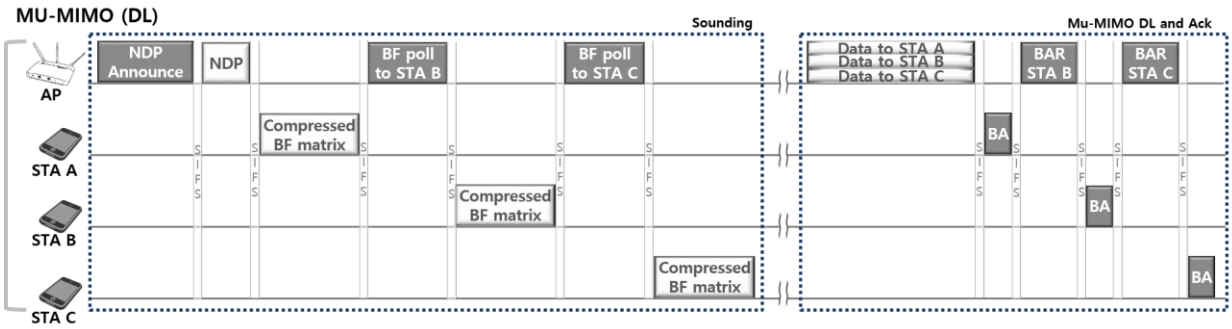
In MU-MIMO (Multi-user MIMO), AP transmits stream to different users (Group) at the same time using an isolated antenna pattern with beamforming and it is also called as "beamforming MIMO". Downlink (from AP to non-AP station) MU-MIMO is defined in 11ac and UP MU-MIMO is introduced in 11ax. Find *MU Operation & Downlink* chapter.



MU-MIMO packet flow example

Until 11ac, only downlink MU-MIMO is defined and 11ax defines uplink MU-MIMO with the introduction of trigger frame. Like Explicit Beamforming, MU-MIMO has sounding process (training) to get the channel state information to compute a steering matrix that is applied to the transmitted signal to optimize reception at receivers. From 11be (after 11ax), WLAN is supposed to run MU-MIMO with implicit way as well.

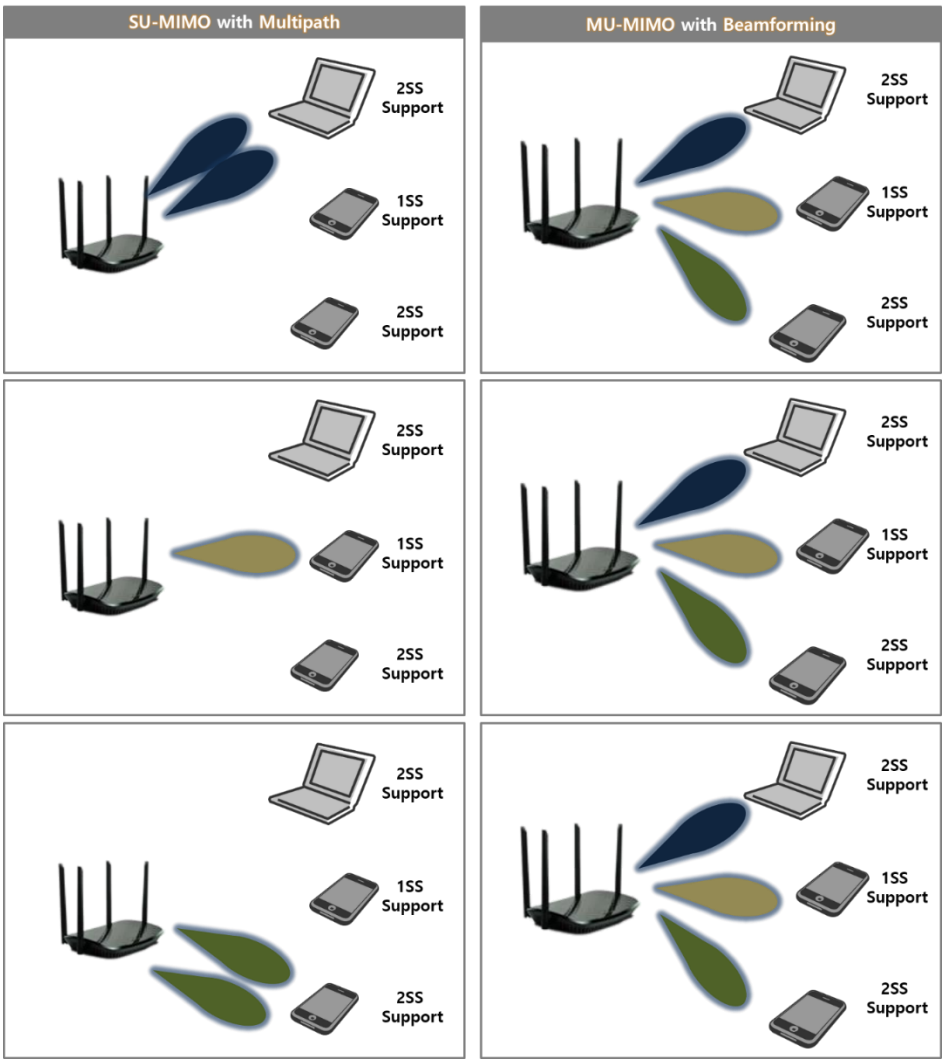
AP requests Ack (BlockAck Request) to STAs of MU-MIMO reception and gets Ack one by one, as STAs cannot send Ack packet together in MU-MIMO uplink. In 11ax, MU-ACK are defined.



MU-MIMO Procedure

SU-MIMO and MU-MIMO

Both SU-MIMO (spatial MIMO) and MU-MIMO (beamforming MIMO) are using multiple stream, while SU-MIMO is for one STA and MU-MIMO is for multiple STAs. Considering the situation that the normal non-AP STAs have only one or two antenna, MU-MIMO can be said to improve efficiency of the channel.



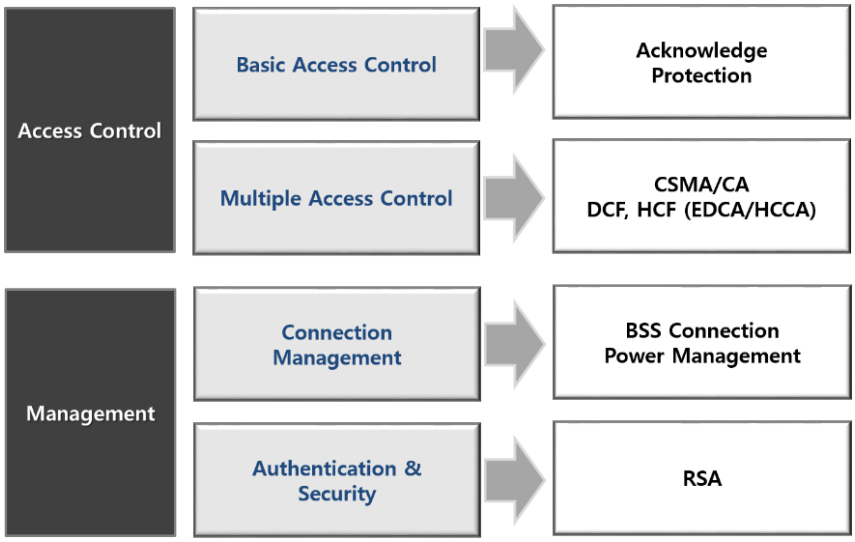
MU-MIMO Pros	MU-MIMO Cons
• Efficient spectrum utilization • In case that AP support 4 stream and STA only support single stream, (SU) MIMO cannot utilize AP's multi stream capability • In the example above, MU-MIMO sent 9 stream (1 stream X 3 STA X 3 times), while (SU) MIMO sent 5 stream (2 stream + 1 stream + 2 stream for each STA in 3 times)	• training overhead for beamforming (channel occupation) • additional signal processing

MU-MIMO Pros and Cons

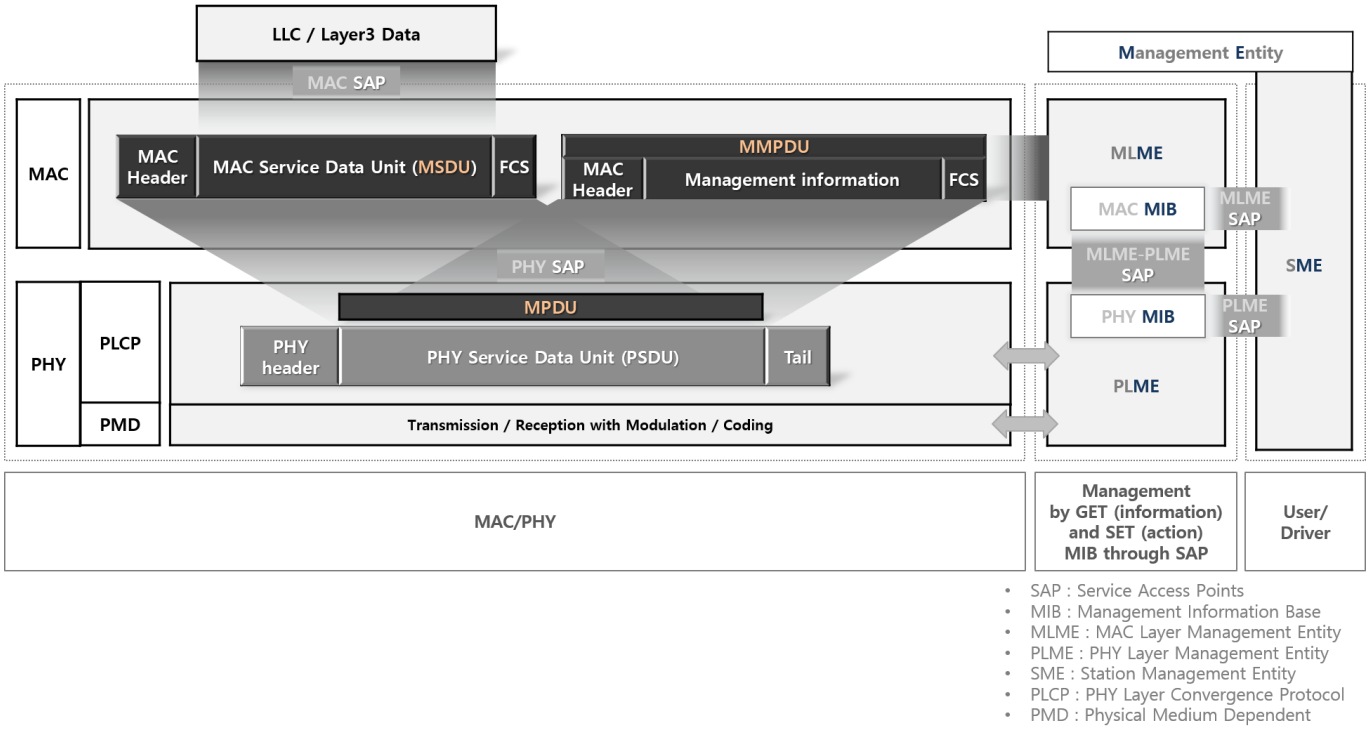
MAC

MAC Layer Overview

Along with the basic function of delivering upper layer (LLC) payload to lower layer (PHY) and vice versa, MAC layer's functions are "Access Control" and "Management"



MSDU contains the payload of upper layer data. For management functions of MAC, management information in MIB are delivered and in action contained in MMPDU through MLME. MPDU with MSDU or MMPDU is the payload of PPDU as PSDU in PHY layer.



- SAP : Service Access Points
- MIB : Management Information Base
- MLME : MAC Layer Management Entity
- PLME : PHY Layer Management Entity
- SME : Station Management Entity
- PLCP : PHY Layer Convergence Protocol
- PMD : Physical Medium Dependent

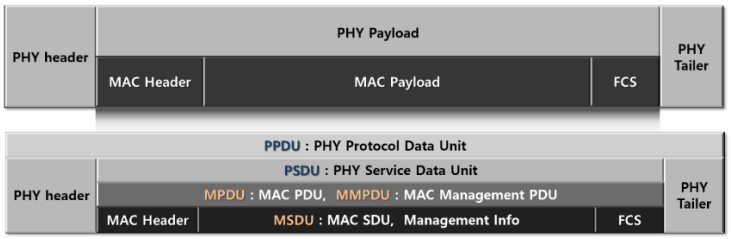
MIB and SAP in MLME,PLME,

Frame Structure and Functions

MAC frame

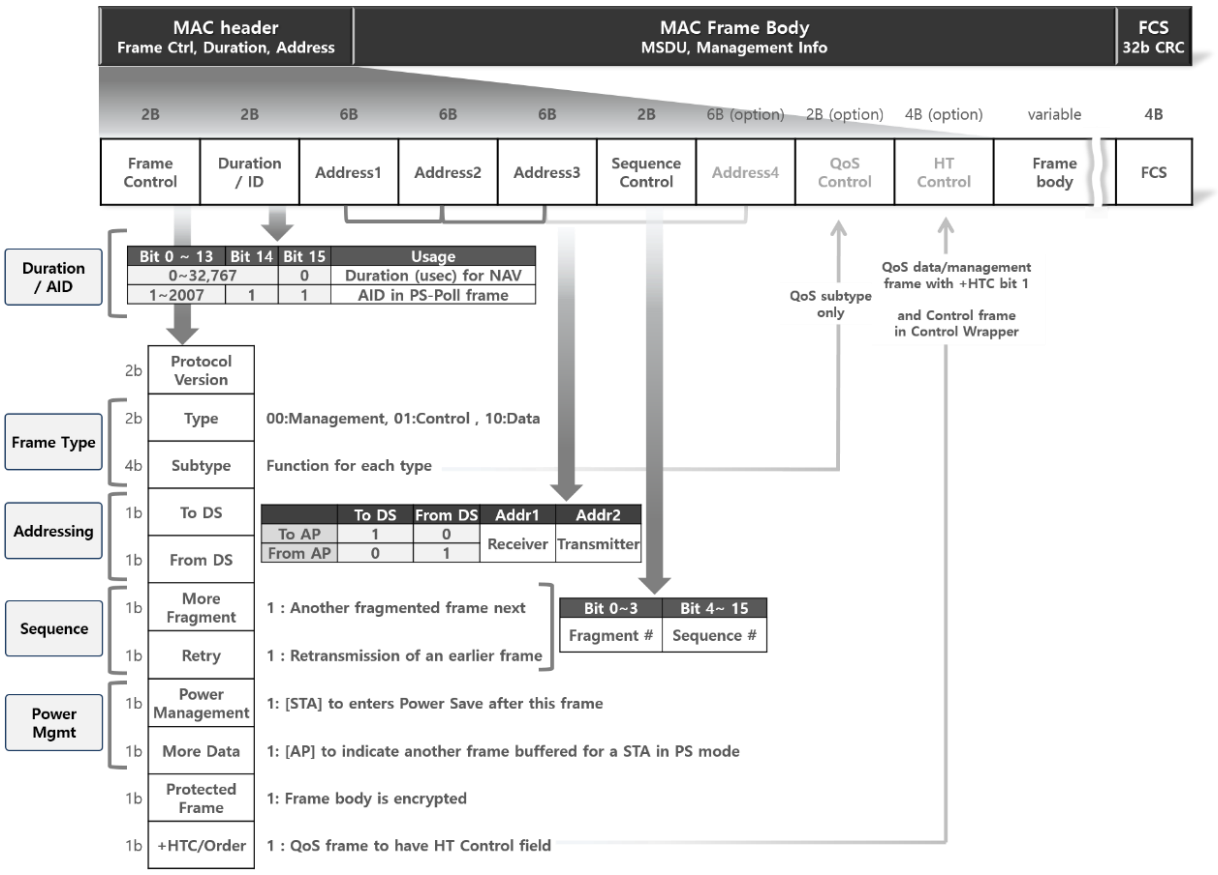
MAC frame consists of Header, Frame body and FCS.

- MPDU : MAC Protocol Data Unit = MAC frame
- MSDU : MAC Service Data Unit = Information that is delivered between MAC SAP, data from upper layer
- MMPDU : MAC Management Protocol Data Unit = MAC management protocol



MAC Header

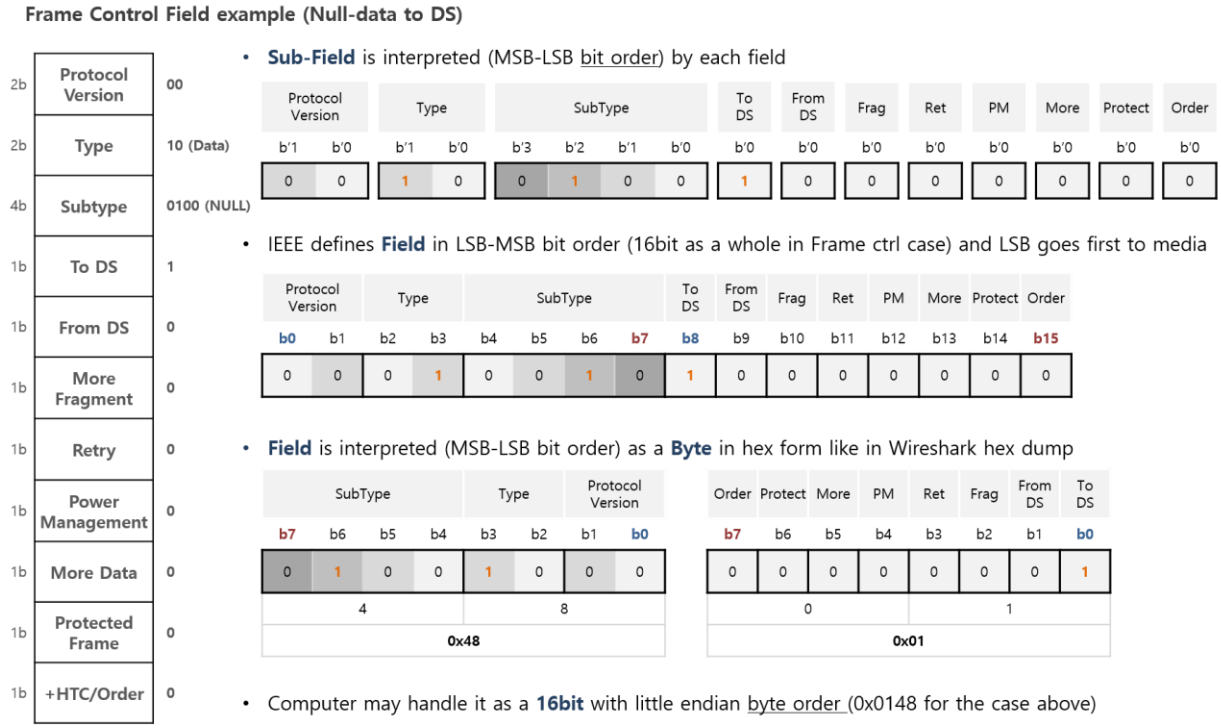
MAC Header contains Frame control (type, direction, PM,…), Duration, Address, Sequence number, and others.



How to read MAC header

Engineers may have chances to read MAC header values expressed as a Byte (4bit) in hex form (8bit) like in Wireshark, while IEEE defines the fields in LSB-MSB bit order as a whole (16bit for header) and each subfield is written and interpreted by each field.

Normally, human read the values MSB-LSB bit order by each unit, while machine defines and reads in LSB-MSB order.



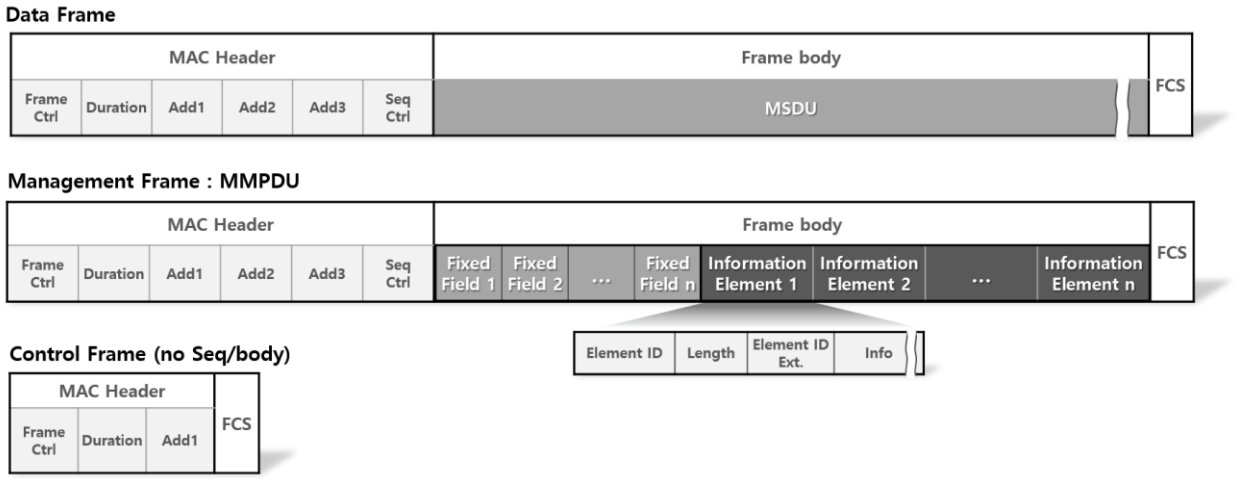
MAC frame bit order

Frame Type

Three Types of Frames

Basic forms for frames of each type (data/mgmt/control) are below with some variations according to subtype and functions.

- Data frame : MSDU as frame body
- Management frame : frame body consists of numbers of “fields that are not element : no-element field” and numbers of “element : Information Elements (IE)” fields
  - No element fields : fixed item and format to each management subframe type. (ex) Beacon Interval, AID, QoS Info,…
  - IE : general format of Element ID, Length, Ext, and information. (ex) TIM IE : ID # 5, HT Operation IE : ID # 61, …
- Control frame : No frame body and No sequence subfield in header. Address is simple as well



Frame Type : Data, Management and Control Frame

Management frame

Beacon, Probe, Authentication, Association, Action, ···

Type	SubType		Subtype bit	Description
Management (00)	Beacon		1000	• AP broadcasts AP info (SSID, regulatory, capability, supported rate, etc) in time base • Used for connection, time synchronization, power management in BSS
	Probe	Request Response	0100 0101	• STA broadcast request to gather the information of APs around • AP to response with AP info (almost same with the information in Beacon)
	Authentication	Authentication	1011	• For (non-AP) STA to be identified by AP • Exchanged between STA and AP (first requested by STA with Auth. Seq# 1)
		Deauthentication	1100	• Out of authentication state
	Association	Request Response	0000 0001	• For STA to request to association AP sharing its information (capability) • AP responses to STA for approval of association
		Reassociation Request Reassociation Response	0010 0011	• For STA to move a current association from one AP to another • Or to change attributes of the current association
		Disassociation	1010	• Out of association state
	Action	Action Action No Ack	1101 1110	• For various actions related to Spectrum management, QoS, DLS, Block Ack, Radio measurement, Vendor-specific, Public, FT, SA, HT/VHT, TDLS, WNM, Mesh, etc
	Timing Advertisement		0110	• Timing Synchronization Function (TSF) for IBSS (Ad-hoc) • TSF is in Beacon, Probe response as well for BSS
	ATIM		1001	• Announcement TIM for Power Save in IBSS, as no AP to send TIM or DTIM

Control frame

Ack, BlockAck, RTS/CTS, PS-Poll, ···

Type	SubType		Subtype bit	Description
Control (01)	Ack		1101	• Positive response to unicast Data and Management frame as well as to control frames like BA, PS-poll in some cases
	Block Ack	BlockAckReq BlockAck	1000 1001	• BAR : To request BA after sending series of QoS frame • BA : Ack to Series of QoS frames requesting BA
	RTS CTS		1011 1101	• To protect and secure channel for a while by exchanging RTS/CTS between two STA
	PS-Poll		1010	• Sleeping STA wakes up to ask buffered data in AP
	Beamforming	VHT NDP announcement	0101	• Beamformer broadcasts the start of BF sounding with this frame followed by NDP.
		RF Report Poll	0100	• In VHT beamforming sounding protocol with more than one beamformee, beamformer requests (polls) reports to each beamformee after sending NDP.
	Control ext.	Control Wrapper	0111	• Carrying control frame with HT control field. • Control frame with +HTC implies it is wrapped in this frame. (ex. RTS+HTC)
		Control Frame Extension	0110	• To increase control subtype by re-using b8~b11.
	Contention Free	CF-END CF-END+CF-ACK	1110 1111	• To indicate the end of Dual-CTS, CF in PCF and TXOP in HCF

Data frame

QoS and non-QoS data, Null data,…

Type	SubType		Subtype bit	Description
Data (10)	Data (non-QoS)		0000	• Normal Data (without QoS)
	NULL (no data)		0100	• To utilize MAC header especially to enter PS mode with Power Management setting
	QoS Data		1000	• Data with QoS control field
	QoS NULL (no data)		1100	• Mainly to utilize QoS Control field like PS mode and Ack policy
	CF data For PCF	Data +CF-Ack Data +CF-Poll Data +CF-Ack +CF-Poll CF-Ack (no data) CF-Poll (no data) CF-Ack +CF-Poll (no data)	0001 0010 0011 0101 0110 0111	• *Obsolete with PCF*
	CF data For HCF	Data +CF-Ack Data +CF-Poll Data +CF-Ack +CF-Poll CF-Null (no data) CF-Poll (no data) CF-Ack +CF-Poll (no data	1001 1010 1011 1100 1110 1111	• For HCCA for HCF

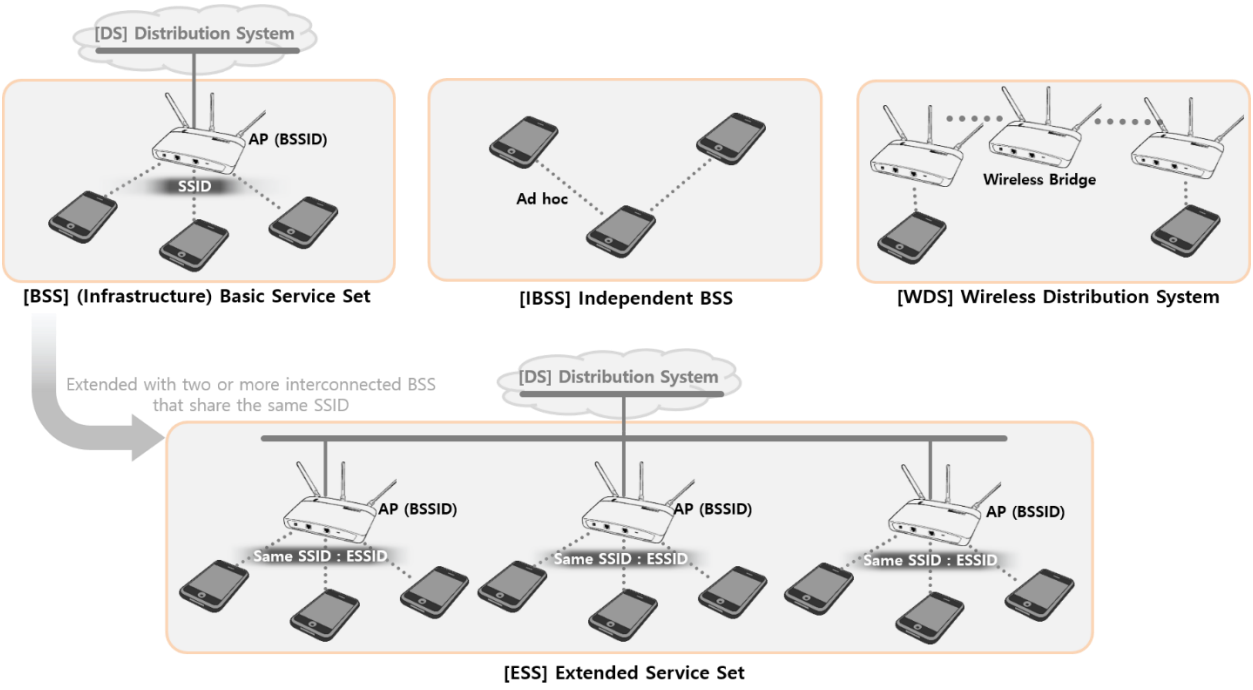
Service Set and Address

Service Set (SS)

BSS consists of a single AP along with non-AP STAs associated in infrastructure mode. This book mostly focus on BSS among BSS, IBSS, ESS and WDS.

- BSSID : The identifier of BSS (BSSID) is MAC address of AP, which is unique number. BSSID is the formal name of BSS.
  - (ex) 00:12:34:67:89:90
- SSID : human readable ID string of BSS with 0~32byte.
  - (ex) MyHomeAP
- ESSID (Extended SSID) : one SSID shared between APs in ESS

Intra-BSS is the BSS where a STA is associated and Iter-BSS is other BSS than Intra-BSS. Overlapped BSS (OBSS) is one of Inter-BSS next to Intra-BSS where RF is overlapped. This concept is handled more in 11ax. Find *Spatial Reuse & BSS Color* chapter



Service Set (BSS, IBSS, WDS, ESS)

Basic rules on Addressing

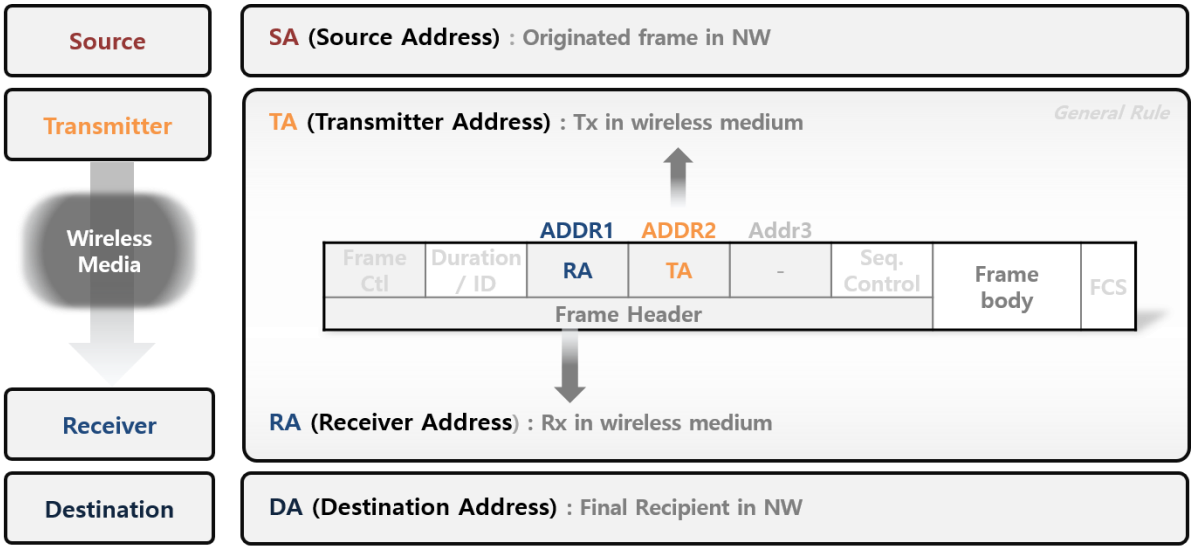
Basic rule of addressing in MAC header

- ADD1 (the first address field) : RA (receiver address) for receiver of wireless media
- ADD2 (the second address field) : TA (transmitter address) for transmitter of wireless media

SA (Source Address) is for Originator and DA (Destination Address) is for the final Recipient in network. AP address is BSSID and for non-AP STA in BSS, SA is TA and RA is DA, as they are the final terminals generally.

- AP : BSSID = TA or RA
- non-AP STA : TA=SA, RA=DA

DS can be regarded as AP. To DS is to AP from STA and From DS is to STA from AP



To DS	From DS	Service Set		ADDR1	ADDR2	ADDR3	ADDR4
0	0	IBSS	STA <> STA	RA / DA	TA / SA	BSSID	Not Used
1	0	BSS	AP << STA	RA / BSSID	TA / SA	DA	Not Used
0	1		STA << AP	RA / DA	TA / BSSID	SA	Not Used
1	1	WDS	AP <> AP	RA	TA	DA	SA

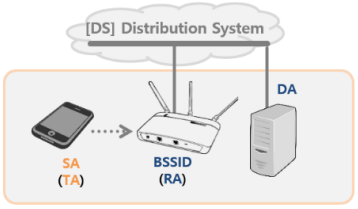
Access Point
- TA = BSSID
- RA = BSSID

STA (non-AP Wireless Client Station)
- TA = SA (Transmitter is Source)
- RA = DA (Receiver is Destination)

General Rule on Addressing in MAC frame

Service Set and Addressing

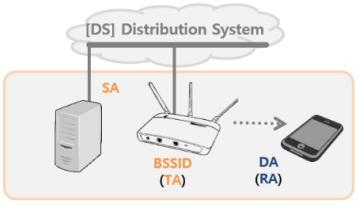
ADD3 and ADD4 depend on SS. Only Wireless Bridge case (WDS) has ADD4.



[BSS] (Infrastructure) Basic Service Set

To DS (AP<STA)

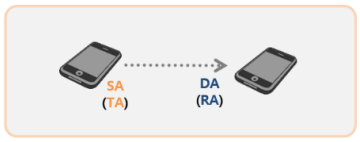
Frame Ctl		Addr1	Addr2	Addr3			
To DS 1 From DS 0	Duration / ID	BSSID (RA)	SA (TA)	DA	Seq. Control	Frame body	FCS



[BSS] (Infrastructure) Basic Service Set

From DS (STA<AP)

Frame Ctl		Addr1	Addr2	Addr3			
To DS 0 From DS 1	Duration / ID	DA (RA)	BSSID (TA)	SA	Seq. Control	Frame body	FCS

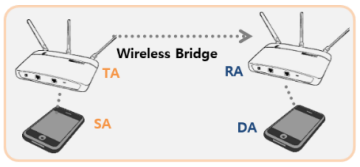


[IBSS] Independent BSS

IBSS

Frame Ctl		Addr1	Addr2	Addr3			
To DS 0 From DS 0	Duration / ID	DA (RA)	SA (TA)	BSSID	Seq. Control	Frame body	FCS

BSSID : for filtering, Random MAC with Universal/Local bit to 1



[WDS] Wireless Distribution System

Wireless Bridge

Frame Ctl		Addr1	Addr2	Addr3		Addr4		
To DS 1 From DS 1	Duration / ID	RA	TA	DA	Seq. Control	SA	Frame body	FCS

Address Field in MAC Header

MAC Address

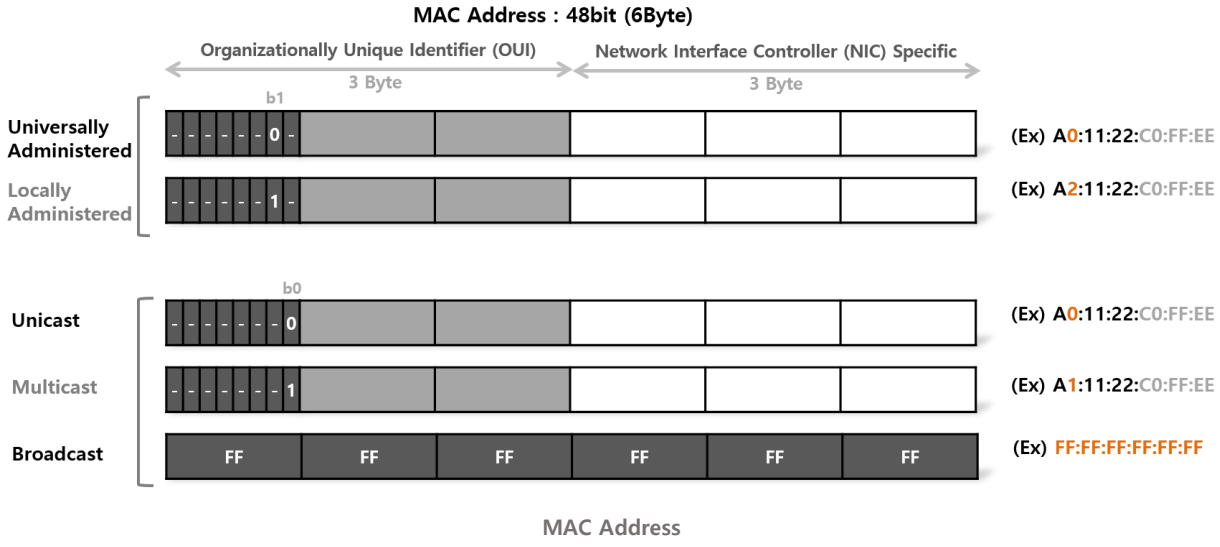
Every WLAN Device has its own unique address. MAC Address is 48bit (6byte) address that consists of OUI and NIC Specific. IEEE specifies it as EUI-48.

Universally and Locally Administrated MAC

- Universally administrated MAC
  - Consists of OUI and NIC Specific
  - Organisationally Unique ID : Vendor ID. Only for Universally Administered MAC
    - OUI registration : IEEE SA Registration Authority
    - OUI list : http://standards-oui.ieee.org/oui/oui.tx
  - Network Interface Controller Specific : Device ID
- Locally administrated MAC
  - Assigned to a device by a network administrator, overriding the burned-in address. The second-least-significant bit of the first octet of the address is 1

Unicast and Broadcast

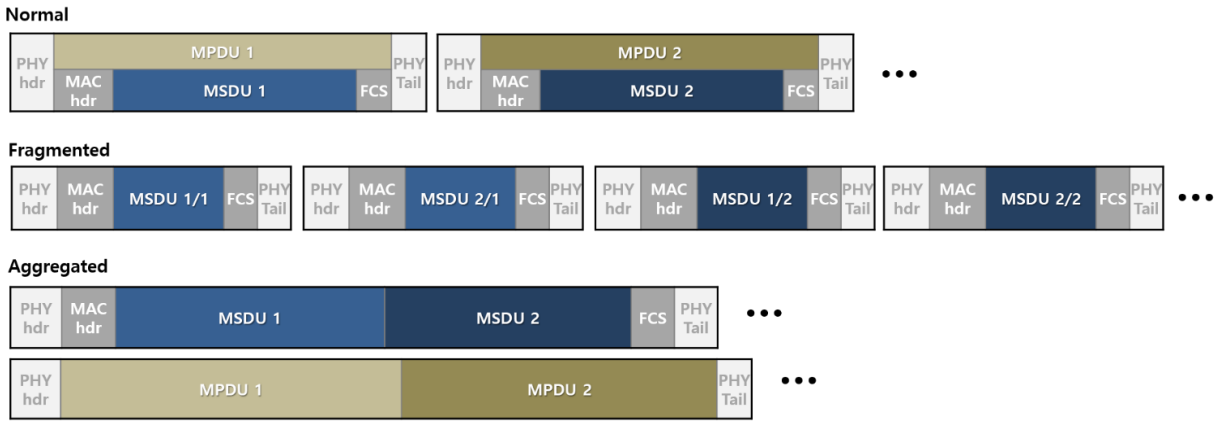
- Unicast MAC : targeting only one recipient of the MAC address
- Broadcast : targeting all the recipients in network (switch)



Fragmentation and Aggregation

Fragmented and Aggregated

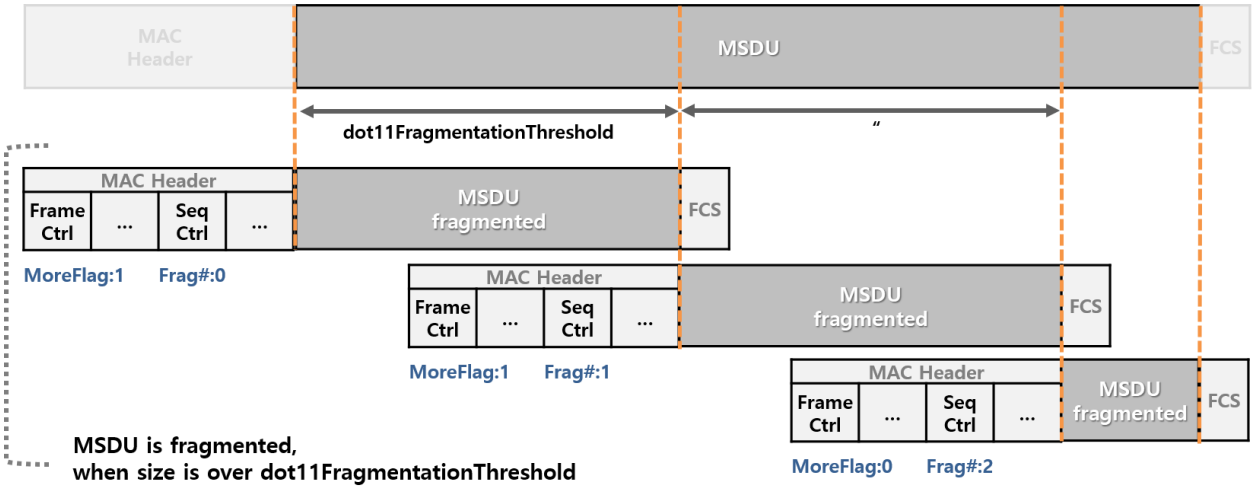
MAC payload can be fragmented (divided) or MAC payload (MSDU) or MAC frame itself (MPDU) can be aggregated (combined)



Fragmented and Aggregated

Fragmentation

MSDU is fragmented when its payload size is over Fragmentation Threshold. More Fragmentation flag is set before the last fragmented MPDU and Fragmentation number in Sequence subfield of MAC header increases while in fragmentation

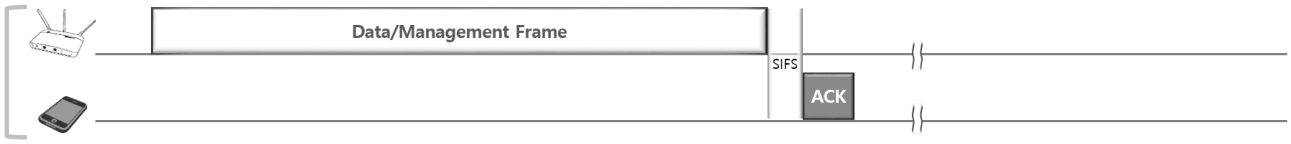


Fragmentation

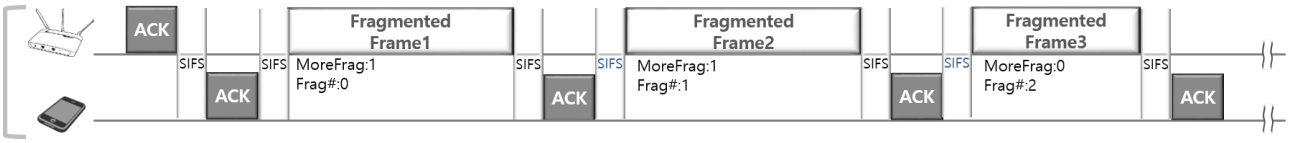
Sequences of fragmented frames vs normal frames

Fragmentation drops efficiency by adding overhead (MAC header, FCS and Ack response). However, in case that a long data fails to send and needs re-transmission, fragmentation can be useful.

Normal (not-fragmented) Frame



Fragmented Data burst



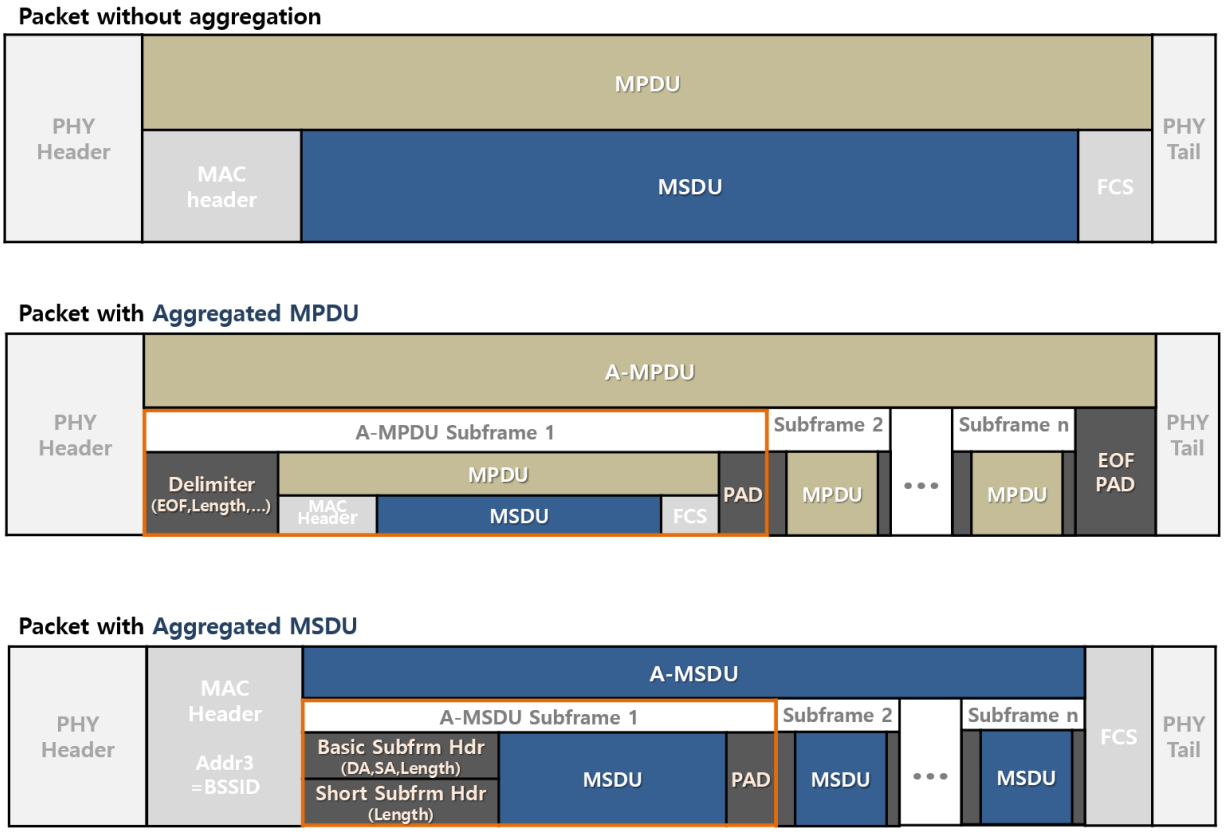
Fragmented Data Burst

Aggregation

MPDU or MSDU can be aggregated to A-MPDU or A-MSDU each. By lowering overhead down, it enhances the efficiency of MAC layer

- A-MPDU : commonly used for aggregation
  - Delimiter : to support extracting each MPDU
  - Padding : to complete OFDM symbol
  - Each A-MPDU subframe has its own MAC header : Encryption done by each subframe
  - Each A-MPDU subframe has it own FCS : error isolated by subframe
  - All subframe in A-MPDU have same RA (Receiver Address)
- A-MSDU
  - Only has one MAC address and FCS

BlockAck is used together with A-MPDU (A-MSDU).



Aggregation : A-MPDU, A-MSDU

Item	A-MPDU	A-MSDU
Max Frame Size	HT : about 64KB, VHT : about 1MB	HT : about 8KB, VHT : about 11KB
Operated by	HW mostly	SW mostly
Overhead	Higher	Lower, One MAC head and one FCS
Reliability	Higher, each subframe has FCS	Lower
Encryption	Each subframe	Whole A-MSDU
QoS	Multiple traffic class	One traffic class

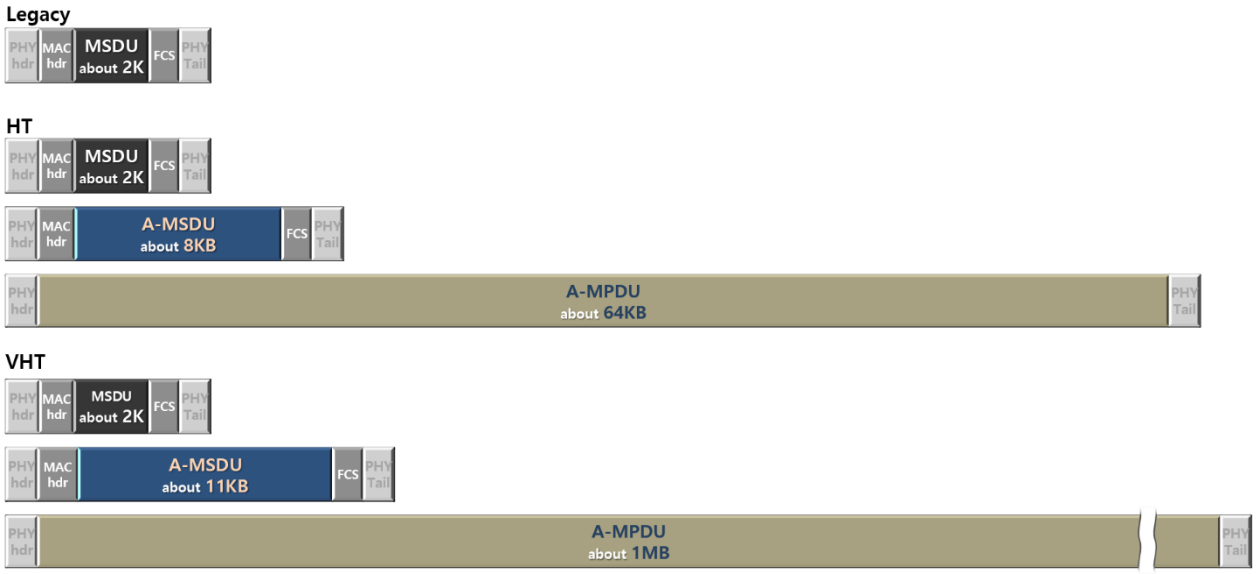
A-MPDU vs A-MSDU

Maximum Frame Length

Maximum Length of MSDU, A-MSDU and A-MPDU in Legacy, HT and VHT.

- A-MPDU max size
  - HT : 2^(13+max_exp)-1, where max_exp is 0,1,2,3
  - VHT : 2^(13+max_exp)-1, where max_exp is 0,1,2,3,4,5,6,7
- A-MSDU max size
  - HT : <3.8KByte or <7.9KByte
  - VHT : <3.8KByte or <7.9KByte or <11.4KByte

Overall PPDU length should be less than 5.484msec



Max Length in Legacy, HT and VHT

Max Length of legacy		
PPDU (by MSDU)		
PHY H'd	PSDU (4KB)	
	MPDU (by MSDU)	
	MAC H'd	**MSDU (2KB)**

Max Length of HT		
PPDU (5.5msec)		
PHY H'd	PSDU (64KB)	
	A-MDPU (64KB) MPDU (by A-MSDU)	
	MAC H'd	**A-MSDU (8KB) MSDU (2KB)**

Max Length of VHT		
PPDU (5.5msec)		
PHY H'd	PSDU (4.5MB)	
	A-MDPU (1MB) MPDU (11KB)	
	MAC H'd	A-MSDU (by MPDU) **MSDU (2KB)**

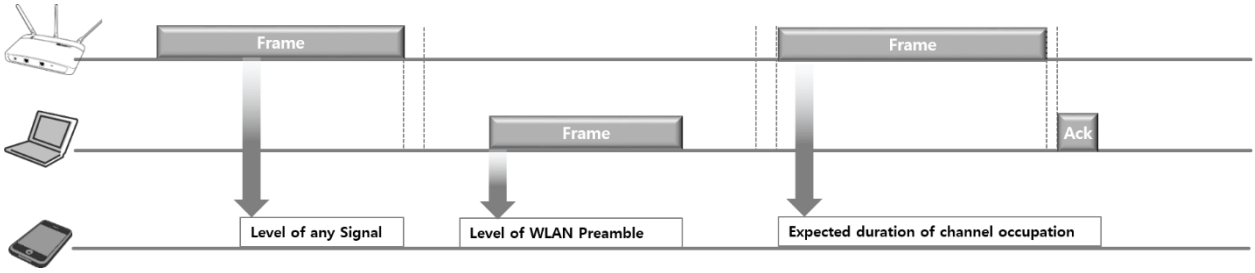
Max size	Legacy	HT	VHT
MSDU	**2,304B**	2,304B	2,304B
A-MSDU	(no aggregation)	**3,839B** or **7,935B** Max A-MSDU Length in HT Capability Info field	By MPDU
MPDU	By MSDU	By A-MSDU (MAC Header + A-MSDU)	**3,895B** or **7,991B** or **11,454B** Max MPDU Length in VHT Capability Info field
A-MPDU	(no aggregation)	By PSDU, **65,535B** in max_exp=3 $2^{(13+\ max\_exp)}$ -1 (max_exp : 0~3) in A-MPDU Param field of HT Capa. element	8K~**1MB** $2^{(13+\ max\_exp)}$ -1 (max_exp : 0~7) in VHT Capability Info field
PSDU (logical)	4,095B 12bit in SIG	65,535B 16bit in HT-SIG	4,692,480B by Length calculation in VHT-SIG
PPDU	By PSDU	**5.484msec**	**5.484msec**

Frame/Packet Max Length Definition in IEEE802.11

CCA and NAV

How to check if channel is occupied or not

Clear Channel Assessment (CCA, physical way) and Network Allocation Vector (NAV, virtual way). And, CCA has two ways of detecting preamble or energy of the signal.



How to check if channel is busy or not

When STA can detect preamble : very clear signaling that there is WLAN packet and CCA level is lower than energy detection. (sensitively catch if there is a packet). CCA should be reported at least 99% for long Slot Time and 90% for short Slot Time. For Slot Time, find *Interframe Space* chapter.

When STA can detect energy : Some cases that STA cannot detect preamble (like when 11b only supporting STA sees OFDM signal or STA starts detecting in the middle of another signal). Threshold is higher than preamble detection

NAV : Every MAC header has duration field from which the time of following sequence is found. Each STA runs its own NAV (a kind of counter/timer) with the information in duration field to estimate how long channel will be occupied.

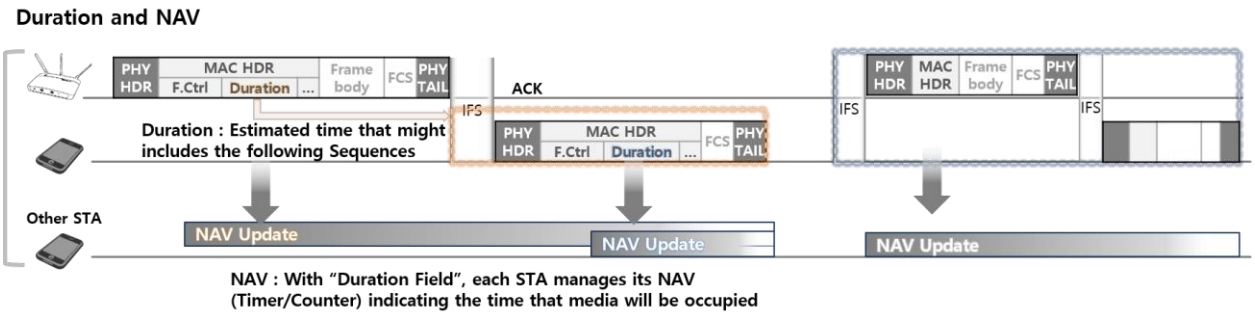
Condition for Channel is busy		20MHz	20MHz	40MHz	80MHz	160MHz
		11b	11a/g, HT/VHT20	HT/VHT40	HT/VHT80	VHT160
CCA	CS (carrier sense) : level of start of signal (preamble)	-73dBm *	-82dBm	-79dBm	-76dBm	-73dBm
	ED (energy detect) : level of any (Unknown) signal	-62dBm				
Virtually Busy		NAV				

11b preamble detection, in case that Tx power is 17dBm~20dBm

CCA type and level in WLAN

Duration field and NAV

Duration field (15bit, in unit of usec, up to 32msec) can set NAV value that protects up to the end of any following data, management and response with any additional overhead frame. It protects up to the estimated end of a sequence of frames. Station updates NAV, when the received duration field is great than the current NAV value that that station manages.

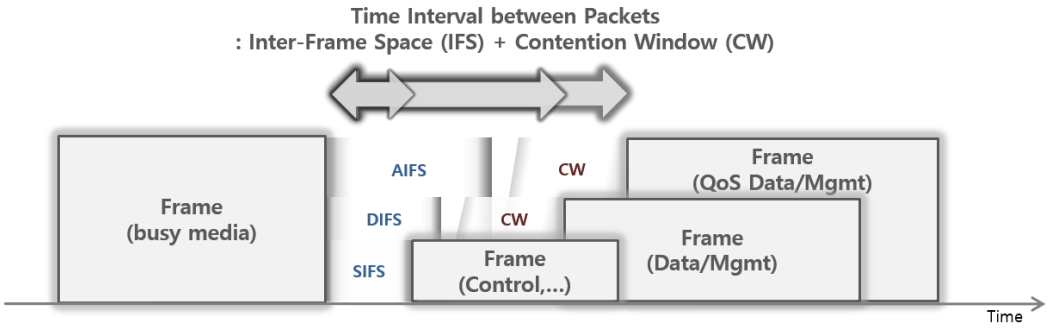


Duration and NAV

Interfame Space

Time Interval between Packets

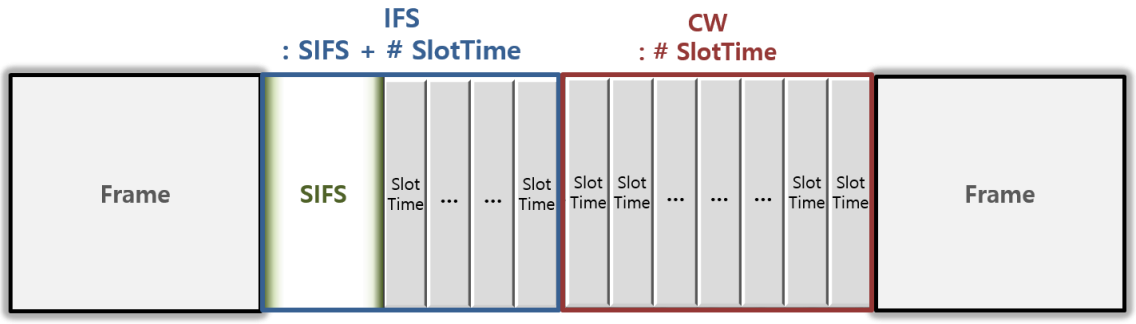
Inter-Frame Space (IFS) is the time interval between frames. (The time gap on media between physical packets). Generally, Control frames follow the previous frame after SIFS and Data and Management frames wait for DIFS/AIFS (QoS) before they back off in contention window.



Time Interval between Frames (Packets)

SIFS and SlotTime

The basic two units of frame spacing are “SIFS” and “SlotTime”. Every IFS consists of SIFS with the number of SlotTime and CW consists of the number of SlotTime. Physical definition of SIFS and SlotTime is as below. Even if they are basic units of frame timing, 2.4GHz has to manage two kinds of SlotTime for the backward compatibility.



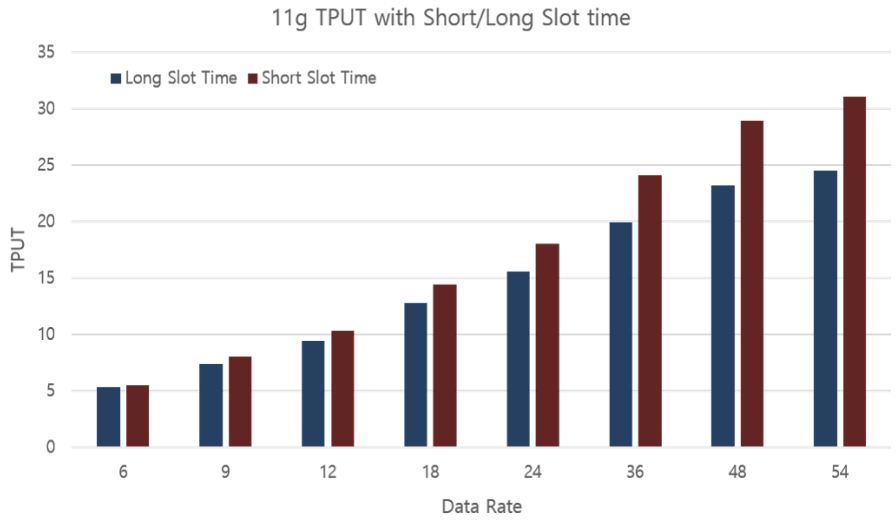
SIFS & SlotTime	Item		SIFS	aSlotTime
	2.4G	11b	10 usec	20 usec
		11g/n/ac		9 usec (short ST), 20 usec (long ST)
	5G		16 usec	9 usec

Physical Definition on SIFS and SlotTime

Short Slot Time in 2.4GHz

To have backward compatibility with 11b, 2.4GHz supports Short Slot Time and Long Slot Time. 11g PHY layer adopts 11a and two standards are identical except for “Slot Time”. Long Slot Time of 20usec significantly reduces throughput of 11g at 2.4GHz compared to 11a at 5GHz. AP sets Short Slot Time Subfield, when all the associated STAs support and AP indicates it in Non-Short Slot Time in Beacon frame. STAs change its mode, when non-short Slot Time device (like 11b) associated and AP can deny association if STA does not support Short Slot Time. Find ERP subfield in Beacon frame at *Scan & Connection* chapter for setting the existence of 11b STA.

For 11g, Short Slot Time and Long Slot Time brings difference in throughput as in the graph below



11g throughput with slot time

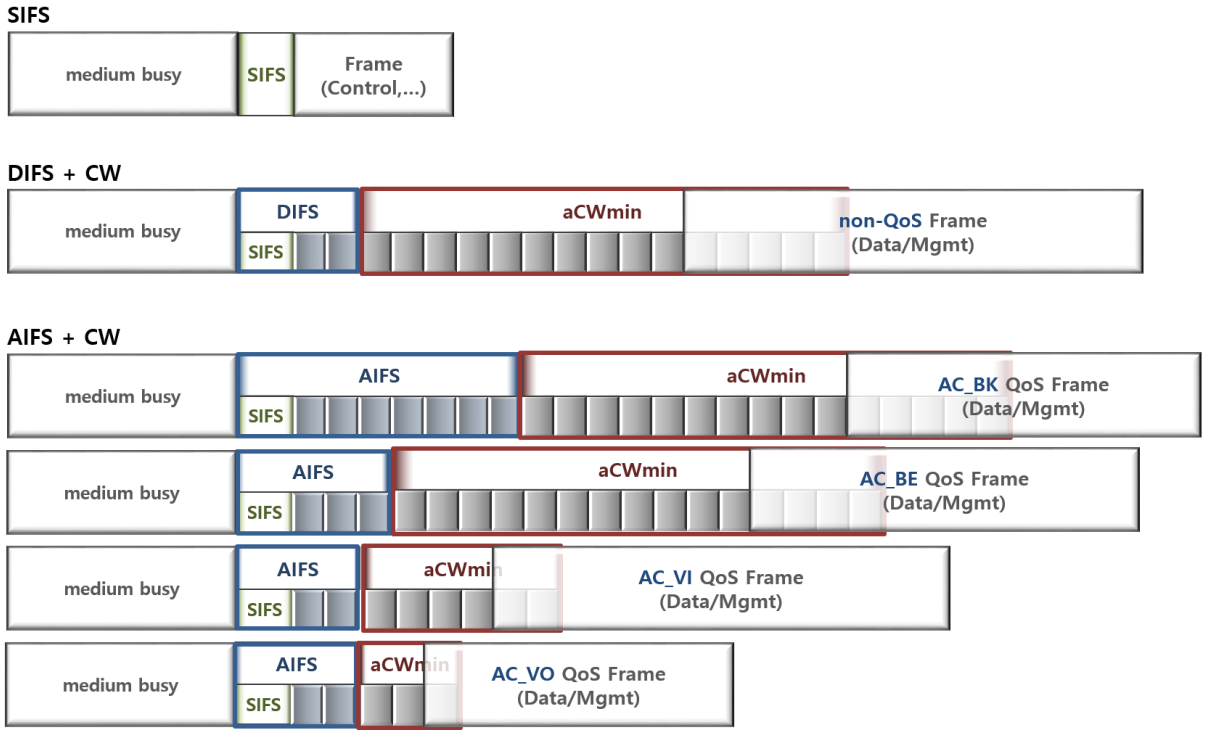
Signal Extension

SIFS of 16usec in 5GHz will be enough to send Ack after convolutional decoding, while 2.4GHz OFDM is using 10usec. When OFDM (11g/n) is operating in 2.4GHz, they can use “Signal Extension” of 6usec for this additional time. Along with it, 11ax has another extension as “Packet Extension” for LDPC decoding with 4 times more subcarrier.

IFS and CW

SIFS is mostly used before Control frame. DIFS is SIFS+SlotTimes in DCF (non-QoS) and AIFS is SIFS+SlotTimes in EDCA for QoS data/management frames. Along with them, many other IFSs are defined in IEEE (RIFS, PIFS, EIFS, SBIFS, BRPIFS, MBIFS, LBIFS). Among them, EIFS (Extended IFS) is used after errorneous frame. For DCF and EDCA, find *Multiple Access Control* chapter.

Contention is the basic mechanism for multiple access in WLAN. For STA to access wireless media, it selects random slot time (Random Backoff) in Contention Window (CW). The initial value of CW starts from CWmin and STA selects random number to back off inside CWmin. Every STA maintains Retry Count (STA Short Retry Count, SSRC or STA Long Retry Count, SLRC) and it increases exponentially CW size at every retry until it reaches CWmax. Basically, STAs try to yield their chance by increasing CW window size, when they think media is congested.



SIFS, DIFS, AIFS and CW

Typical values on DIFS, AIFS and Contention Window Size

DIFS is SIFS + 2 SlotTime used in DCF. AIFS has four values according to Access Categories in EDCA. AIFS is defined as SIFS + AIFSN (AIFS Number), which are typically set as in the table.

CW size is between CWmin and CWmax and the typical value of CWmin is 15, and CWmax is 1023.

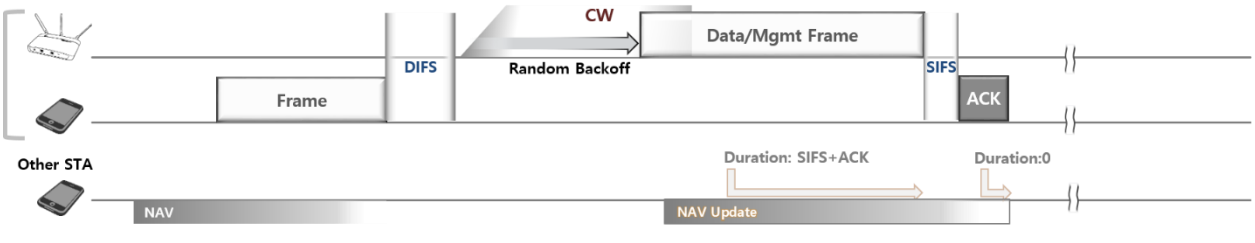
	IFS		Formula	2.4G		5G
				Short ST	Long ST	
IFS	SIFS		SIFS	10 usec		16 usec
	DIFS		SIFS + 2 aSlotTime	28 usec	50 usec	34 usec
	AIFS	BK	SIFS + 7 aSlotTime	73 usec	150 usec	79 usec
		BE	SIFS + 3 aSlotTime	37 usec	70 usec	43 usec
		VI	SIFS + 2 aSlotTime	28 usec	50 usec	34 usec
		VO	SIFS + 2 aSlotTime	28 usec	50 usec	34 usec

	Item		Contention Window (CW)		Contention Window (CW) value	
			CWmin	CWmax	CWmin	CWmax
Contention Window					When, aCWmin 15 (Short/Long)	When, aCWmax 1023 (Short/Long)
	DCF		aCWmin	aCWmax	**15 aSlotTime** (135 / 300 usec)	**1023 aSlotTime** (9,207 / 20,460 usec)
	HCF (EDCA)	BK	aCWmin	aCWmax	**15 aSlotTime** (135 / 300 usec)	**1023 aSlotTime** (9,207 / 20,460 usec)
		BE	aCWmin	aCWmax	**15 aSlotTime** (135 / 300 usec)	**1023 aSlotTime** (9,207 / 20,460 usec)
		VI	(aCWmin+1)/2-1	aCWmax	**7 aSlotTime** (63 / 140 usec)	**15 aSlotTime** (135 / 300 usec)
		VO	(aCWmin+1)/4-1	(aCWmax+1)/2-1	**3 aSlotTime** (27 / 60 usec)	**7 aSlotTime** (63 / 140 usec)

Definition and Default Values on IFS and CW

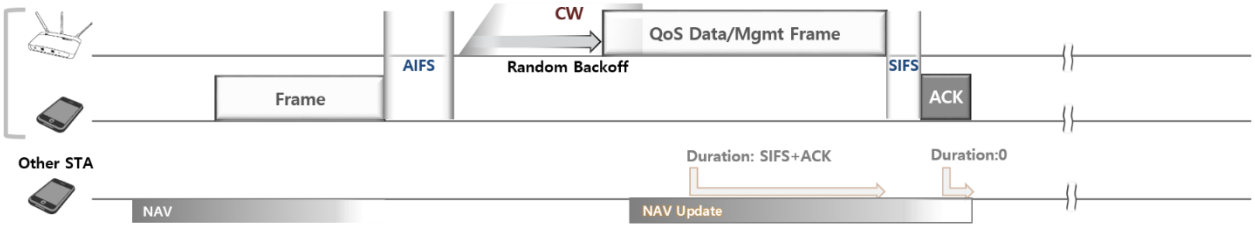
Cases on Interframe Space

Data/Management Frame (Non-QoS) + ACK

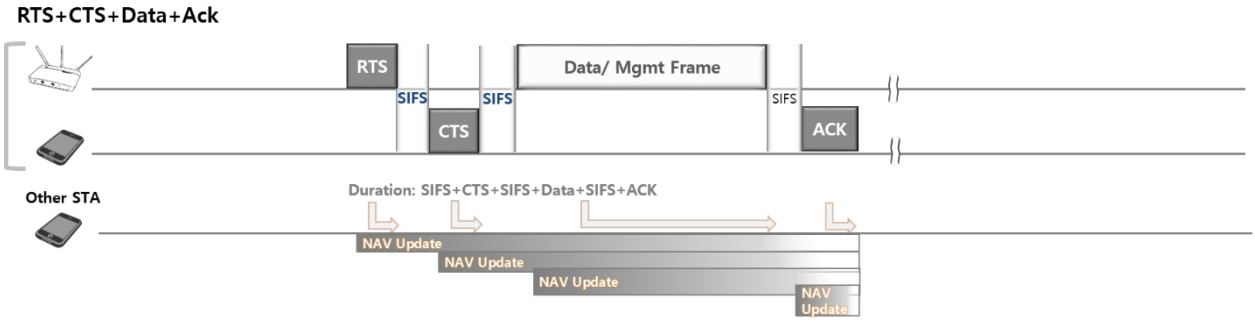


NVA and IFS Case : Data + ACK

Data/Management Frame (QoS) + ACK



NVA and IFS Case : QoS data + ACK



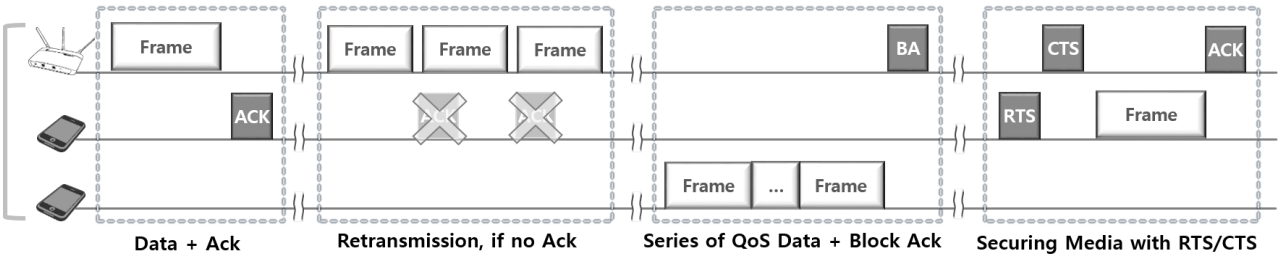
NVA and IFS Case : RTS+CTS

Basic Access Control

Overview

Basic Access Control in MAC layer is as below

- Data and Management frame to be Acknowledged by receiver
- If no Ack from counterpart, STA transmits the frame again. There is only (positive) Ack and no negative Ack (NACK) defined in WLAN. The receiver keeps silent, when the received frame has unrecoverable errors.
- Block Ack for series of QoS data
- Protecting media with RTS/CTS



Basic Access Control

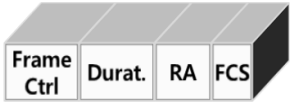
Ack

Positive response to “unicast” Data and Management frame indicating that the packet has been received without error in FCS (after error be corrected in PHY layer by FEC, if any or if possible). In some cases, Control frames like BAR or PS-Poll also require Ack.

Ack frame does not have TA (transmitter address) and only has RA (recipient address). Ack frame is short notice and needs to be delivered for sure. If Ack frame is carried in a non-HT PPDU, the primary rate is defined to be the highest rate in the BSSBasicRateSet (the set of data rates that all STAs in BSS are able to use for Tx and Rx, defined by AP) or highest mandatory rate that is less than or equal to the rate of the previous frame. For example, if data frame was sent in 54Mbps, Ack data rate will be 24Mbps. If data frame is 6Mbps, Ack should be 6Mbps. This mechanism is used in OTA test (Ack count for TIS, 6Mbps for TRP)

Basic Rate is defined by AP in BSS. Mandatory Data Rates are…

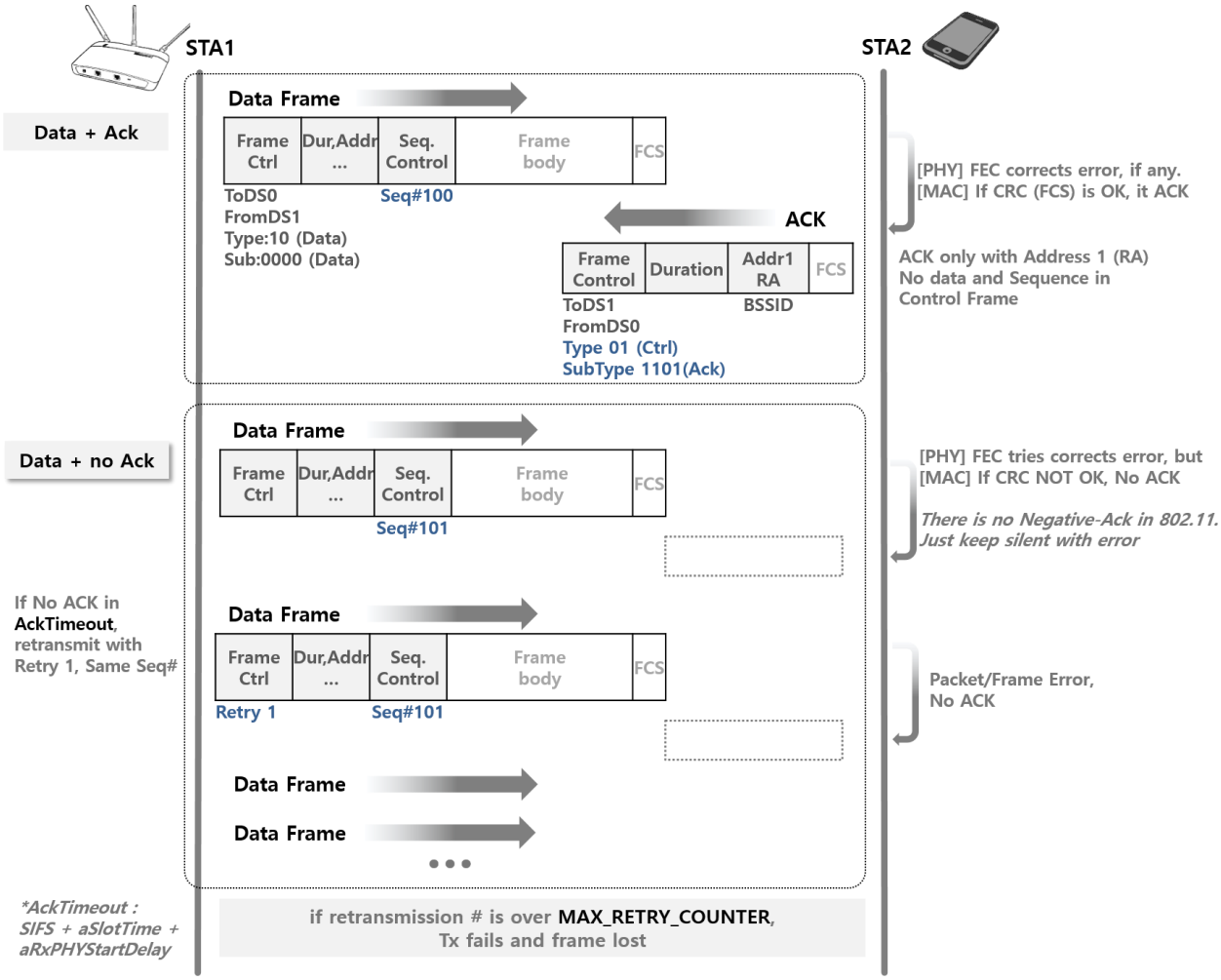
- 11b : 1, 2, 5.5, 11Mbps (Short preamble option : 2, 5.5, 11Mbps)
- 11a/g : 6, 12, 24Mbps



ACK frame

Ack flows

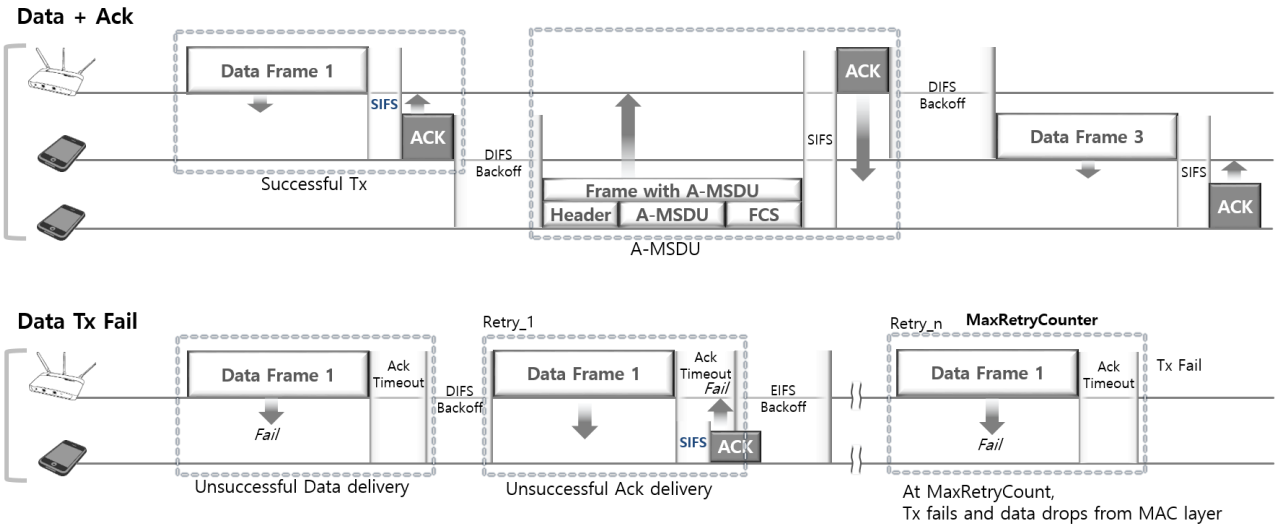
Data frame may not be reached or get error in channel and in some cases, ACK itself cannot be reached. In the case that originating STA cannot get Ack in AckTimeout, it re-transmits until MAX_RETRY_COUNTER. After MAX_RETRY_COUNT, the frame is given up from MAC layer.



Data Frame and Ack

Ack sequence

Data with successful Ack and Data transmission fail without Ack and Retry

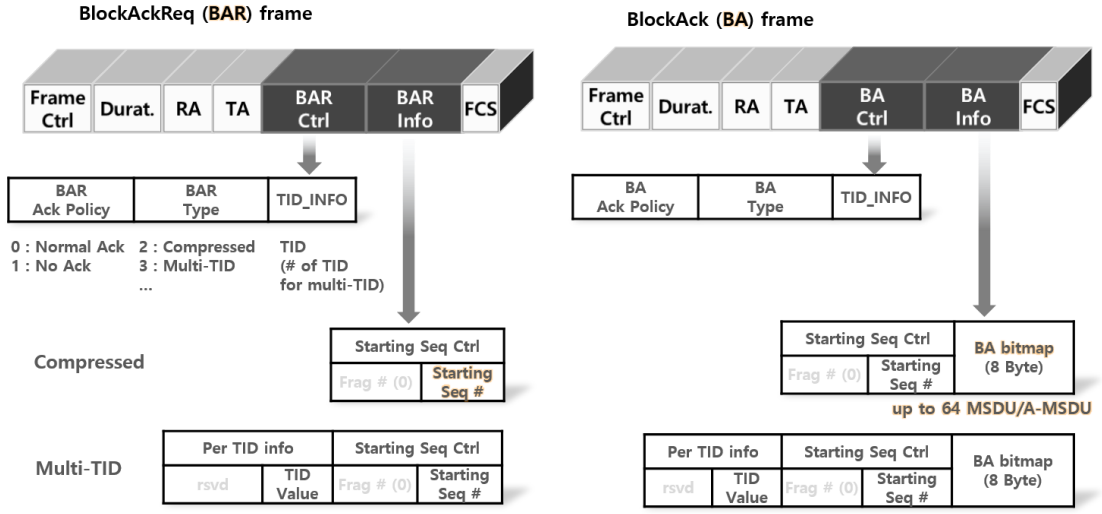


Cases on Ack

BlockAck

BlockAck mechanism improves efficiency by aggregation several acknowledgments into one frame.

BlockAck Request (BAR) and BlockAck (BA) have almost same structure except that BA has additional BA bitmap to indicate MSDU or A-MSDU to Ack to. The most commonly used type of "Compressed" has BA bitmap up to 64 MSDU. This will be expanded in 11ax. Find *MU ACK* chapter.

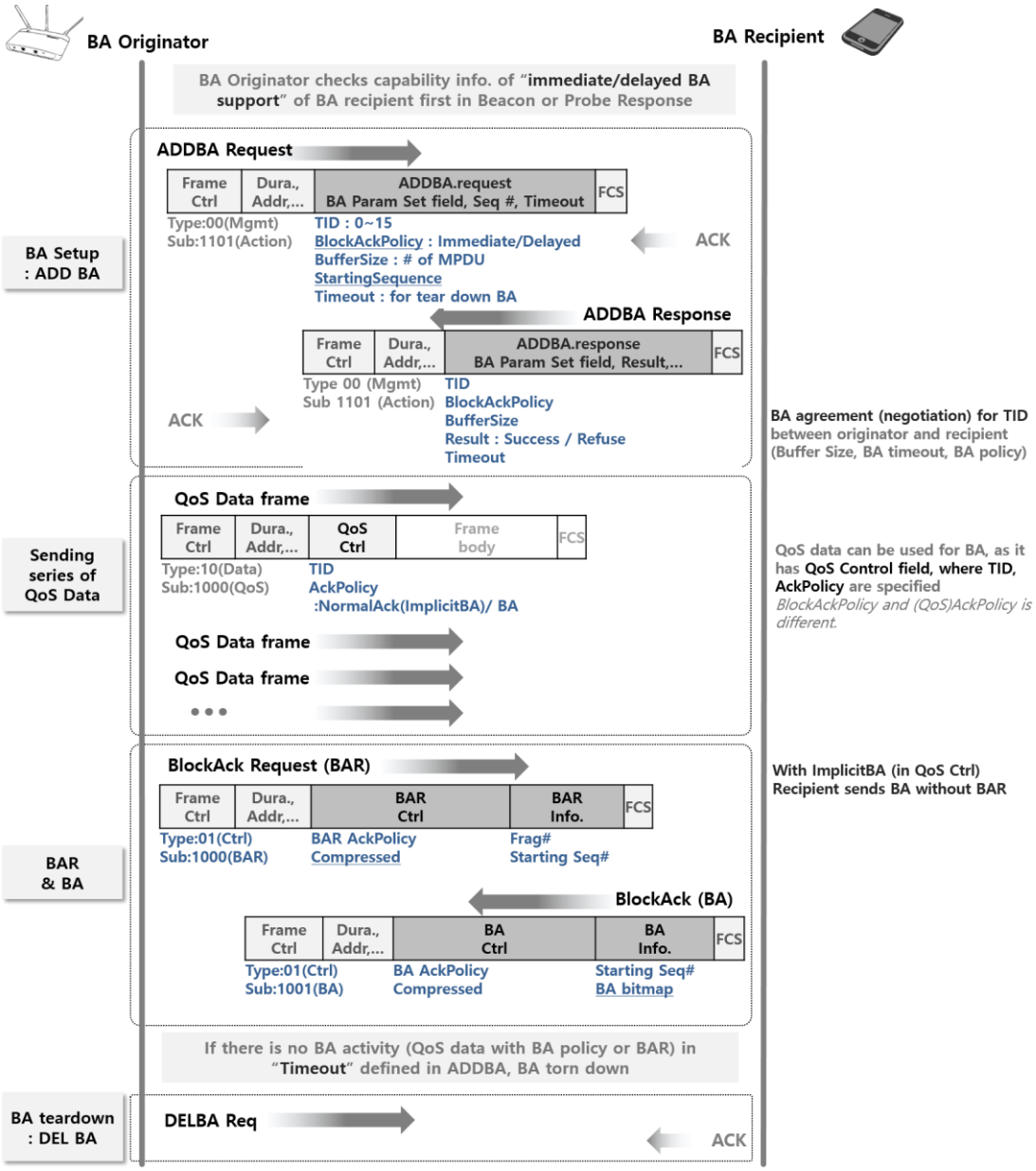


BAR and BA frame

BA flows

BA mechanism is initialized by BA setup with an exchange of ADDBA Request and Response. After initialization, blocks of QoS Data frames may be transmitted. A block may be started within a polled TXOP, within SP or by winning EDCA contention. MPDU within the block of frames are acknowledged by BA frame requested by BAR.

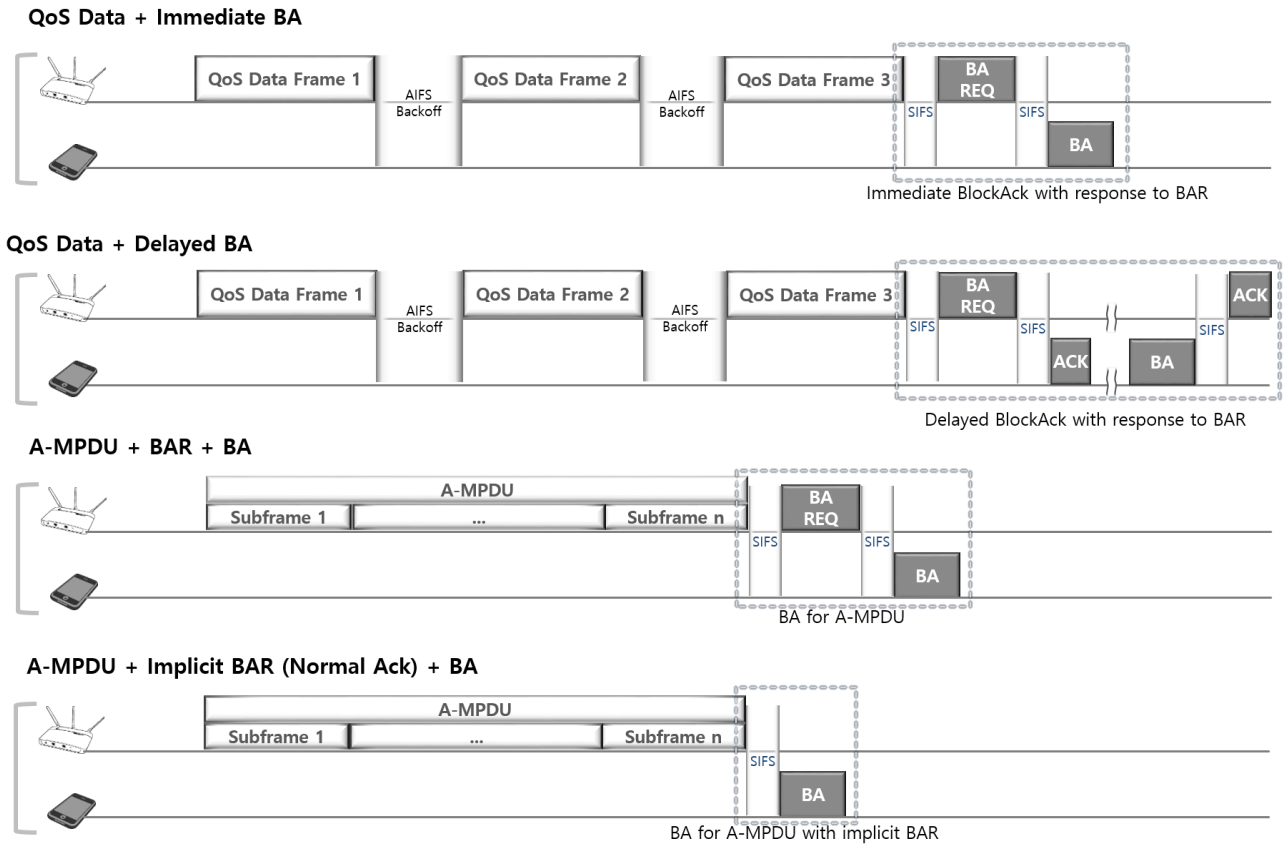
BA can be used only for QoS frames; QoS subfield in MAC header has TID and Ack Policy are set. In BA agreement, TID is indicated and QoS frames in the same TID may be transmitted during multiple TXOPs/SPs and get BlockAck, which gives flexibility to STA. For more about TID, find *Multiple Access Control* chapter. If there is no BA activity, BA is torn down by DELBA.



QoS Data Frame and Block Ack

Cases on BA sequence

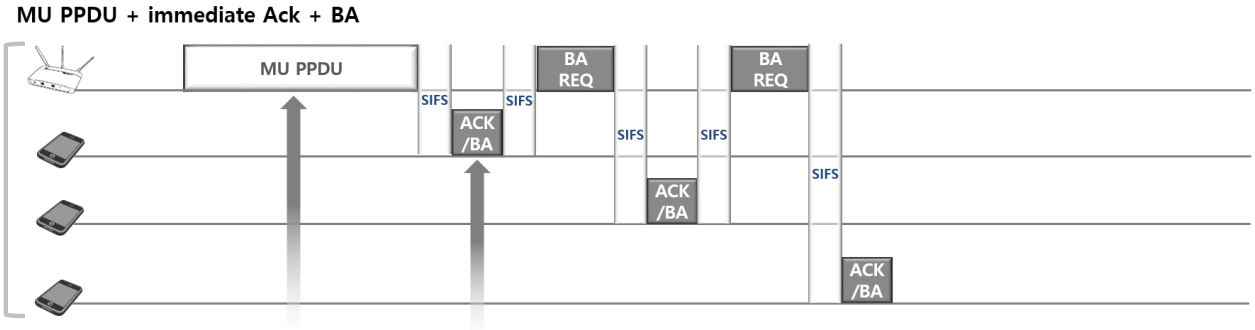
There are two types of BA mechanism: immediate and delayed BA. Immediate BA is suitable in low-latency application.



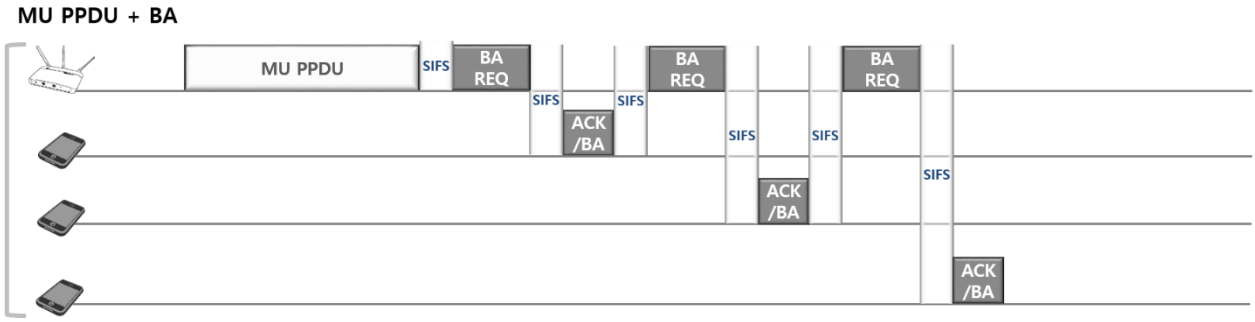
Cases on Block Ack

ACK for MU PPDU

11ac has one MU PPDU scheme (MU-MIMO) and there is no way for UL MU scheme. All MPDU with MU PPDU are contained within A-MPDU and acknowledge from each STA is done as in the picture below. MU acknowledge scheme gets diverse from 11ax with the advent of various MU scheme. (MU PPDU with OFDMA, TB PPDU with Trigger frame). Find more on *MU Access Control* in 11ax chapter.



MU PPDU does not carry more than one A-MPDU that contains one or more MPDU soliciting an immediate ACK



Protection with RTS and CTS

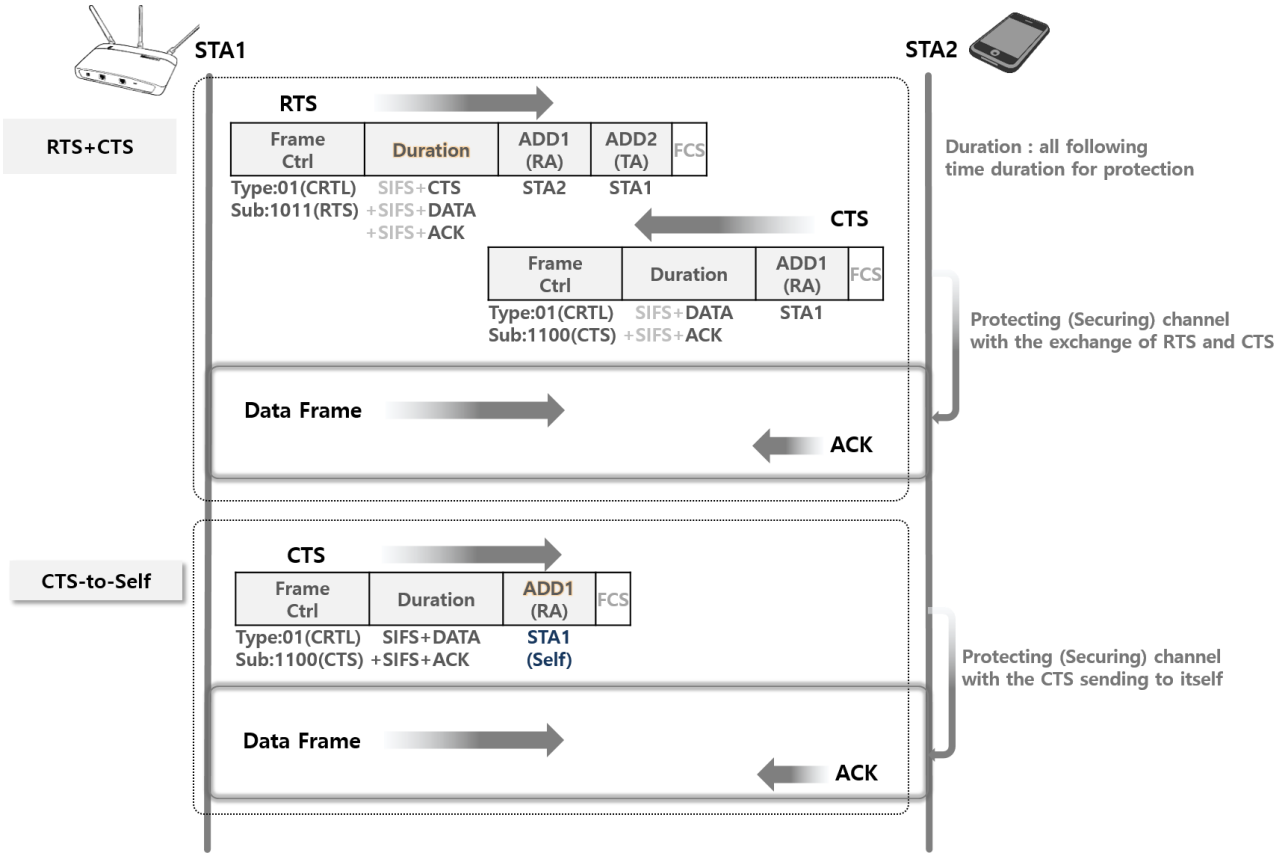
The protection mechanism makes STA that is a potential interferer to defer any transmission for a known period of time. STAs that listen to RTS/CTS between other STAs do not transmit frame duration the period in duration subfield.

Request To Send (RTS) frame is send to another STA (unicast only) to gain control of media for a period of time and Clear To Send (CTS) is used to answer to RTS frame. CTS-to-self frame is CTS frame where RA is equal to transmitter MAC address for transmitter itself to occupy the channel.

The protection mechanism is used for several purpose like…

- To send data securely
- To avoid “hidden node” problem. A STA who hears one of RTS or CTS between other two STAs holds transmission for period. Find hidden node problem at *Spatial Reuse and BSS Color* chapter
- For 11g (ERP) STA to be protected from 11b (non-ERP) who does not know what OFDM is. With backward compatibility, 11g STA can detect 11b, while opposite is not true. Exchanging RTS/CTS between 11g STAs with 11b rate of 11Mbps will let 11b STA know if channel is occupied. In Beacon frame, there is ERP element, which indicates if there is any 11b (non-EPR) STA in BSS, which will help 11g STA to understand the existence of 11b STA in BSS.
- Dynamic bandwidth allocation

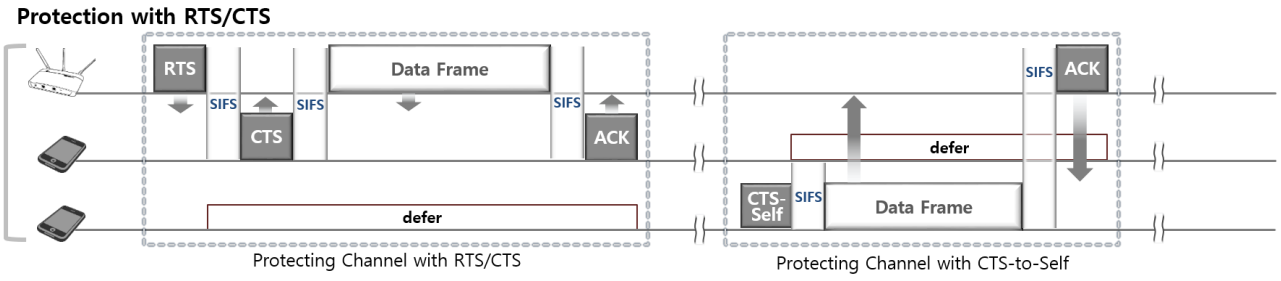
Data rate of CTS follows the same rule with Ack



Protection with RTS and CTS

Cases on RTS/CTS sequence

Exchange of RTS/CTS and protection with CTS-to-Self



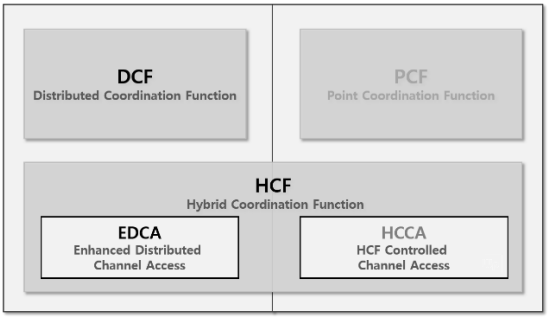
Protection cases with RTS and CTS

Multiple Access Control

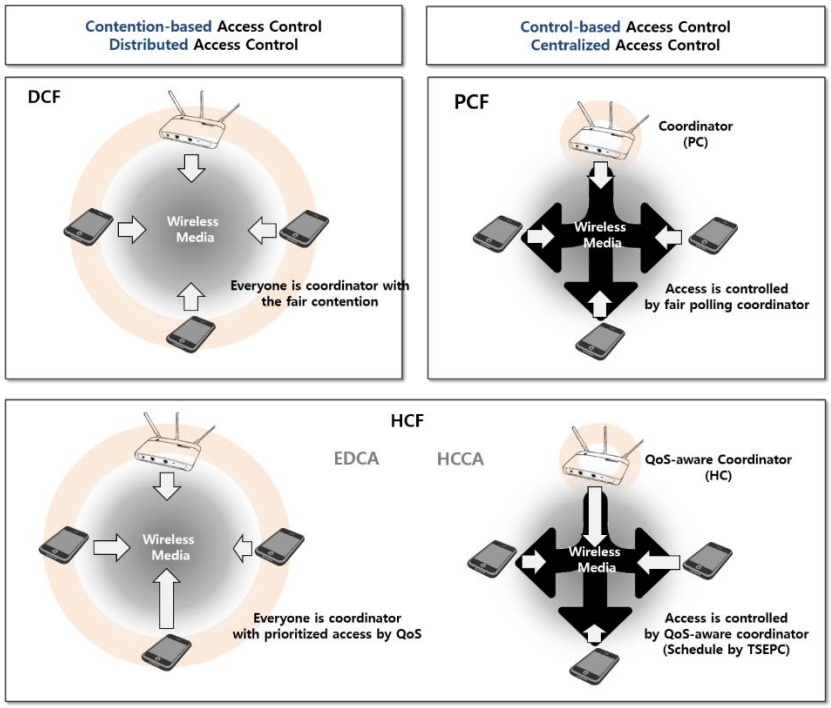
Coordination Functions : how to coordinate the access from multiple users

In WLAN, every STA (including AP and non-AP STA) takes the role of coordinator and decides when and how to access wireless media by itself. The mechanism that every STA tries to access media with the fair contention is Distributed Coordination Function (DCF), while prioritized media access by QoS is Enhanced Multimedia Distributed Control Access (EDCA) in Hybrid Coordination Function (HCF).

On the other hand, IEEE802.11 also defined the centralized access control, where AP takes roles of central coordinator. The original one was Pointed Coordination Function (PCF), which has not been used and is obsolete now. In HCF, QoS-aware coordinator schedules media access of other STA, which is called Hybrid Controlled Channel Access (HCCA).



Coordination Functions



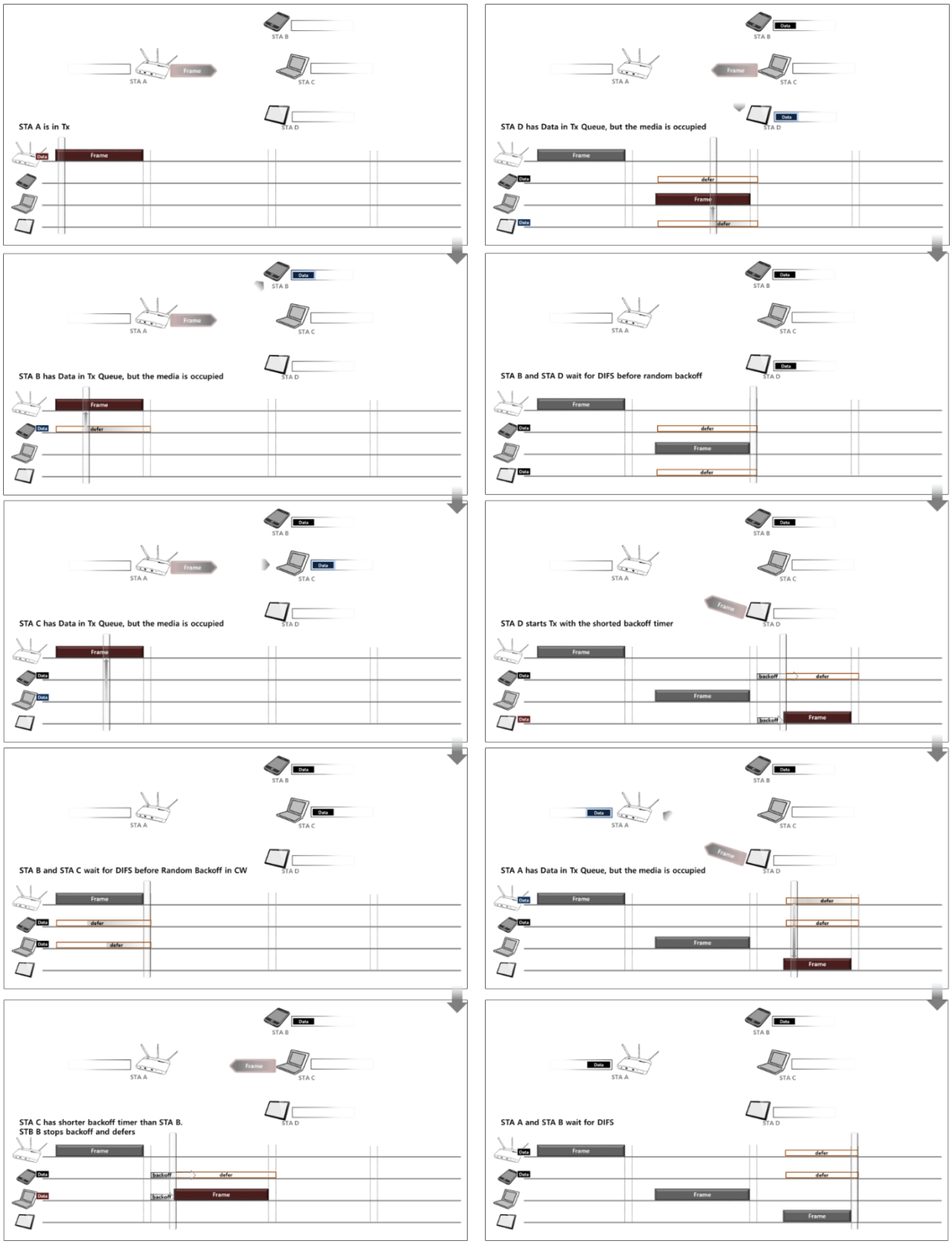
Coordination Function		Description	Wi-Fi	Wi-Fi Certification
DCF Distributed Coordination Function		• Fundamental Access Control • Contention-based • Base for PCF, HCF		
PCF *Point Coordination Function*		• *Central controlled by PC* • *Contention–Free*	*Obsolete*	
HCF Hybrid Coordination Function (802.11e)	**EDCA** Enhanced Multimedia Distributed Control Access	• Extension of DCF • Prioritized QoS • Access Category (BK, BE, VI, VO)	**WME** Wi-Fi multimedia Extension	**WMM** Wi-Fi multimedia
	HCCA HCF Controlled Channel Access	• Controlled by HC (HCF Coordinator) • Extension of PCF • Parameterized QoS	**WSM** Wi-Fi Scheduled Multimedia	**WMM-SA** WMM Scheduled Access

Coordination Function Comparison

Basic Multiple Access : CSMA/CA in DCF

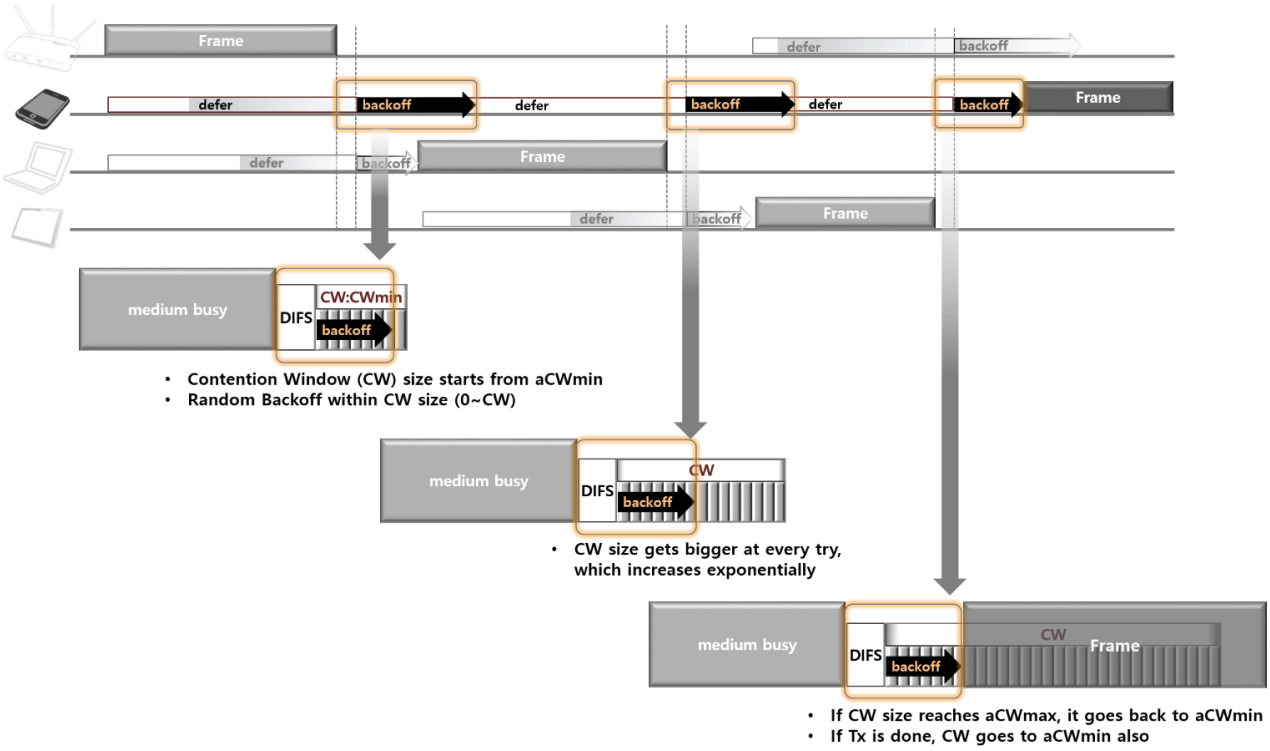
Carrier Sensing Multiple Access with Collision Avoidance in Distributed Coordination Function.

For Multiple Access, every STA needs to sense the carrier (channel/media) to see if the channel is occupied, before STA tries to transmit frame. When the STA found that channel is occupied by another STA, it waits for the frame to end and takes random back off. At this point after back-off, if channel is not occupied, the STA transmits data. If channel is occupied by another STA that already started transmission, the STA defers again to Avoid Collision.


STA A is in Tx
STA D has Data in Tx Queue, but the media is occupied
STA B has Data in Tx Queue, but the media is occupied
STA B and STA D wait for DIFS before random backoff
STA C has Data in Tx Queue, but the media is occupied
STA D starts Tx with the shorted backoff timer
STA B and STA C wait for DIFS before Random Backoff in CW
STA A has Data in Tx Queue, but the media is occupied
STA C has shorter backoff timer than STA B.
STB B stops backoff and defers
STA A and STA B wait for DIFS
STA A
STA B
STA C
STA D
Frame
Data
defer
backoff

Contention Window and Random Backoff

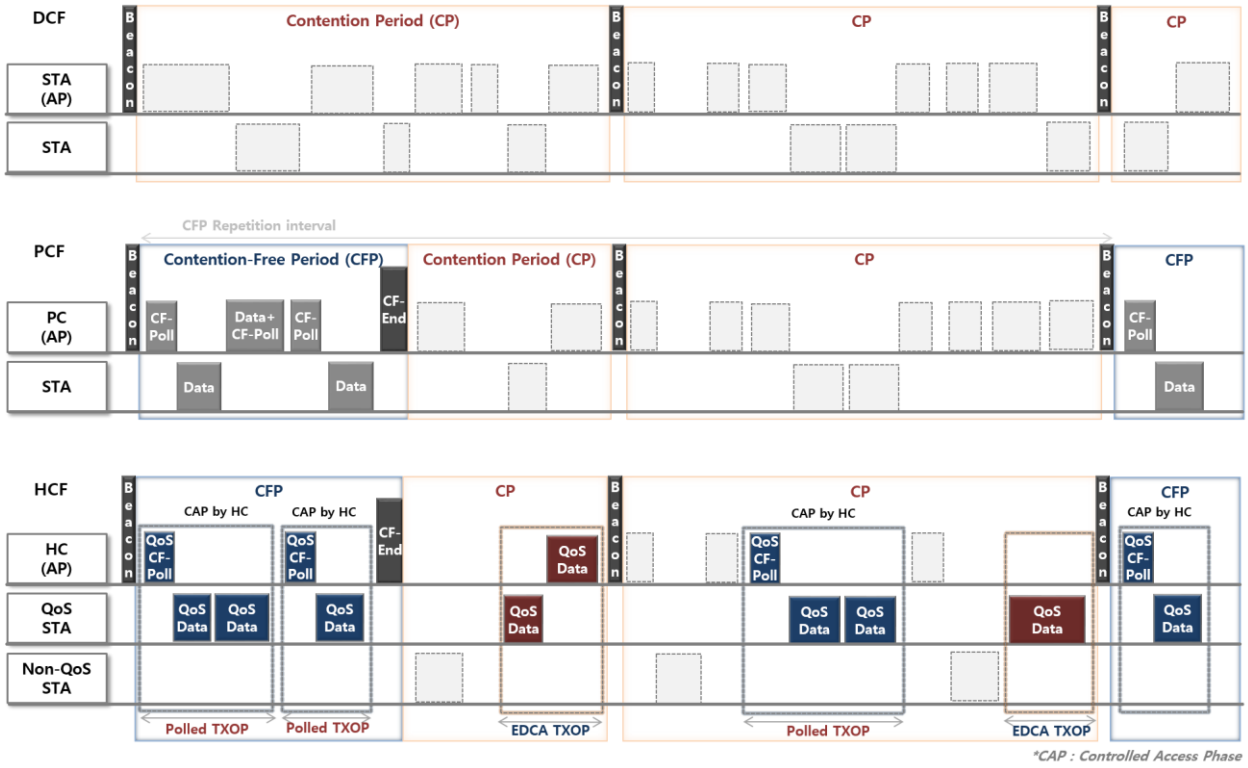
Collision will happen, if several STAs wait for the current frame to end and start to transmit at the same time. STAs takes random Slot Time in Contention Window (CW) to avoid collision after the frame. The size of CW increases after STA fails to send data to share the chance for transmission together. For more about interframe space, find *Interframe Space* chapter.



Backoff in Contention Window

Contention Period and Contention Free Period in DCF, PCF, HCF

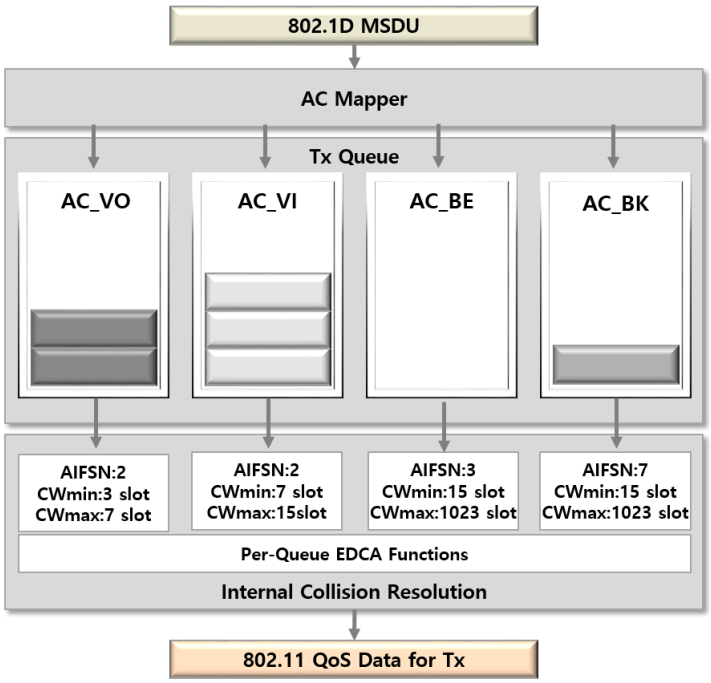
- DCF : Every STA is in Contention Period to obtain the media
- PCF (obsolete) : In contention free period (CFP), the Point Coordinator (AP) solicits the transmission of a specific STA with CF-Poll (Contention Free Polling)
- HCF
  - Like PCF, the coordinator (HCF Coordinator, AP) runs Controlled Access Phase (CAP) by asking transmission with QoF CF-Poll, which is Polled TXOP (transmission opportunity, defined by starting time and max duration). CAP can be run in Contention Period also
  - Prioritized access by QoS in EDCA TXOP in Contention Period



Contention Period and Contention Free Period

EDCA (QoS) Reference Model

WLAN defines four Access Categories (AC) for prioritized access for QoS (Quality of Service). Four AC may have different parameters on AIFS and CWmin/max to have different priority accessing wireless media.



EDCA Reference Model

EDCA Access Category

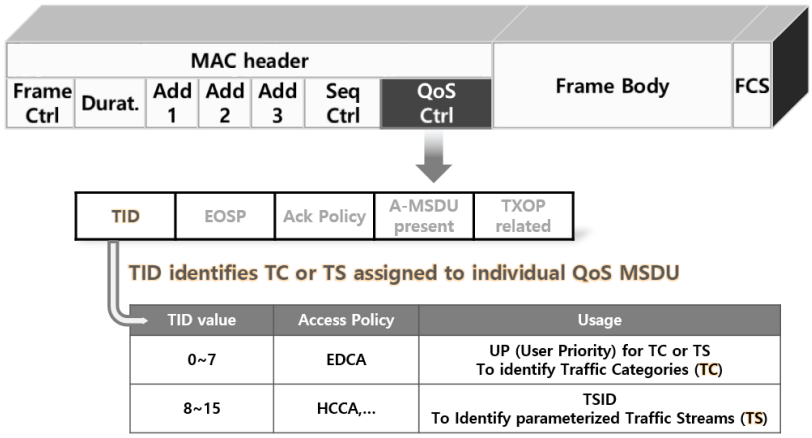
Four Access Categories (AC) in WLAN are mapped with Traffic Type and User Priority (UP) in MAC bridge protocol. AC is used as parameter accessing media and UP is managed by TID for WLAN QoS.

IEEE802.11				IEEE802.1D (MAC Bridge)		
Access Category (AC)	ACI (Index)	Designation	Priority	Designation	Traffic Type	UP User Priority
AC_BK	00	Background	Low	BK	Background	1
				-	Spare	2
AC_BE	01	Best Effort		BE	Best Effort	0
				EE	Excellent Effort	3
AC_VI	10	Video		CL	Controlled Load	4
				VI	Video	5
AC_VO	11	Voice	High	VO	Voice	6
				NC	Network Control	7

EDCA Access Category

Traffic ID

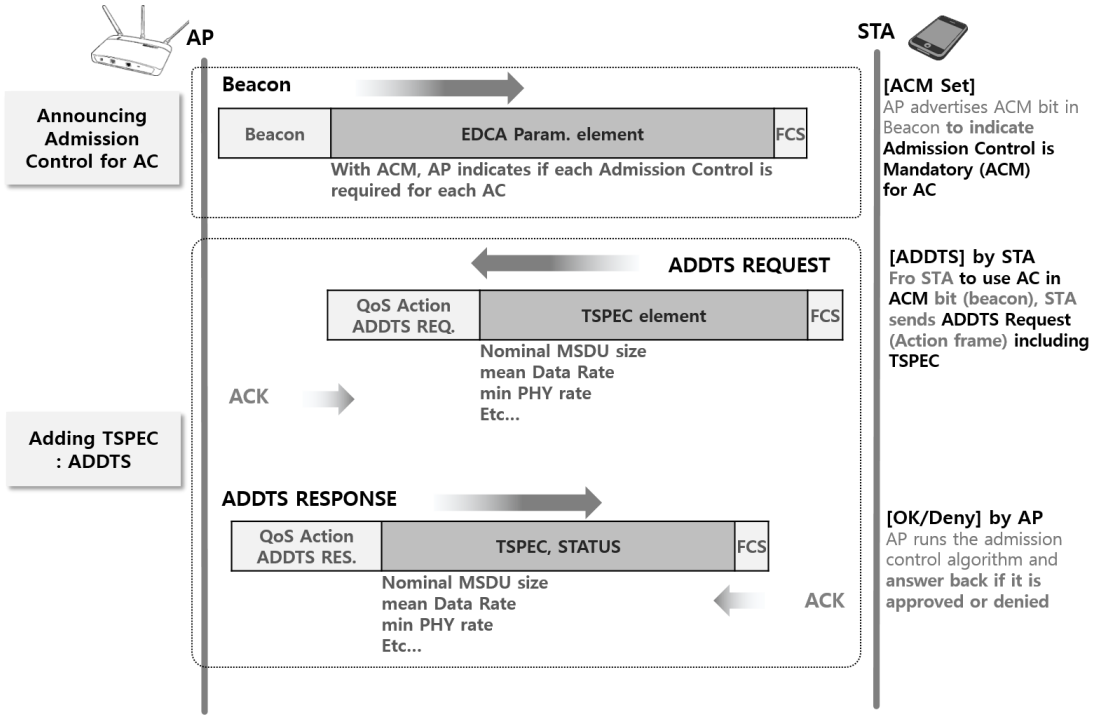
Along with AC, QoS facility supports 8 priority value, which is User Priority (UP) and it is identical to IEEE802.1D. QoS Control subfield in MAC header has TID (Traffic ID) which expresses TC (Traffic Category) and TS (Traffic Stream) ID. TSID is for parameterized QoS (TS with a particular traffic specification, TSEPC).



TID in QoS Control Field

Admission Control

EDCA helps QoS, while it does not guarantee for QoS. Admission Control controls and limits Admission (latency) for AC (QoS Stream), which can improve QoS. It is used by HC (HCCA Coordinator) for parameterized QoS. For STA to use AC in ACM (Admission Control Mandatory), it sends Add TS (ADDTS) Request including TSPEC (Traffic Spec). HC approves or denies it. TSPEC has information like mean data rate, min PHY rate, nominal MSDU size, etc for QoS Scheduling (Admission Control).

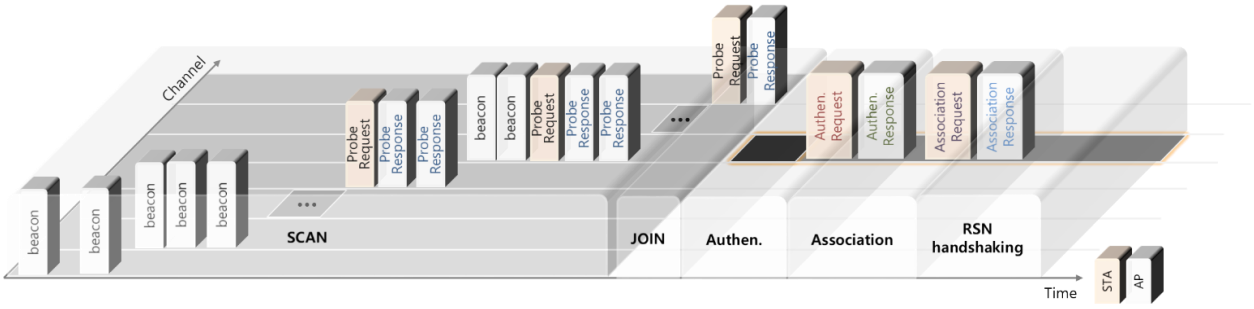


Scan and Connection

Overview on Scan and Connection

Scan is for gathering AP (BSS) information, before STA tries to join one of BSSs.

- STA scans the channels defined in ChannelList with ScanType (passive/active)
- Passive Scan receives Beacon frame from APs. In one channel, STA listens no longer than MaxChannelTime
- STA broadcasts Probe Request and receives Probe Response from APs in Active Scan. If there is no response in MinChannelTime STA moves to the next channel. STA processes Probe response until MaxChannelTime.



Scan and Connection overview

Flows on Scan and Connection

After user decides which AP to join among scanned lists of APs, STA tries to get Authentication from AP and requests Association sharing its capabilities and information, which AP approves or rejects.

Authentication is the sequential processes that is originally devised for Open or Shared Key (WEP) scheme. Shared Key is not recommended anymore as it is even weaker than Open. In addition, as higher level authentication method (RSN) is done after Association, Authentication process by Authentication frame is just an identification process for non-AP STA to inform to AP.

AP

STA 

Beacon

Beacon	AP Information	FCS
Type:00, Sub:1000 ADR1: ff:ff:ff:ff:ff:ff ADRR2/3: BSSID	SSID, Time Sync info, TIM, Supported Rate, Capability QoS, RSN	

Passive Scan
by **receiving beacon for AP information** like Supported Rate, Capability, QoS, RSN (Security), etc

[SCAN]
STA gathers AP Info. around

Probe Request

Probe Request	To Specific SSID or Broadcast SSID	FCS
Type:00, Sub:0100 ADDR1: ff:ff:ff:ff:ff:ff ADDR2: STA to send ADDR3: ff:ff:ff:ff:ff:ff	SSID, Request Element Info., Supported Rate and capability : just for communication	

Active Scan
STA actively sends Probe Request to receive AP information by Probe Response.

Probe Response

Probe Response	AP Information (Same with Beacon except TIM)	FCS
Type:00, Sub:0101 ADDR : Unicast	SSID, Time Sync info, ~~TIM~~, Supported Rate, Capability, QoS, RSN	

ACK

[JOIN]
User/Driver decides which AP to join and starts action

Authentication Seq #1

Authentication	Auth. Request with Open System	FCS
Type:00, Sub:1011 ADDR : Unicast	Authentication Algorithm (Open, Shared Key)	

Authentication
with Seq#1 (Request) and Seq#2 (Response) in case of Open System

[AUTHENTICATION]
STA be identified by AP

ACK

Authentication Seq #2

Authentication	Auth. Response with Open System	FCS
Type:00, Sub:1011 ADDR : Unicast		

ACK

Not much things happen here, as WEP is not recommended and RSN handshaking is after Association is done.

Association Request

Association Request	STA Information Supported Rate, Capability	FCS
Type:00, Sub:0000 ADDR : Unicast	SSID to associate Listen interval Supported Channel, Capability, RSN	

[ASSOCIATION]
AP approves connection based on STA's info.

ACK

Association Response

Association Response	Status, AID	FCS
Type:00, Sub:0001 ADDR : Unicast		

ACK

Association
STA sends Request with its information (capability) and **AP approves the connection** with Association Response

[RSN handshaking]
EAP/PSK , when needed

Scan and Connection flow

Beacon frame

At every TBTT (Target Beacon Transmission Time), Beacon frame is periodically sent by AP, where every information of BSS is contained.

Time Synchronization Function (TSF) : TSF keeps the timer for all STA in BSS to be synchronized.

MAC Header	Beacon frame body	FCS
Type:00, Sub:1000 FromDS ADDR1: ff:ff:ff:ff:ff:ff ADDR2/3: BSSID	• **Fixed Length : Timestamp, Beacon Interval, Capability Information** • **Information Element : SSID, TIM, Supported Rate, HT/VHT Capability and Operation, Regulatory, DFS, etc...**	

	Order	Field Name	Description
SSID	4	**SSID**	In case of **NULL or zero-length which is hidden SSID**, STA needs to specify the real SSID of AP for connection
Time Sync & Power Mgmt	1F	**Timestamp**	Timing Sync Function (**TSF**) timer value in usec. 2^64usec = 585K year Keeps timers for all STA to be synchronized
	2F	**Beacon Interval**	Time Unit (**TU**,1024usec) between Target Beacon Transmission Time (**TBTT**) Default 100 TU = 100 X 1024usec = **102.4msec**
	9	**TIM**	**Traffic Indication Map for Power Management**. Probe Response frame does not have TIM info. element **DTIM Count** (1B) : Count down to DTIM. If 0, current TIM is DTIM. **DTIM Period** (1B) : Beacon interval between DTIM. If 1, all TIM is DTIM. **Bitmap Control** (1B) : multicast, bitmap offset **Partial Virtual Bitmap** (~251B) : Traffic indication to STA in Power Save. Each bit for AID (251X8 = 2008)
Supported Rate & Capability	5	**Supported Rate**	**Each Byte for one rate : MSB(bit7) 1 for Basic Rate, (bit0~bit6) X 500kbps** (Ex) 1 001100 : Basic Rate, 12(001100)X500kbps = 6Mbps 8Byte : up to 8 rates **Setting Basic Rate is AP's role** and non-AP STA does not set the bit in this field.
	17	**Extended Supported Rate**	When the supported rate is more than 8 HT, VHT Supported rate is defined in HT capability
	3F	**Capability Info**	Each bit as flag for a particular function support **QoS**, Short Preamble, Short Slot Time, Delayed Block Ack Support, **APSD** (power management) etc
	34	**HT Capability**	**LDPC**, **BW**, **Short GI**, **STBC**, **A-MSDU max length**, **A-MPDU Length exp.**, **Supported HT MCS**, **# of SS**, **Beamforming** : implicit/explicit, HT-delayed BA, etc
	35	**HT Operation**	**Primary Ch#, Secondary Ch offset**, (used for VHT also), **Basic HT Rate**, etc
	57	**VHT Capability**	**Max MPDU length**, **BW support**, **Rx LDPC**, **Short GI**, **STBC**, **SU/MU Beamformer/ Beamformee capable**, **max A-MPDU Len exp.**, **Max VHT MCS for SS #**
	58	**VHT Operation**	**BW**, Center Freq. for 80/160MHz
QoS	20	**EDCA param set**	For **AP to establish or change QoS policy**. STA updates MIB with this info. QoS Info and BE/BK/VI/VO param : **AIFSN, ECWmin/max, TXOP limit**
	21	**QoS Capability**	QoS Info. Used in case that beacon does not have EDCA param set (EDCA param has the same field)
11i (EAP/PSK)	18	**RSN**	Information required to establish **RSNA (Robust Secure Network Association, EAP/PSK)** RSN of AP is shared in Beacon or Probe Response and RNS of STA is shared in Association Request.
BSS Management	10	**Country**	**Regulatory Domain.** Country String + N X (Starting Ch + # of Ch + **max_power**)
	16	**ERP**	For 11g network to indicate **the existence of 11b** Non-ERP_Present 1 : 11b associated to the cell or 11b data in neighboring cell
	11 12 13 15	**Power Constraint** **Channel Switch** **Quite** **TPC**	11ah related

Beacon Frame

Probe Request and Response

When non-AP STA broadcasts Probe Request, the recipient APs send Probe response with almost same information as Beacon.

MAC Header	Probe Request frame body	
Type:00, Sub:0100 ToDS ADDR1: ff:ff:ff:ff:ff:ff ADDR2: STA to send ADDR3: ff:ff:ff:ff:ff:ff	• **Fixed Length : X** • **Information Element : SSID, Supported Rate, HT/VHT Capability, etc...**	FCS

Order	Field Name	Description
1	**SSID**	SSID for recipient AP or APs Probe Request is mostly **broadcast (RA, ff:ff:ff:ff:ff:ff)**, while **SSID can be either Broadcast Set (zero-length info. element) or specified. (Directed Probe Request)**. Basically the role of probe request to ask recipients the information, it is up to STA to ask to whom (everyone with broadcast SSID) or some with specific SSID). Broadcasting RA (Mac address) is valid, as SSID can be for ESS with more than one AP. In case of directed probe, AP (BSS) or APs (ESS) with the specified SSID respond with Probe Response. 0 : Wildcard SSID for mesh STA
3	**Request**	Requesting information to recipient (AP, mostly) by specifying Element IDs #.
2 4 7 17	**Supported Rate** **Ext. S. Rate** **HT Capability** **VHT Capability**	Just for reference for communicating with the current AP (not for capability negotiation) Usually data rate of **probe request is lowest one to maximize visibility to receiving AP's** and AP can choose data rate among in this field. non-AP STA does not set Basic Rate bit in this field, as it is the role of AP to manage basic data rate in BSS.

Probe Request Frame

MAC Header	Probe Response frame body	
Type:00, Sub:0101 FromDS ADDR : Unicast	• **Fixed Length : Timestamp, Beacon Interval, Capability Information** • **Information Element : SSID, ~~TIM~~, Supported Rate, HT/VHT Capability and Operation, Regulatory, DFS, etc...**	FCS

Order	Field Name	Description
-	**Almost all fields with Beacon**	Probe Response send **almost same information of AP except TIM**. TIM is used to send traffic for Power Save STA in BSS. No need here.
Last	**Requested Element**	Answering information element in response to Probe Request

Probe Response Frame

Authentication frame

Authentication transaction sequence is different by Open (2 steps) or Shared Key/WEP (4 steps). WEP is vulnerable to hacking (worse than Open), and sequences for Open (STA's Request and AP's response) are used. This frame has nothing to do with RSN.

MAC Header	Authentication frame body	
Type:00, Sub:1011	• **Fixed Length : Auth. Algorithm #, Transaction Sequence #, Status code.** • **Information Element : Challenge Text, RSN, ...**	FCS

Order	Field Name	Description
1F (2B)	**Auth. Algorithm #**	**0 : Open System : Used also for RSN as well as just Open** 1 : Shared Key (WEP) (2 : FT, 3 : SAE) **Both Open and SK algorithm have nothing to do with RSN (EAP and PSK) and Open System is used for RSN**. WEP is not recommended any more and RSN process continues after Association done.
2F (2B)	**Auth. Transaction Sequence #**	Current state of progress **Open** • **1 STA>AP (Request, ToDS)** • **2 STA<AP (Response with Success/Fail, FromDS)** Shared Key • 1 STA>AP (Request) • 2 STA<AP (Response with not encrypted Challenge Text, randomly generated 128B plain text) • 3 STA>AP (Request with WEP encrypted Challenge Text) • 4 STA<AP (Response with Success/Fail)
3F	**Status Code**	**0 : Success** Non-0 : Failure/Reserved
4	**Challenge text**	Used in Shared Key (Sequence 2, 3) : WEP (not recommended any more), Challenge Text can be hacked easily and.

Authentication Frame

Association Request and Response frame

AP and Non-AP STA (STA) should know each other's capabilities before association. STA gets AP's information from Beacon or Probe Response frame and after that STA needs to share its information with AP. STA requests association by sharing its information in Association Request frame and AP responses with Association Response frame. AID (Association ID) is assigned to STA, when Association is done successfully

MAC Header	Association Request frame body	
Type:00, Sub:0000 To DS ADDR1,3 : AP to assoc	• **Fixed Length : Capability, Listen Interval, SSID.** • **Information Element : Supported rate, Supported Channel, HT/VHT capability, QoS capability, Power Capability,...**	FCS

Order	Field Name	Description
1F	**Capability Information**	Each bit as flag for a particular function support **QoS, Short Preamble, Short Slot Time, Delayed/Immediate Block Ack,** etc
4 5 13 22 9	**Supported Rate** **Ext. Supported Rate** **HT Capability** **VHT Capability** **QoS Capability**	STA's supported rate, HT/VHT and QoS capability to share with AP requesting approval for association.
2F	**Listen Interval**	**To inform AP how often STA in power save to wake to listen to Beacon**. (**AP estimates buffer size and setting AgingTime**). STA should listen DTIM anyway. 0 means insomnia STA.
3F	**SSID**	SSID for STA to associate
8	**RSN**	With RSN (EAP/PSK) information of AP in Beacon or Probe Response, **STA shares its RSN information** in Association Request
7	**Supported Channel**	AP may use to select a new channel for BSS or reject if it is not acceptable. Algorithm and criteria is beyond IEEE

Association Request Frame

AID is 16bit (2B) ID of STA assigned by AP. The range is 1 to 2007 with 11bit and 5 MSBs are reserved.

MAC Header	Association Response frame body	
Type:00, Sub:0001 From DS ADDR: Unicast	• **Fixed Length : Capability, Status Code, AID.** • **Information Element : Supported rate, HT/VHT capability, EDCA capability, etc.**	FCS

Order	Field Name	Description
2F	**Status code**	0 : Success Non-0 : Failure/Reserved
3F	**AID**	**AP assigns Association ID (16bit) for STA for management in BSS**
1F	**Capability Information**	Each bit as flag to advertise a particular function support QoS, Short Preamble, Short Slot Time, Delayed/Immediate Block Ack, etc
4 5 14 27	**Supported Rate** **Ext. Supported Rate** **HT Capability** **VHT Capability**	Not for capability negotiation. AP information shared with Beacon and Probe response.

Association Response Frame

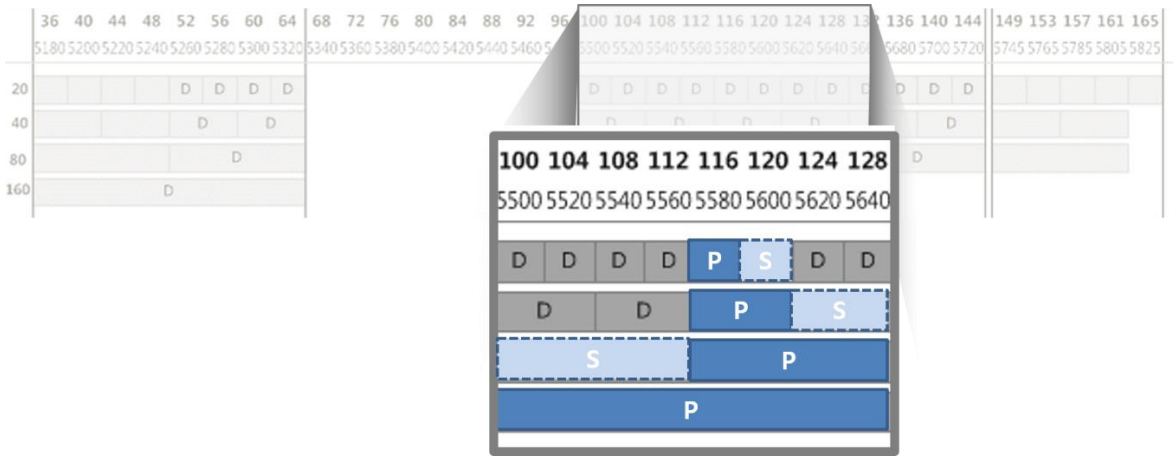
Channel Management

Channel is wireless media for WLAN STAs to transmit and receive the frame through and in WLAN, 20MHz, 40MHz, 80MHz, 160MHz, 80+80MHz bandwidths are used. (~11ax) As wider bandwidth is used, the efficient management of channel gets more important. The concept of primary/secondary channel and multiple channel widths is introduced in 11n and the dynamic bandwidth operations are handled from 11ac. In 11ax, preamble puncturing is for utilizing channel in a more efficient way, which topic is handled later in 11ax chapter. This idea is supposed to be polished allowing the preamble punctured frame to one user in 11be.

For co-existence with other wireless systems (RLAN) in 5GHz, TPC and DFS are used and STAs are classified to Standard, LPI(Low Power Indoor) and VLP(Very Low Power) in 6GHz according to regulatory domain. This topic will be discussed in *6GHz operation* in 11ax chapter.

Primary and secondary channel

- Primary channel : the common channel of operation for all STAs in BSS. Primary 20MHz is the 20MHz channel used in transmission of BSS using 40MHz or higher bandwidth. If one BSS supports up to 80MHz, 20MHz operations is done only through the primary 20MHz. Primary 40MHz is the 40MHz channel for BSS of 80MHz or higher bandwidth.
- Non-primary channel and secondary channel : Any 20MHz other than the primary 20MHz in BSS of 40MHz or higher bandwidth. The secondary channel is non-primary channel creating higher bandwidth associated with the primary channel. The secondary 20MHz together with the primary 20MHz create the primary 40MHz.



How/who to set the primary channel?

AP (or a mesh STA) sets the channel and all STA associated with BSS share the channel set by AP. When AP set the channel, if some or all the channels are occupied by the existing BSSs, AP selects a primary channel that is identical to the primary channel of the existing AP.

Multiple channel width support and dynamic bandwidth operation

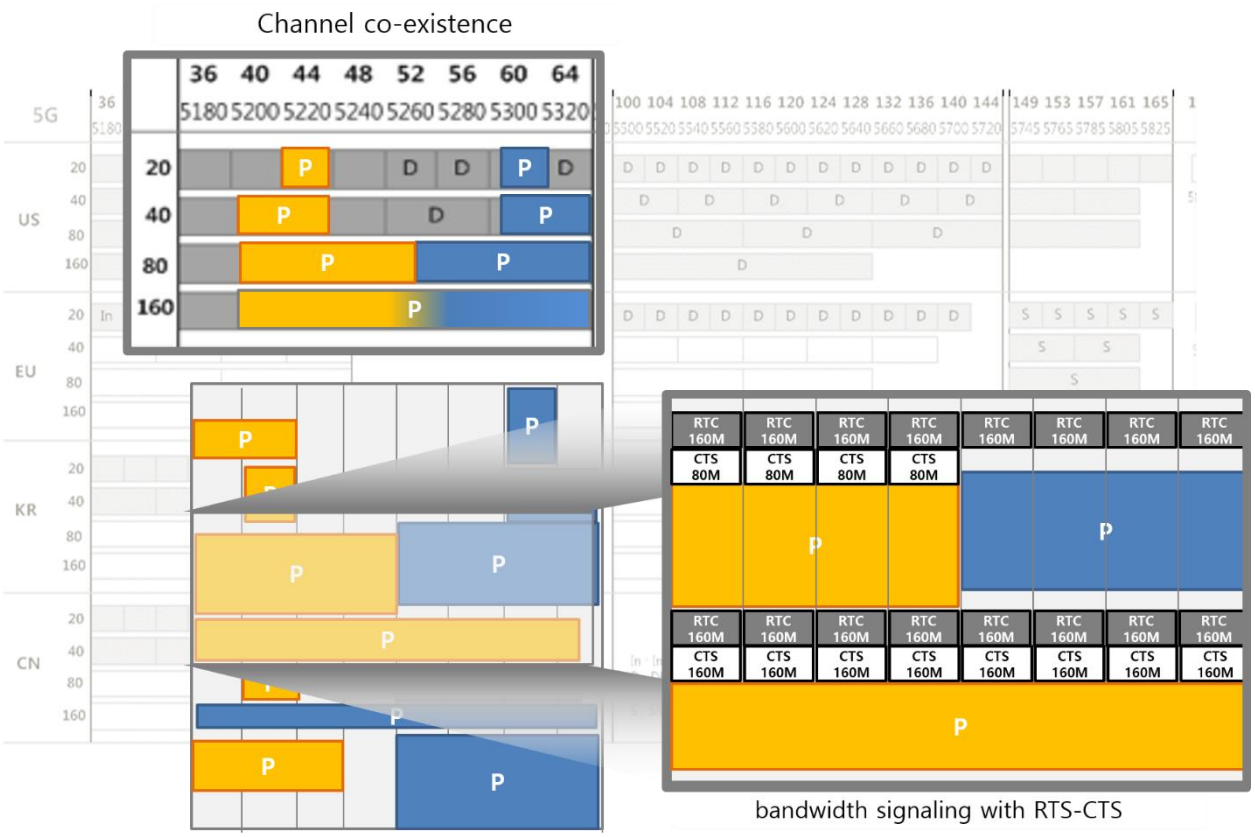
Multiple channel widths support

When BSS and STA both support multiple channel widths, EDCA TXOP is obtain based solely on activity of the primary channel. Once EDCA TXOP has been obtained, further constraints might limit the width of transmission during TXOP or deny the channel access, based on CCA on secondary channel.

VHT STA that is a member of a BSS that supports multiple channel widths is granted a TXOP for a specified duration and for a channel width that is equal to the channel width of the frame containing the QoS CF-Poll.

Dynamic bandwidth operation

STA shall set one of dynamic bandwidth operation or static bandwidth operation. VHT STAs exchange RTS/CTS negotiates a potentially reduced channel width compared to the channel width indicated by RTS.



TPC : transmit power control

Initially, TPC is for STAs to adjust transmit power protecting RLAN (radio local area network, EESS Earth Exploration Satellite Service) in 5GHz, while it is widely in other purposes by WLAN.

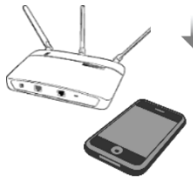
STA shall inform an AP its minimum and maximum transmit power capability for the current channel when (re)associating, using a Power Capability element in (Re)Association Request frames. AP may reject a (re)association request from a STA if it considers the STA's minimum or maximum transmit power capability to be unacceptable. STAs (AP and non-AP STA) use transmit power under a regulatory maximum power. STA may use any criteria, and in particular any path loss and link margin estimates, to dynamically adapt the transmit power for transmissions of an MPDU to another STA

DFS : dynamic frequency selection

DFS is a mechanism to avoid co-channel operation with radar system in 5GHz DFS channels of some regulatory domains. It is also used for uniform channel spreading and automatic frequency planning.

In association

- STAs provide AP with a list of channel in which STA can operate when (re)associating, which AP uses in selecting a new channel while in DFS.
- AP may reject STA with unacceptable channel list



Measurement

- AP runs Quieting the channel to test the presence of radar with less interference from other STAs. AP schedules quiet interval (Quiet Period and Quiet Duration) in beacon or probe response frame
- STAs in BSS (AP or non-AP STAs) measure radar or can request/report measurements each other in the current and other channels

Detecting radar and switching channel

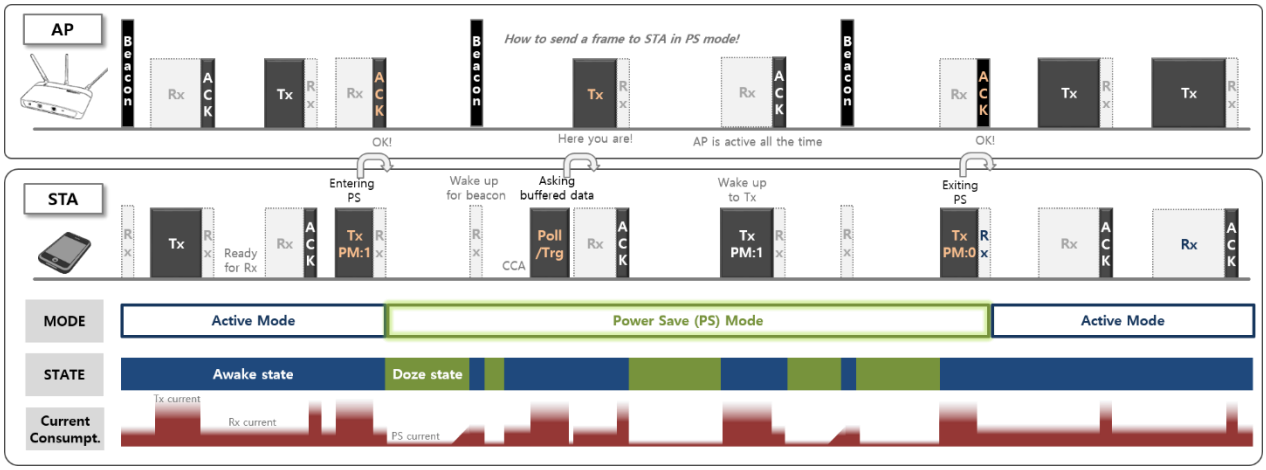
- If STA detects radar operating in the channel or accepts that another STA detects radar, STA stop transmission
- AP shall inform associated STAs that AP is moving to the new channel using CSA (Channel Switch Announcement) in beacon or probe response frame. AP may force STAs to stop transmission by setting Channel Switch Mode 1.
- The decision for channel switch in BSS shall only made by AP. AP may make use of the information on Supported Channel and measurement result to select the new channel.
- Non-AP STAs that receives CSA can switch the channel or choose to move to a different BSS

Power Management

Power Management Concept

IEEE specifies various way of power management (the current consumption management). Power Save (PS) mode in IEEE and doze (sleeping) state are not same.

- AP is always on, while non-AP STAs choose which Mode to go between Active and Power Save (PS) mode
- STA informs to AP when it enters or exits PS mode by setting Power Management bit in Frame Control subfield of MAC header
- In Power Save (PS) mode, STA is in one of “Doze state” or “Awake state”, while STA is always in “Awake state” in Active mode. STA is in deep sleep and consumes little current in Doze state and cannot transmit nor even receive frames.
- STA can wake up and send data, if it has something to send in PS mode. Key situation of PS mode is for AP to send data frame to STA in PS mode, as AP does not know if STA in PS mode is Awake state or Doze state. PS mechanism focuses on STA’s Rx in PS mode.
- Generally, the current consumption on doze state is about dozens of micro ampere, about dozens of milli-ampere in receiving active mode and about hundreds of milli-ampere in transmitting active mode. It highly depends on solution and hardware, but just to share the rough idea of how much current is consumed.



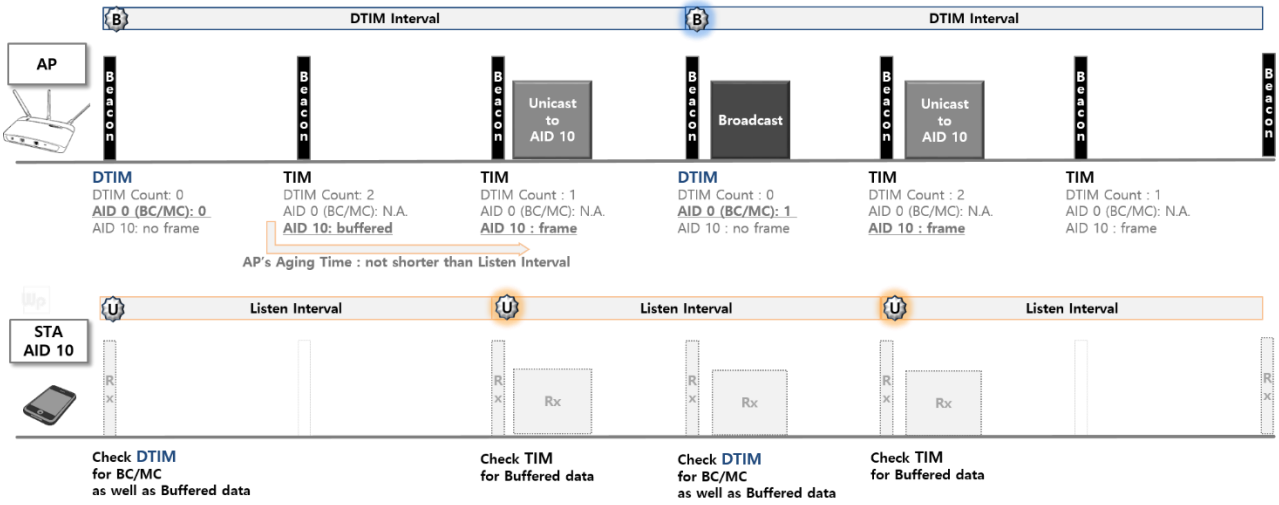
Power Management Concept

TIM and DTIM

Traffic Indication Map (TIM) element in Beacon frame has Virtual Bitmap that indicates STA's AID that AP has buffered the traffic for.

For AP to deliver broadcast or multicast frame to all the STAs that might be in PS mode, AP indicates that there is buffered broadcast/multicast frames by setting AID 0 in TIM. The TIM with the indication of broadcast/multicast as well as unicast buffered frame is Delivery TIM (DTIM). Beacon frame with DTIM is broadcasted by AP at every DTIM Interval and every STA should wake up and listen to it.

Along with DTIM, STA wakes up at every Listen Interval to check if there is any (unicast) buffered frame for the STA. AP uses the listen interval in determining the lifetime of frames that it buffers for STA. Listen interval is related to AP's buffer (memory) size.

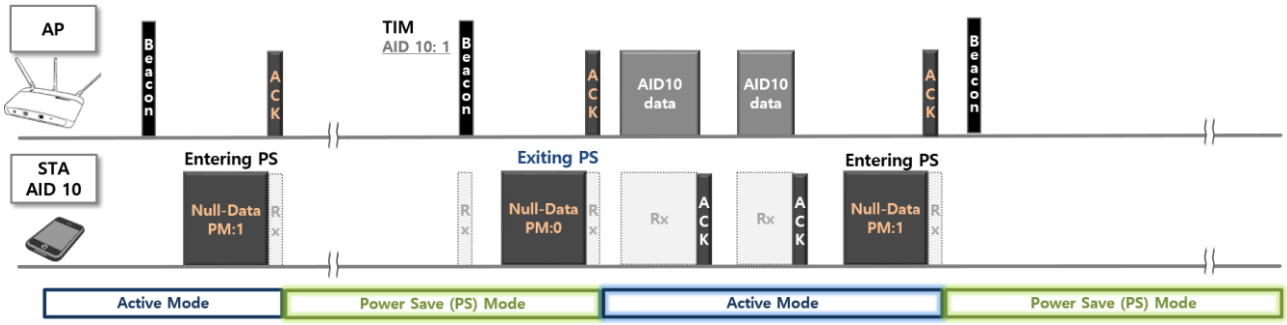


TIM and DTIM

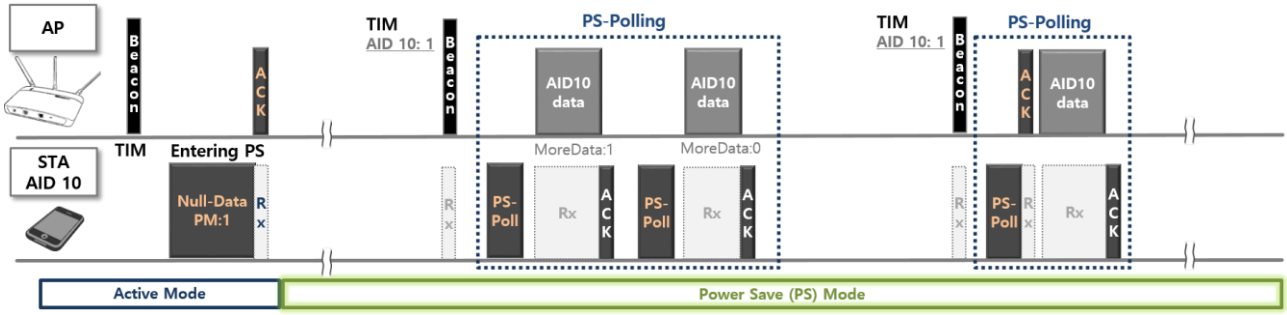
Legacy PM Mode

Supposing the situation that STA found the buffered frame for it in TIM of Beacon frame.

- Case 1 : STA exits from PS mode and gets the buffered frame, as AP knows STA is now in Active mode by exiting PS mode and AP can sends frame. After receiving, STA enters PS mode again by setting PS mode.
- Case 2 : STA stays in PS mode and it sends PS-Poll frame to AP indicating that it is ready for receiving the buffered frame.



Legacy PS Mode (Case 1)

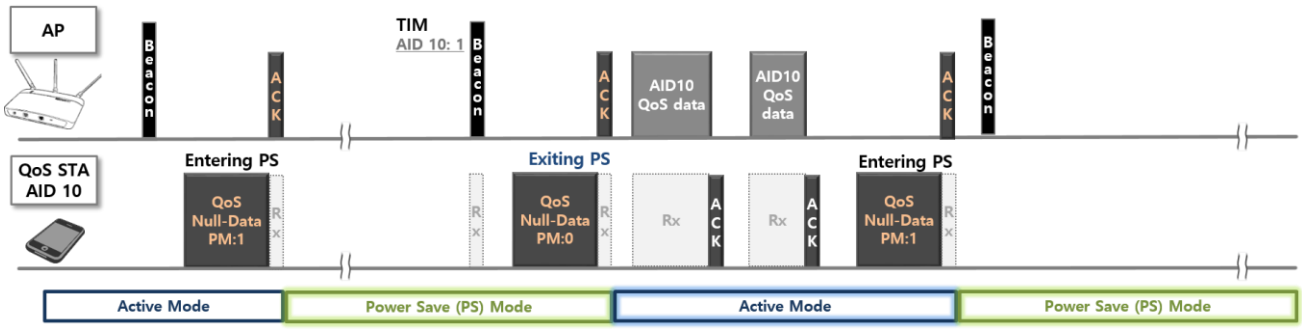


Legacy PS Mode (Case 2)

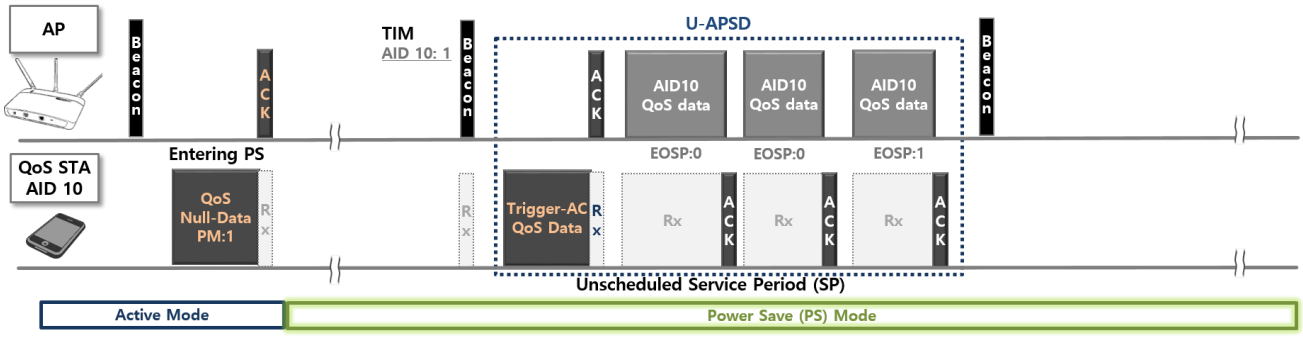
QoS PM Mode

When QoS STA found that there is buffered frame for it by TIM in Beacon frame,…

- Case 1 : STA exits from PS mode to get the buffered frame
- Case 2 : U-APSD (Unscheduled Automatic Power Save Delivery)
  - As WMM is Wi-Fi alliance certifications for EDCA of 802.11, WMM-PS is for U-APSD
  - STA may use U-ASPD to have some or all of buffered data during unscheduled SP (Service Period)
  - Unscheduled SP starts when QoS STA transmits a trigger frame to QoS AP
    - trigger frame is QoS (Null) Data using AC the STA has configured to be trigger-enabled. (different from the trigger frame in 11ax)
  - By setting EOSP (End of SP) subfield to 1 in the last frame during SP, unscheduled SP may be terminated



QoS PS Mode (Case 1)

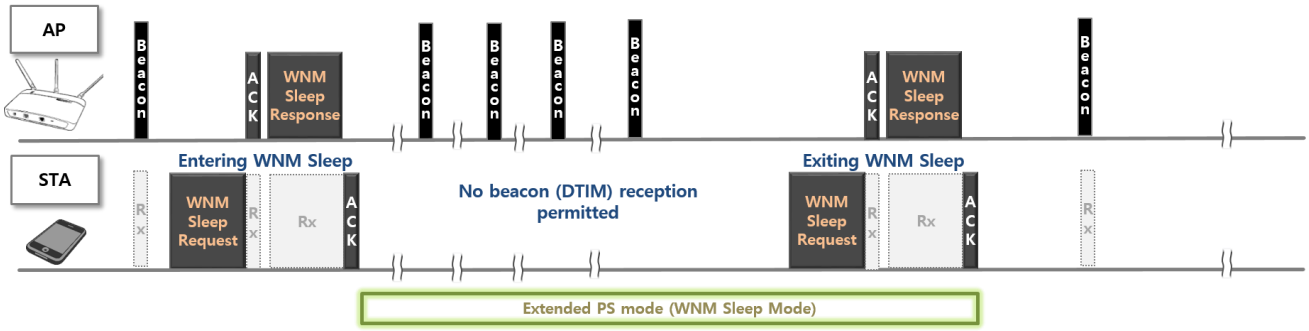


QoS PS Mode (Case 2)

WNM PS Mode

Wireless Network Management (WNM) Sleep mode is an extended PS mode.

Non-AP STA does not need to listen for every DTIM Beacon frame in WNM sleeping mode. WNM sleep mode is enabled, when a non-AP STA to signal to an AP that it might sleep for a specified time. It enables to reduce power consumption and remain associated. 11ax has advanced scheduling scheme of TWT.

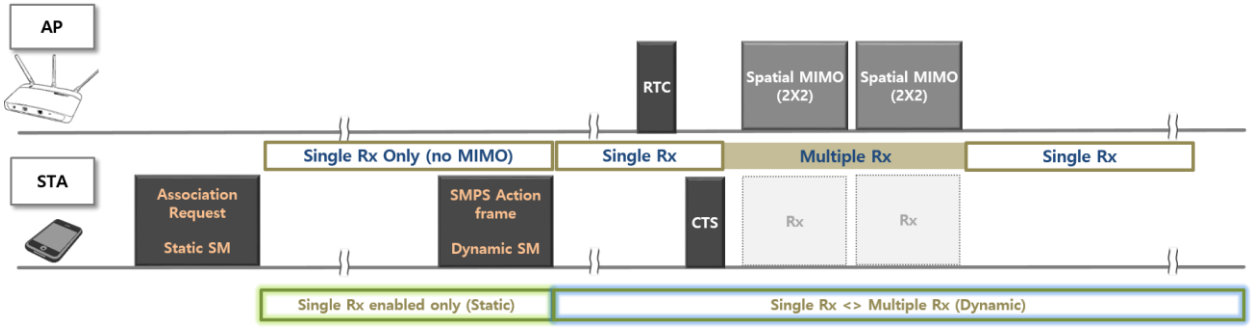


WNM PS Mode

Spatial Multiplexing (SM) Power Save Mode

It allows non-AP STA in BSS to operate with only one active Rx chain for a significant portion of time.

- Static SM PS mode : STA maintains only a single Rx chain active
- Dynamic SM PS mode : STA enables multiple Rx chain, after the frame addressed to the STA is received. RTS/CTS may be used.

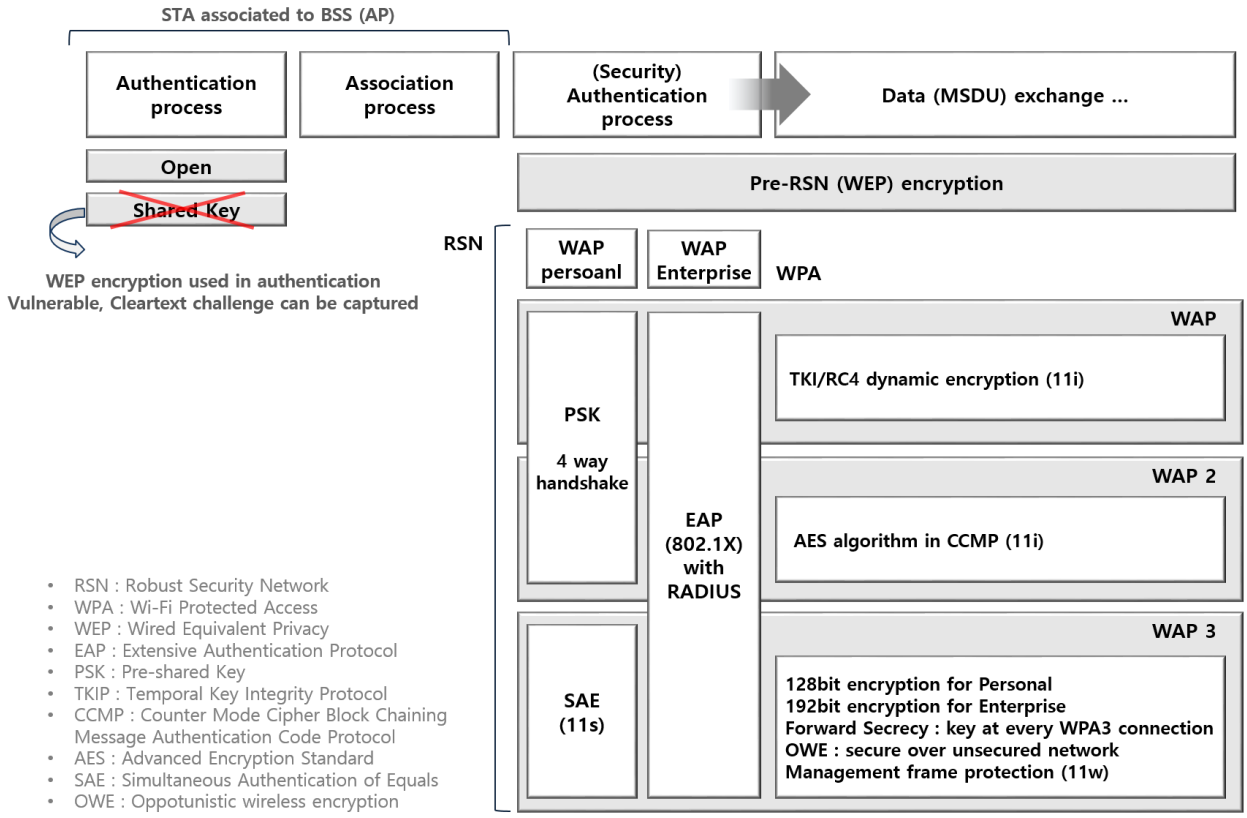


SM PS Mode

Authentication and Encryption

Authentication and Encryption

For Security, both Authentication and Encryption are applied and RSN with EAP (WAP Enterprise) or RSN with PSK (WPA Personal) is recommended for Authentication. WPA3 is a mandatory for Wi-Fi from 2018.



Authentication and Encryption

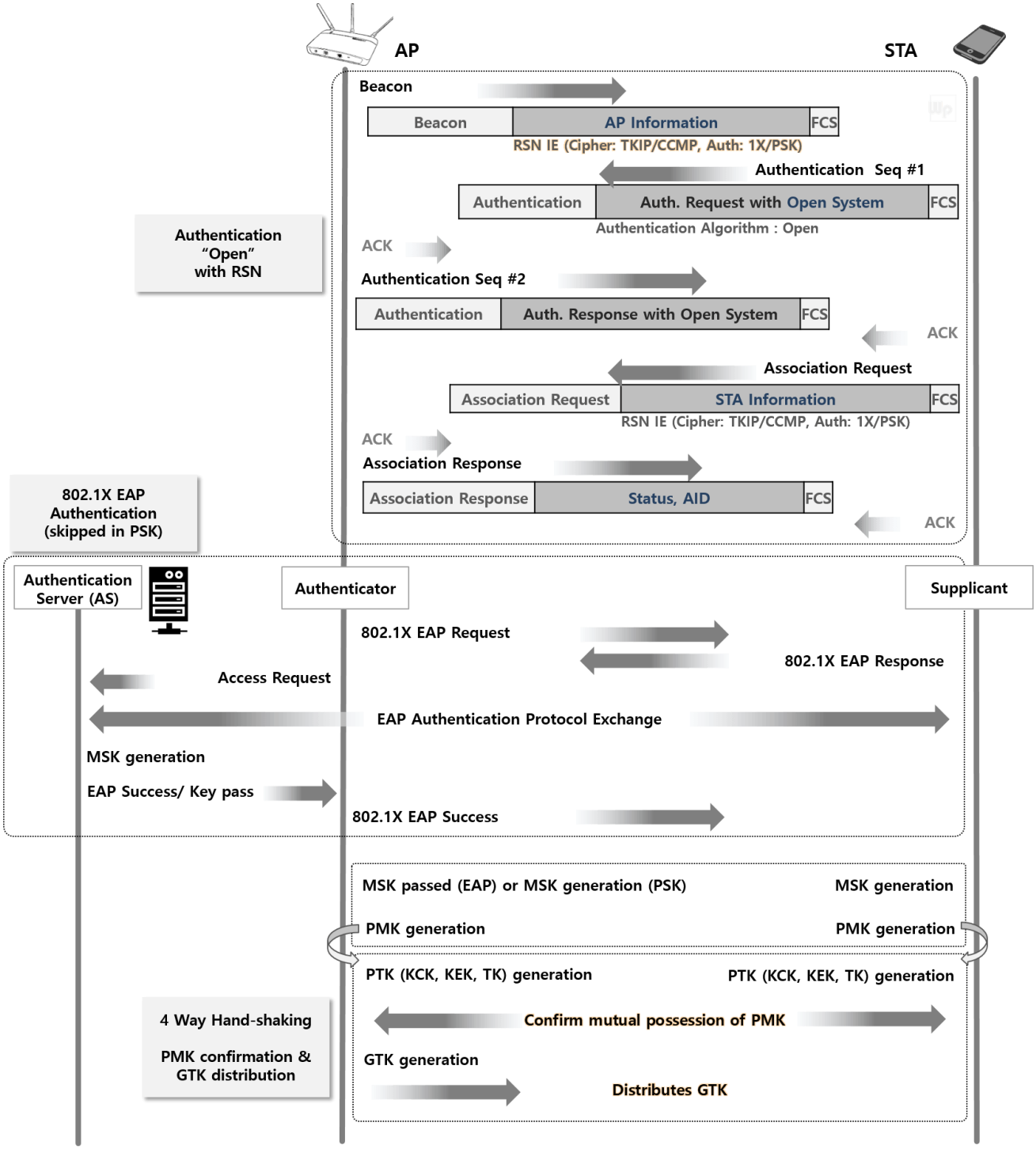
RSN flow

For RSN (Robust Security Network), Authentication frame exchange is with “Open” and EAP (Extensive Authentication Protocol) has additional Authentication between Supplicant (non-AP STA), Authenticator (AP) and Authentication Server (RADIUS server), which process is skipped in PSK. After that, confirming mutual possession of PMK and distributing GTK by AP is Key management and distribution process in 4-way handshaking.

- MSK (Master Session Key) : Keying material between EAP peers
- PMK (Pairwise Master Key) : The key derived from a key by EAP method or obtained directly from PSK
- PTK (Pairwise Transient Key) : Concatenation of session key derived from PMK. Its components are KCK, KEK, TK, which are used to protect information
  - KCK (Key Confirmation Key)

- KEK (Key Encryption Key)
- TK (Temporal Key)

- GTK (Group Temporal Key) : A random value, assigned by group source. Mapped to TKIP, CCMP keys



RSN flow

11ax, High Efficiency WLAN

11ax HE Overview

11ax facilitates WLAN outdoor operation and enhances the average throughput per station. Looking inside the details, there are changes in OFDM modulation, introduction of multi-user operation with OFDMA and the new features like spatial reuse (BSS Color) and TWT.

What is 11ax for?

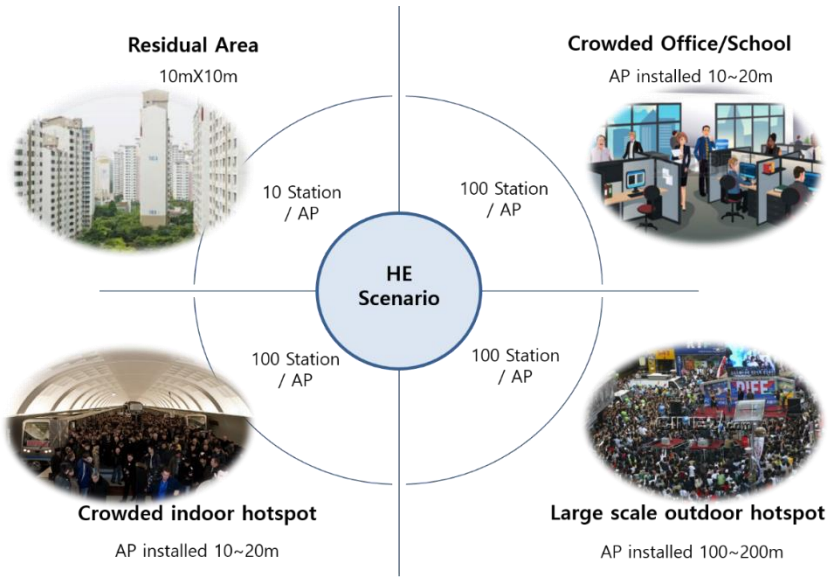
Looking over 11ax Project Authorization Request, we can find the purpose of 11ax amendment. The main change is for outdoor operation of WLAN and the improvement of average throughput enhancing spectral efficiency. Specification framework is as below

11ax PAR (Project Authorization Request)

- The focus of this amendment is on WLAN indoor and outdoor operation in the 2.4 GHz and the 5 GHz frequency bands. Additional bands between 1 GHz and 6 GHz may be added as they become available.
- The increase in average throughput per station is not limited to four times improvement. Improvement values in the range of 5-10 times are targeted, depending on technology and scenario.
- Outdoor operation is limited to stationary and pedestrian speeds.
- Since the values of the metrics of interest will depend on the scenario, the focus will be on the relative improvement of these metrics compared to previous IEEE 802.11 amendments (IEEE 802.11n in 2.4 GHz and IEEE 802.11ac in 5 GHz).

Use case

Considering very crowded WLAN environment outdoor as well as indoor. 11ax is expected to operate with the scenario.



HE Use Cases

11ax vs. 11ac

Frequency, bandwidth and MIMO stream of 11ax will be the same with 11ax, while there will be changes in OFDM modulation, multi-user operation along with many additional features in MAC and PHY layer for spectral efficiency. (6GHz support in 11ax is discussed later)

		11ac	11ax
Frequency		(2.4G and) 5GHz ***11ax supports 6GHz***	
Bandwidth		20, 40, 80, 80+80, 160MHz	
MIMO		8 stream	
Modulation	OFDM	OFDM	OFDM
	Subcarrier Spacing	312.5KHz	78.125KHz
	Up to	256QAM	1024QAM
Multiplexing	Basic operation	CSMA/CA	CSMA/CA
	Multi-User	MU-MIMO	OFDMA, MU-MIMO
	MU-MIMO	DL MU-MIMO (4 users)	DL/UL MU-MIMO (8 users)

11ac vs 11ax Comparison

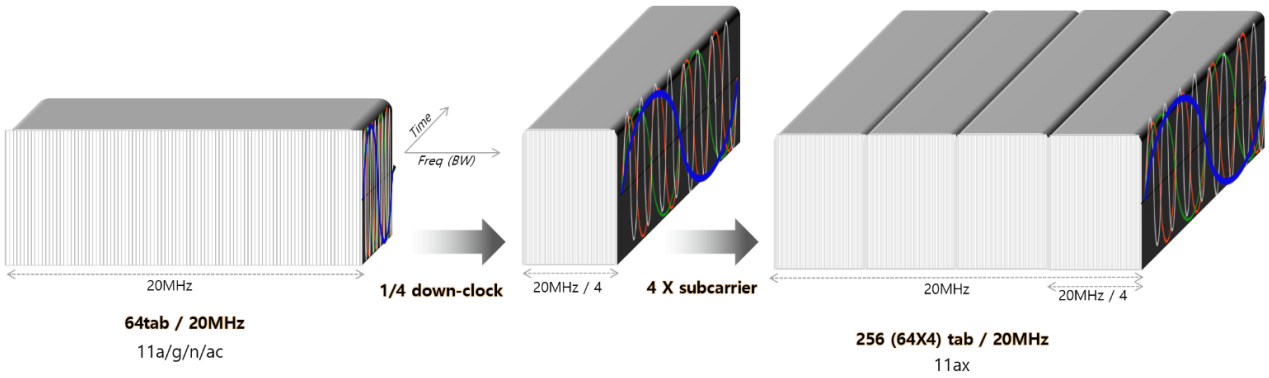
- New feature : OFDMA, UL MU-MIMO, 1024QAM, Spectral Reuse
- Frequency, bandwidth and MIMO stream : same as 11ac

Change in OFDM and Outdoor operation

OFDM symbol changes in 11ax with 4 times more subcarriers allocated to have 4 times longer OFDM symbol. Logically, data rate from this change is the same with the previous OFDM, while 11ax can apply 4 times longer Guard Interval without dropping data rate. The delay spread from multipath fading in outdoor space is longer than the fading indoor and Guard Interval in legacy OFDM cannot handle it effectively, while new Guard Interval in 11ax can.

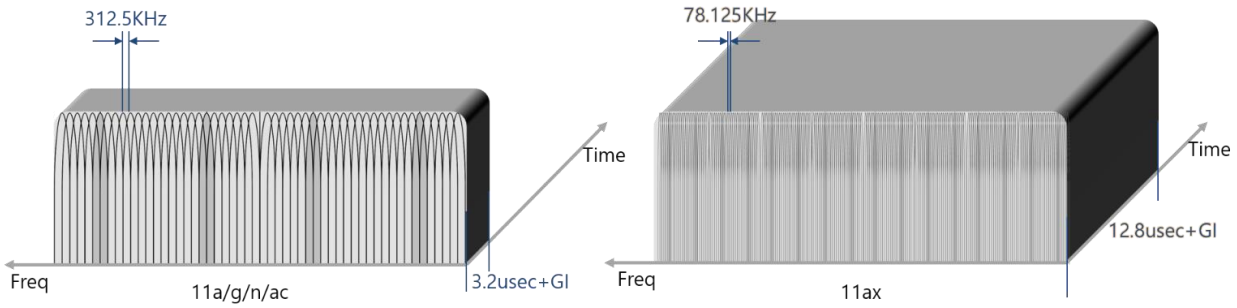
Change in OFDM modulation

Different from OFDM symbol in 11a/g/n/ac that uses subcarrier assigned in 64 tab per 20MHz, 11ax allocates 4 times more subcarriers and subcarrier spacing becomes 1/4 accordingly. The symbol duration increases 4 times more, as it is inversely proportional to subcarrier spacing. To sum up, 11ax OFDM has 4 times more subcarriers in 4 time longer symbol.



Subcarrier Spacing and Symbol Duration

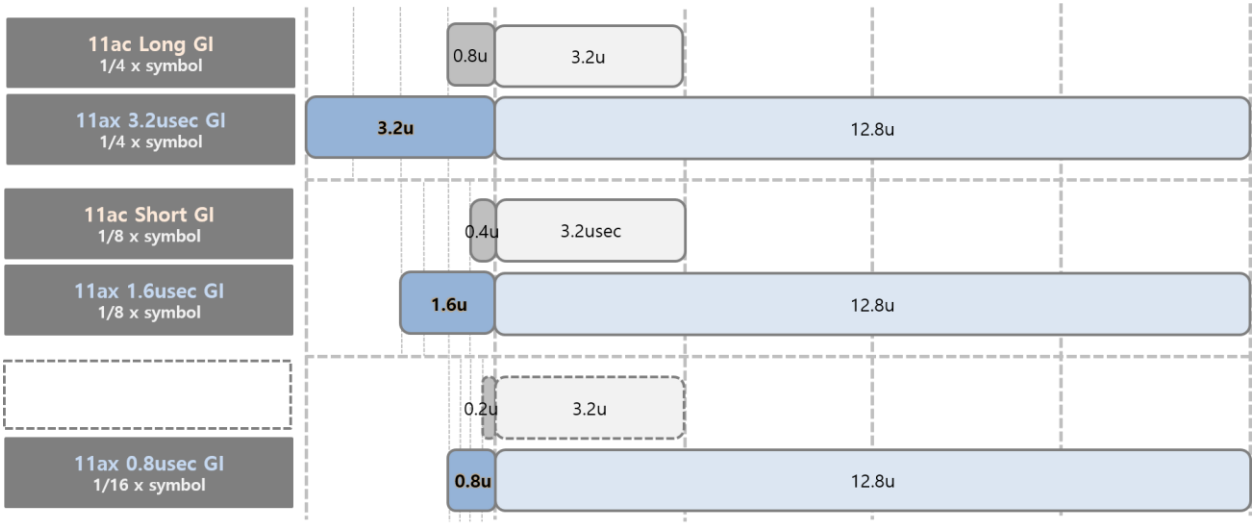
Subcarrier spacing becomes 1/4 of the previous OFDM symbol and symbol duration gets 4 times longer. Logically, data rate from this change will be the same.



	11ac	11ax	
FFT for OFDM (20MHz)	**64 tab**	**256 tab**	4 times of 11ac
Spacing of subcarrier	**312.5KHz** (20MHz/64)	**78.125KHz** (20MHz/256)	1/4 times of 11ac
FFT period	**3.2usec** (1/ 312.5KHz)	**12.8usec** (1/ 78.125KHz)	4 times of 11ac

Guard Interval in 11ax

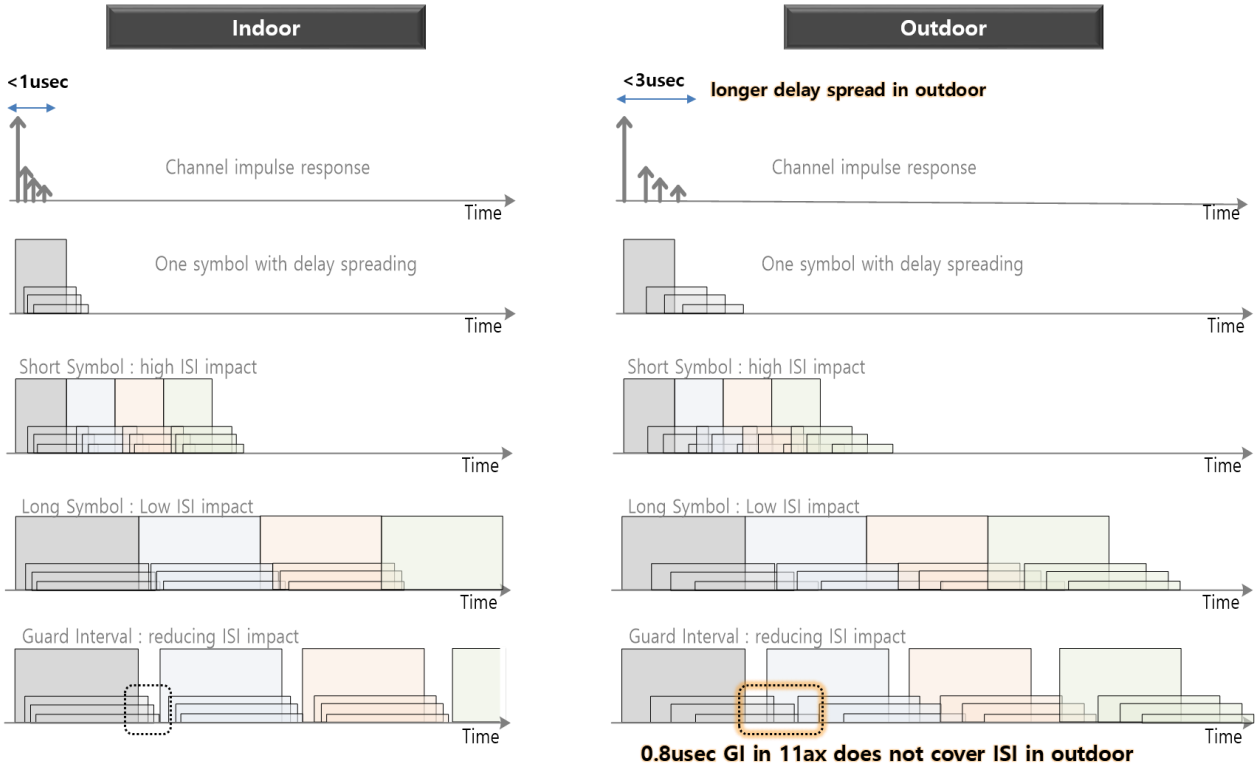
There are two Guard Interval (GI) of Long GI (0.8usc) and Short GI (0.4usc) in 11ac and 11ax adopts three types of GI, which are Quadruple (3.2usec), Double (1.6usec) and Normal (0.8usec) GI. As the symbol duration gets longer by 4 times, 4 time longer GI compared to Long/Short GI does not drop the data rate. In addition, Normal GI makes data rate slightly higher than the legacy symbol with short GI.



Guard Interval	Duration	IFFT period	Symbol duration	comments
Quadruple	**3.2usec**	12.8usec	16usec	**robustness in outdoor delay spread** Same as long GI of 11ac in percent-wise
Double	**1.6usec**	12.8usec	14.4usec	**Same as short GI** of 11ac in percent-wise
Normal	**0.8usec**	12.8usec	13.6usec	About 15% faster than 3.2u GI symbol **high indoor efficiency**

Pre-HE OFDM in outdoor operation

Long GI of pre-HE OFDM (11a/g/n/ac) effectively prevents Inter-Symbol Interference (ISI) of indoor delay spread (<1 usec). However, as outdoor delay spread is longer than indoor one (considering the case that RF signal experiences long multipath), 0.8usec GI cannot effectively prevent ISI from outdoor multipath fading.

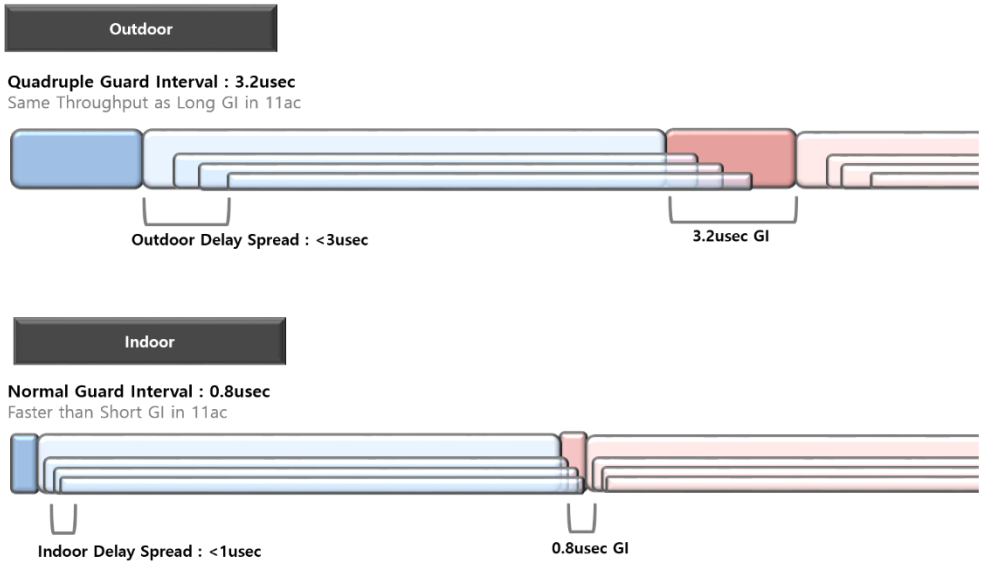


What happens with 11ac in outdoor operation?

11ax OFDM in indoor and outdoor operation

3.2usec GI in 11ax is relatively same with Long GI (0.8usc) in pre-HE and it can effectively prevent the outdoor delay spread (<3 usec) without the data rate drop compared with Long GI. Normal GI (0.8usec) in 11ax covers the indoor delay spread, while it makes overall relative symbol duration shorter than Short GI of pre-HE.

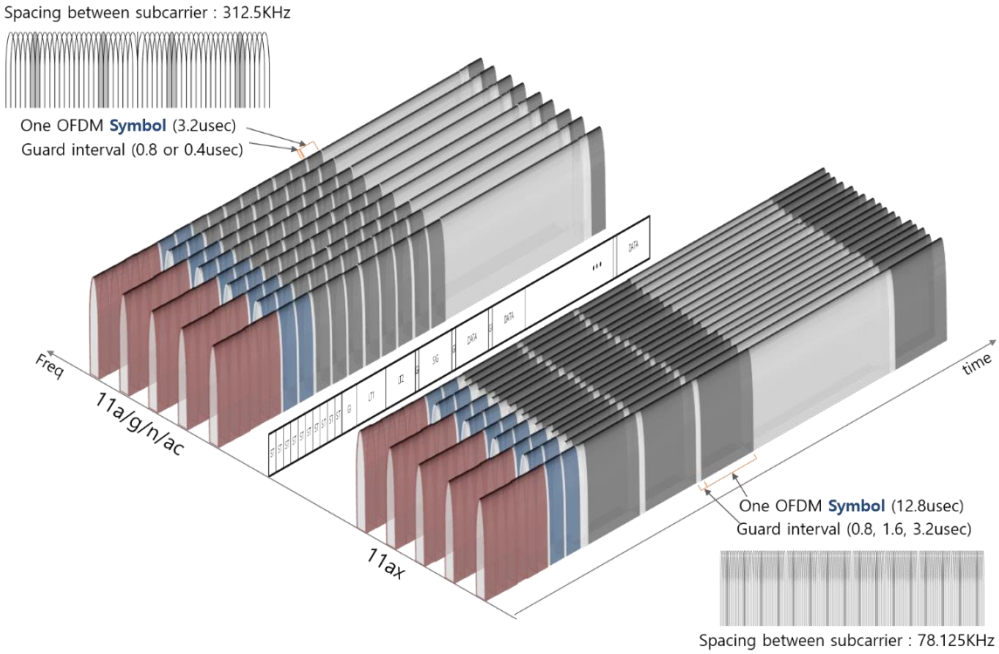
There is no criteria to decide if STA is operating indoor or outdoor environment. GI is one of the factors for the data rate decided by the rate adaptation algorithm.



11ax in Indoor and Outdoor Fading Channel

Legacy packet and 11ax packet

The image below is just to give you the brief concept of PHY packet. In 11ax, there will be more number of subcarriers in each symbol and the duration of the symbol will be longer. Overall 11ax packet length does not necessarily get longer than 11ac, as 4 times more subcarriers carry more data. Preamble of the packet of 11ax is the same with 11ac for backward compatibility.



PHY Packet for 11ac and 11ax (Conceptual)

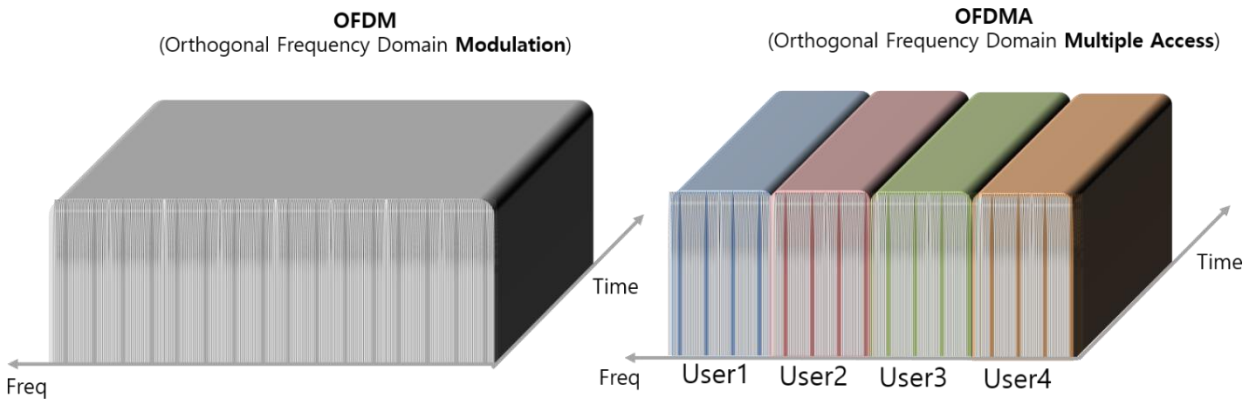
OFDMA and Average TPUT

One packet is used by one user in 11ax like pre-HE. Along with it, one packet can be used by/for the multiple users with newly devised OFDMA scheme in 11ax. OFDMA allocates subcarrier groups to users, which is called as Resource Unit (RU) and 26, 52, 106, 242, 484, 996 tone (subcarrier) can be allocated to one RU.

Logically, there is no benefit on the average throughput using OFDMA compared to non-OFDMA in pre-HE. However, comparing the situations that the same power is transmitted in one RU (small portion of BW) and in whole BW, SNR gests better with transmission of one RU and the gain can be utilized for the higher data rate. This improves the average throughput in 11ax uplink OFDMA. In Downlink, the transmit power and SNR cannot be improved as in uplink, as packet is transmitted by only one station, AP. Instead, there can be efficiency by reducing overhead like receiving Ack or minimizing contention. Access Point can also utilize Power Boost for partial SNR enhancement.

OFDM and OFDMA

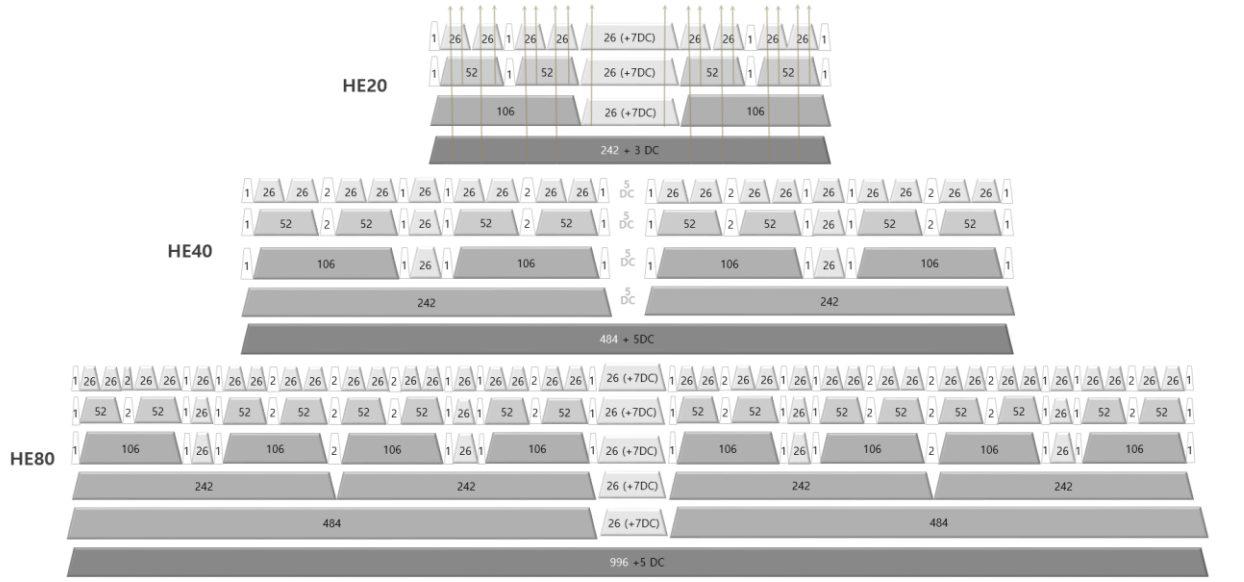
OFDM (Orthogonal Frequency-Division Multiplexing) and OFDMA (Orthogonal Frequency Division Multiple Access) are different level of concept. OFDM is modulation scheme and OFDMA is multiple access scheme using OFDM. 11ax introduces OFDMA to maximize the “resource utilization” and “multiplexing flexibility”. 11ax subchannelizes subcarrier group assigned to each user, which is “Resource Unit, RU”



OFDMA, newly introduced in HE

RU allocation in 11ax

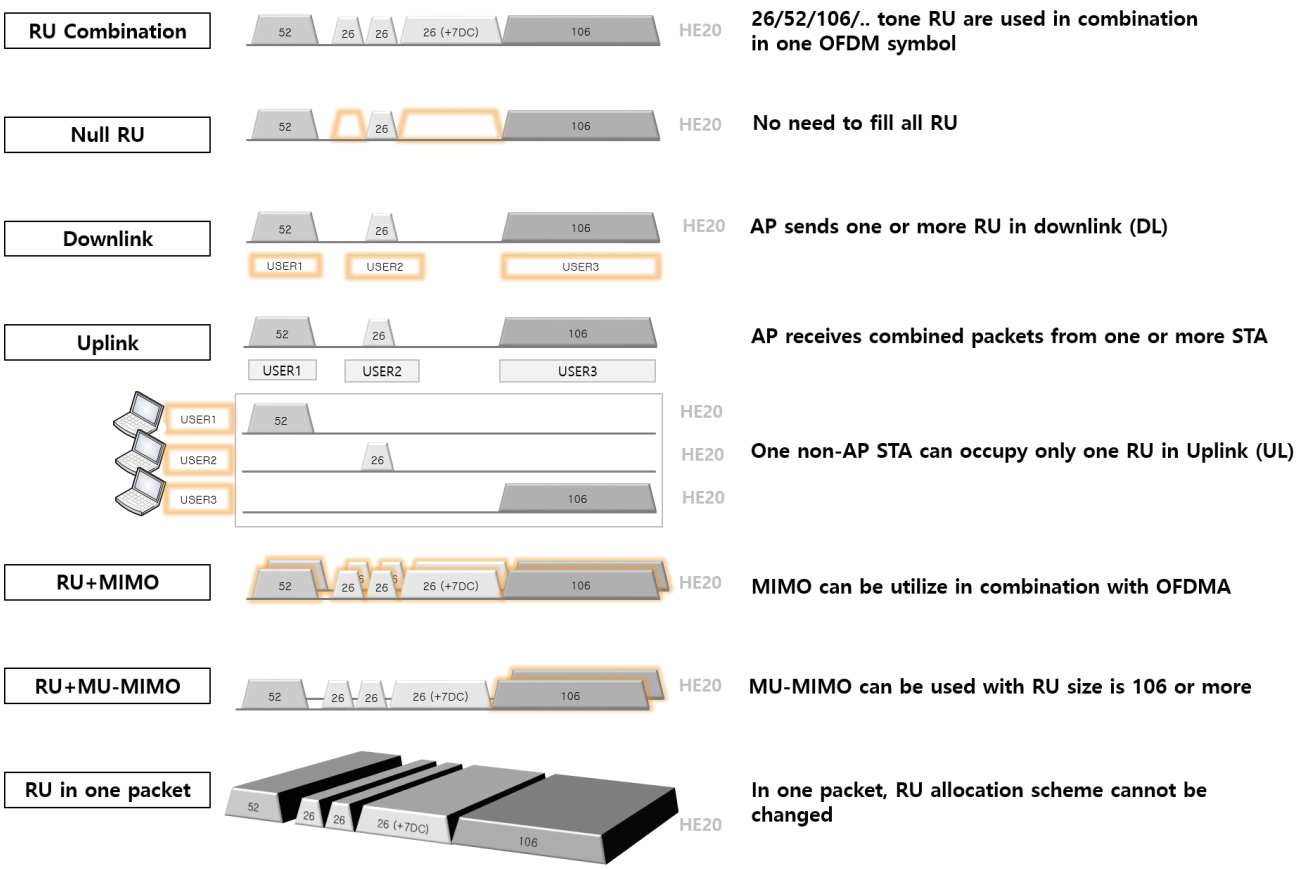
Based on tone size of subcarrier, 6 kinds of RU are defined, which are 26, 52, 106, 242, 484 and 996 tone RU. In 20MHz (HE20), up to nine 26-tone RU, four 52-tone RU and two 106 RU can be allocated. 242-tone RU occupies 20MHz and 26-tone RU occupies about 2MHz (about 1/10 of 20MHz). OFDM in HE has 256 subcarriers in 20MHz BW and most of the subcarriers are used for data, while some subcarriers in band edge, center and between RU are not used and some are used for Pilot subcarrier. The arrows in the image below indicate Pilot subcarriers. The center of RF signal should be suppressed to minimize carrier leakage and the subcarriers in OFDM center are nulled (5DC or 7DC)



RU type	CBW20	CBW40	CBW80	CBW160 and CBW80+80
26-subcarrier RU	9 RU	18 RU	37 RU	74 RU
52-subcarrier RU	4 RU	8 RU	16 RU	32 RU
106-subcarrier RU	2 RU/MU-MIMO	4 RU/MU-MIMO	8 RU/MU-MIMO	16 RU/MU-MIMO
242-subcarrier RU	1-SU/MU-MIMO	2 RU/MU-MIMO	4 RU/MU-MIMO	8 RU/MU-MIMO
484-subcarrier RU	N/A	1-SU/MU-MIMO	2 RU/MU-MIMO	4 RU/MU-MIMO
996-subcarrier RU	N/A	N/A	1-SU/MU-MIMO	2 RU/MU-MIMO
2x996 subcarrier RU	N/A	N/A	N/A	1-SU/MU-MIMO

RU allocation in HE

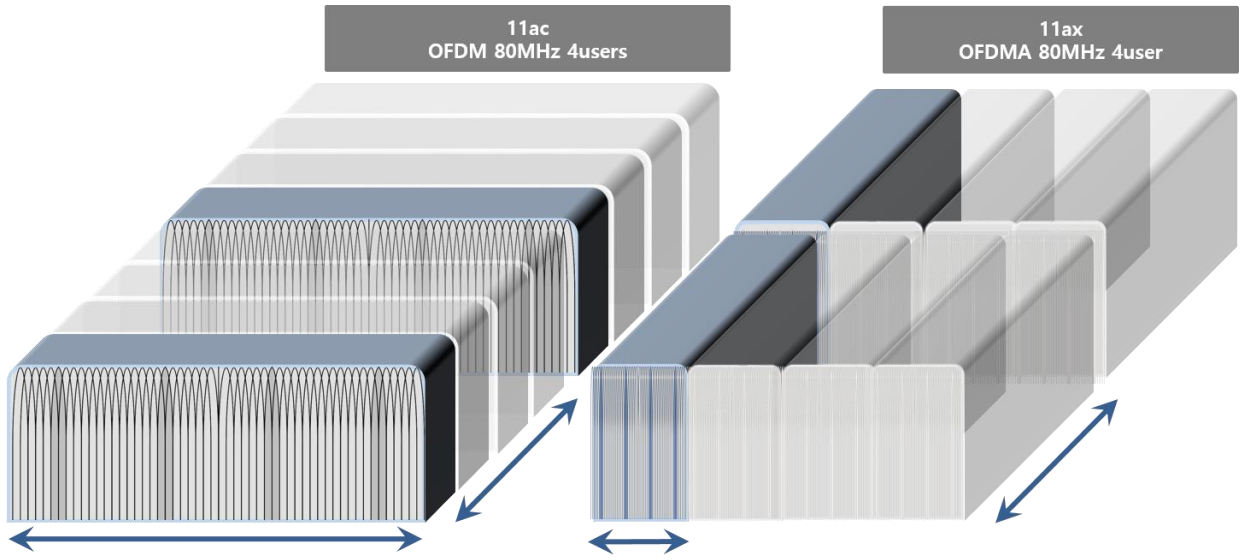
Basic Concepts on RU allocation



Basic concepts on RU allocation

Does 11ax network have higher average throughput per user than 11ac?

Considering the case that 4 users are in 11ac non-OFDMA and 11ax OFDMA network. Blue user in both 11ac (left) and 11ax OFDMA (right) in the image below sends data carried in the same number of subcarrier during the same average period of time. Logically, per-user average throughput between 11ac and 11ax is the same.



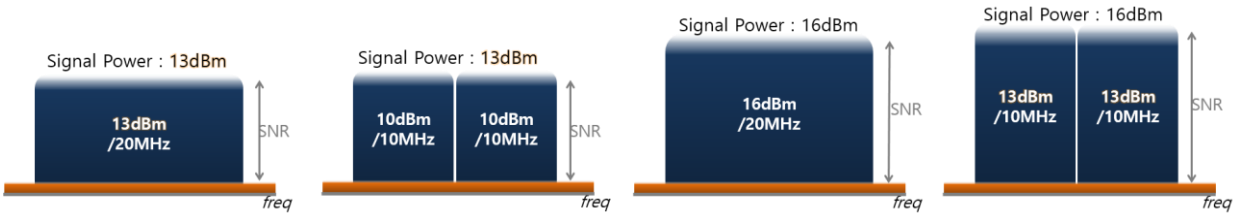
Blue user in 11ac and 11ax send information in same number of subcarrier in same period
➔ Logically, 11ac and 11ax have the same average TPUT

Does 11ax network have higher throughput than 11ac?

Signal Power, Bandwidth and SNR

To see how OFDMA brings spectral efficiency, let's take a look at signal power and SNR (Signal to Noise ratio). Power concept in frequency domain is better to be approached by power spectral density. When the signal power over 20MHz is 13dBm, the partial signal power of 10MHz is 10dBm (half) each. If the power of 10MHz portion is 13dBm, the overall 20MHz signal with 13dBm/10MHz + 13dBm/10MHz is 16dBm (double).

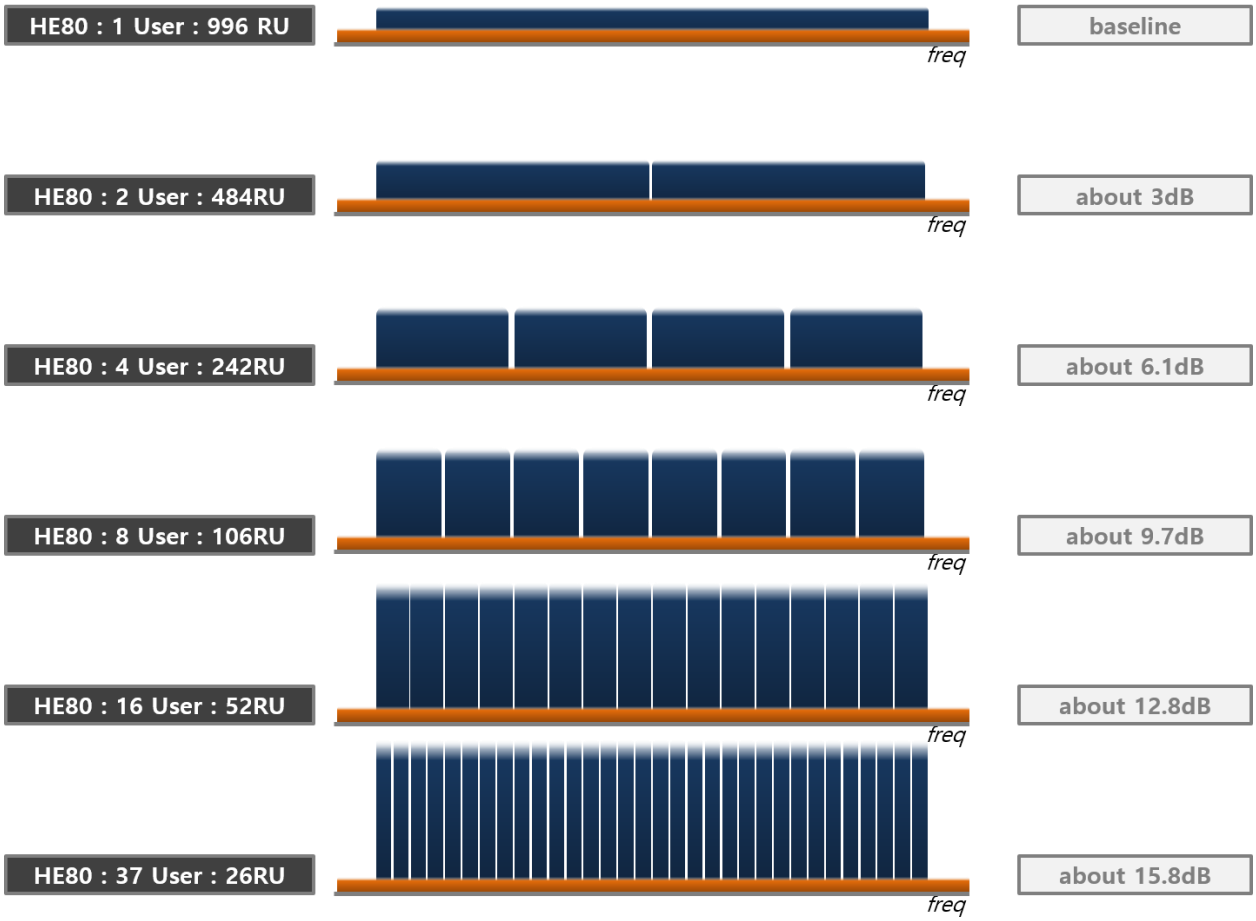
Noise (orange portion in the picture) is proportional to bandwidth. Considering two cases (1) one user transmits the signal in 13dBm/20MHz (the first picture) and (2) two users transmit the signals in 13dBm/10MHz each (the last picture), SNR of the last case is 2 times higher than the first case. No wonder is the high overall power signal (the last one with 16dBm) has 3dB (2 times) higher SNR than the low power signal (the first one with 13dBm).



Concept on 106 tone RU power and SNR

When one or many users transmit the signal with the same RU power in 80MHz

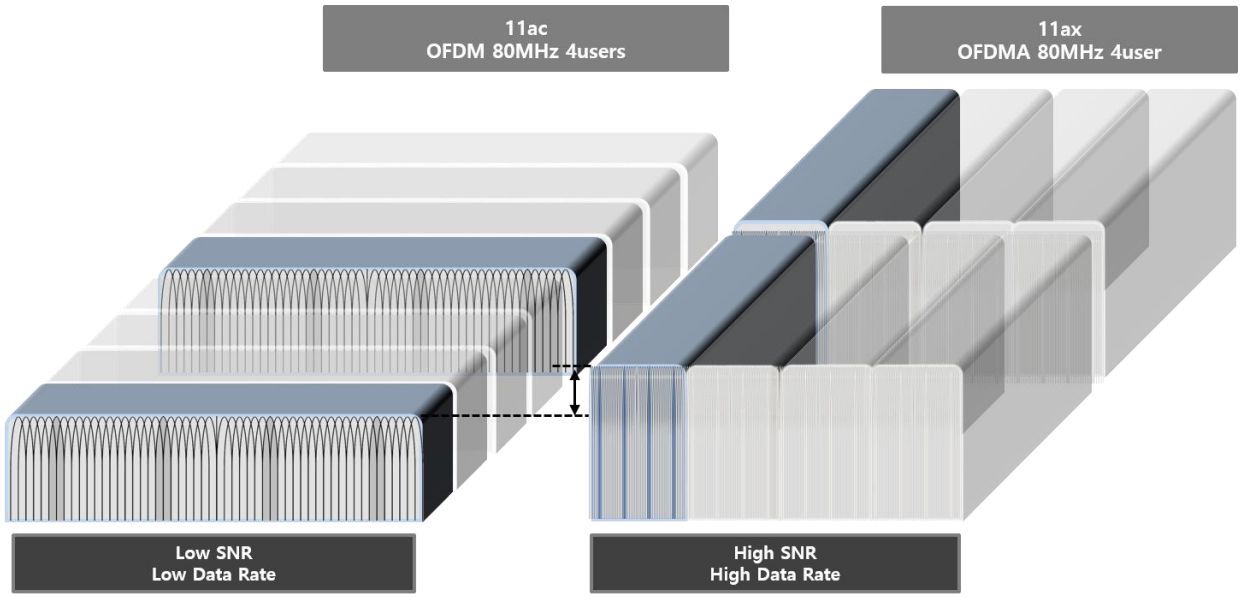
When one user transmit signal with 10dBm power over 80MHz, the signal power is 10dBm. If two users are transmitting with 10dBm over 40MHz each, the overall power of 80MHz is 13dBm. If 37 users are transmitting 10dBm with 26-tone RU over 80MHz, the overall signal power becomes about 15.8dB more, which is 25.8dBm. SNR increases accordingly.



OFDMA gain : SNR in case of the same RU power

Average Throughput improvement with OFDMA : Uplink

Even if average throughput is the same between 11ac and 11ax logically, 11ax can utilize higher data rate with higher SNR from OFDMA gain, which results in high average throughput. This benefit is mainly true for uplink, as the transmitted power from each users are combined in uplink packet, while AP's transmit power is supposed to be the same and has nothing to do with OFDMA.



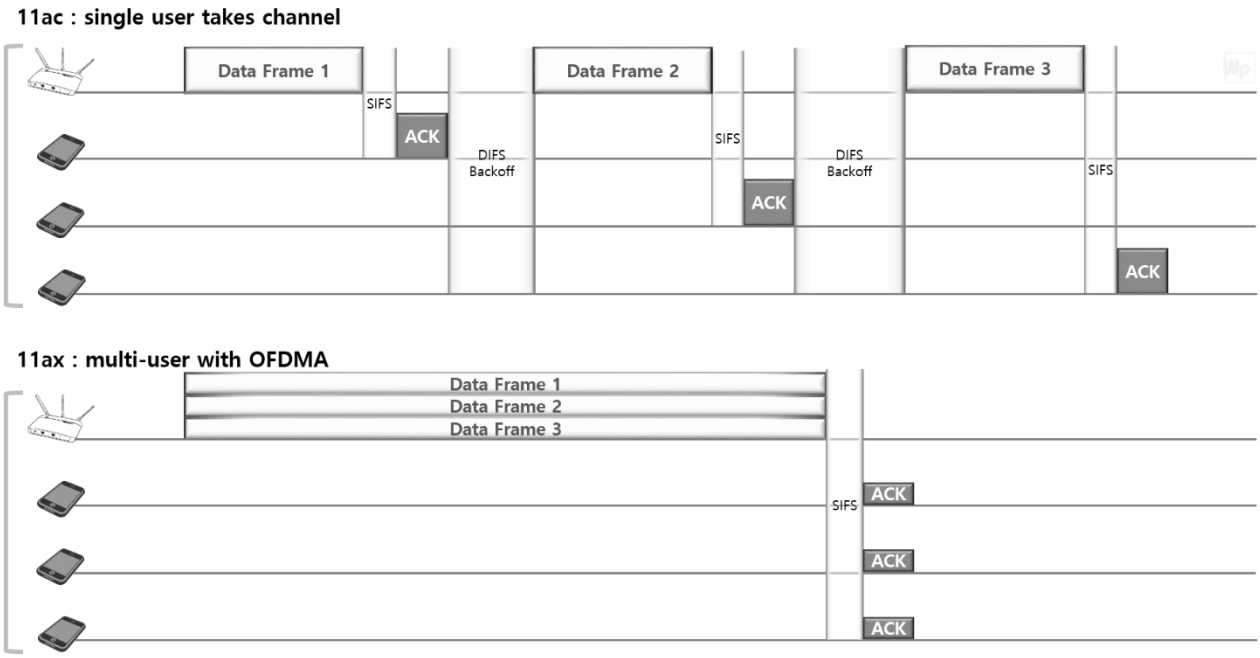
If each User in 11ac and 11ax transmit with the same power

OFDMA → RU (1/user) → Small bandwidth → High SNR → High Data Rate → High average throughput

Average Tput improvement with high SNR

Downlink Efficiency : reducing Access Control overhead

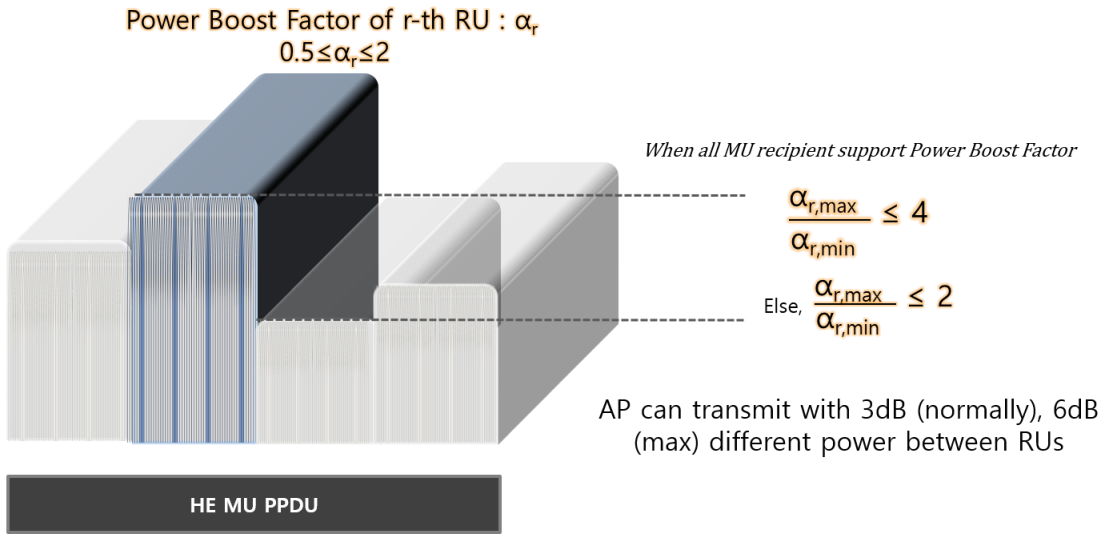
With OFDMA, downlink can get efficiency by reducing access control and contention that happens in DCF. As access is more frequent with many short packets in network, the efficiency from downlink OFDMA will be increased.



OFDMA efficiency in DL

Downlink Efficiency : Power Boost

AP can transmit with different power to each RU with Power Boost factor in HE MU PPDU, which may bring another benefit in downlink OFDMA. Minimum and Maximum ratio of Power Boost factor is limited to 2 (3dB) and AP can use up to 4 (6dB), when Power Boost Factor Support subfield of HE PHY Capability information field in HE Capability element from all the recipient STA is set. Power Boost factor is 1 in single user packet (HE SU PPDU and ER PPDU).



Power Boost for DL

HE PHY Packet

Before 11ax, there has been little difference in physical layer between AP and non-AP STA with no concept of downlink or uplink. It is still true in 11ax in case of single user, while downlink (from AP) and uplink (to AP) notion was brought out with the new types of packet for multi-user. MU PPDU is for multi-user DL and TB PPDU is for multi-user UL.

IEEE defines some mandatory features in 11ax and OFDMA (Tx/Rx of MU PPDU and TB PPDU) support is one of them. Guard Interval and LTF size are defined by the packet type and LDPC coding is mandatory for higher rate (MCS10, 11) and wider BW than 20MHz. DCM is delivering same information in two subcarriers to get diversity and it is only applied in low data rate. To give the receiver the time for decoding and processing the complex signal with more subcarriers with LDPC, 11ax defines Packet Extension in combination of Padding. Midamble (LTF in the middle of packet) is the new concept introduced in 11ax to handle the time variant fading like Doppler effects.

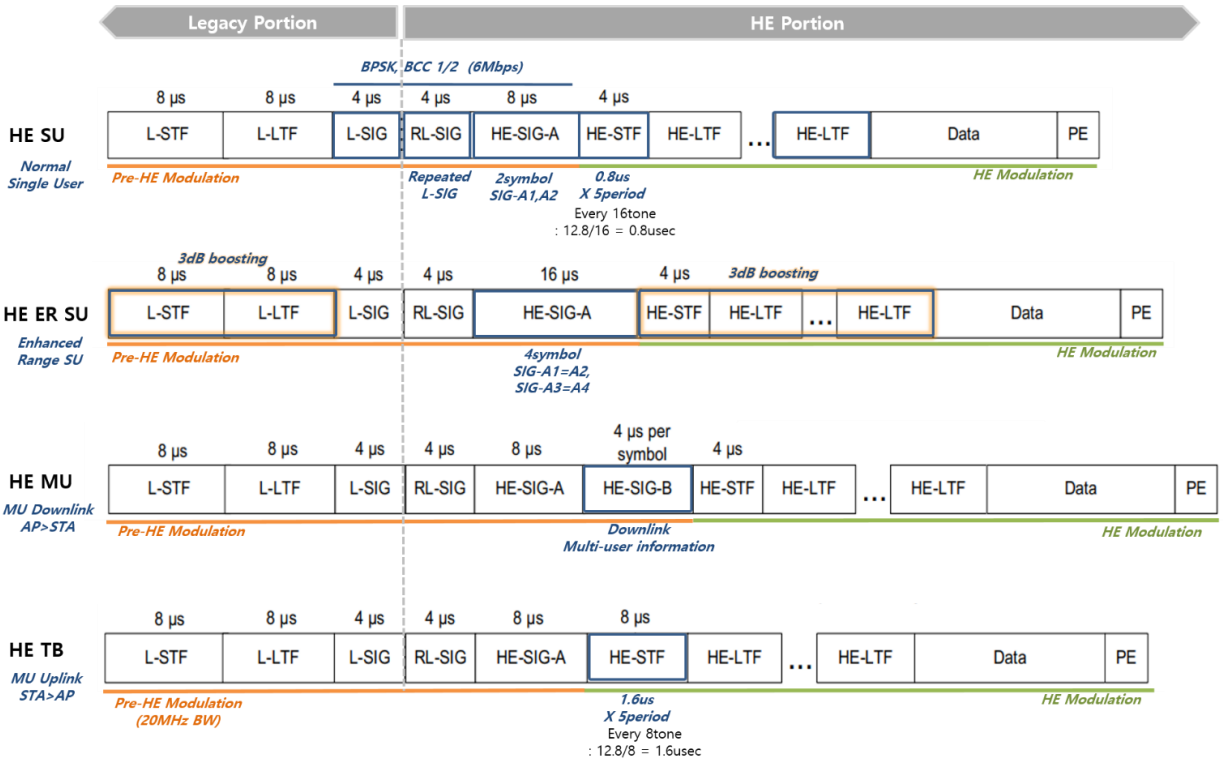
Four types of PHY packet

Before 11ax, WLAN has been using the same type of PPDU between STAs (AP or non-AP STA) and STAs are treated equally in PHY layer, while 11ax starts adopting the concept of Downlink (AP to non-AP STA) and Uplink (non-AP STA to AP) in multi-user case.

- HE SU PPDU : [DL/UL] Normal Single User PPDU
- HE ER SU PPDU : [DL/DU] Enhanced Range SU PPDU, Training fields are boosted by 3dB to extend range. Packet structure is same with HE SU PPDU except HE-SIG-A field repetition.
- HE MU PPDU : [DL] Multi-user PPDU from AP
- HE TB PPDU : [UL] Trigger-based PPDU for Multi-user (OFDMA, MU-MIMO) operation from each non-AP STA

Each type of PPDU consists of Legacy portion and HE portion. And Legacy portion consists of L-STF, L-LTF and L-SIG, which is for backward compatibility. In terms of modulation, there is Pre-HE modulation part which is modulated and encoded in legacy OFDM. Legacy portion and Pre-HE part do not match. RL-SIG is repeated legacy SIG field, which helps the recipient STA to interpret the packet.

- HE-SIG-A : duplicated on each 20MHz which contains PHY information of the packet like DL/UL, BSS Color, CP(GI)+LTF size, Spatial Reuse, Duration, MCS, BW, etc
- HE-SIG-B : separately encoded on each 20MHz which contains multi-user information. This field exits only in MU PPDU (DL)



11ax Packet Types

HE Mandatory Features

To call WLAN STA as 11ax device, OFDMA DL and UP should be supported. AP shall transmit MU PPDU and receive TB PPDU and non-AP STA shall transmit TB PPDU and receive MU PPDU. Find the details in the table below

	HE Mandatory
All STA	• SU with 1 RU for entire BW • 1SS, MCS0~7 • 20MHz, All RU size • ER in 1SS, 20M BW, MCS0~2 • Not used : SS > 1, BW > 20MHz, >MCS2 with 242 tone, >MCS0 with 106 tone
AP STA	• Tx of MU PPDU (DL) without MU-MIMO • Rx of TB PPDU without MU-MIMO • Tx of MU PPDU with 1 RU for whole BW with MU-MIMO, when AP of 4SS • MU PPDU at HE-MCS0~5 • 1SS HE-MCS0~7 for all supported BW and RU for MU PPDU (Tx) and TB PPDU (Rx)
Non-AP STA	• Rx of MU PPDU without MU-MIMO • Tx of TB PPDU without MU-MIMO • Rx of MU PPDU with 1 RU for entire BW with MU-MIMO • Responding with the requested beamforming feedback • Rx of MU PPDU at HE-MCS0~5 • 1 SS HE-MCS0~7 in all supported BW and RU sized for MU PPDU (Rx) and TB PPDU (Tx) • All RU in 40 and 80M BW in 5GHz, if STA is not 20M only-STA. • 20M operating STA support 26,52,106 tone RU

HE Mandatory features

GI and LTF

GI and LTF are defined differently by PPDU type. GI_LTF is defined in SIG-A field of SU PPDU, ER PPDU and MU PPDU, while Trigger frame has the information for the following TB PPDUs.

GI/LTF	HE SU / ER SU		HE MU PPDU		HE TB PPDU	
	GI	LTF	GI	LTF	GI	LTF
0	0.8u	1x (3.2u)	0.8u	4x (12.8u)	1.6u	1x (3.2u)*
1	0.8u	2x (6.4u)	0.8u	2x (6.4u)	1.6u	2x (6.4u)
2	1.6u	2x (6.4u)	1.6u	2x (6.4u)	3.2u	4x (12.8u)
3	3.2u (0.8u when DCM&STBC:1)	4x (12.8u)	3.2u	4x (12.8u)	reserved	
Defined in	SIG-A (B21-B22)		SIG-A (B23-B24)		Common Field of Trigger Frame (B20-B21)	

HE-LTF and GI support by packet type

FEC Coding

Until 11ac, BCC has been the basic and mandatory FEC coding scheme, while the situation changes in 11ax. In 11ax, both BCC and LDPC can be used, when bandwidth is 20MHz or lower. Only LDPC should be used, if the bandwidth is 40MHz or higher. For highest data rate of MCS10 and 11 and for 4 or more MIMO stream, only LDPC can be used. For more about BCC and LDPC inside, find *FEC Coding* chapter.

	HE Condition		BCC	LDPC
	SU	MU PPDU / TB PPDU		
BW	20MHz	=<242 tone	Support	Support
	40/80/160/80+80MHz	484/996/996*2 tone	X	Mandatory
Spatial Stream	Spatial Stream > 4		X	Mandatory
MCS	MCS10, MCS11		X	Mandatory

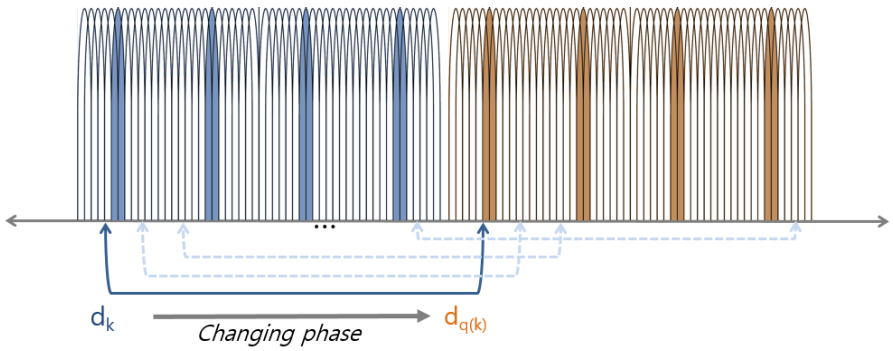
BCC and LDPC in HE

Dual subCarrier Modulation : DCM

DCM is a kind of diversity technique carrying the same information on a pair of subcarriers. It is applied to the low data rates of MCS0,1,3,4 up to 2 spatial stream for Data and HE-SIG-B field. DCM can be enabled in SU PPDU, ER-SU PPDU, MU and TB PPDU with one user case only. It is not applied in MU-MIMO nor STBC.

With DCM, there is no change in Tx/Rx physical block and no latency and little complexity are added. DCM has diversity gain, robustness for narrow-band interference and the significant improvement on PER performance. Downside is it drops data rate to half.

Allocating same information to a pair of subcarriers, the phase of each subcarrier is assigned differently to reduce PAPR. For PAPR, find *OFDM* chapter.



DCM : Dual Subcarrier Modulation

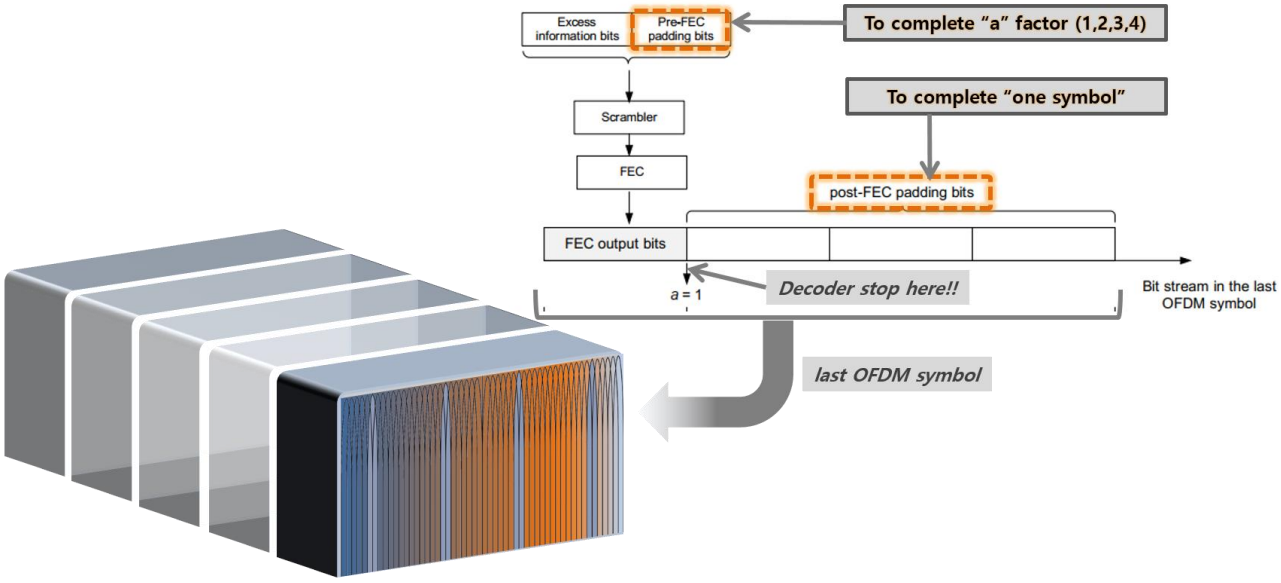
DCM supports MCS0, 1, 3, 4 and there is no DCM support in MCS2. If data is delivered in MCS2 (QPSK, 3/4) with DCM in HE20, the number of data bit is the half of 234 data subcarriers multiplied by 3/4, which is not integer. DCM is to make modulation scheme lower by one step as in the table below and there is no BPSK with 3/4 coding.

Mod.	C/R	MCS without DCM	One order higher for DCM	C/R	MCS with DCM
			BPSK	1/2	MCS0
BPSK	1/2	MCS0	BPSK > QPSK	1/2	MCS1
QPSK	1/2	MCS1	QPSK > 16QAM	1/2	MCS3
QPSK	3/4	MCS2	QPSK > 16QAM	3/4	MCS4
16QAM	1/2	MCS3			
16QAM	3/4	MCS4			
64QAM	2/3	MCS5			
64QAM	3/4	MCS6			
64QAM	5/6	MCS7			
256QAM	3/4	MCS8			
256QAM	5/6	MCS9			
1024QAM	3/4	MCS10			
1024QAM	5/6	MCS11			

Why there is no MCS2 for HE DCM?

Padding

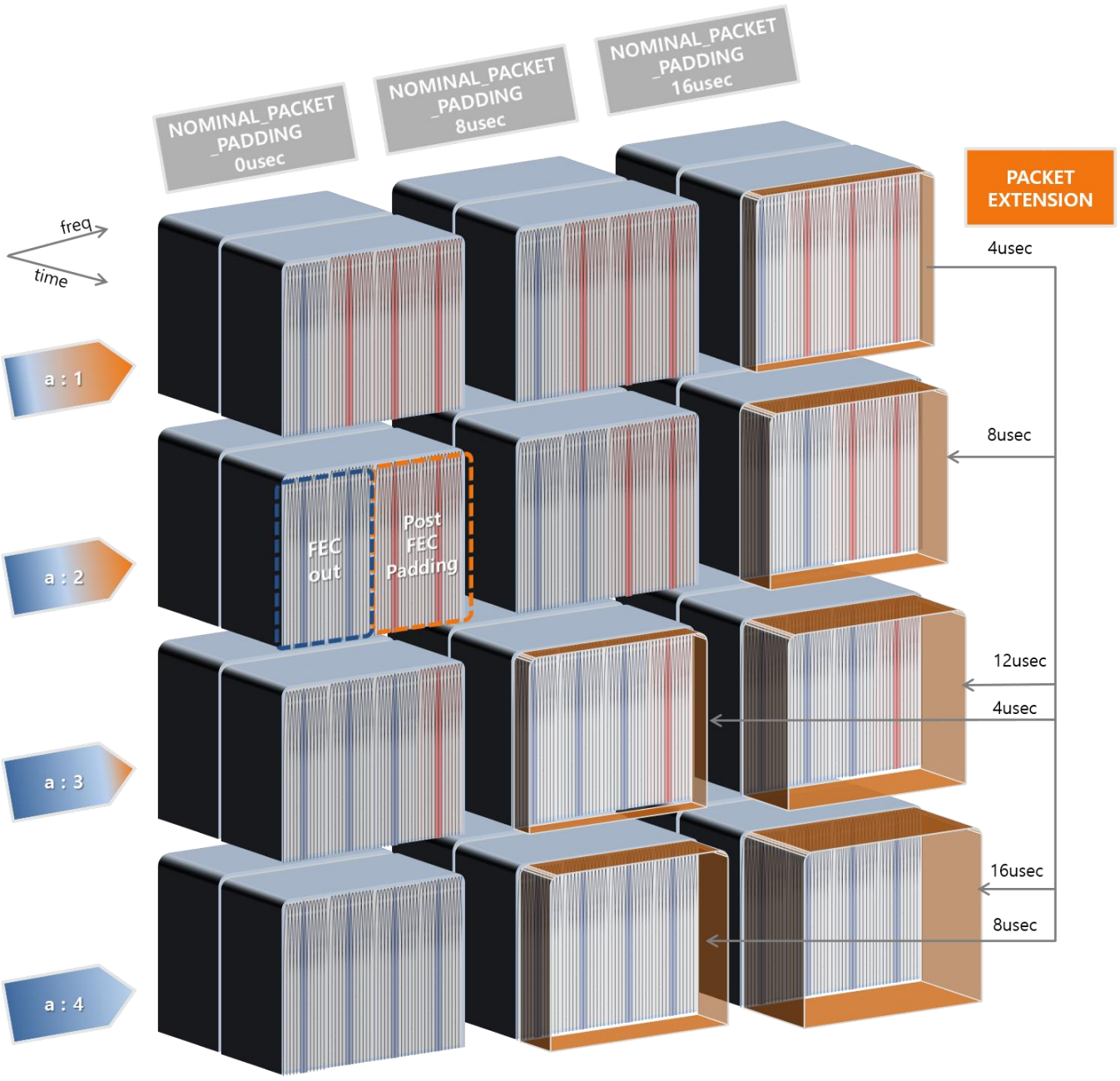
Two step padding process is applied to HE PPDU; pre-FEC padding and post-FEC padding. Pre-FEC padding has 4 possible boundaries in the last OFDM symbol (in case of STBC, two last symbol), which is 'a' factor, and it is applied before conducting FEC coding. Post-FEC padding is applied on FEC encoded bits to complete one last OFDM symbol.



Padding in HE : Pre-FEC and Post-FEC

Packet Extension (PE)

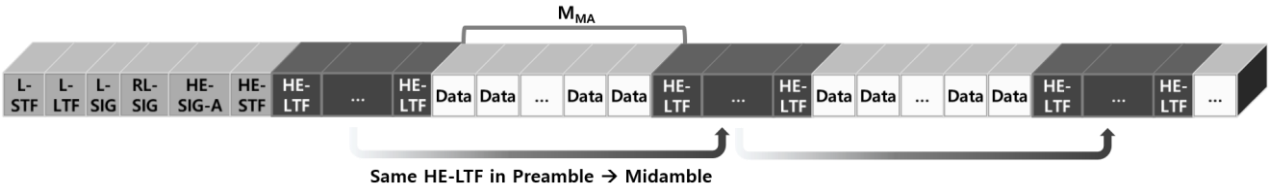
Receiver must finish processing with the received frame within SIFS in order to send Ack, while 4 times more subcarriers in 11ax require faster processing speed as well as complex LDPC decoding time. To give receiver an additional processing time at the end of HE PPDU, PE is added with the same average power as data field and arbitrary contents. PE duration is one of 0, 4, 8, 12, 16 usec, which is determined by pre-FEC padding factors and NOMINAL_PACKET_PADDING.



Packet Extension (PE)

Midamble

WLAN starts considering the fast time-variant channel like Doppler effect. (Think about flying drone with Wi-Fi). When Doppler field of HE-SIG-A is set with the number of MIMO stream of 4 or less, Midambles are present every 10 or 20 OFDM symbols for time variant channel estimation. The contents of Midamble is same with HE-LTF in the packet.



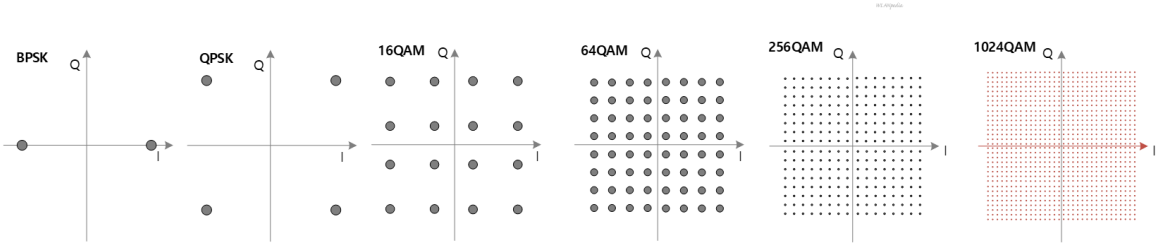
Midamble for Doppler effect

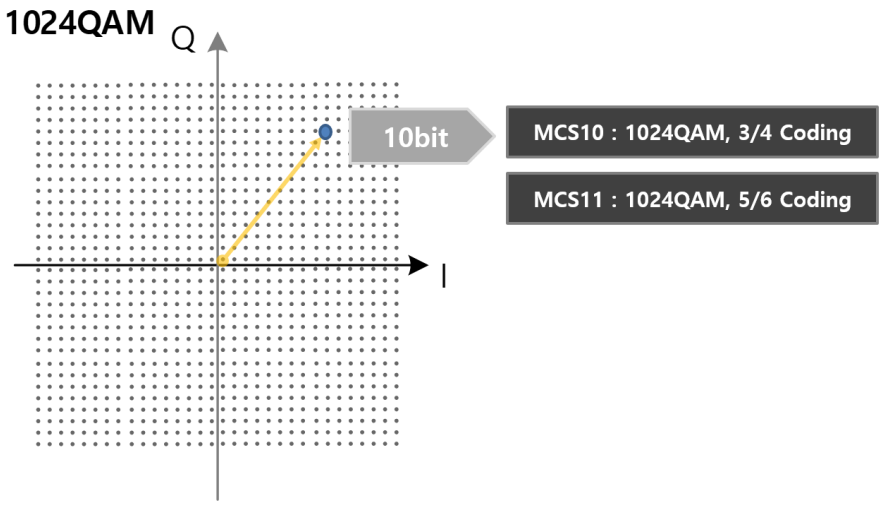
HE Data Rate

With the new modulation scheme of 1024QAM (10bit), MCS9 and MCS10 are introduced in 11ax. The change in OFDM scheme does not bring much difference in Data rate between 11ac and 11ax, when the same MCS is applied. The highest data rate (MCS11) with 80MHz bandwidth in 1SS of 11ax is about 600Mbps, while 11ac (MCS9) has 433.3Mbps.

Introduction of 1024QAM

One subcarrier now carries up to 10 bit information in 11ax. With 1024 QAM, 11ax has higher data rate of MCS10 (1024QAM, 3/4 coding rate) and MCS11 (1024QAM, 5/6 coding rate). LDPC is mandatory and BCC cannot be used in MCS10 and MCS11 for coding scheme. For more about modulation, find *Modulation & Constellation* chapter.



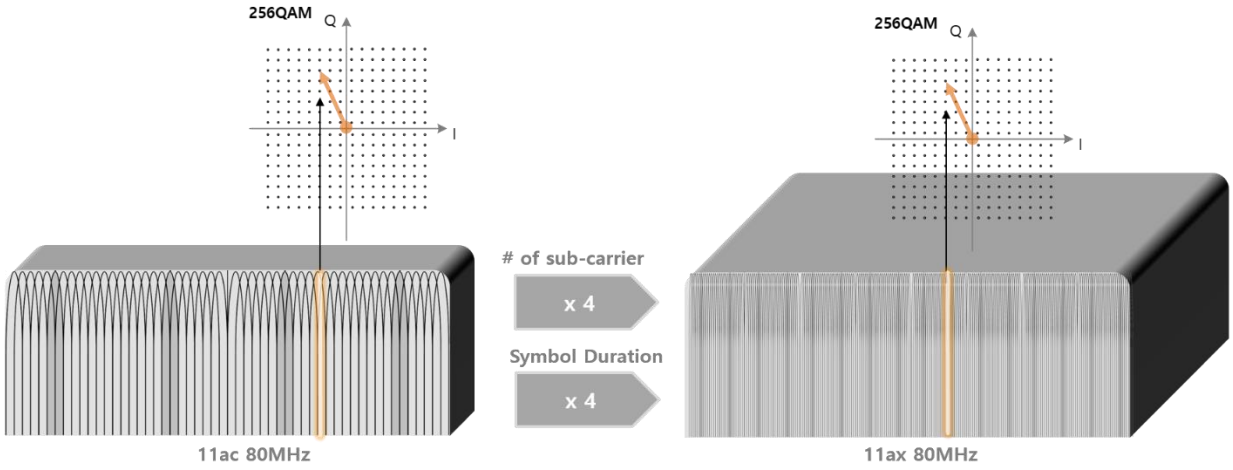


Comparison on MCS9 between 11ac and 11ax

With 4 time more subcarriers in 4 times longer symbol, 11ax OFDM makes the almost same data rate with 11ac OFDM. With the same modulation and coding rate, and with the longest GI (Long GI for 11ac and 3.2usec GI for 11ax), VHT80 and HE80 data rate are 390Mbps and 408.33Mbps each. The reason they have a little difference is the number of subcarrier utilized. 234 data subcarriers are in 11ac and 980 data subcarriers in 11ax in case of 80MHz BW. 980 is slightly over 4 times of 234. (234 x 4 = 936 < 980).

80MHz	11ac
8	8 bit (256QAM)
X 234	234 data subcarrier
X 5/6	5/6 coding
/ 4	3.2usec + 0.8usec Long GI
= 390	390Mbps

80MHz	11ax
8	8 bit (256QAM)
X 980	980 data subcarrier
X 5/6	5/6 coding
/ 16	12.8usec + 3.2usec Normal GI
= 408.33	408.33Mbps



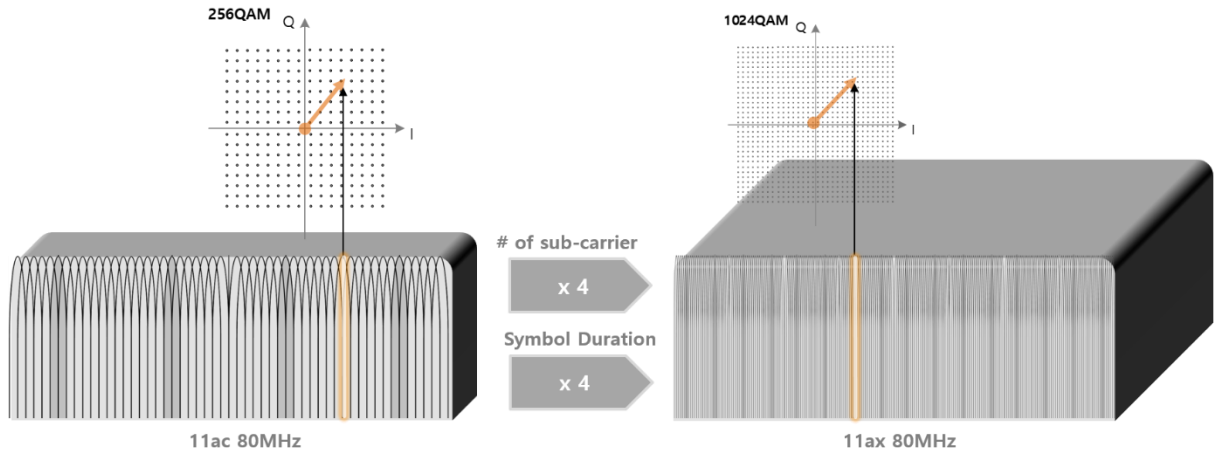
VHT and HE Data Rate Comparison : MCS9

Comparison on highest data rate between 11ac and 11ax

Along with Normal GI, 2 bit more information on each subcarrier and 4 times more subcarrier in one symbol in 11ax masks a big difference (about 30%) between 11ac and 11ax at highest data rate.

80MHz	11ac
8	8 bit (256QAM)
X 234	234 data subcarrier
X 5/6	5/6 coding
/ 3.6	3.2usec + 0.4usec Short GI
= 433.3	433.3Mbps

80MHz	11ax
10	10 bit (1024QAM)
X 980	980 data subcarrier
X 5/6	5/6 coding
/ 13.6	12.8usec + 0.8usec Normal GI
= 600.4	600.4Mbps



The highest Data Rate goes up more than 30% in 11ax with 1024QAM

Data rate for HE20/40/80/160 of SU and full RU

Modulation	C/R	MCS	HE20 SU, 242 RU			HE40 SU, 484 RU			HE80 SU, 996 RU			HE160, 80+80		
			0.8u GI	1.6u GI	3.2u GI	0.8u GI	1.6u GI	3.2u GI	0.8u GI	1.6u GI	3.2u GI	0.8u GI	1.6u GI	3.2u GI
BPSK	1/2	MCS0	8.6	8.1	7.3	17.2	16.3	14.6	36.0	34.0	30.6	71.2	68.1	61.3
QPSK	1/2	MCS1	17.2	16.3	14.6	34.4	32.5	29.3	72.1	68.1	61.3	144.1	136.1	122.5
QPSK	3/4	MCS2	25.8	24.4	21.9	51.6	48.8	43.9	108.1	102.1	91.9	216.2	204.2	183.8
16QAM	1/2	MCS3	34.4	32.5	29.3	68.8	65.0	58.5	144.1	136.1	122.5	288.2	272.2	245.0
16QAM	3/4	MCS4	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8	432.4	408.3	367.5
64QAM	2/3	MCS5	68.8	65.0	58.5	137.6	130.0	117.0	288.2	272.2	245.0	576.5	544.4	490.0
64QAM	3/4	MCS6	77.4	73.1	65.8	154.9	146.3	131.6	324.3	306.3	275.6	648.5	612.5	551.3
64QAM	5/6	MCS7	86.0	81.3	73.1	172.1	162.5	146.3	360.3	340.3	306.3	720.6	68.6	551.3
256QAM	3/4	MCS8	103.2	97.5	87.8	206.5	195.0	175.5	432.4	408.3	367.5	864.7	816.7	735.0
256QAM	5/6	MCS9	114.7	108.3	97.5	229.4	216.7	195.0	480.4	453.7	408.3	960.7	907.4	816.6
1024QAM	3/4	MCS10	129.0	121.9	109.7	258.1	243.8	219.4	540.4	510.4	459.4	1080.9	1020.8	918.8
1024QAM	5/6	MCS11	143.4	135.4	121.9	286.8	270.8	243.8	600.4	567.1	510.4	1201.0	1134.2	1020.8

(Unit : Mbps) based on 1SS, DCM Off

HE Data Rate for SU and full RU

Data rate for 26, 52, 106 tone RU

Modulation	C/R	MCS	26 RU			52 RU			106 RU		
			0.8u GI	1.6u GI	3.2u GI	0.8u GI	1.6u GI	3.2u GI	0.8u GI	1.6u GI	3.2u GI
BPSK	1/2	MCS0	0.9	0.8	0.8	1.8	1.7	1.5	3.8	3.5	3.2
QPSK	1/2	MCS1	1.8	1.7	1.5	3.5	3.3	3.0	7.5	7.1	6.4
QPSK	3/4	MCS2	2.6	2.5	2.3	5.3	5.0	4.5	11.3	10.6	9.6
16QAM	1/2	MCS3	3.5	3.3	3.0	7.1	6.7	6.0	15.0	14.2	12.8
16QAM	3/4	MCS4	5.3	5.0	4.5	10.6	10.0	9.0	22.5	21.3	19.1
64QAM	2/3	MCS5	7.1	6.7	6.0	14.1	13.3	12.0	30.0	28.3	25.5
64QAM	3/4	MCS6	7.9	7.5	6.8	15.9	15.0	13.5	33.8	31.9	28.7
64QAM	5/6	MCS7	8.8	8.3	7.5	17.6	16.7	15.0	37.5	35.4	31.9
256QAM	3/4	MCS8	10.6	10.0	9.0	21.2	20.0	18.0	45.0	42.5	38.3
256QAM	5/6	MCS9	11.8	11.1	10.0	23.5	22.2	20.0	50.0	47.2	42.5
1024QAM	3/4	MCS10	13.2	12.5	11.3	26.5	25.0	22.5	56.3	53.1	47.8
1024QAM	5/6	MCS11	14.7	13.9	12.5	29.4	27.8	25.0	62.5	59.0	53.1

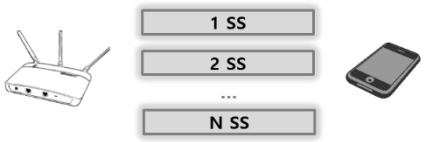
(Unit : Mbps) based on 1SS, DCM Off

HE Data Rate for 26,52,106 tone RU

HE data rate with MIMO, DCM and GI

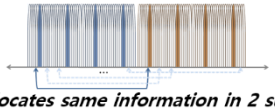
Data rate with DCM is half of data rate without DCM. With normal GI (0.8 usec), data rate goes up by 15% compared with Quadrature GI (3.2 usec)

MIMO data rate
- (data rate of 1SS) X (# of SS)



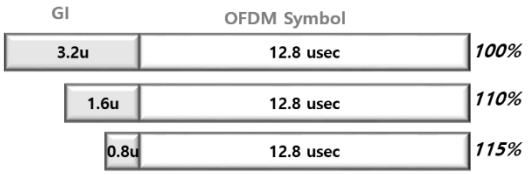
Data rate is doubled, tripled, ... according to SS

Data Rate gets half, when DCM is ON
- Data Rate with DCM = 0.5 X Data Rate without DCM



DCM allocates same information in 2 sub-carrier

Data Rate between GI
- Data rate goes up by 10% with 1.6u GI
- Data rate goes up by 15% with 0.8u GI



Downlink MU Operation

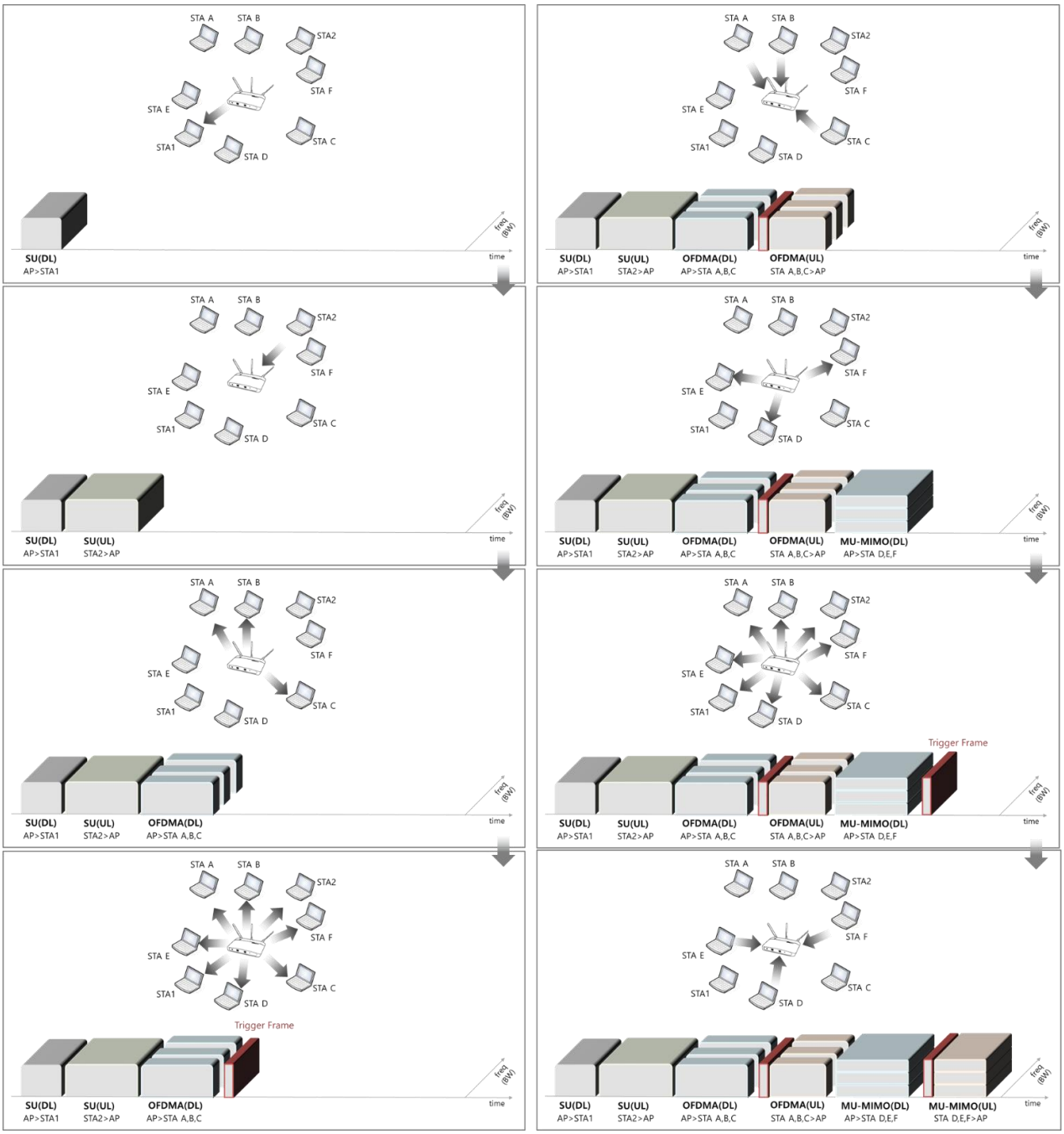
Basic mechanism for multiple access in WLAN is to access media when STA finds the media is not used by other STAs to avoid a collision. This scheme (CSMA/CA) is valid throughout WLAN including 11ax regardless of SU or MU. MU operation (OFDMA or MU-MIMO) is to carry data for multiple users in one TXOP based on the same multiple access scheme of WLAN.

Among 4 types of HE packets, MU PPDU is for DL multiple user with OFDMA (or/and MU-MIMO). MU PPDU has payload for multiple users and its information with RU structure is in HE-SIG-B. OFDMA can be used along with MU-MIMO and this information can be found in Common field also.

Multiple Access in WLAN

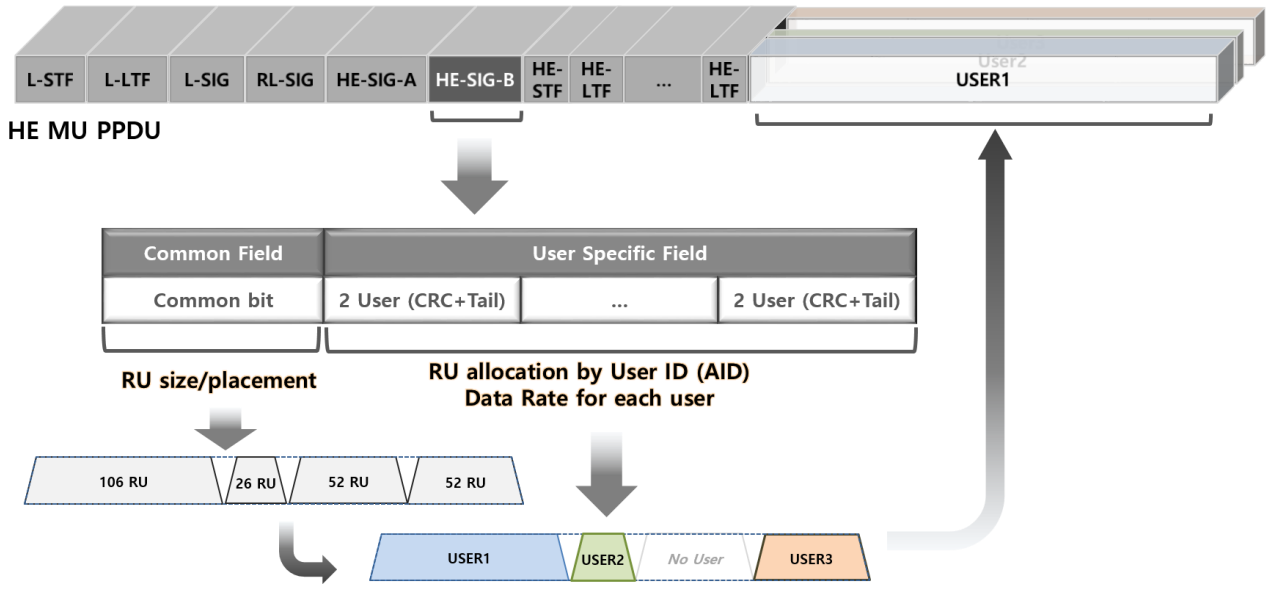
Distributed Coordination Function (DCM) and EDCA is the basic multiple access mechanism in WLAN, which is based on CSMA/CA. In this access control, only one STA can occupy the channel to transmit the packet with the payload directing to another STA (unicast) or other STAs (multicast) or broadcasting (broadcast). Find *Multiple Access Control* in MAC for details. This scheme itself is valid in overall WLAN including 11ax and it is called as Single User (SU) operation to distinguish it from Multi User (MU) operation. MU operation is relatively new concept using OFDMA and MU-MIMO. It is either for AP to transmit the packet containing the payload for multiple users (DL) or for the multiple users (non-AP STAs) to transmit the packets at the same time to AP (UL). MU operation of DL MU-MIMO had been introduced in 11ac and the OFDMA DL/UL and UL MU-MIMO are introduced in 11ax.

Why wasn't UL MU-MIMO defined in 11ac? AP can transmit the packet to multiple user at the same time, while multiple non-AP STAs cannot transmit the signal without knowing information for synchronizing their packets each other with the exact timing or information. 11ax introduces "Trigger frame" that enables UL Multi-User (MU) operation like UL MU-MIMO and UL OFDMA. As you can see, DL and UL operation are quite different and this chapter will handle MU DL first.


STA A
STA B
STA2
STA F
STA E
STA1
STA D
STA C
freq (BW)
time
SU(DL)
AP>STA1
SU(UL)
STA2>AP
OFDMA(DL)
AP>STA A,B,C
OFDMA(UL)
STA A,B,C>AP
MU-MIMO(DL)
AP>STA D,E,F
MU-MIMO(UL)
STA D,E,F>AP
Trigger Frame

MU PPDU and Multi-User information in HE-SIG-B

MU PPDU is downlink packet and used by AP to send the payloads for multiple users. Data for each user is allocated to the specific RU, which information can be found in HE-SIG-B. HE-SIG-B consists of Common Field and User Specific Field. Common field indicates RU structure (RU size and placement) and User Specific field has information which STA (by AID) is allocated to RU structure defined by Common Field. No need to assign User to every RU structure.



11ax HE-SIG-B and MU Packet

Common field

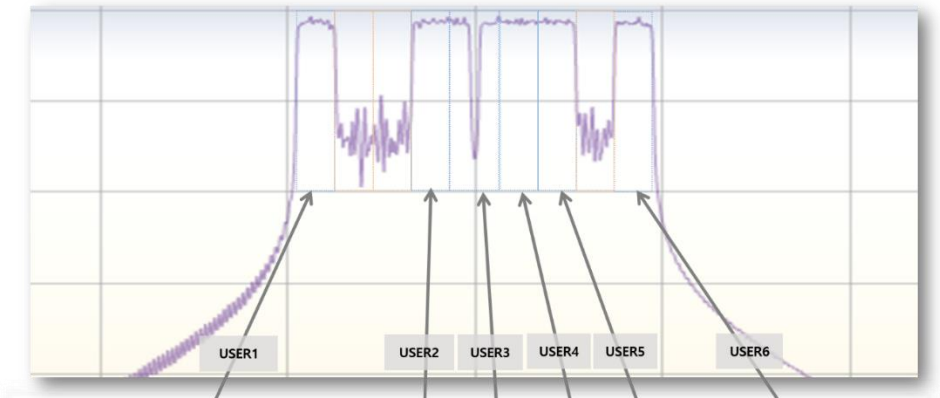
8 bit indices in Common field are RU Allocation subfield which indicates RU structure in MU PPDU.

8 bits indices	#1	#2	#3	#4	#5	#6	#7	#8	#9	# of entries
0000 00 00	26	26	26	26	26	26	26	26	26	1
0000 00 01	26	26	26	26	26	26	26	52		1
0000 00 10	26	26	26	26	26	52		26	26	1
0000 00 11	26	26	26	26	26	52		52		1
0000 01 00	26	26	52		26	26	26	26	26	1
0000 01 01	26	26	52		26	26	26	52		1
0000 01 10	26	26	52		26	52		26	26	1
0000 01 11	26	26	52		26	52		52		1
0000 10 00	52		26	26	26	26	26	26	26	1
0000 10 01	52		26	26	26	26	26	52		1
0000 10 10	52		26	26	26	52		26	26	1
0000 10 11	52		26	26	26	52		52		1
0000 11 00	52		52		26	26	26	26	26	1
0000 11 01	52		52		26	26	26	52		1
0000 11 10	52		52		26	52		26	26	1
0000 11 11	52		52		26	52		52		1
001 00 yyy	26	26	26	26	26	106				8
001 01 yyy	26	26	52		26	106				8
001 10 yyy	52		26	26	26	106				8
001 11 yyy	52		52		26	106				8
010 00 yyy	106				26	26	26	26	26	8
010 01 yyy	106				26	26	26	52		8
010 10 yyy	106				26	52		26	26	8
010 11 yyy	106				26	52		52		8
00010 yyy	52		52		-	106				8
00011 yyy	106				-	52		52		8
01110 000	52		52		-	52		52		1
0110 yyzz	106				-	106				16
10 yyyzzz	106				26	106				16
11000 yyy	242									8
11001 yyy	484									8
11010 yyy	996									8
0111 0001	242 empty									1
0111 0010	484 empty									1
0111 0011	996 empty									1

MU-PPDU Common Field in HE-SIG-B

Example of MU PPDU

This example is for 6 users allocated to six 26 tone RU among 9 RU in 20MHz. Common Field is “0000 0000” and users are assigned to #1, #4, #5, #6, #7, #9 RU.

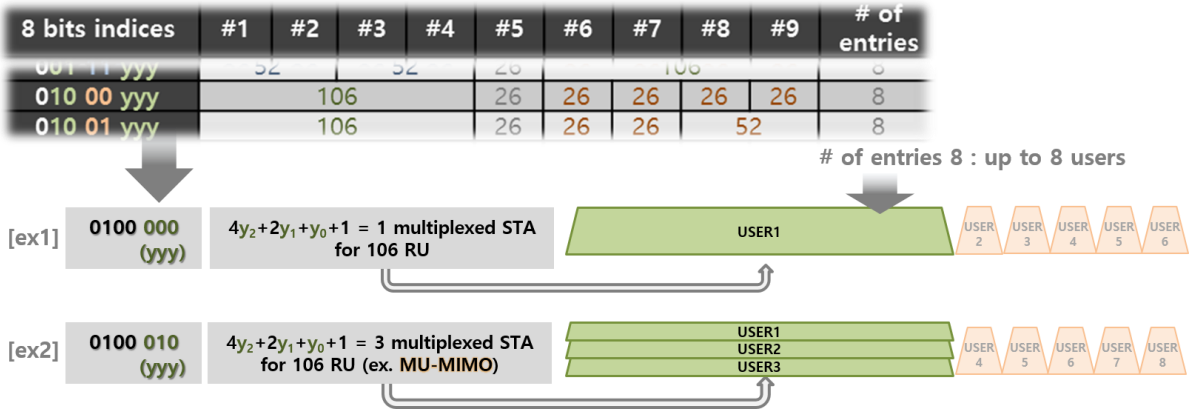


8 bits indices (b7 b6 b5 b4 b3 b2 b1 b0)	#1	#2	#3	#4	#5	#6	#7	#8	#9	Number of entries
00000000	26	26	26	26	26	26	26	26	26	1
00000001	26	26	26	26	26	26	26	52		1
00000010	26	26	26	26	26	52		26	26	1

Example of DL RU allocation : 6users in nine 26-RU

Multiplexed RU

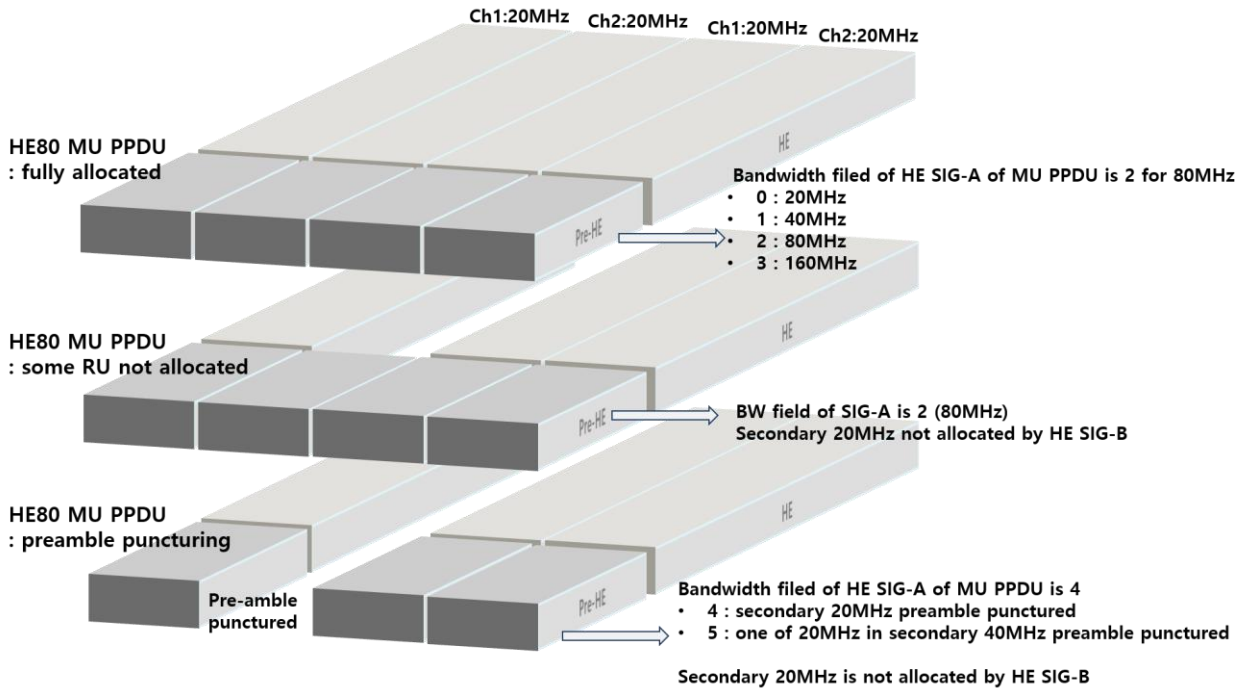
If RU tone size is same or more than 106, MU-MIMO can be used together with OFDMA. In Common field, it reads as “yyy” or “yyzz”. Number of entries in the table above is the number of maximum MU-MIMO users.



11ax DL multiplexed RU

Preamble puncturing

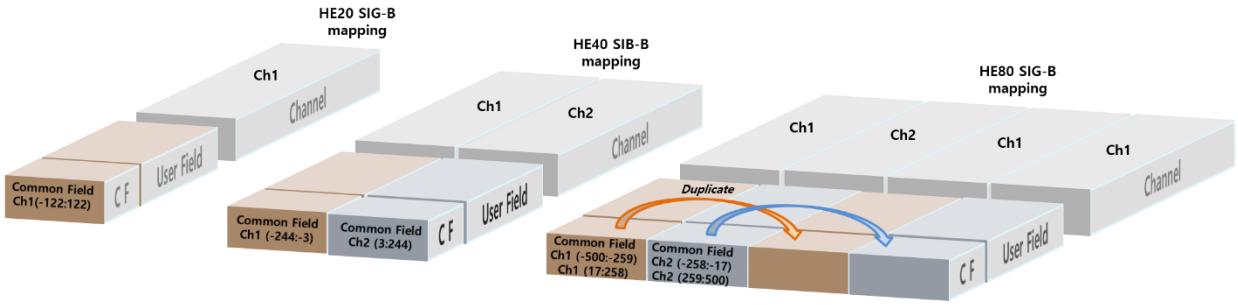
In MU PPDU some RUs are not allocated to any user (nulled) according to RU allocation scheme by AP. In MU PPDU with 80MHz or more, pre-HE modulated fields (preamble) are not transmitted (punctured) in one or more non-primary channels not allocating RU in the sub-channel.



The entire nulling of some sub-channel enhances channel utilization. Preamble puncturing can be used in 80 MHz, 160 MHz or 80+80 MHz DL HE MU PPDU and AP transmits the packet with one or more non-primary 20 MHz sub-channels to be empty.

HE SIG-B mapping

RU Allocation subfield is 8bit that indicating the following 20MHz PPDU. For HE20 and HE40, RU Allocation is 8bit and it is 2 X 8bit for HE80 and 4 X 8bit for HE160.



11ax DL SIG-B mapping

Uplink MU Operation

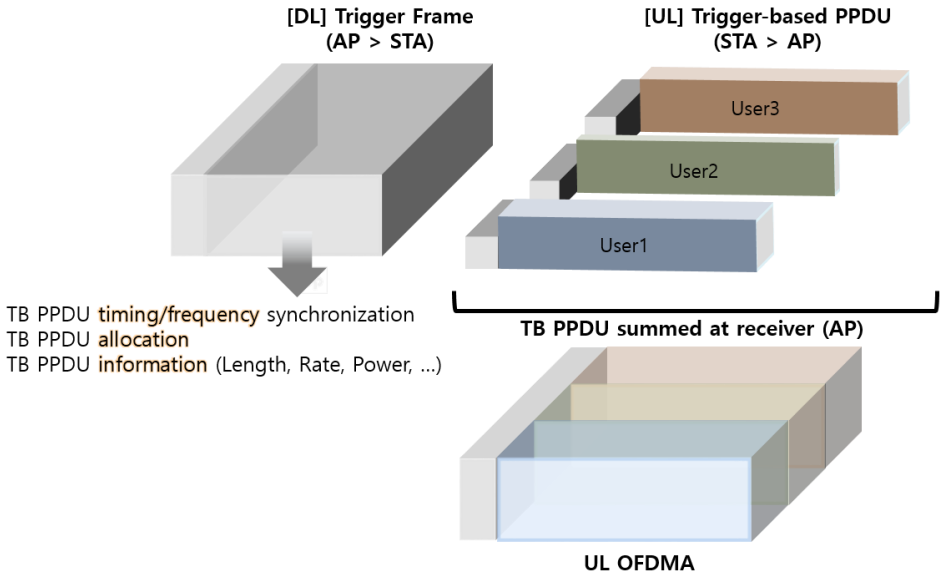
Uplink MU operation is more complicated than Downlink, as all user that transmits uplink frame follow the predefined rules. UL user should know which RU to be allocated and the frames should be synchronized physically. Trigger frame from AP takes these roles in MU UL. Uplink MU packet is transmitted based on Trigger frame and it is called as Trigger-based PPDU (TB PPDU).

UL RU is allocated by trigger frame with two ways; direct allocation and/or random access. TB PPDUs from users are combined, when they reach AP. If the received signal power of TB PPDUs have a big gap, AP cannot decode it properly and each user needs to correct transmit power based on information in trigger frame.

As TB PPDU is vulnerable to interference and some portions are overlapped from each other, it has strict requirement in timing and frequency as well as power. In addition, IEEE specifies the new requirement of Unused-tone EVM to restrict RU leakage. TB PPDU is solicited by Trigger frame and it does not have SIGNAL information itself.

MU UL operation

For multiple users to transmit the packet to AP with the payload filled in a specific RU, they need “Trigger frame” from AP. It commands uplink packets as a physical signaling for timing/frequency and with the information for RU allocation and the packet information of the following uplink packet like length, MCS and power. Uplink packet from non-AP STA in response to Trigger frame is called as Trigger Based PPDU (TB PPDU).

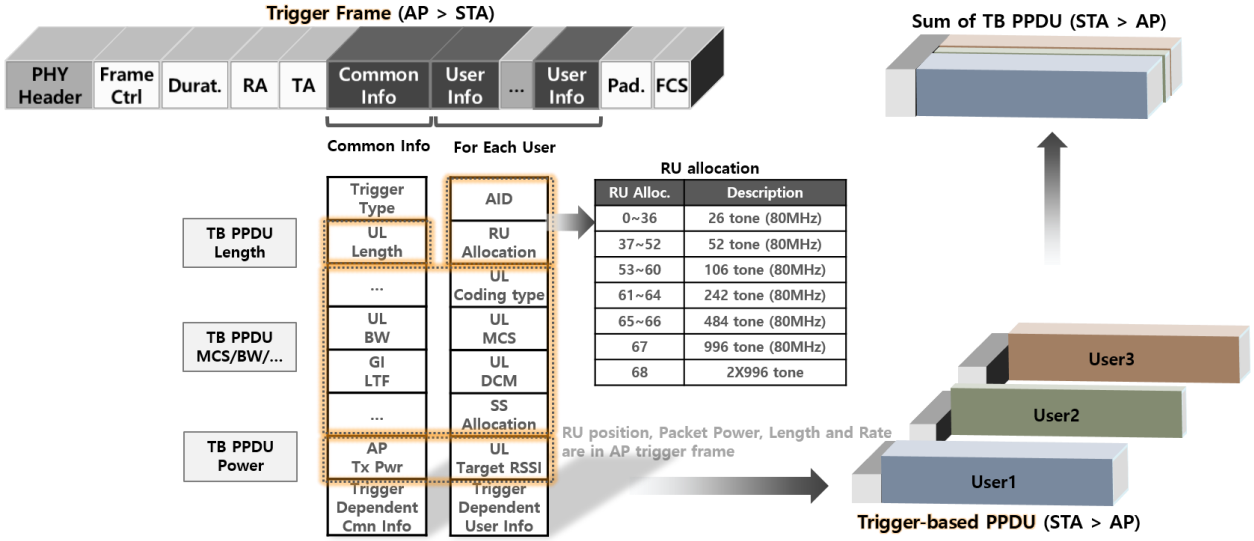


MU Uplink Operation

Trigger Frame

Trigger frame consists of one Common Information field and one or more User Information fields (Don't confuse with Common field and User field of HE-SIG-B in DL MU PPDU). It has the information like Length, MCS, BW, Power as well as RU allocation information for the following TB PPDU.

Along with this basic function of triggering uplink packet, it can be used as other functions like MU BAR (BlockAck Request), Buffer Status Report Poll (for AP to get the information which STA to have how many data to send to AP), MU-RTS and Trigger-enabled Service Period (SP) in TWT. These functions are encoded in Trigger Type sub-field.



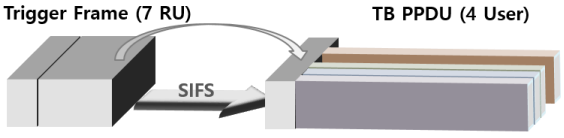
Trigger Frame and Trigger-based PPDU

RU Allocation by Trigger frame

There are two ways in allocating RU for the following TB PPDUs, (1) the direct allocation by AID and (2) Random Access, which methods can be used together. Random Access is called as UORA (UL OFDMA-based Random Access) and it has two cases, random access for the associated STAs (AID = 0) and for STAs that did not join the BSS (un-associated STAs with AID = 2045).

For UORA, each STA manages OFDMA random access Back-Off (OBO) that is a kind of timer. If STA's OBO number is same or less than the number of RU allocated by Trigger frame, STA tries to access one of RUs open by Trigger frame. If not, STA decreases OBO number by the number of RU and waits for the next chance.

For the direct allocation, STA AIDs between 1 and 2044 are specified by each RU assigned by Trigger frame. RUs for AID 0 in Trigger frame is for random access between the associated STAs and AID 2045 is for the un-associated STAs.

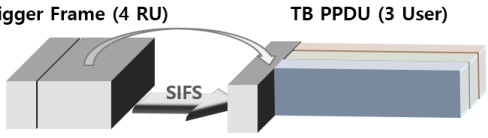


RU	AID	allocation
RU 1	AID 11	Direct allocation by AID
RU 2	AID 12	
RU 3	AID 0	Random Access for OBO ≦ # RU (3) between associated STAs
RU 4	AID 0	
RU 5	AID 0	
RU 6	AID 2045	Random Access for OBO ≦ # RU (2) between unassociated STAs
RU 7	AID 2045	

RU	Allocated	base
RU 1	STA 1	Allocation to AID 11
RU 2	STA 2	Allocation to AID 12
RU 3	STA 6	OBO ≦ 3
RU 4	-	No OBO ≦ 3
RU 5	STA 4	OBO ≦ 3
RU 6	-	No OBO ≦ 2
RU 7	-	No OBO ≦ 2

STATION Status

STA	AID	Initial OBO	OBO update
STA 1	AID 11	5	Unchanged 5
STA 2	AID 12	3	Unchanged 3
STA 3	AID 13	5 (>3)	5-3=2
STA 4	AID 14	2 (≦ 3)	2-3 : reset to 6
STA 5	Unassociated	3 (> 2)	3-2 = 1
STA 6	AID 16	1 (≦ 3)	1-3 : reset to 5



RU	AID	allocation
RU 1	AID 0	Random Access for OBO ≦ # RU (2) between associated STA
RU 2	AID 0	
RU 3	AID 16	Direct allocation by AID
RU 4	AID2045	Random Access ≦ # RU (1)

RU	Allocated	base
RU 1	-	No OBO ≦ 2
RU 2	STA 3	OBO ≦ 2
RU 3	STA 6	Allocation to AID 16
RU 4	STA 5	OBO ≦ 1

STATION Status

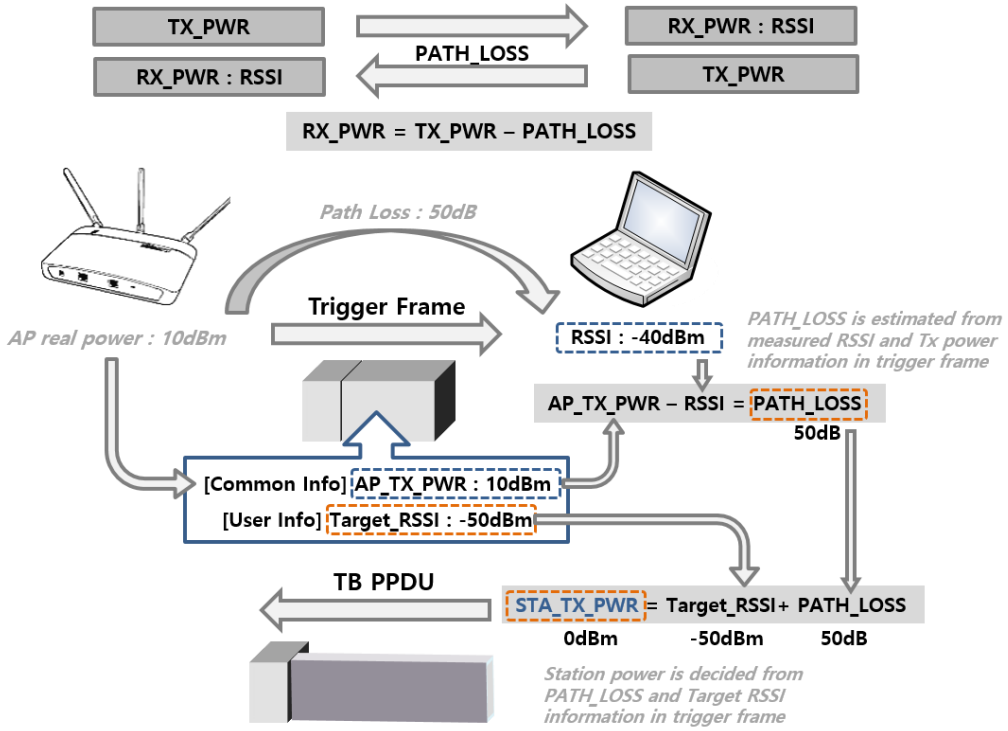
STA	AID	Initial OBO	OBO Update
STA 1	AID 11	5 (>2)	5-2 = 3
STA 2	AID 12	3 (>2)	3-2 = 1
STA 3	AID 13	2 (≦ 2)	2-2 : reset to 5
STA 4	AID 14	6 (>2)	6-2 = 4
STA 5	Unassociated	1 (≦ 1)	1-1 : reset to 8
STA 6	AID 16	5	Unchanged 5

RU allocation and UORA (UL OFDMA-based Random Access)

Power Pre-Correction for TB PPDU

Generally, WLAN STA transmits the fixed power defined for each MCS and there has been no dynamic power control defined by IEEE. Power correction (a kind of power control) for TB PPDU is required, as AP has a limited dynamic range in receiver and it cannot decode the packet properly when the received power gap between RUs from each STAs is too high. Think about the situation that one STA is in near and another is in far distance transmitting the same power.

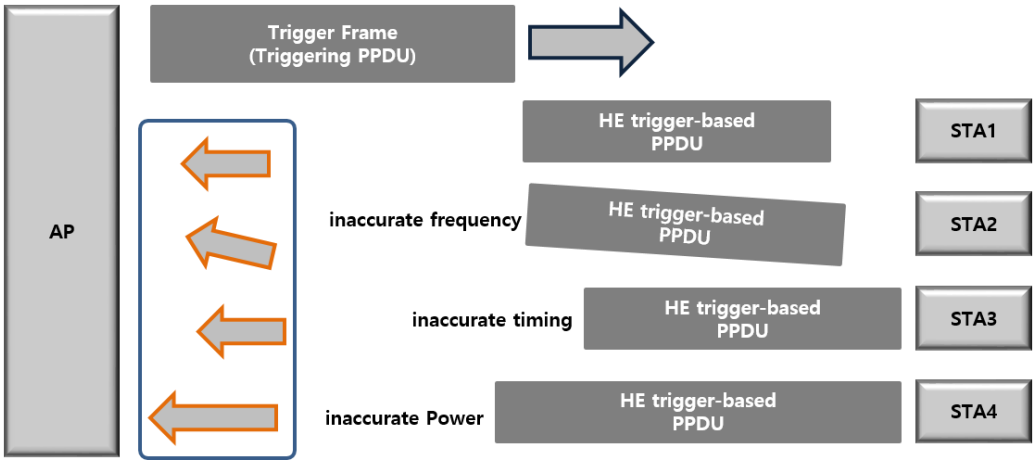
When AP transmits Trigger frame, AP's Tx power is written in Trigger frame. STA that receives the Trigger frame can find out the path loss between AP and STA with this AP power value and the level of Trigger frame signal (RSSI) received at STA. If STA finds out the signal strength value that AP wants to receive, it can set the power with the path loss value. The Target power value is also written in Trigger frame as Target_RSSI.



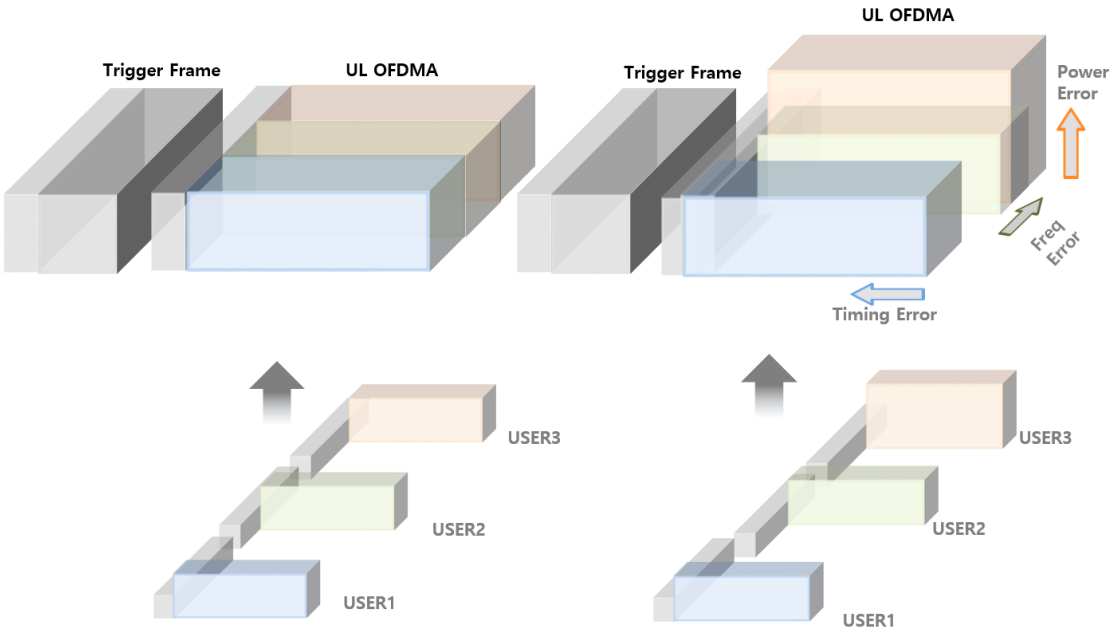
Power Correction of TB PPDU

Pre-correction accuracy requirement for TB PPDU

AP receives the summed TB PPDU packets from each user. If TB PPDUs are not synchronized in timing or frequency, the received packet at AP will be in a mess. IEEE802.11 strictly manages these requirements and they are called as “pre-correction accuracy”



Timing/Freq/Power error on RU



TB PPDU with/without errors

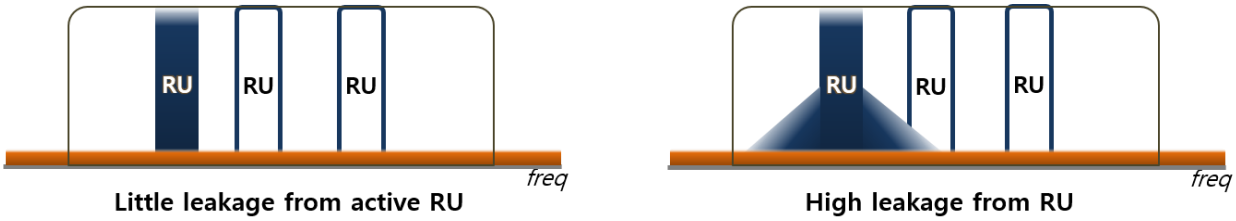
For the accurate Power Correction, IEEE defines the requirement on the Tx power accuracy and RSSI accuracy (RSSI is used to figure out the path loss). Frequency and timing accuracy is the relative value to Trigger frame, which should be extremely accurate. As RUs from each STA go together, RU leakage (Unused-tone EVM) is newly introduced requirement along with RU’s EVM itself (Used-tone EVM).

	TB PPDU RF Requirement
minimum Tx power	• max(P-32, -10) • P : STA max power using MCS0, while meeting Tx EVM and mask • STA shall support EVM requirement for MCS7
Absolute Tx power accuracy	• +/-3dB for the entire Tx power range (class A)
RSSI accuracy	• +/-3dB (class A) in -82 dBm to -20 dBm (2.4GHz) or -30 dBm (5GHz)
Frequency accuracy	• The absolute value of residual CFO error with respect to the corresponding Trigger frame shall not exceed 350 Hz at a received power of -60 dBm in the primary 20MHz
Symbol Clock error	• pre-compensated by the same ppm amount as CFO
Timing accuracy	• A STA that transmits an HE TB PPDU in response to a triggering PPDU from an AP shall ensure that the arrival time of the HE TB PPDU at the AP is within ±0.4 μs of TXTIME + aSIFSTime + RTD from the transmission start time of the triggering PPDU ➔ SIFS (i.e. 10 μs in the 2.4 GHz band and 16 μs in the 5 GHz band)
Used tone EVM and Unused tone EVM	• TB PPDU EVM requirement depends on Tx power compared to max Power of MCS7 • RU leakage is measured with Unused-tone EVM

RF Requirement for HE TB PPDU

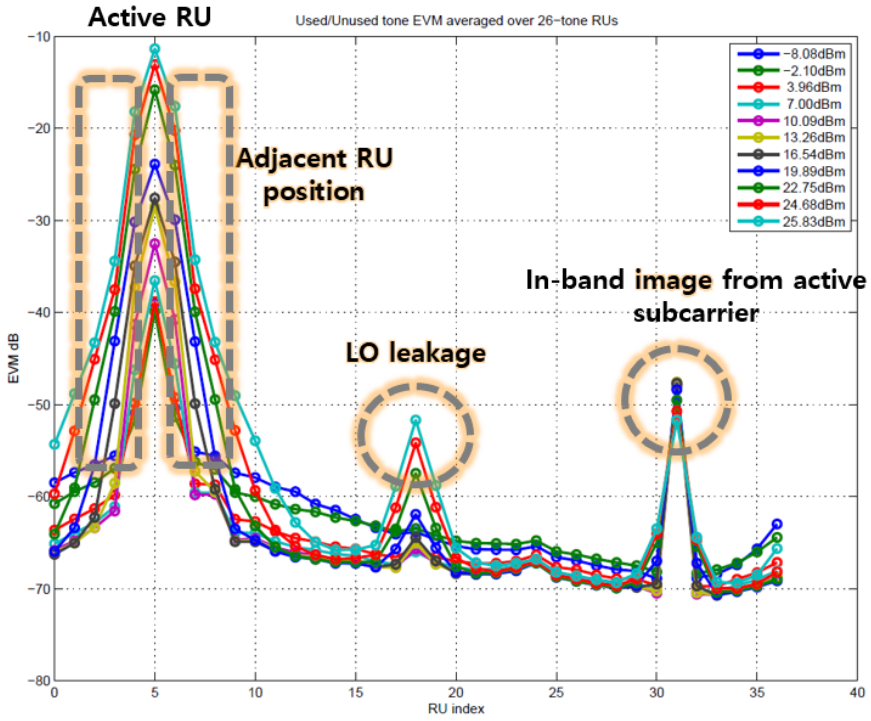
RU Leakage

When RU has high leakage, it could affect the performance of other RU.



RU with high leakage

The picture below is the example of RU leakage in HE80 to show the leakage as EVM floor in the unit of 26 tone RU. (RU is active at index 5) Leakages are found around the active RU and at center frequency and at mirror image position.



RU leakage case (Reference : IEEE 802.11-16/1393R0, edited by WLANpedia)

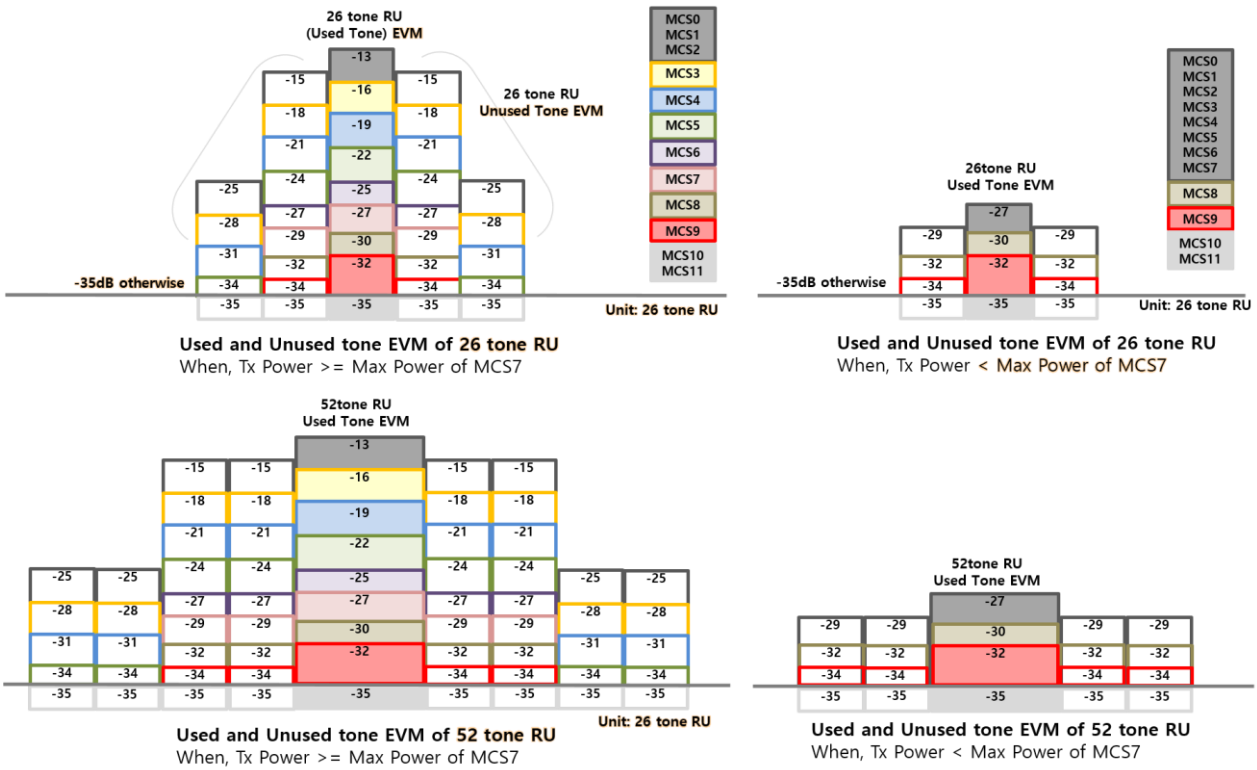
Unused Tone EVM

IEEE specifies RU leakage as a staircase mask requirement, which is called as Unused Tone EVM. It is EVM floor of 26 tone RU for the whole bandwidth except the position(s) for the active RU.

For TB PPDU, EVM of active RU (Used tone EVM) and EVM floor of inactive RU (Unused tone EVM) have two cases. TB PPDU is under the power pre-correction and it does not have the fixed power value. Instead, TB PPDU has the power range between Min and Max. EVM requirement of each MCS depends on its power compared to "max power of MCS7". For example, supposing the max power of MCS7 is set to 15dBm, if MCS0 power under the test is 10dBm, (Used tone) EVM requirement of MCS0 is -27dB. If MCS0 power is 18dBm, EVM requirement is -13dB. EVM requirement value of Used/Unused tone changes according to the power compared with MCS7 max power.

$$UnusedToneError_{RMS}(m) \leq \begin{cases} \max(UsedToneError_{RMS} - 2, -35\ \text{dB}), 1 \leq m \leq r \\ \max(UsedToneError_{RMS} - 12, -35\ \text{dB}), r+1 \leq m \leq 2r \\ \max(UsedToneError_{RMS} - 22, -35\ \text{dB}), 2r+1 \leq m \leq 3r \\ -35\ \text{dB, otherwise} \end{cases}$$

Staircase mask requirement for Unused-tone EVM

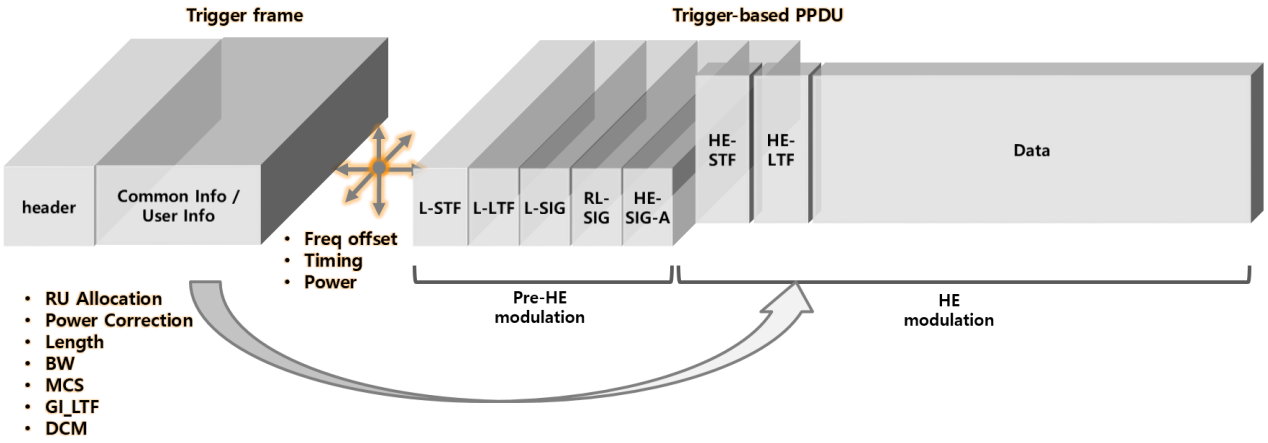


IEEE Requirement on Used and Unused-tone EVM (26 and 52 tone RU)

How to analyze TB PPDU

When STA receives the packet, it needs physical signal information to decode. The information is fundamentally in SIG field in the received packet header and the receiver finds out value of length, modulation, coding, Guard interval and the like. TB PPDU is triggered by AP with Trigger frame and this signal information is not in TB PPDU. AP, which receives TB PPDU, has no problem to decode the packet as the information on TB PPDU is defined by AP.

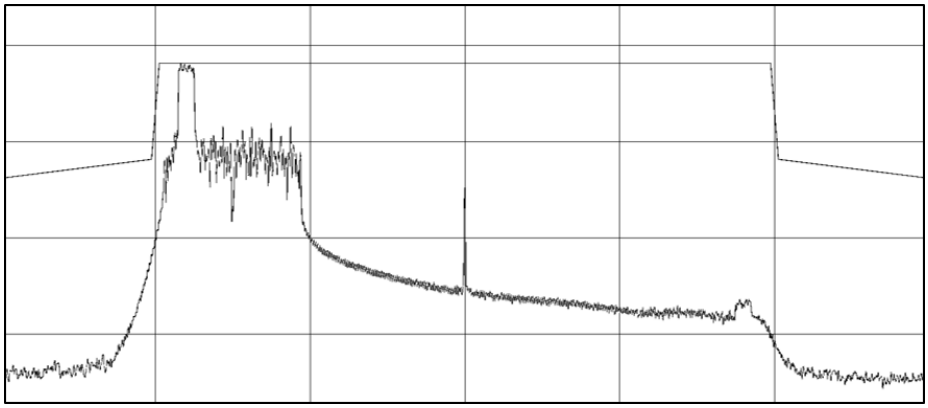
As TB PPDU does not contain the signal information, tester need to know the information on which MCS it is modulated and coded and which GI value the packet has. Without setting them, RF performance like EVM cannot be measured. In addition, if you want to measure CFO (center frequency offset) or TB PPDU timing, Trigger frame needs to be used to trigger TB PPDU, as these items are relative value from Trigger frame.



How to analyze TB PPDU

Frequency Components of TB PPDU

Even if TB PPDU occupies the RU assigned by Trigger frame, Pre-HE portion, which is processed with the legacy modulation, has at least 20MHz BW and this portion might be overlapped by other TB PPDUs. (TB PPDU shall meet Pre-correction accuracy requirement) When RU tone size is more than 20MHz, pre-HE modulated fields duplicated over the multiple 20MHz channels. The image below is 26 tone RU (index 1) in HE80. Pre-HE modulated part occupies 20MHz where RU is indexed.



Frequency components of TB PPDU

MU Access Control

This chapter handles partial information related to Multi-user access control that are newly introduced in 11ax. Fundamental information on Basic Access Control can be found in *Multiple Access Control* in MAC chapter.

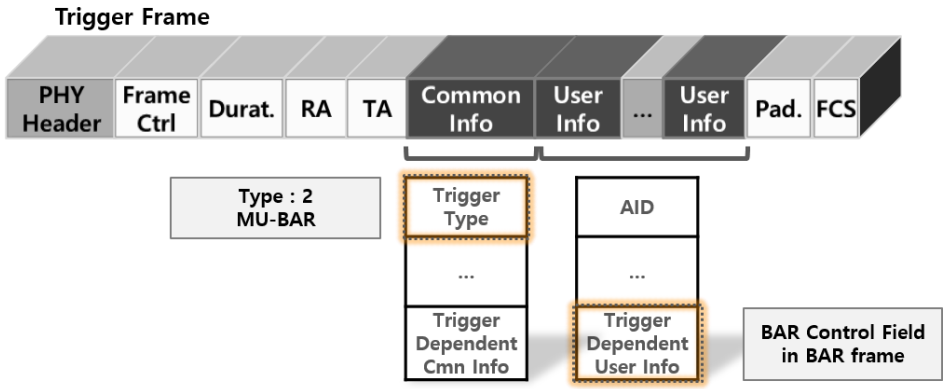
For MU PPDU (DL), users can respond with Ack in TB PPDU simultaneously, when Trigger frame is used for MU-BAR. For AP to send Ack back to TB PPDU (UL), MU PPDU can be used. Block Ack, which has been used for multiple frames, has additional type as Multi-STA BS and can be used for Ack to TB PPDU. Trigger frame is also used for MU-RTS, which can be used to secure media for MU DL or MU UL.

MU Ack

New acknowledgement mechanism for Multi-User (MU) is introduced in 11ax. TB PPDU is used for non-AP STAs to ack and Trigger frame is used for BAR. (Block Ack Request) For AP to ack to multiple STAs, MU PPDU or BA with Multi-STA is used.

MU BAR

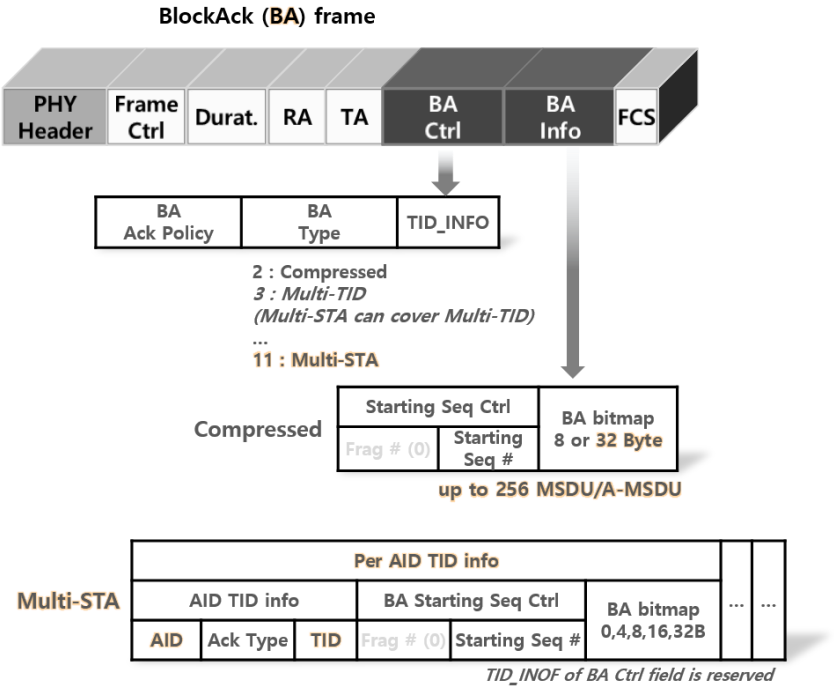
Trigger frame can be used for Multi-user BlockAck Request. Trigger Dependent User Information in User Information field in Trigger frame contains the information on BAR Control field of BAR frame.



Trigger Frame as MU-BAR

Multi-STA BA

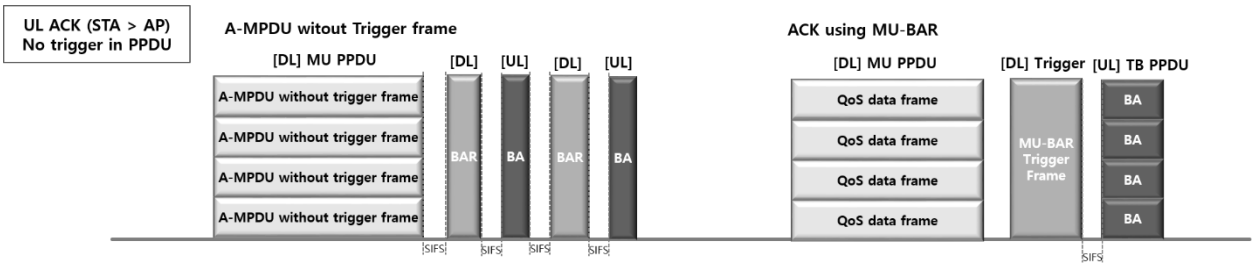
BlockAck (BA) has been widely used in QoS data. In 11ax, BA's bitmap expands up to 256 MSDU and A-MSDU. The second change is the new BA type of Multi-STA. Along with Multi-TID in Pre-HE, Multi-STA BA can be used for BA for multiple station as well. For more about BA, find *Basic Access Control* chapter.



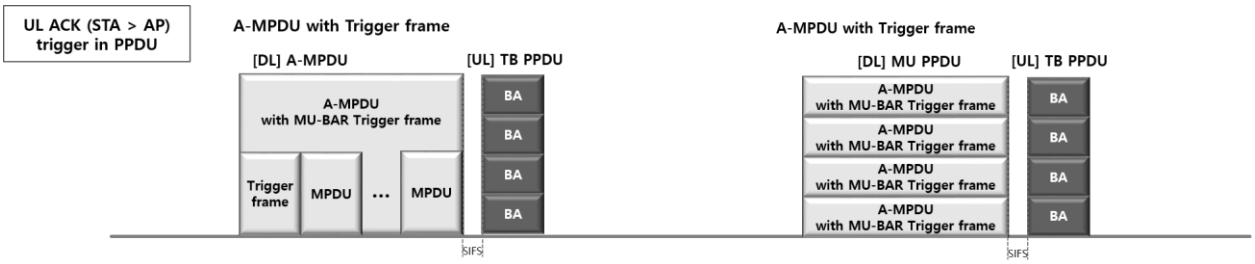
Multi-STA BA frame

UL ACK

Ack for MU PPDU is defined in 11ac and this scheme can be used as in the first picture below. Find more in *ACK for MU PPDU* in MAC chapter. Trigger frame can be used for MU-BAR and BA is delivered in TB PPDU. Non-AP STAs transmit ACK contained in TB PPDU, when there is MU-BAR from AP. When MU-BAR Trigger frame is included in A-MPDU, it is requesting the Immediate BA contained in TB PPDU.

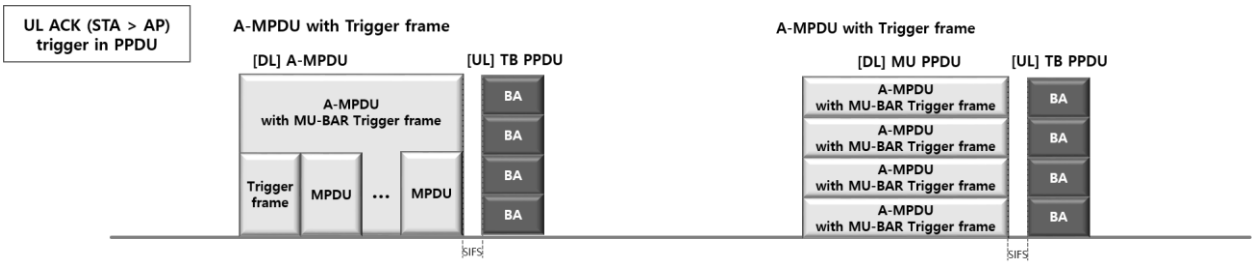


MU ACK case for DL frame



DL ACK

MU PPDU or Multi-STA BA is used for MU Ack in response to TB PPDU (UL).



MU ACK case for UL frame

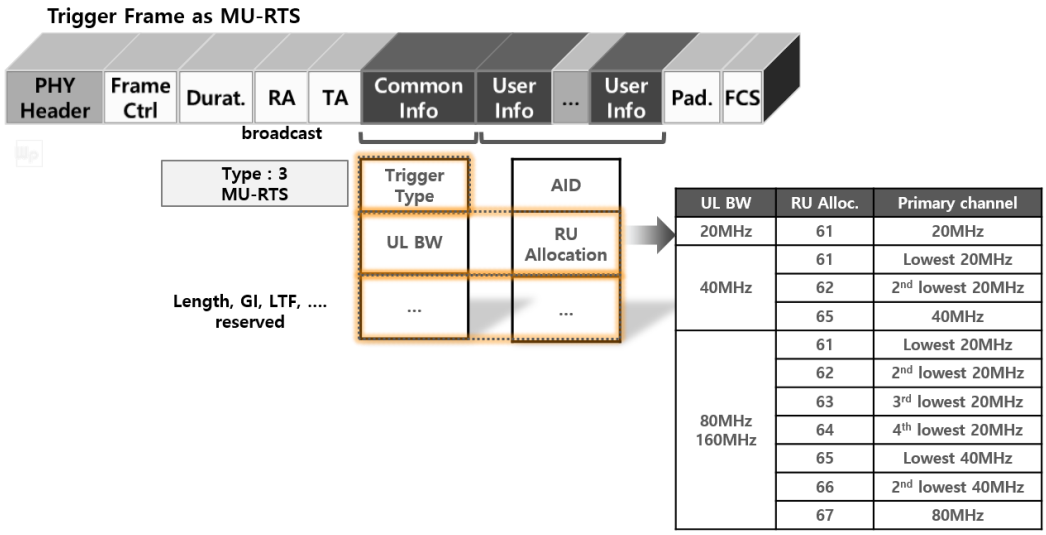
MU-RTS and CTS

As protection mechanism for MU PPDU (DL) and TB PPDU (UL), MU-RTS and CTS are used.

- Trigger frame as MU-RTS

HE AP transmits MU-RTS in Trigger frame to solicit CTS responses from one or more HE STAs.

Trigger type subfield is set to “3” for MU-RTS and RA is set to broadcast. UL BW in Common Info field indicates the total PPDU bandwidth and RU Allocation subfield in the User Info field addressed to STA indicates whether CTS frame is transmitted on the primary 20MHz, 40MHz, 80MHz or 160MHz. CS Required subfield is described above. Other fields like Length, GI, LTF, MCS, Coding type, DCM, … are reserved.



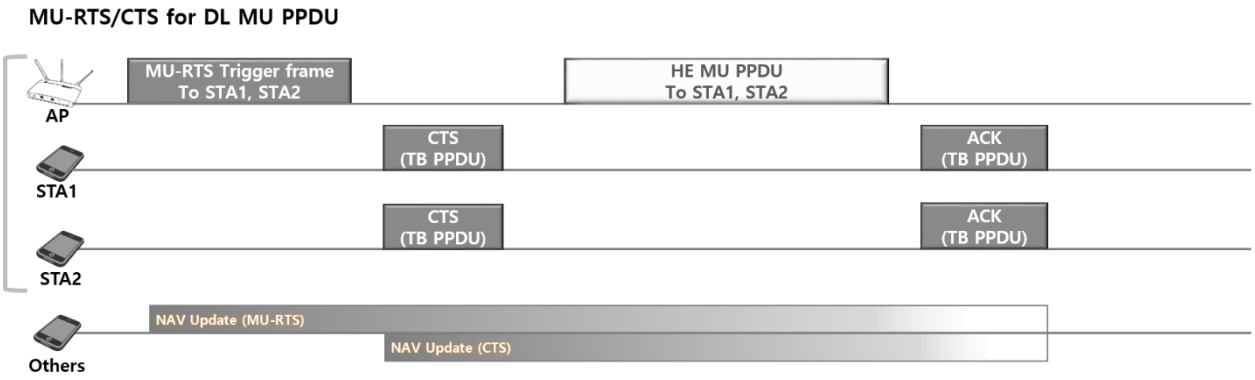
UL BW	RU Alloc.	Primary channel
20MHz	61	20MHz
40MHz	61	Lowest 20MHz
	62	2nd lowest 20MHz
	65	40MHz
80MHz 160MHz	61	Lowest 20MHz
	62	2nd lowest 20MHz
	63	3rd lowest 20MHz
	64	4th lowest 20MHz
	65	Lowest 40MHz
	66	2nd lowest 40MHz
	67	80MHz

MU-RTS trigger frame

- Example of MU-RTS/CTS and DL MU PPDU/Ack

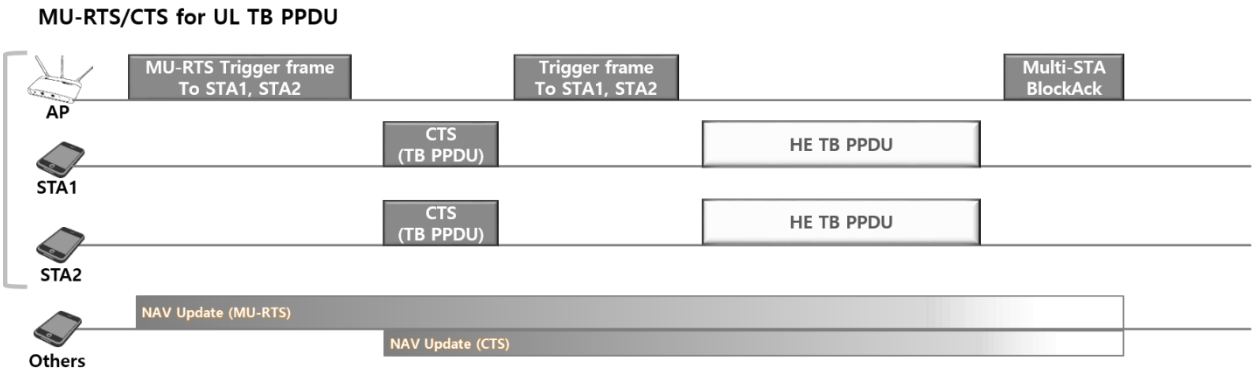
User Info field of MU-RTS trigger frame is addressed to a STA, if AID12 subfield is equal to 12 LSB of AID of STA. CTS frame sent in response to MU-RTS Trigger frame shall be in non-HT or non-HT duplicated PPDU and the data rate is 6Mbps. (backward compatibility) The bandwidth of CTS is indicated in RU Allocation subfield in MU-RTS trigger frame.

MU-RTS Trigger frame is the only Trigger frame that solicits transmission of non HE TB PPDU. CTSs from one or more users can be overlapped and CTS frame in response to MU-RTS Trigger frame shall follow the synchronization requirement. (CFO error less than 2KHz, timing error +/-0.4usec of TXTIME+SIFS+RTD)



MU-RTS and CTS for Downlink

Example of MU-RTS/CTS and Trigger/HE TB PPDU and Multi-STA BlockAck



MU-RTS and CTS for Uplink

Spatial Reuse and BSS Color

11ax suggests the way for medium to be used more often to enhance spectral efficiency. And, for spatial reuse, the frame from intra-BSS and inter-BSS need to be identified. Frame from overlapped (inter) BSS is managed differently from intra-BSS and its CCA threshold is managed by OBSS PD.

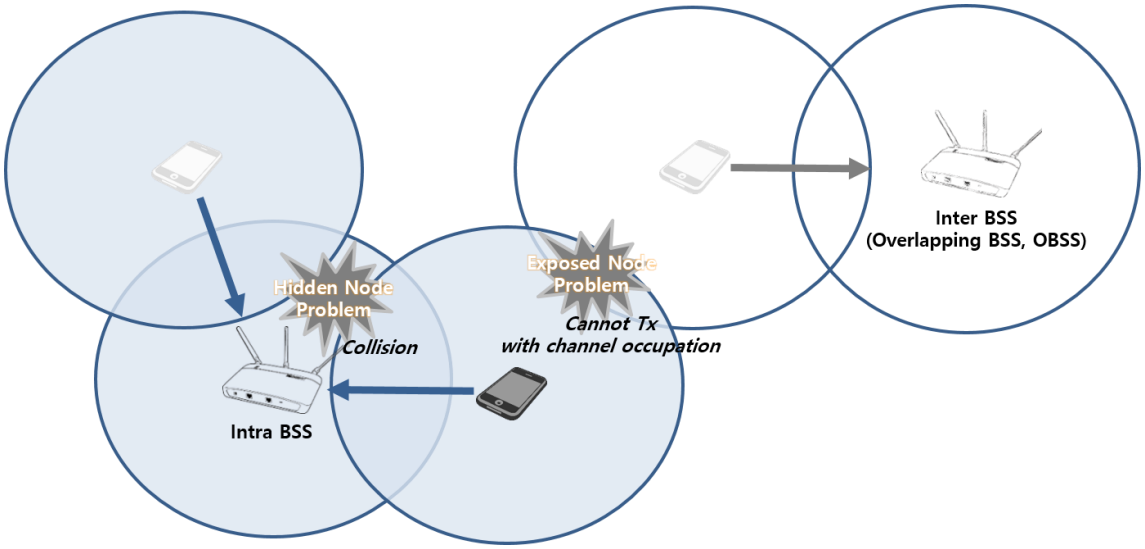
BSS ID is MAC address of access point and 11ax introduces new BSS ID for PHY layer, which is BSS Color. It can be used in OBSS PD, Intra-PPDU power save and Two NAV update.

Spatial Reuse

The purpose of spatial reuse is to allow the medium to be re-used more often in dense deployment scenarios by the early identification of signals from OBSS and by interference management. There are two independent spatial reuse modes, one is OBSS PD-based spatial reuse and the other is SRP-based spatial reuse. This chapter focuses on OBSS PD Spatial reuse.

Hidden Node problem and Exposed Node problem

Let's start with the well-known issues related to the interference between STAs in WLAN. As each STA has its RF range, there can be a hidden node problem in intra-BSS (A STA transmits without sensing the other STA in the same BSS) and an exposed node problem in inter-BSS (A STA unnecessarily does not transmit by sensing the STA in the different BSS). As WLAN gets dense with more and more STAs, the exposed node problem gets worse.



Hidden Node and Exposed Node Problem

Intra-BSS and Inter-BSS

The pre-condition for spatial reuse is to identify intra-BSS and inter-BSS.

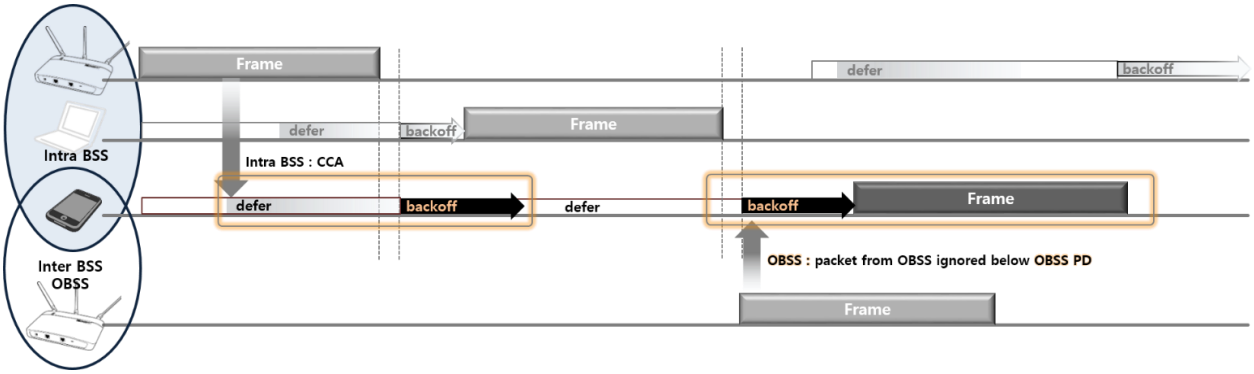
How to classify Intra-BSS

There has been no distinct notion of my BSS and your BSS in WLAN and 11ax starts distinguishing Intra-BSS (my BSS) from Inter-BSS (your BSS) or OBSS (Overlapped) for the spatial reuse. STA shall classify the received PPDU as an intra-BSS in the conditions below

- BSS_COLOR : 0 or the value of my BSS (defined by AP)
- BSSID (AP MAC address) : PPDU with RA, TA or BSSID field as BSSID of my BSS

How to deal with the packet from Intra-BSS and Inter-BSS

Legacy WLAN (~11ac) has run CCA irrelevant to intra-BSS or inter-BSS and STA considers that the channel is occupied by sensing the preamble or detecting signal energy from STA in any BSS. 11ax starts handling intra-BSS packets differently from inter-BSS (Overlapped BSS, OBSS) and OBSS packets are ignored if its level is below the newly defined CS threshold for BSS or OBSS PD (Power Detect).

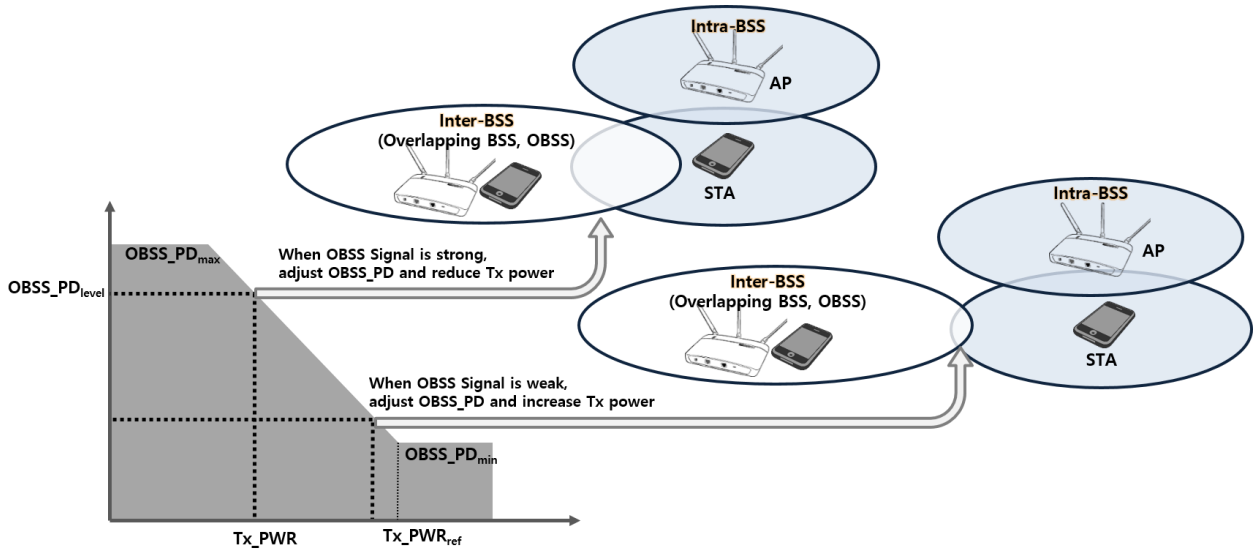


Packet from Intra-BSS and inter-BSS (OBSS)

OBSS PD based spatial reuse

Adjusting OBSS_PD and Tx Power according to OBSS signal level

- In case that Inter-BSS is overlapped in close distance (High OBSS Signal) : Adjusting OBSS_PD higher and its Tx power lower
- In cast that Inter-BSS is overlapped in far distance (Low OBSS Signal) : Adjusting OBSS_PD lower and its Tx power higher

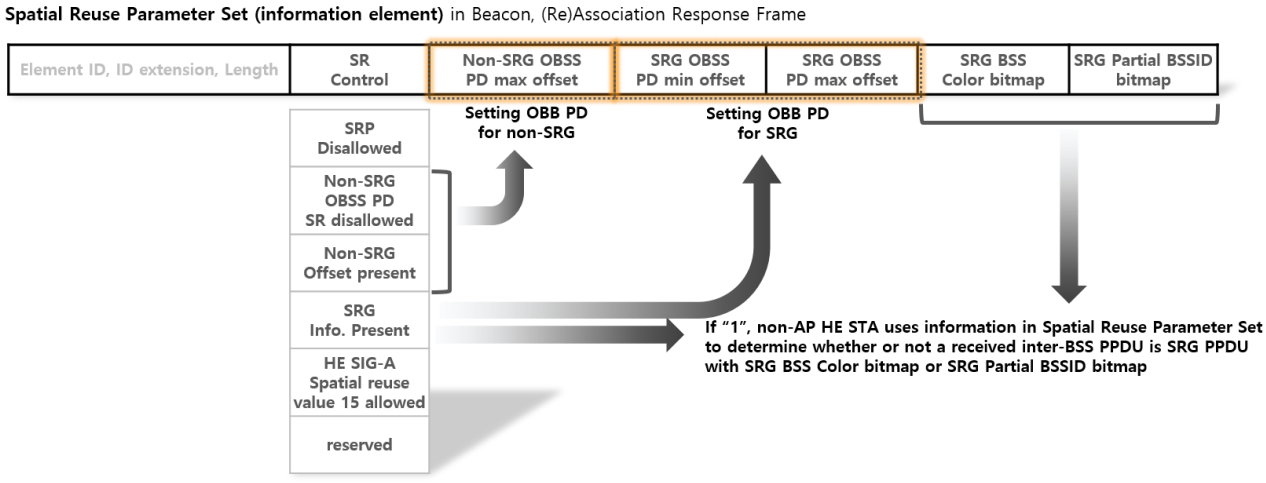


Adjusting OBSS_PD and Tx Power

SRG and non-SRG

Spatial reuse focuses on how to deal with "inter-BSS" and inter-BSS is managed into two categories; SRG (Spatial Reuse Group) and Non-SRG. Identification of SRG and non-SRG PPDU is used during OBSS PD spatial reuse.

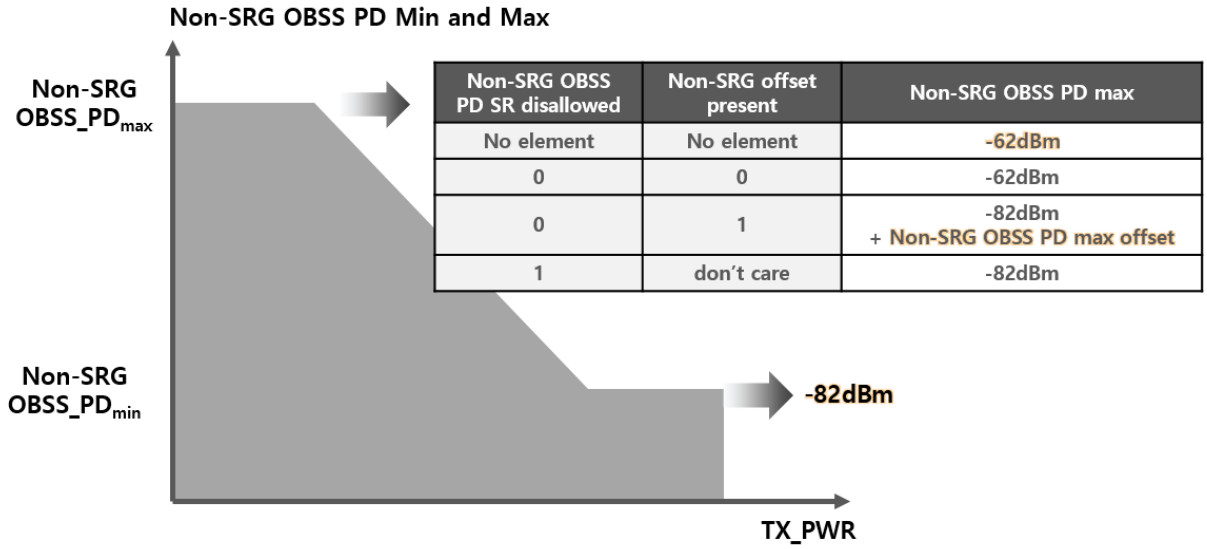
When non-AP HE STA receives Spatial Reuse Parameter Set element from AP via Beacon or (Re)Association response, it uses the information, if SRG Information Present in SR Control field is set, to determine whether the received inter-BSS PPDU is SRG PPDU or not.



Spatial Reuse Parameter Set element

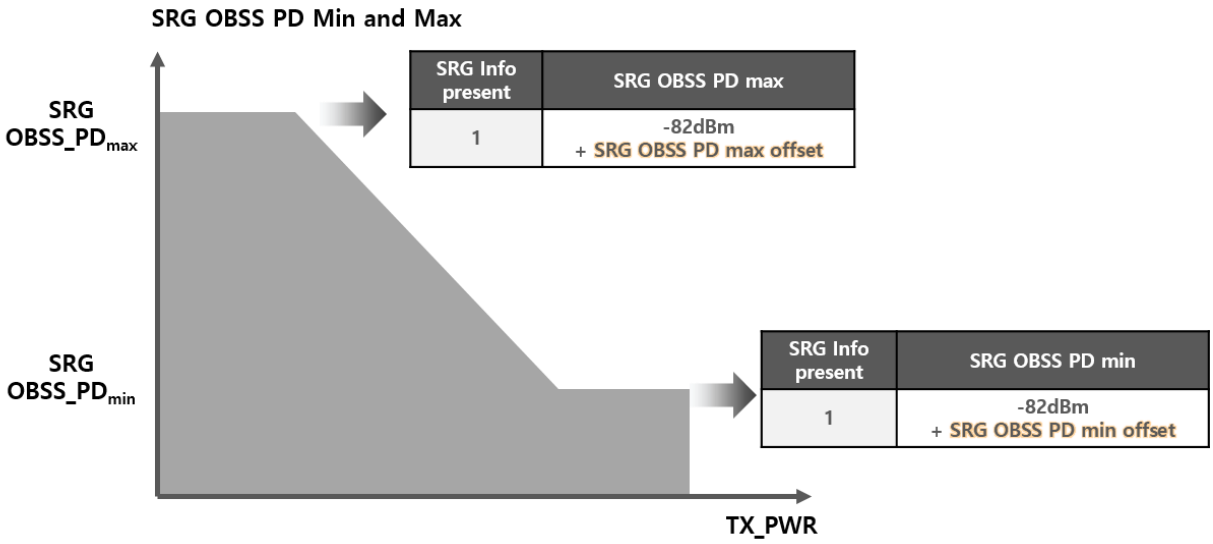
OBSS PD min/max value from SRG and non-SRG

With the information in Spatial Reuse Parameter Set element, OBSS PD min/max value of SRG and non-SRG are handled each.



Non-SRG OBSS PD SR disallowed	Non-SRG offset present	Non-SRG OBSS PD max
No element	No element	-62dBm
0	0	-62dBm
0	1	-82dBm + Non-SRG OBSS PD max offset
1	don't care	-82dBm

Non-SRG OBSS PD



SRG Info present	SRG OBSS PD max
1	-82dBm + SRG OBSS PD max offset

SRG Info present	SRG OBSS PD min
1	-82dBm + SRG OBSS PD min offset

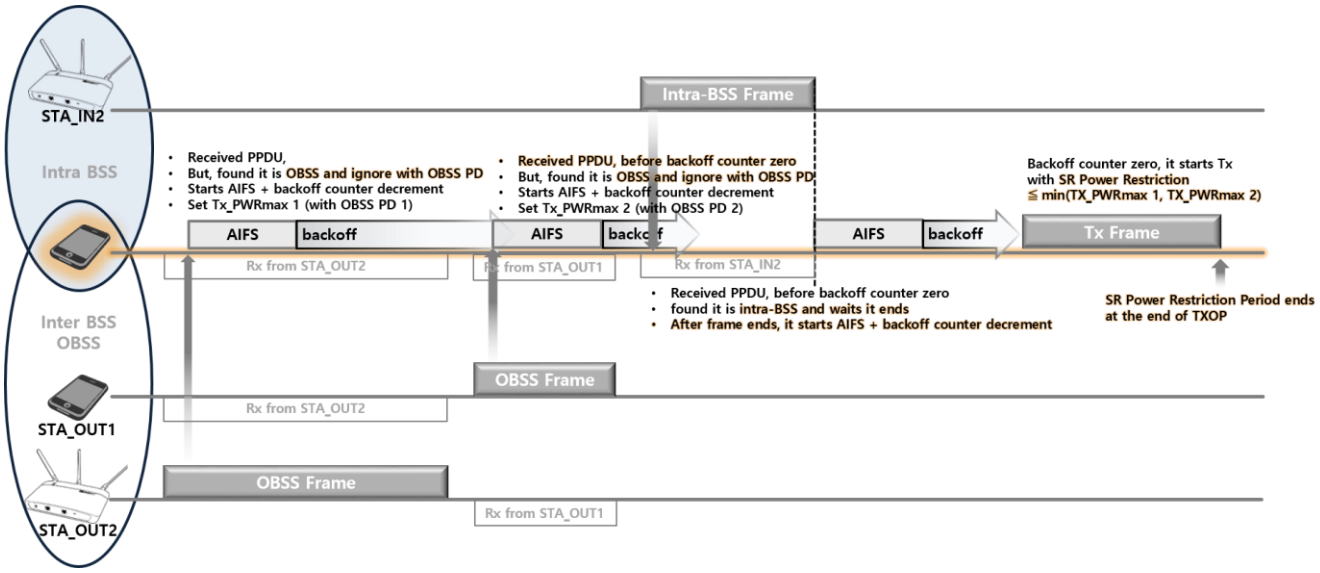
SRG OBSS PD

OBSS PD SR Operation with SR Power Restriction

The example is four cases STA experiences with the packet from OBSS and Intra-BSS to explain SR operations.

- If STA finds the received PPDU is from OBSS, it ignores it based on OBSS PD and starts IFS+Backoff. STA's Tx power is set with TX_PWRmax 1.

- Before backoff couter decreased to zero, STA receives PPDU. When STA finds it is from OBSS, it starts IFS+Backoff. STA sets Tx_PWRmax 2.
- Before backoff couter decreased to zero, STA receives PPDU from intra-BSS. STA waits PPDU ends and start IFS+Backoff.
- When backoff count is zero, STA starts Tx. But, Tx power shall be the same or less than TX_PWRmax1 and TX_PWRmax2. SR Power Restriction period ends with TXOP.



OBSS PD SR operation with SR PWR restriction

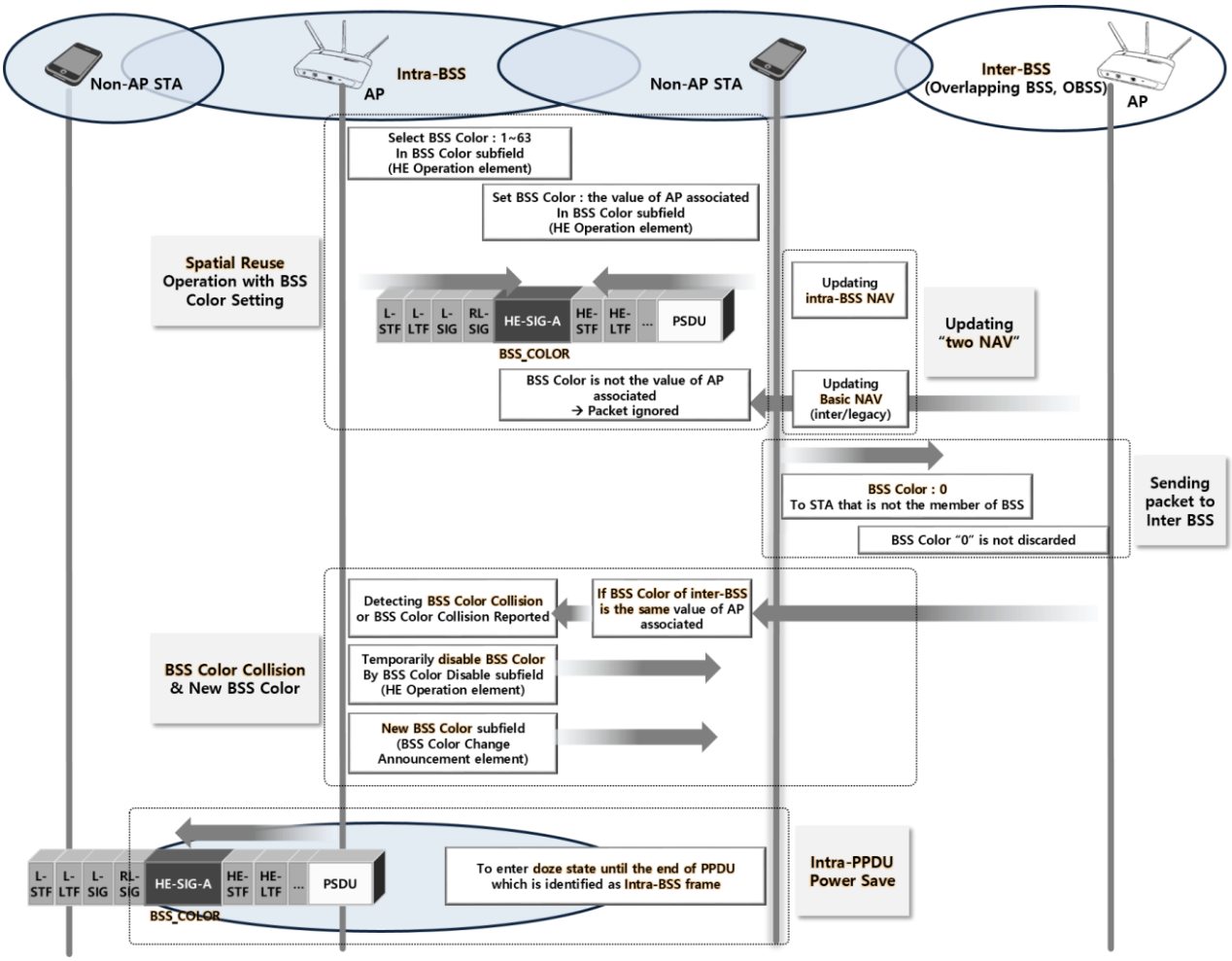
BSS Color

BSS Color is PHY layer BSS identifier in 11ax. MAC address of AP is BSS identifier, while there has been no way to see if the received packet is from intra-BSS and inter-BSS in PHY layer in Pre-HE.

AP selects BSS Color between 1 and 63 and all STAs uses that color exchanging packets inside BSS. When STAs send the signal outside the BSS, it chooses a specific BSS Color of “0”, as STAs outside the may discard the packet if it has a different BSS color of its BSS. If AP detects BSS Color Collision (AP receives the inter-BSS packet with the same BSS Color it selected) or STA in BSS reports BSS Color collision, it temporarily disable BSS Color and set the new BSS Color (BSS Color Collision case)

BSS Color has several usages.

- Spatial Reuse operation : OBSS PD
- Power Consumption reduction : Intra-PPDU power save
- Two NAVs update : Intra-BSS NAV and Basic NAV (Inter-BSS/Legacy)
- Non-AP HE STA “shall” maintain two NAV and HE AP “may” maintain two NAV.



Functions with BSS Color

TWT

TWT is to manage STA's wake up time for Tx and Rx to reduce the contention and the current consumption. TWT setup is made between TWT Requesting STA and TWT Responding STA (AP, mostly) and TWT Scheduled STA joins Broadcast TWT by TWT Scheduling STA (AP, mostly). STA in TWT does not need to receive Beacon and can receive DL packet in TWT Service Period. It is not recommended for TWT STA to transmit frame outside TWT SP. TWT element is used for TWT setup and operation

Non-AP STA can join Broadcast TWT and it can setup TWT individually. They can be used together. In TWT trigger-enabled Service Period, Trigger frame is used to check if STAs are awake, before AP send MU PPDU. TB PPDU is used for UL.

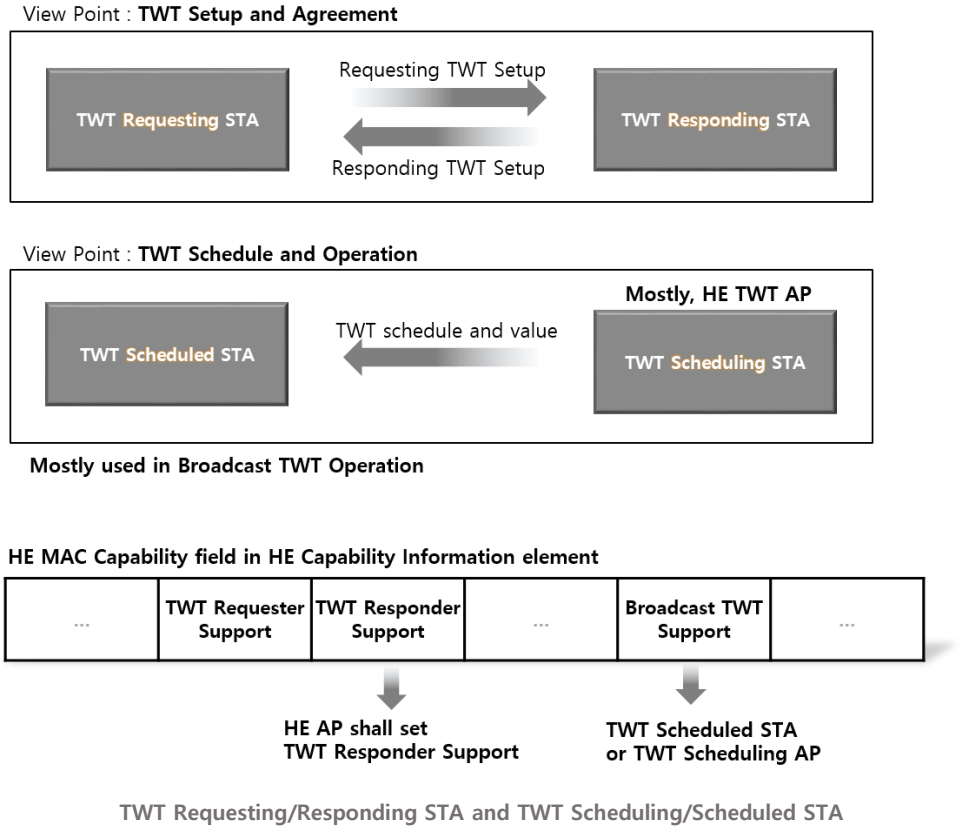
Target Wake Time (TWT) Overview

Target wake time (TWT) allows an AP to manage activities in the BSS in order to minimize contention between STAs and to reduce the required amount of time that STA in PS mode needs to be awake. It reduces contention and overlap between users as well as saves power consumption.

TWT is defined in a complicated way in the Standard, Let's see TWT terminologies first.

- Individual / Broadcast TWT : Two STAs can have agreement of TWT (Individual TWT) or non-AP STA can join Broadcast TWT Operation of AP. Both operation can be used simultaneously.
- TWT Requester / Responder (in TWT Setup) : STA who requests (Request/Suggest/Demand) TWT Setup and STA who responds (Accept/Reject) to it. Non-AP STA is Requester and AP is Responder.
- TWT Scheduling / Scheduled STA (in TWT operating) : In Broadcast TWT, non-AP STAs join Broadcast TWT Operation by AP. TWT Scheduling STA is HE AP and Scheduled STA is non-AP STAs. TWT Scheduling STA and Scheduled STA set Broadcast TWT Support.
- Target Wake Time : The representative name for TWT operation. In a narrow sense, Target Wake Time is the time for the following TWT SP (Service Period)
- TWT Wake Duration : Duration for TWT SP
- TWT Wake Interval : Time between the current and next TWT SP (Periodic TWT)
- Explicit / Implicit TWT : TWT requesting STA receives the next TWT information from TWT responding STA in explicit TWT. In implicit TWT, TWT requesting STA calculates the Next TWT by adding a fixed value to the current TWT value
- TWT Trigger-enabled SP : AP uses Trigger frame to notice STAs for buffered data and STAs sends back PS-Poll or U-APSD frame contained in TB PPDU.

Mostly, non-AP HE STA is TWT "requesting" STA, as it requests individual TWT setup first to "responding" HE AP. And, HE AP is mostly TWT "scheduling" STA, as it broadcasts TWT information to non-AP STA to be "scheduled"



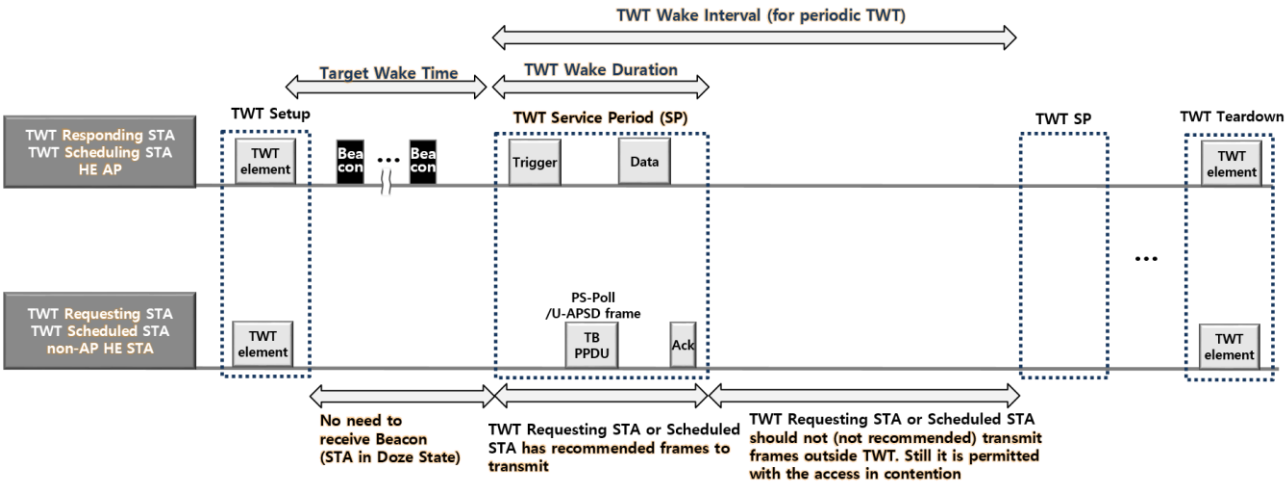
TWT Requesting/Responding STA and TWT Scheduling/Scheduled STA

TWT operation concept

After TWT Setup, TWT Requesting/Scheduled STA can in be doze state and is exempt from receiving Beacon frame (saving current consumption). TWT Requesting/Scheduled STA should not (not recommended) transmit frames outside TWT SP and within trigger-enabled broadcast TWT SP, except STA can transmit frames within negotiated individual TWT SP.

- There is Broadcast TWT Recommendation in TWT element for frame type transmitted by scheduled STA and scheduling STA during broadcast TWT SP.
- In individual TWT, TWT Requesting STA or Scheduled STA should not transmit frames that are not contained within HE TB PPDU in trigger-enabled TWT SP. TWT responding STA should solicit buffer status reports at the start of TWT SP

TWT scheduled STA decides what frames to transmit within or outside TWT SP. While it is recommended that STA not to transmit, it is still permitted to transmit with media access with contention.



11ax TWT Operation and Concept

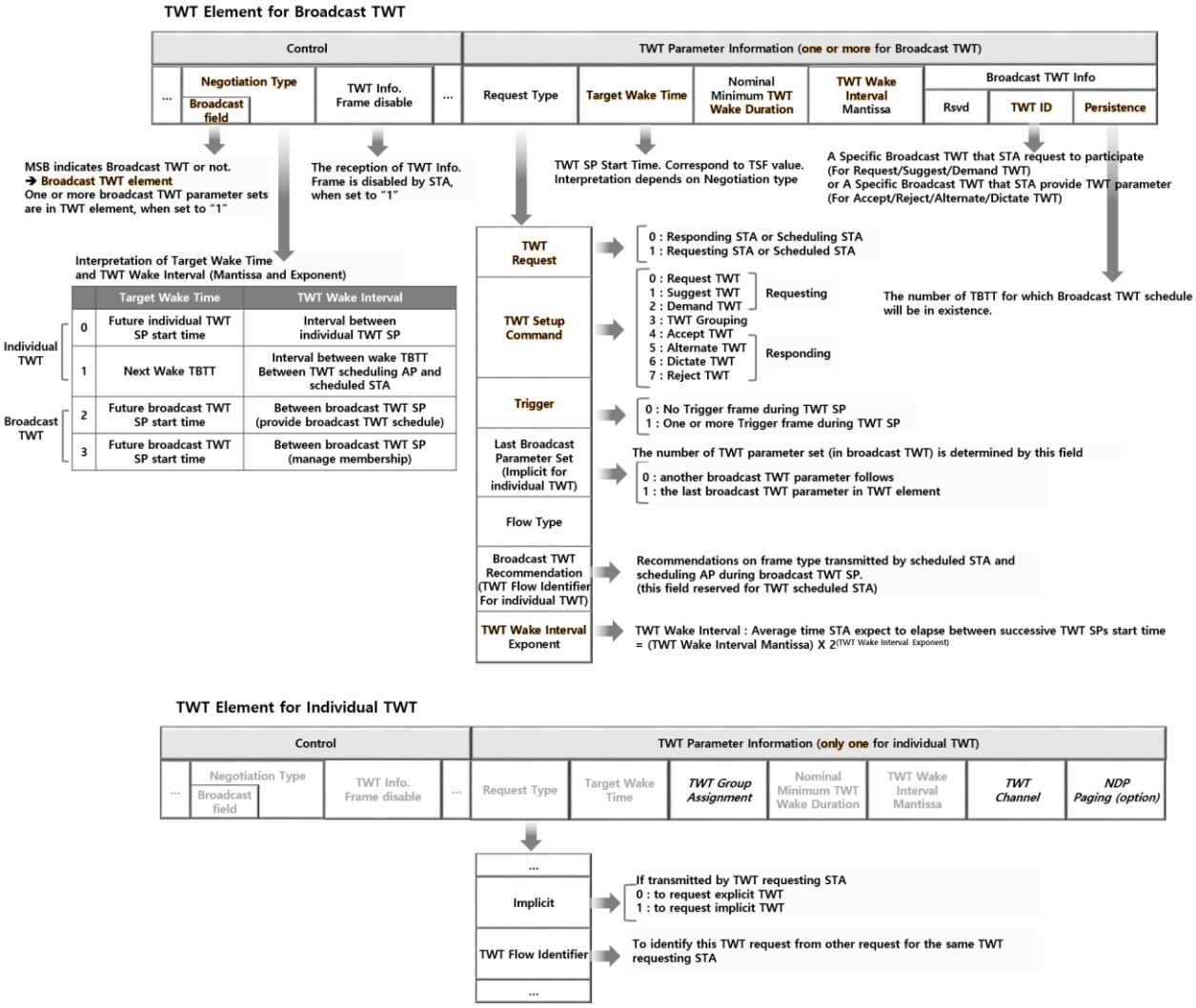
TWT element

TWT information element is contained in Beacon Frame, Probe Response Frame, (Re)Association Request/Response Frame, etc. It is used for both individual TWT and broadcast with some differences. Broadcast TWT has one or more TWT Parameter Information, while Individual TWT only has one TWT Parameter Information. In TWT element for individual TWT image below, the same field with TWT element for Broadcast is in grey color.

- Negotiation type : it indicates Broadcast TWT or Individual TWT. It also tells the way to interprets the following field; Target Wake Time and Interval
- Request Type
  - TWT Request : Requesting STA or Responding STA
  - TWT Setup Command : TWT Setup commands like Request/Suggest/Demand/Accept/Alternate/Dictate/Reject
  - Trigger : In TWT SP, it is set if there will be one or more Trigger frame
- Schedule related parameter : TWT Wake Interval Exponent/Mantissa, Target Wake Time, TWT Wake Duration

Broadcast TWT Information (Broadcast TWT only)

- TWT ID : a specific Broadcast TWT ID used for STA to request to participate or to provide TWT parameter
- Persistence : TBTT (Target Beacon Transmission Time) number for Broadcast TWT schedule.



11ax TWT element

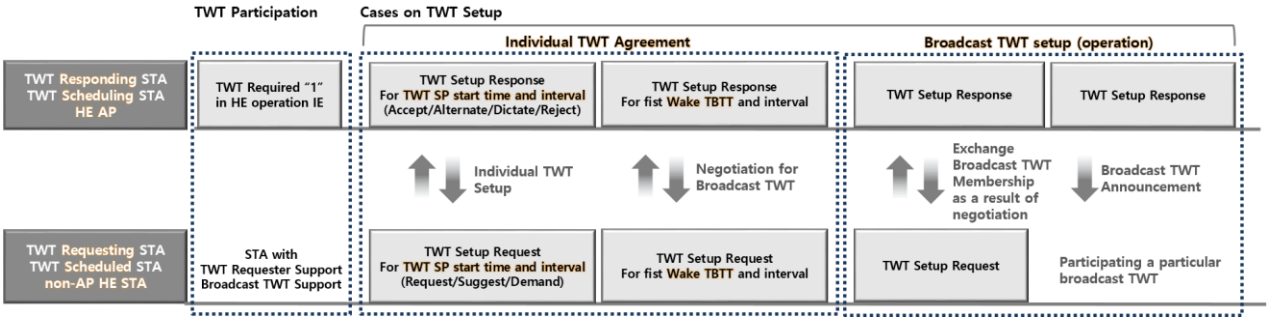
TWT Setup

TWT Individual Agreement

- TWT values for individual TWT (TWT SP Start Time, TWT Wake Interval) or for broadcast TWT negotiation (Wake TBTT, Interval) are agreed between TWT Requesting STA and TWT Responding STA according to Negotiation Type (0 or 1) in TWT element

TWT Broadcast participation or negotiation

- TWT Scheduled STA can join a particular Broadcast TWT (by Broadcast TWT ID and TA) and follow the schedule provided by TWT scheduling AP with Broadcast TWT announcement. Or the scheduled/scheduling STA negotiate and exchange membership according to Negotiation Type (2 or 3) in TWT element



TWT Setup

Individual TWT agreement

TWT Requesting STA	
Request	STA does not provide TWT parameter, leaving the choice to responding STA
Suggest	STA offers preferred TWT parameter, but might accept alternative TWT parameter from responding STA
Demand	STA will currently accept only the indicated TWT parameter for TWT agreement

TWT Responding STA	
Accept	STA has initiated TWT agreement with the given parameter
Alternate	A counter-offer of TWT parameter without the creation of TWT agreement
Dictate	No TWT agreement is created. Likely to be accepted only if the requesting STA transmit a new TWT setup request with the indicated TWT parameter
Reject	The negotiation has ended in failure to create a new TWT agreement

If the response it other than Accept or Reject, STA send a new request modifying parameter

If Accept TWT, STA successfully completed TWT setup with TWT Flow Identified indicated in TWT response and Requesting STA may enter Doze state until TSF matches the next TWT value.

Individual TWT agreement : Unsolicited TWT (Responding without request)

TWT Requesting STA
HE STA with TWT Requester Support "1"

TWT Responding STA

Accept	STA has initiated TWT agreement with the given parameter
Alternate / Dictate	contains an advisory notification to the recipient of TWT parameter that are likely to be accepted by AP, if recipient transmits a subsequent TWT request to AP that includes those TWT parameters

STA that receives an unsolicited TWT response with Accept may transmit TWT Teardown to delete unsolicited individual TWT agreement

Broadcast TWT announcement and membership exchange

TWT Scheduled STA
TWT Requesting STA

TWT Scheduling AP
TWT Responding STA

Broadcast TWT announcement

Accept	TWT parameter used by TWT scheduled STA
Alternate	TWT parameter will change after Broadcast Persistence reaches to 0
Reject	TWT schedule will be terminated after Broadcast Persistence reaches to 0

Broadcast TWT schedules are advertised by TWT scheduling AP in frames with TWT elements with Negotiation type "2"

Membership exchange (negotiation)

Demand		Accept	Broadcast TWT schedule exists or is created according to request. TWT scheduled STA is member of broadcast TWT ID and TA in response frame
Request / Suggest		Accept	Broadcast TWT schedule exists or is created by TWT scheduling AP. TWT scheduled STA is member of broadcast TWT ID and TA in response frame

• • •

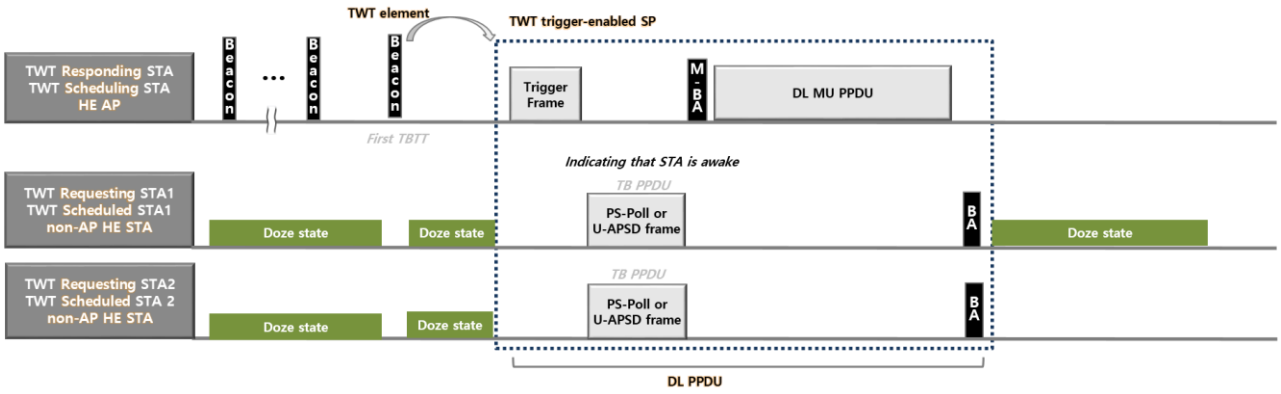
• • •

Negotiation to join or leave Broadcast TWT (identified by Broadcast TWT ID >0) are performed with an exchange of frames with TWT element with Negotiation Type "3"

TWT Operation and Service Period

TWT Requesting STA or Scheduled STA should not (not recommended) transmit frames outside TWT. However, it is still permitted with the access in contention between STAs.

In TWT SP, TWT Requesting STA or Scheduled STA has recommended frames to transmit (Broadcast TWT Recommendation in TWT element) or use additional Individual TWT for transmission. In individual trigger-enabled TWT SP, TWT requesting STA or scheduled STA should not transmit frames that are not contained within HE TB PPDU. TWT responding STA should solicit buffer status reports at the start of TWT SP



TWT Service Period

6GHz Operation

About 1.2GHz BW in 6GHz is being unlicensed and 11ax is ready for it. For 6GHz, IEEE specifies only 11ax supports and there is no significant change compared to 5GHz operation in MAC/PHY protocol and RF requirement.

6GHz Frequency

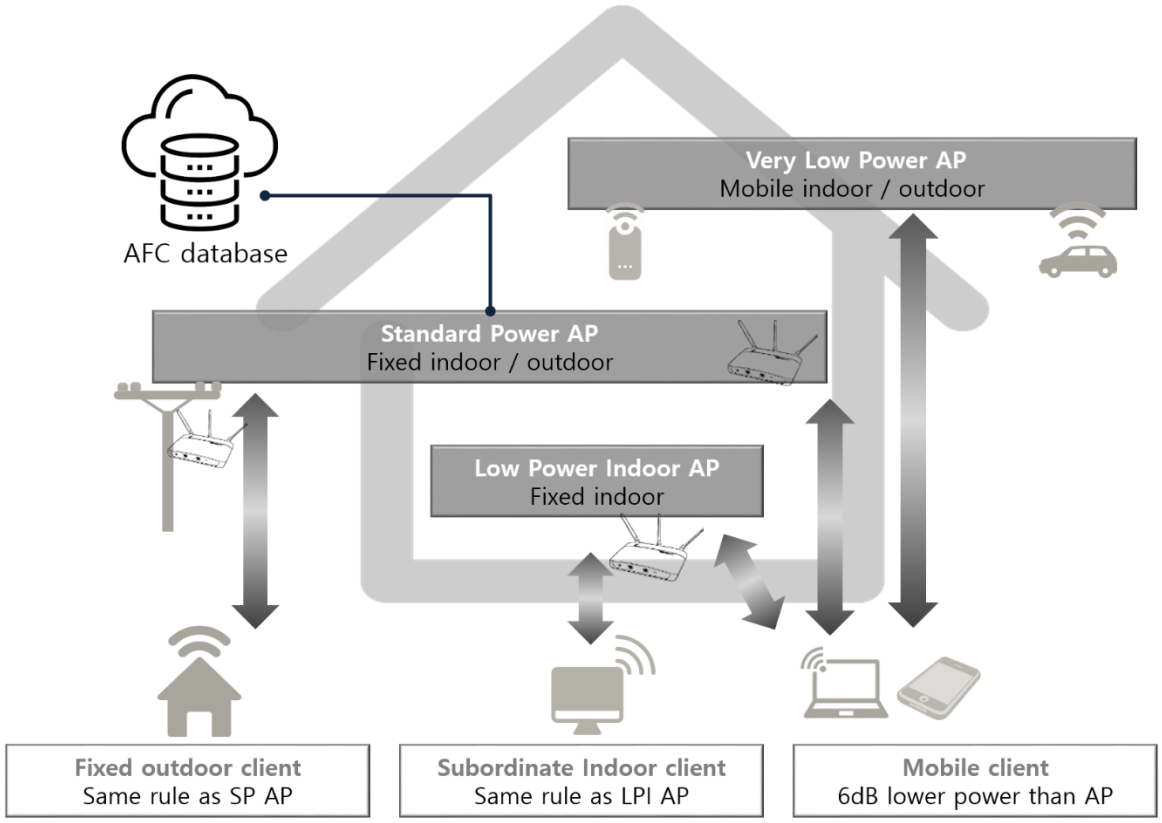
WLAN has been used mainly in 2.4GHz/5GHz and the new frequency band of 6GHz is being open (unlicensed). Even if it is not only for WLAN operation, more deployment of WLAN and more utilization of wider BW of 160MHz are expected. (about 80MHz BW of 2.4GHz , about 700MHz BW of 5GHz, about 1.2GHz BW of 6GHz). For the details on WLAN frequency and channel, find *WLAN Frequency* chapter.

6GHz Operation and Requirement

- WLAN only supports 11ax HE for 6GHz.
  - STA shall not transmit HT/VHT/DSSS/HR/ERP PPDU in 6GHz band
  - STA shall not transmit HT/VHT Capability element or Operation element in 6GHz band
- HE PHY for 6GHz
  - HE PHY for 6GHz band operation is the same as HE PHY for 5GHz band operation
  - HE transmit and receive (RF) requirement is same with 5GHz
- HE Beacon is used in 6GHz.
  - Beacon frame in HE SU PPDU (Basic/Mandatory rate, 1 SS, 20MHz, BCC)
  - HE Beacon shall not be used in 2.4G or 5GHz
- For 6GHz supporting AP
  - AP shall support at least 80MHz BW
  - 2.4GHz/5GHz AP that is co-located with 6GHz (co-located = in one device) shall provide 6GHz AP information (channel, class) by Reduced Neighbor Report element in Beacon or Probe Response frame.
  - 6GHz-only AP (without 2.4G or 5GHz in one device) should set up BSS with a primary 20MHz with PSC (Preferred Scanning Channel) that is every 16th channel from the channel starting frequency (5940MHz might be).

Device Classes

Three AP classes and three client classes are defined in 6GHz under the regulatory domain. The most popular case must be the combination of LPI AP and mobile client.



AP classes

- SP (Standard Power) AP : SP AP operates in full power indoor or outdoor (fixed). In FCC, 36dBm EIRP or 23dBm/MHz. It is under the control of AFC (Automated Frequency Coordination) database. SP AP is required to connect to AFC database to assign a list of frequencies to the AP, based on where it can operate safely without interfering with any incumbent fixed microwave receiver.
- LPI (Low Power Indoor) AP : AP is in fixed indoor operation only without AFC and it should not have antenna connector for replacing antenna. In FCC case, LPI APs will have a maximum allowed EIRP of 30 dBm or 5 dBm/MHz PSD.
- VLP (Very Low Power) AP : Mobile indoor or outdoor with very low power like Wi-Fi service in a car or a mobile router. In FCC, transmit power is 14 dBm EIRP or -8 dBm/MHz PSD.

Client classes

- Fixed outdoor client : same rule as SP AP
- Subordinate indoor client : same rule as LPI AP
- Mobile client : 6dB lower power than AP

11be, Extremely High Throughput

11be overview

Extremely High Throughput (EHT), 11be is for enhancing a maximum throughput fully-utilizing 6GHz frequency band with a wider bandwidth. 11be standard will be finalized in year of 2024 and it is going to be in market as Wi-Fi 7. There will be upgraded features of 320MHz BW, 16 SS MIMO and 4K QAM modulation and new features like MLO and HARQ. The upgrade from 11ax to 11be seems to be no drastic change as in 11ax from 11ac and it looks similar to the previous upgrade from 11n to 11ac. (Higher BW, higher QAM, and higher SS number for higher TPUT). However, you may find so many terminologies that start with "multi" in 11be; multi-link, multi-band, multi-channel, multi-RU and multi-AP and the main purpose and scheme underlying 11be seems to be the best utilization of the channels and frequency resources, which might bring higher benefit for Wi-Fi users.

Some key features on 11be is described in this chapter, which are subject to change, as 11be activity is on-going.

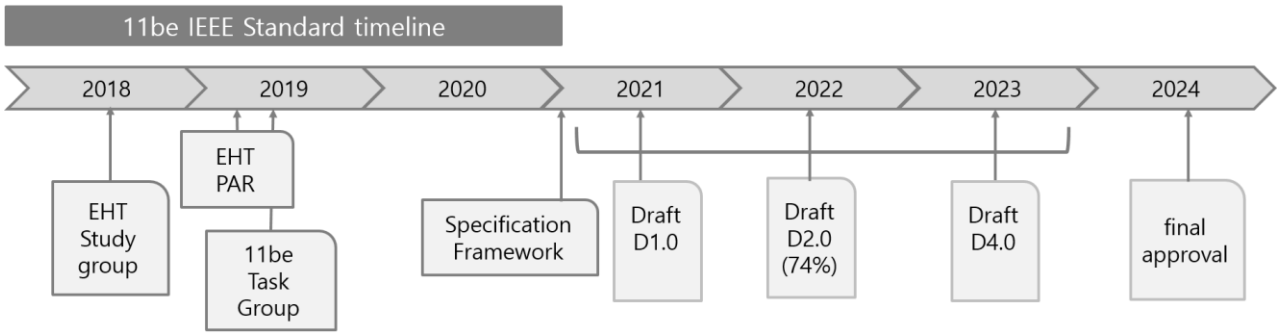
11be PAR

11be EHT (Extremely High Throughput) for a maximum throughput up to 30Gbps at MAC layer using the same frequency band with 11ax.

> This amendment defines standardized modifications to both the IEEE Std 802.11 physical layers (PHY) and the Medium Access Control Layer (MAC) that enable at least one mode of operation capable of supporting a maximum throughput of at least 30 Gbps, as measured at the MAC data service access point (SAP), with carrier frequency operation between 1 and 7.250 GHz while ensuring backward compatibility and coexistence with legacy IEEE Std 802.11 compliant devices operating in the 2.4 GHz, 5 GHz, and 6 GHz bands.

Schedule

11be amendment will be finalized in 2024.



Operating conditions and Features

Compared with 11ax, 11be is going to use higher BW, modulation and MIMO SS for a maximum throughput with the same frequency band and modulation scheme. New candidate features like MLO, HARQ and multi-AP coordination are also introduced.

		11ax	11be
Frequency		2.4G, 5GHz, 6GHz	
Bandwidth		20, 40, 80, 80+80, 160MHz	Up to 320MHz
MIMO		8 SS	16 SS
Modulation	OFDM	OFDM (312.5KHz)	
	Up to	1024QAM	4096QAM
Upgrading features	MU MIMO sounding	Explicit	Implicit
	RU allocation	1 RU / 1 User	Multi-RU / 1 User
New featues			MLO HARQ Multi-AP coordiation

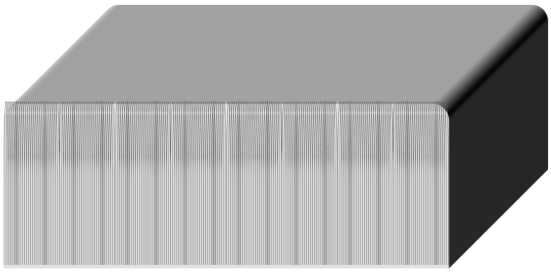
4K QAM and data rate

4K QAM modulation and data rate

With 4096 QAM modulation, each subcarrier now carries information up to 12bit and the maximum data rate is about 5.75GMps/320MHz (1SS). EVM requirement for 4Q QAM is -38dB.

EHT 80MHz 1SS Data Rate (MCS13, 0.8u GI)

80MHz	11be
12	12 bit (4096QAM)
X 980	980 data subcarrier
X 5/6	5/6 coding
/ 13.6	12.8usec + 0.8usec Normal GI
= 720.6bit/usec	720.6Mbps



11be 80MHz

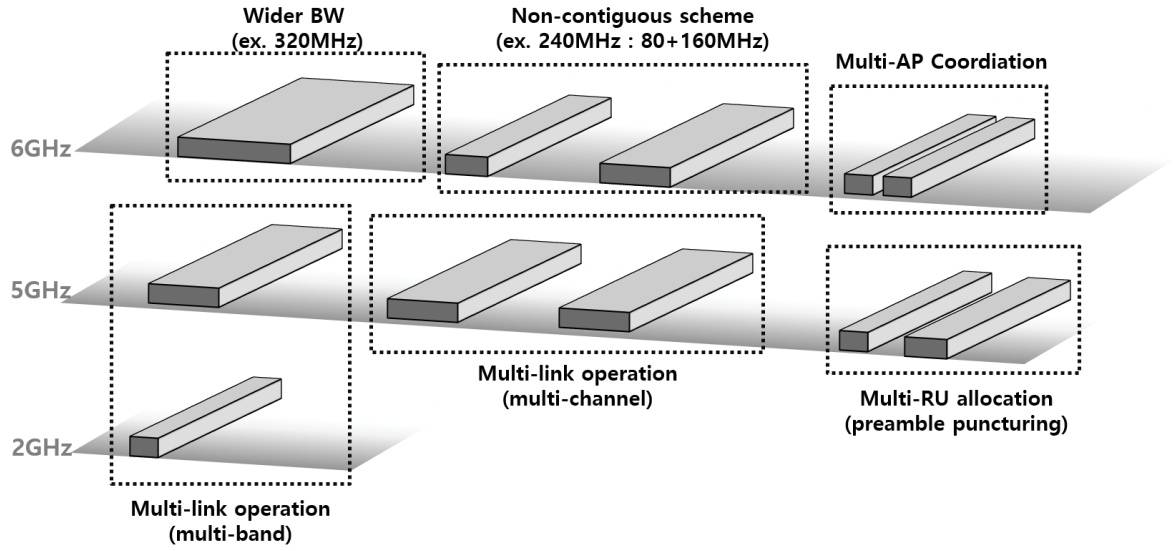
EHT highest data rate

BW	SS	Data rate
80M	1	720.6Mbps
160M 80M	1 2	1,441.2Mbps
320M 160M	1 2	2,882.4Mbps
320M	2	5,764.7Mbps
320M	16	46,118.4Mbps

11be MIMO supports up to 16 SS and around 46Gbps data rate can be achieved. Considering the situation of non-AP STA that supports one or two antenna and spectral efficiency of about 150bps/Hz in 16SS, you can say that 16 SS is too much. MIMO can be used for one user (SU-MIMO) or multi-user (MU-MIMO) and 16SS is mainly for MU-MIMO for higher channel efficiency and implicit sounding process along with explicit sounding is revised in 11be for efficient usage of MU-MIMO.

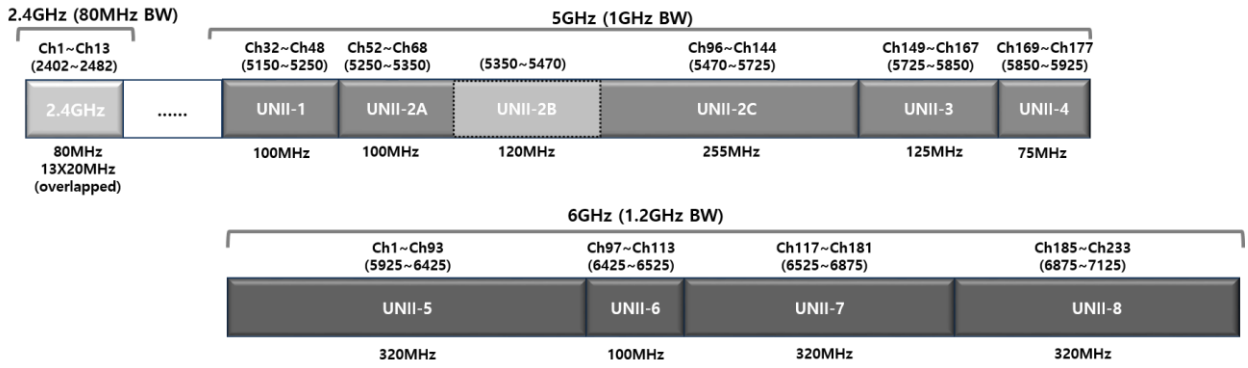
Higher Channel Utilization

For the full-scale usage of Wi-Fi channel with 2.4GHz, 5GHz and 6GHz, 11be devises many features for the channel utilization. The benefit of higher channel utilizations may not be just enhancing maximum throughput. The diverse multi-operations (multi-link, multi-band, multi-channel, multi-RU, multi-AP) grant a flexible and maximized usage of the frequency resource for a load balancing and a reliable and low-latency Wi-Fi operations.



Various bandwidth support

WLAN has been supported 20MHz, 40MHz, 80MHz, 160MHz, 80+80MHz. You can fine one or two 160MHz channel in 5GHz, while vendors are reluctant to use it if it has DFS channel. With the advent of 6GHz, wider channels are open and up to 7 contiguous 160MHz and 3 contiguous 320MHz can be utilized.



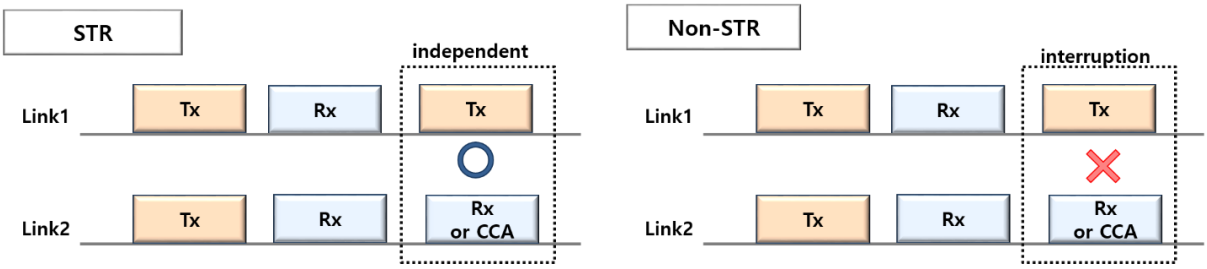
Along with the previous bandwidth of 11ax, 11be supports wider bandwidth of 240MHz and 320MHz in contiguous and non-contiguous mode; 160+80MHz, 160+160MHz.

MLO : Multi-link operation

MLO is the concurrent utilization of multiple radio links of different frequency channels/bands by AP and non-AP STA (MLD : multi-link device). AP is likely to support a simultaneous transmission and reception without interference between them, while non-AP STA can be capable of STR or non-STR. Asynchronous access is for STR MLD and synchronous operation is for non-STR MLD.

STX capability : Simultaneous transmission and reception

- STR MLD : Individual link operates independently. Tx on one link does not affect Rx or CCA on other links.
- Non-STR MLD : Operation on one link is restricted by operation on another link. Tx is not allowed in one link, if Rx or CCA is affected in other links.

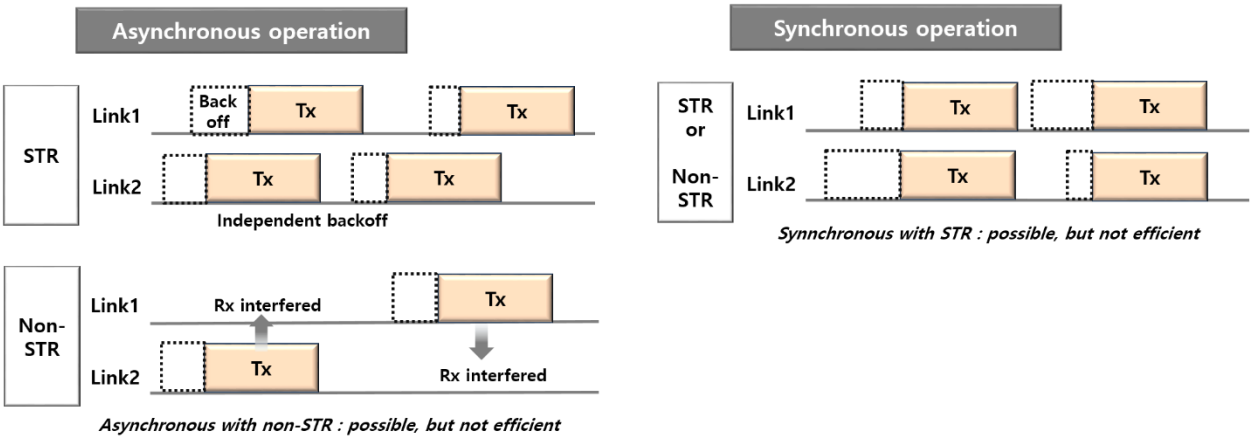


In general, AP MLD should be capable of STR, while non-AP STAs may have STR or non-STR.

MLO access scheme : Asynchronous and Synchronous operation

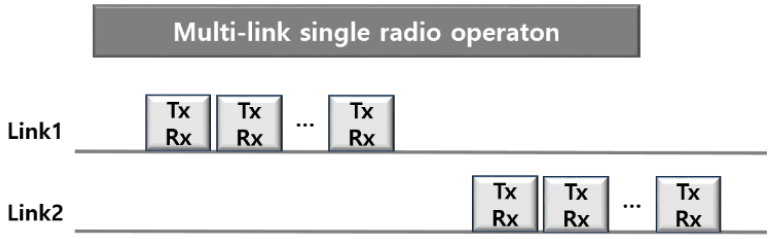
Both STR and non-STR MLD can operate Asynchronous or Synchronous mode, while Asynchronous operation is mainly designed for STR MLD and Synchronous operation is made for non-STR MLD.

- Asynchronous operation : Asynchronous Tx initiations are allowed with independent backoff. Mainly for STR MLD.
- Synchronous operation : Only simultaneous Tx initiation is allowed on all links. Mainly for non-STR MLD. Non-contiguous channel support (ex. 80+80MHz) can be said a kind of synchronous operation. But, non-contiguous channel is PHY/RF scheme, while MLO is a broad concept that runs in higher level (MAC).



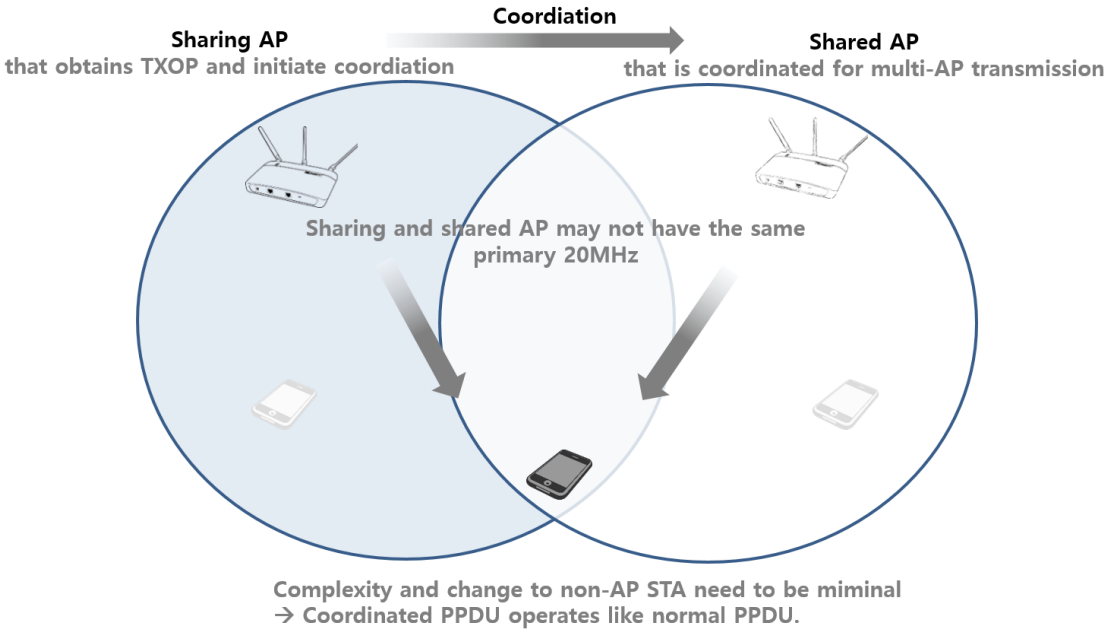
Multi-link single radio operation

A non-AP MLD operates on more than one link but can only receive, or transmit frames on one link at a time. This STA transmits data/management frame on one link, while listens on another link.



Multi-AP coordination

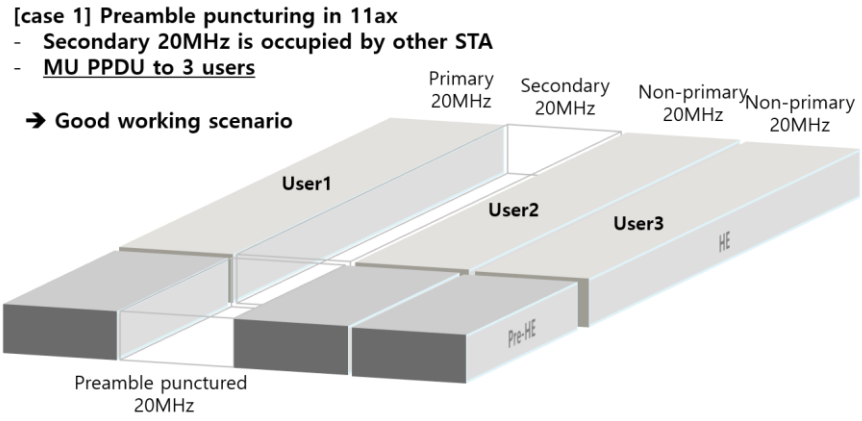
Neighboring AP's are coordinated to transmit PPDU to STA and the packet operates like normal PPDU to minimize the change and complexity to STAs.

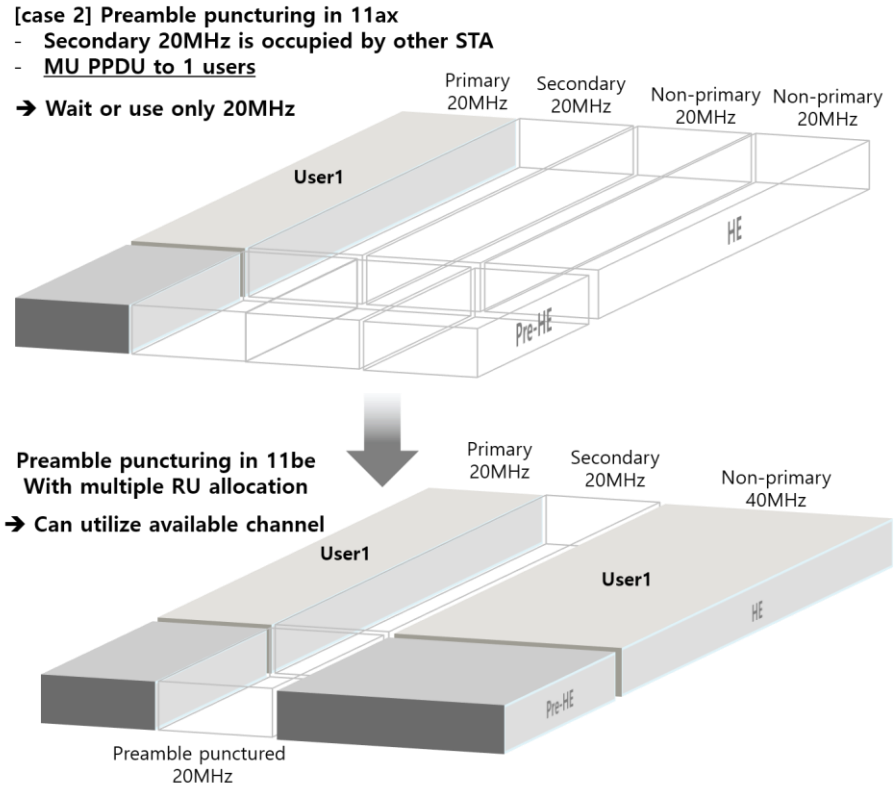


Multiple RU

11be allows more than one RU to be assigned to a single STA. RU with 242 (20MHz) or more tone is called as “large-size RU” and RU with less than 242 tone is “small-size RU”. Large size RU can be combined only with large size RU and small size RU is only with small size RU.

This multiple RU scheme gives flexibility allocating user, and we can also see the benefit of channel utilization. In case of preamble puncturing which was introduced in 11ax, one RU allocation for one user has limitation as below and 11be can assign one user for the whole preamble punctured frame with multi-RU scheme.

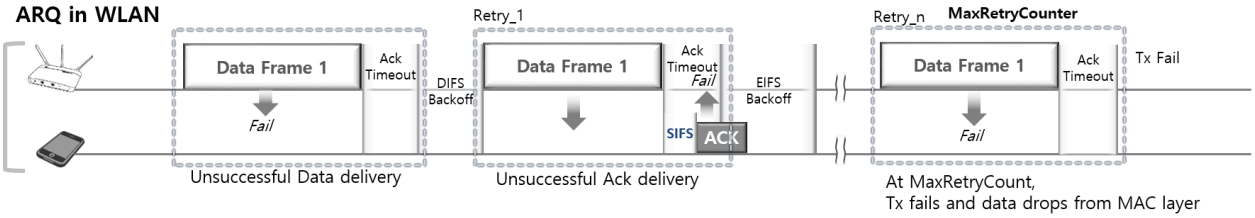




Other candidate features

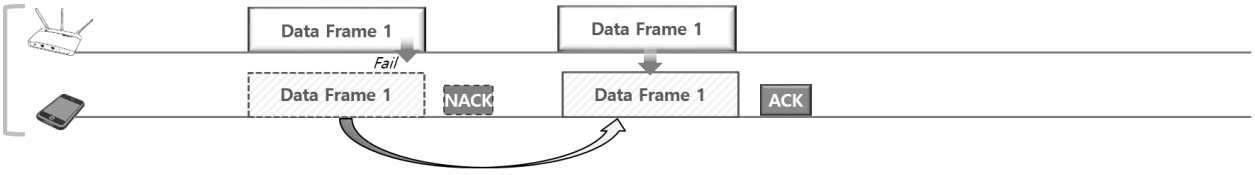
HARQ

For correcting error in wireless communication, two methods are widely used. (1) FEC (2) re-transmission. Retransmission is a kind of ARQ (automatic repeat request) in WLAN, which is the transmitter transmits the packet again when there is no ACK from the receiver. Hybrid ARQ has been discussed for a long time in WLAN standard and 11be deals with it again. The receiver uses the information on the previous packet which may have error to decode the currently received packet. In ARQ, only the last packet is used for decoding.



Automatic Repeat Request in WLAN : STA repeats the transmission if there is no ACK from the counterpart

Hybrid ARQ in 11be



HARQ

- **Combination of ARQ and FEC**
- **Receiver uses the previous data (bit or symbol level) to decode**

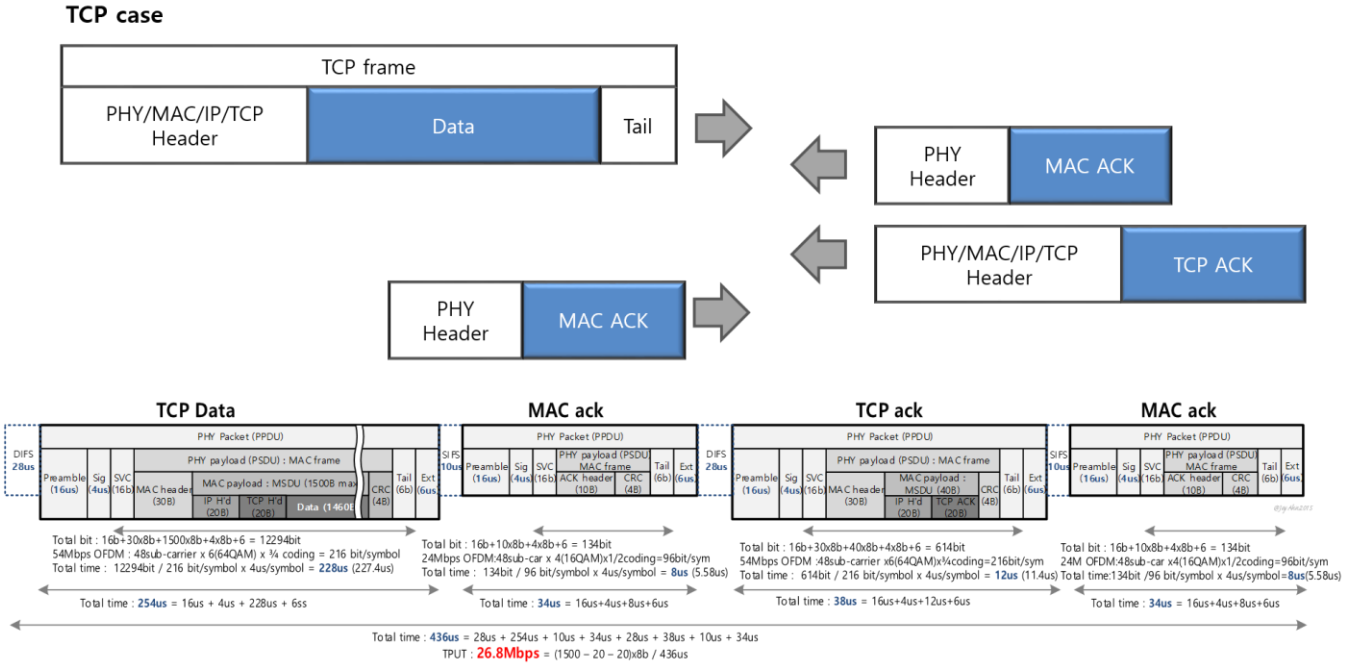
Appendix

Throughput Calculation

11g 54Mbps throughput is calculated in both TCP and UDP scenario. There is a big gap between data rate and throughput value, as there are many overhead factors. HT and VHT throughput efficiency is better with aggregation, while calculation is much complicated.

- TCP Case

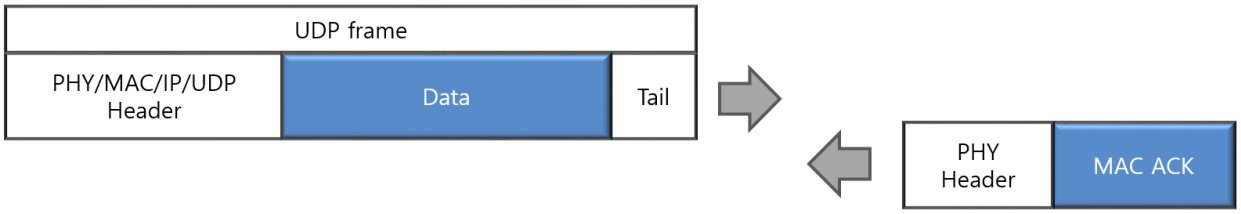
Every MAC data frame requires Ack and Every TCP frame in upper layer also needs to receive TCP Ack. TCP Ack is data from in MAC layer which needs MAC Ack. Assuming near-perfect condition. No re-transmission in any layer, 1:1 connection and no backoff, No buffer empty or full, MSDU size is based on 1500 Byte and Short Slot Time is used in 2.4GHz

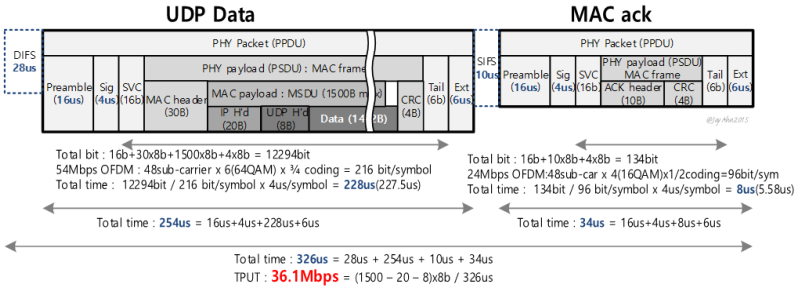


- UDP Case

UDP layer does not request Ack.

UDP case





WLANpedia for Wi-Fi Engineers

The latest version download from

www.wlanpedia.com

Jay Ahn