Hack Wi-Fi using ESP32

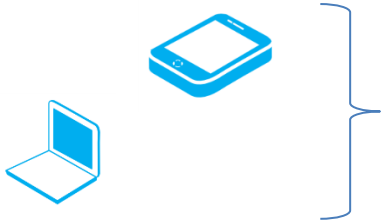
I am working at

http://gs-labs.ru

- Specialize in ICS security of embedded devices
- Dedicate a lot of time to programming industrial controllers for ICS
- Took part in smart home development projects

- Wi-Fi introduction
- Some Wi-Fi Attack
- ESP32
- Practical

Wi-Fi introduction



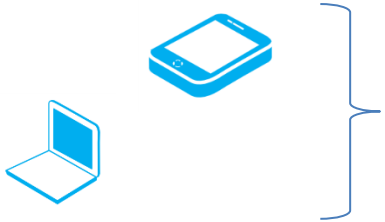
Station

(STA)

Any device, which support PHY & MAC 802.11

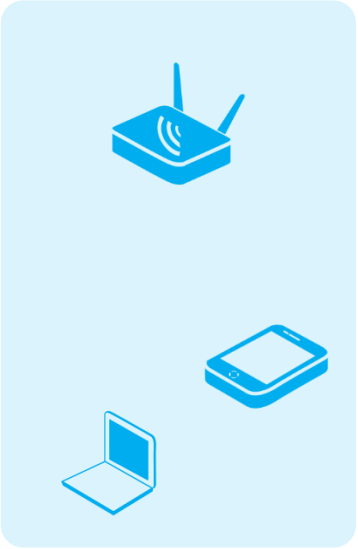
Access point (AP)

Any entity that has station functionality and provides access to the distribution services, via the wireless medium for associated STAs



STA

Basic Service Set (BSS)

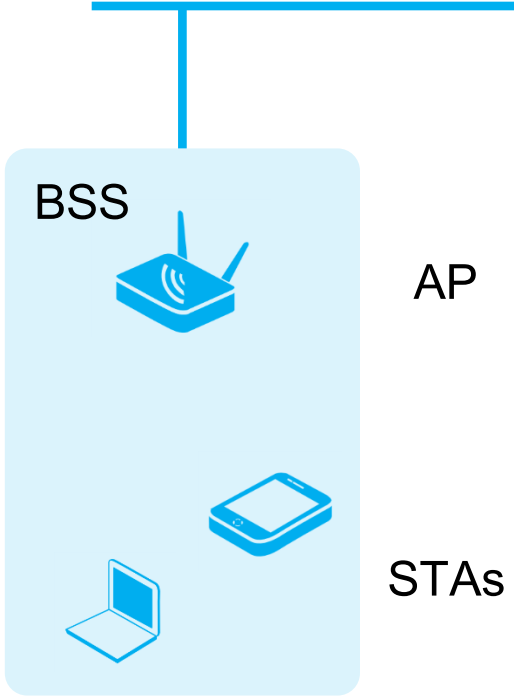


A set of stations (STAs) that have successfully synchronized for 802.11 communications.

All basic service sets can be identified by a 48-bit (6-octet) MAC address known as the “**BSSID**” (**basic service set identifier)**

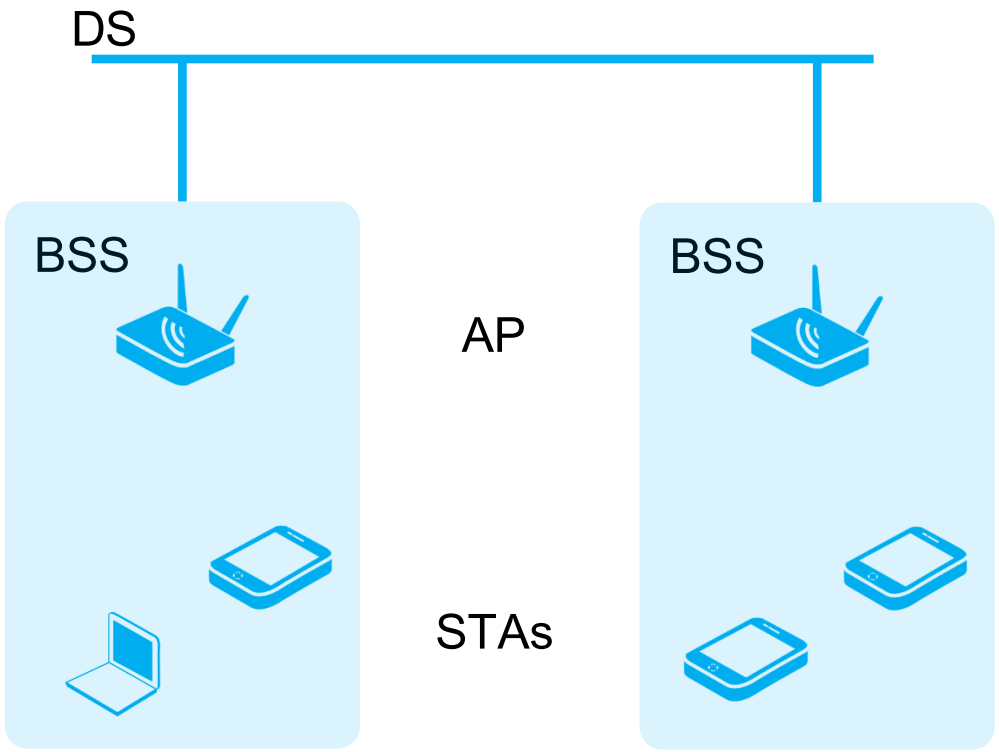
Distribution System (DS)

A system used to interconnect a set of basic service sets and integrated local area networks (LANs) to create an extended service set (ESS)



Ethernet

Extended Service Set (ESS)



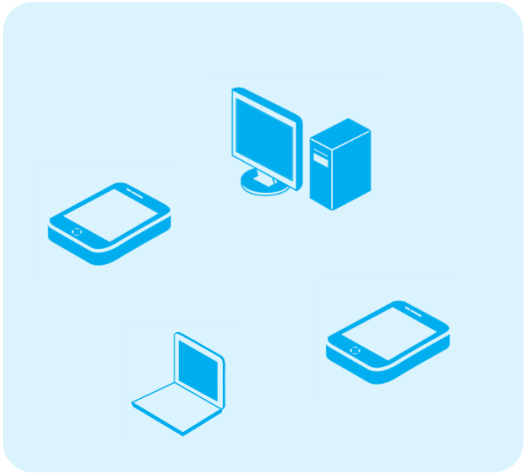
An extended service set is one or more basic service sets connected by a distribution system medium.

The logical network name of an ESS is often called an extended service set identifier (ESSID), or, more simply, the service set identifier (**SSID**)

SSID – max 32 bytes

Ethernet

Independent basic service set (IBSS)



STAs

An IBSS consists solely of client stations that use **peer-to-peer communications**. An IBSS is a self-contained network that does not use an access point and has no access to a distribution system.

MSDU MAC Service Data Unit

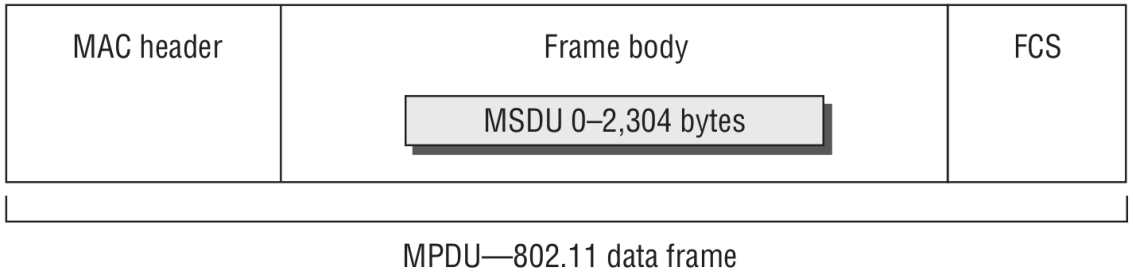
When the Network layer (layer 3) sends data to the Data-Link layer (layer 2), the data is handed off to the LLC and becomes known as the MAC Service Data Unit (MSDU)

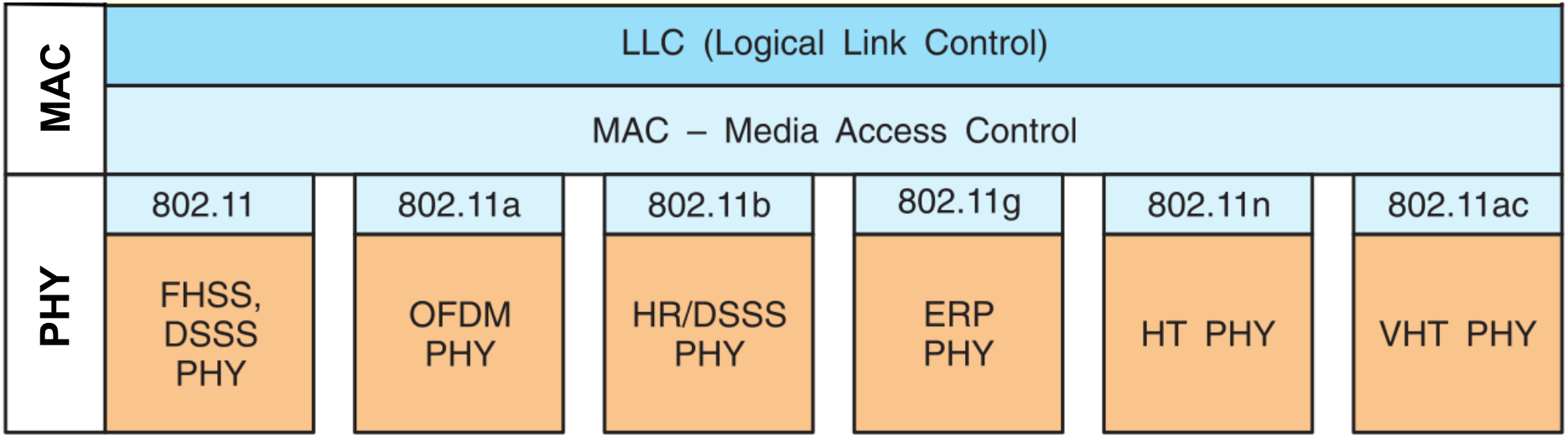
MSDU === data payload(IP packet + some LLC data)

MPDU MAC Protocol Data Unit

When the LLC sends the MSDU to the MAC sublayer, the MAC header information is added to the MSDU to identify it.

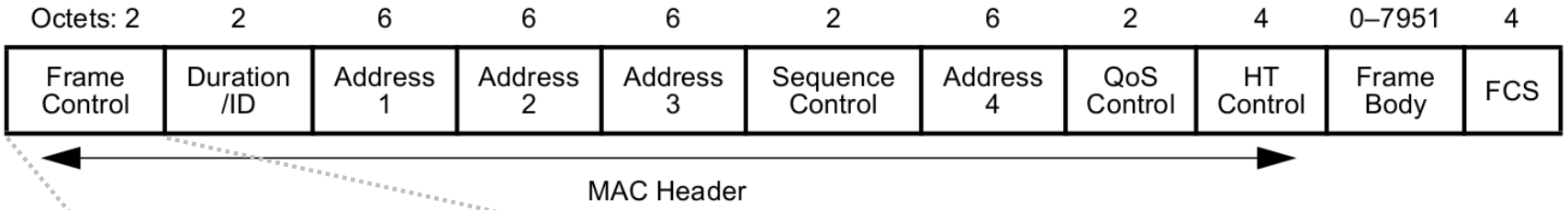
MPDU === 802.11 frame



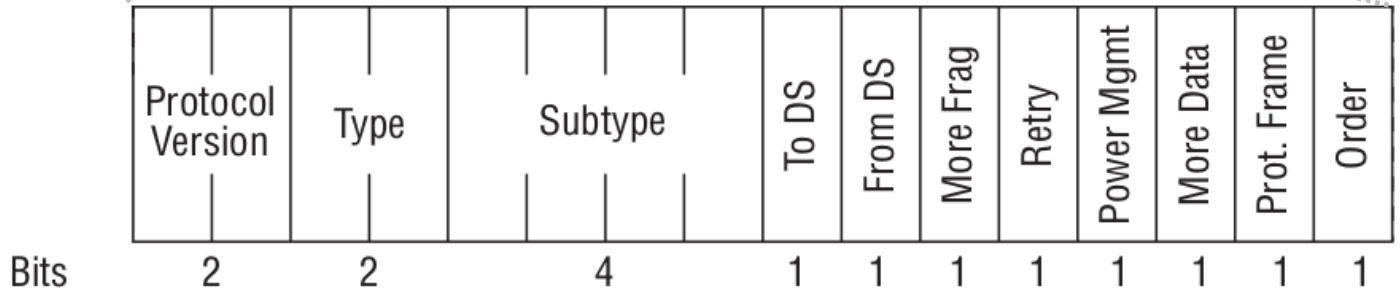

MAC
LLC (Logical Link Control)
MAC – Media Access Control
PHY
802.11
FHSS, DSSS PHY
802.11a
OFDM PHY
802.11b
HR/DSSS PHY
802.11g
ERP PHY
802.11n
HT PHY
802.11ac
VHT PHY

Standard	Max Speed	Frequency	Backwards Compatible
802.11a	54 Mbps	5 GHz	No
802.11b	11 Mbps	2.4 GHz	No
802.11g	54 Mbps	2.4 GHz	802.11b
802.11n	600 Mbps	2.4 GHz or 5 GHz	802.11b/g
802.11ac	1300 Mbps	2.4 GHz or 5 GHz	802.11b/g/n
802.11ad	7000 Mbps	2.4 / 5 / 60 GHz	802.11b/g/b/ac
802.11ax	Up to 10747 Mbps		

802.11 frame



Frame Control

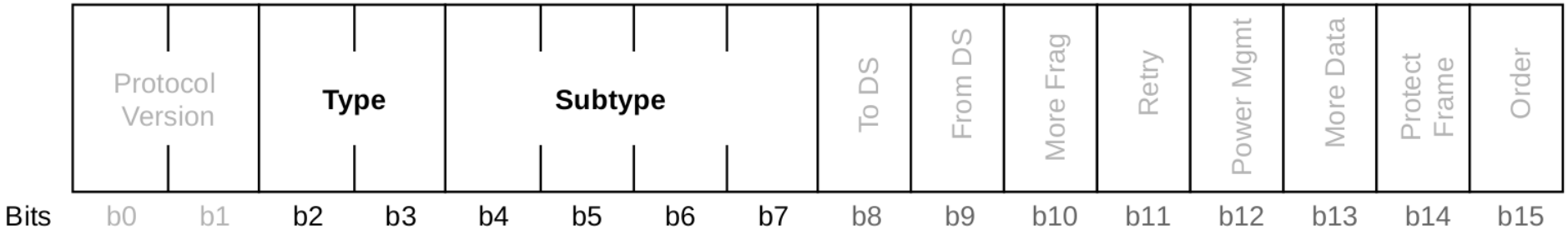


Protocol Version

To indicate which protocol version of 802.11 technology is being used by the frame

All 802.11 frames have the value of the "*Protocol Version*" field always set to 0

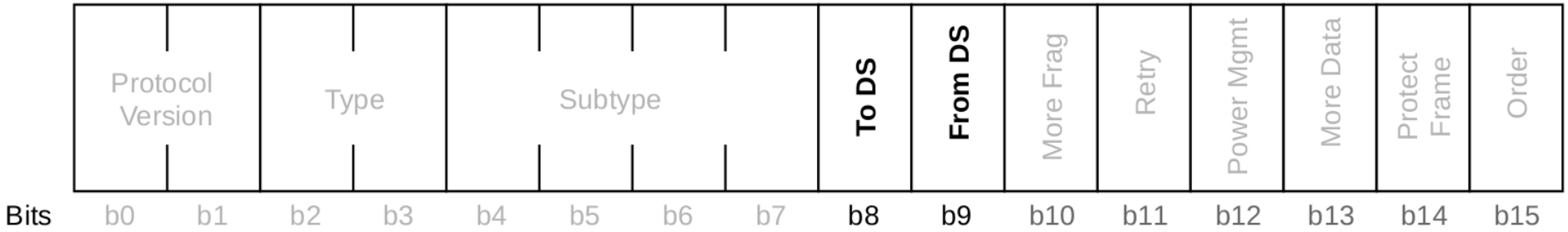
Type & Subtype



Bits	Frame type
0, 0	Management frame
0, 1	Control frame
1, 0	Data frame
1, 1	Reserved

+ Subtype

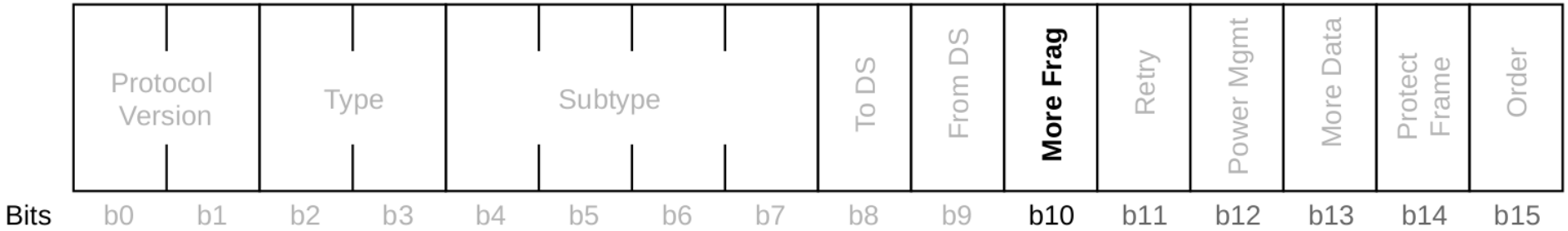
“To DS” and “From DS”



used in combination to change

the meaning of the four MAC addresses in an 802.11 MPDU

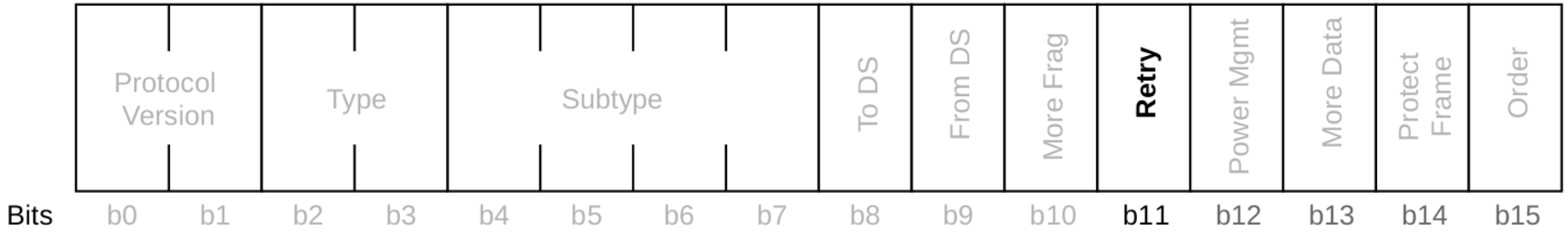
More frag



Only on "*Data*" or "*Mgmt*" frame

that have another fragment of the current MSDU or current MMPDU to follow

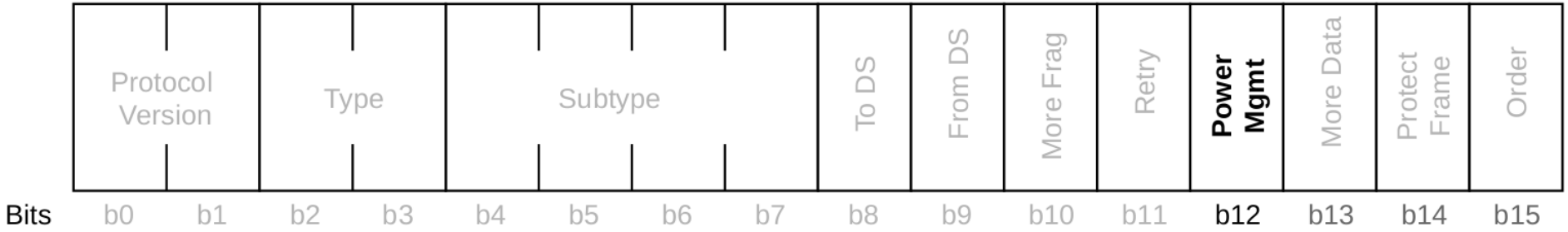
Retry



Only on "*Data*" or "*Mgmt*" frame

that is a retransmission of an earlier frame

Power Mgmt

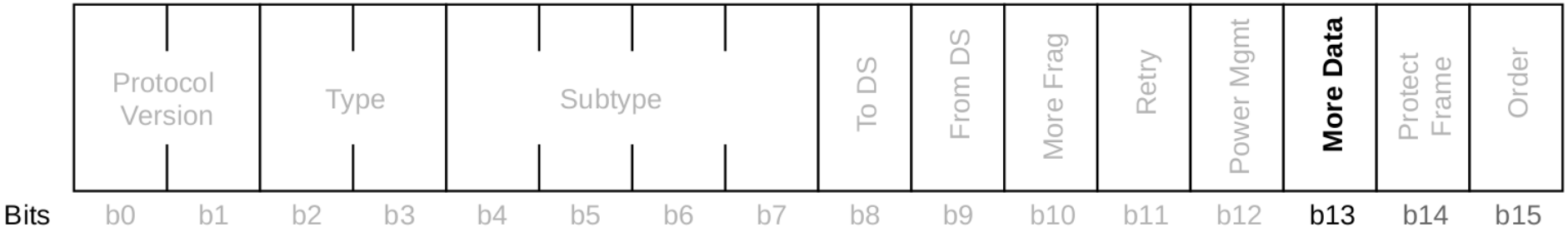


to indicate the power management mode of a STA

1 – Power Save mode

0 – Active mode

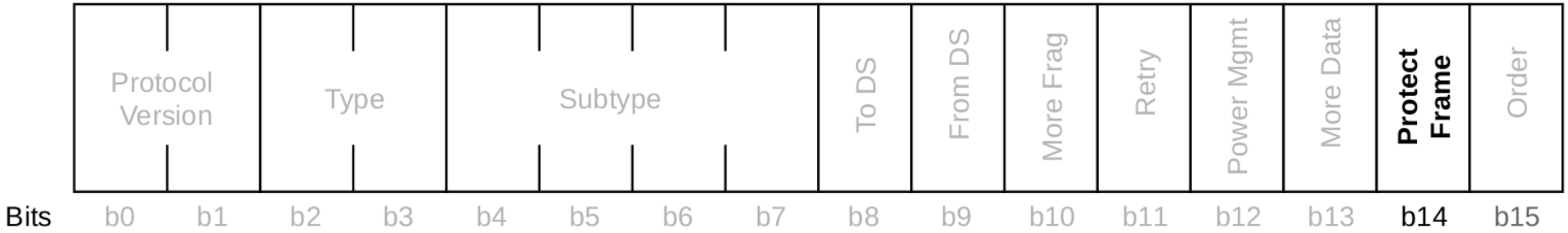
More Data



Only on "*Data*" or "*Mgmt*" frame

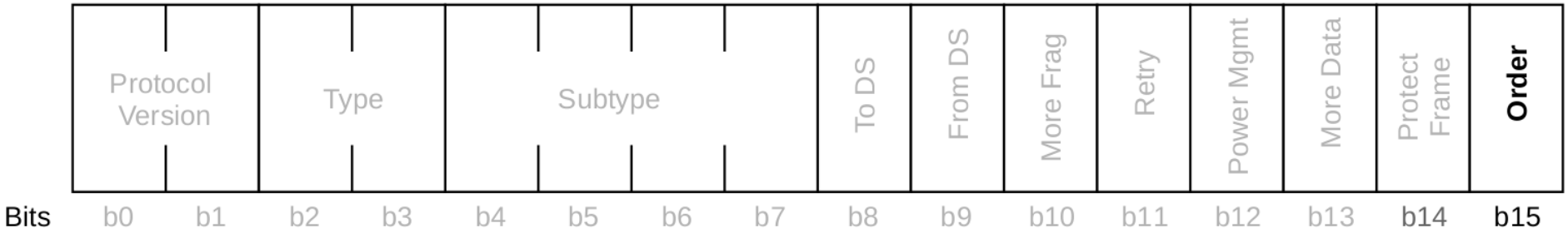
AP indicate to a STA in PS mode that more data available to STA

Protect Frame



indicate whether the MSDU payload of a data frame is encrypted

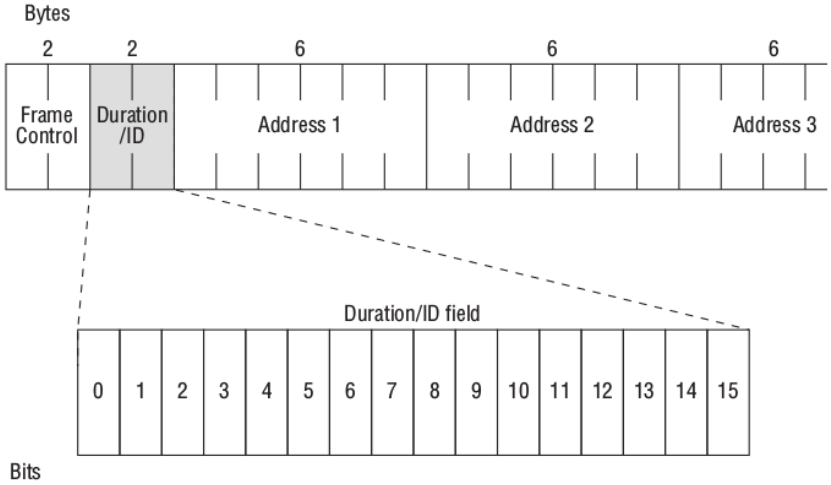
Order



"*non-QoS data frame*" indicate that the frame contains an MSDU, or fragment thereof, that is being transferred using the StrictlyOrdered service class

"*QoS data or mgmt frame*" to indicate that the frame contains an "*HT Control*" field

Duration/ID



- **Virtual Carrier Sense**

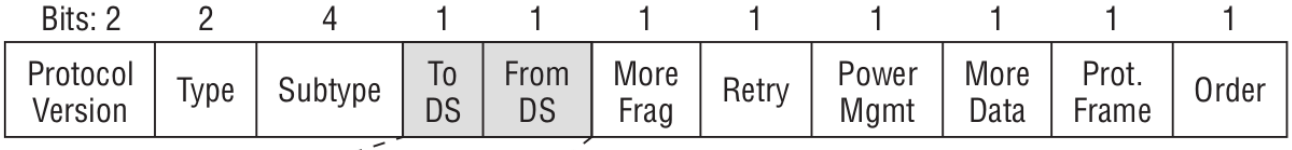
This is the main purpose which used to reset the NAV timer of the other stations

- **Legacy Power Management**

PS Poll frames use this field as an association identifier (AID)

- **Contention-free Period**

This field is used as an indicator that a point coordination function (PCF) process has begun



To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	RA = DA	TA = SA	BSSID	N/A
0	1	RA = DA	TA = BSSID	SA	N/A
1	0	RA = BSSID	TA = SA	DA	N/A
1	1	RA	TA	DA	SA

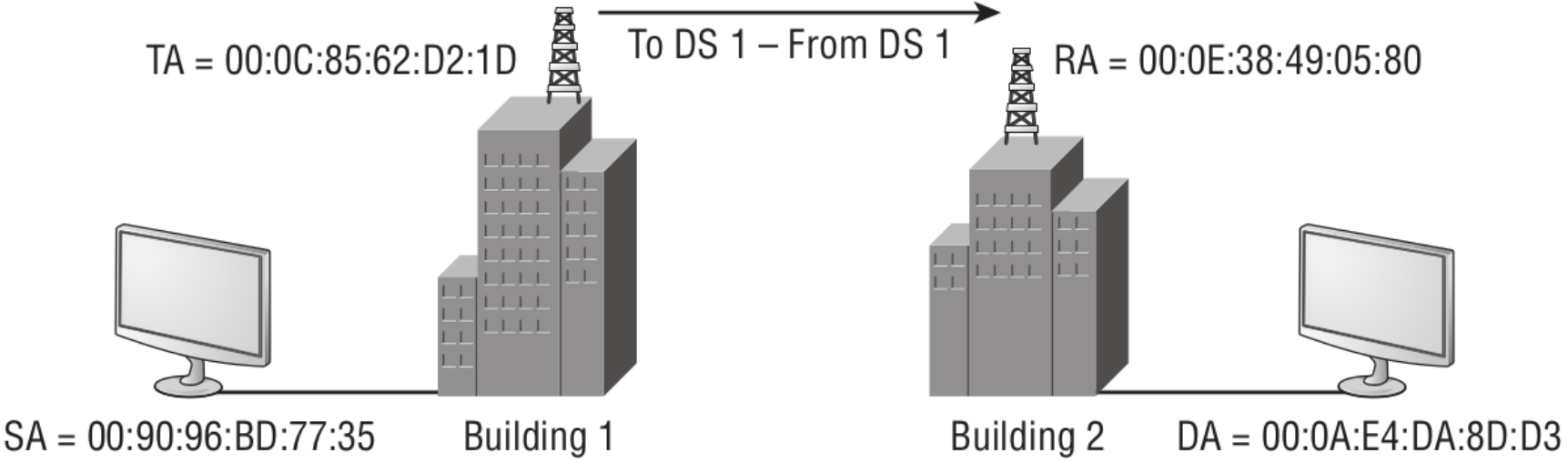
SA - MAC address of the original sender

DA - MAC address of final destination

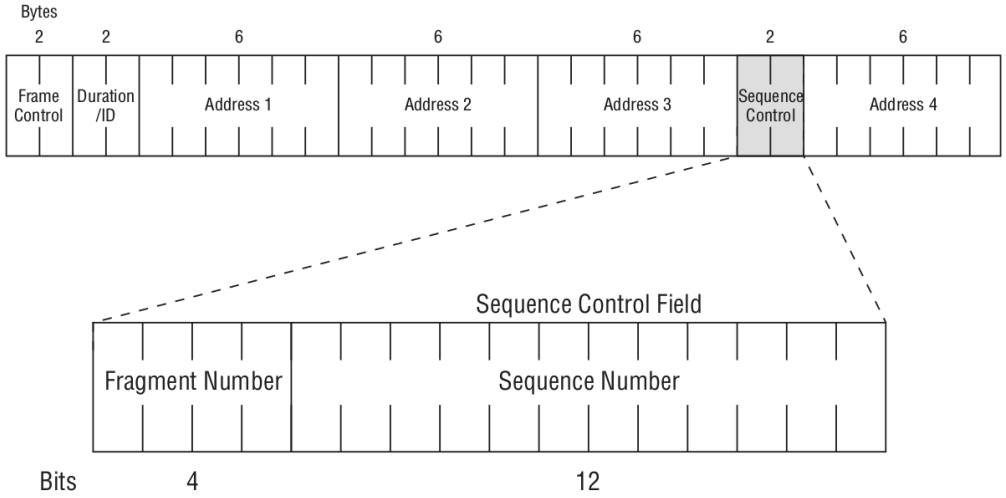
TA - MAC address of the transmitting 802.11 radio

RA - MAC address of the receiving 802.11 radio

BSSID - L2 identifier of the basic service set (BSS)


TA = 00:0C:85:62:D2:1D
To DS 1 – From DS 1
RA = 00:0E:38:49:05:80
SA = 00:90:96:BD:77:35
Building 1
Building 2
DA = 00:0A:E4:DA:8D:D3

Sequence Control



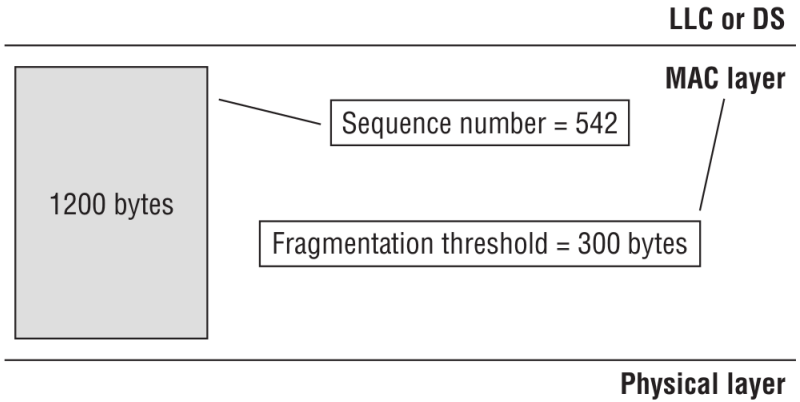
Not present in "***Control frame***"

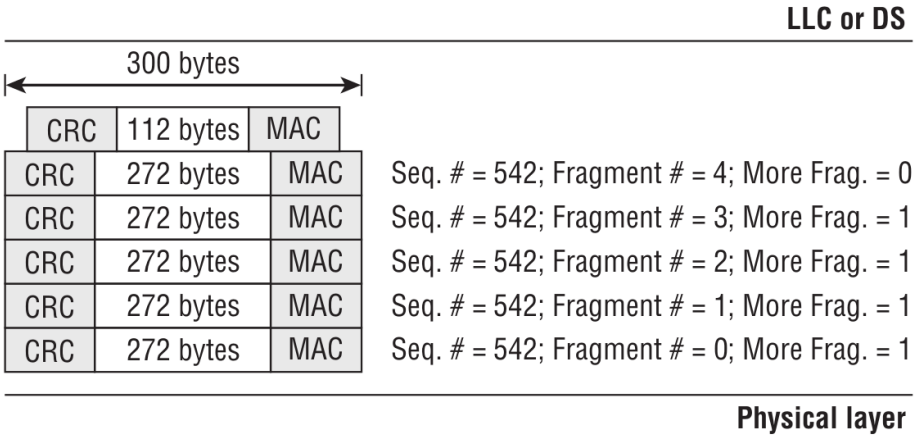
- **Sequence Number**

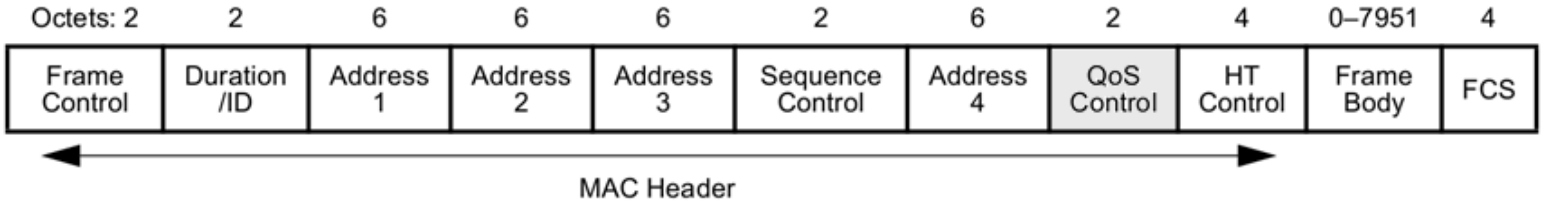
12-bit field indicating the sequence number of an MSDU, A-MSDU, or MMPDU

- **Fragment Number**

4-bit field indicating the number of each fragment of an MSDU or MMPDU

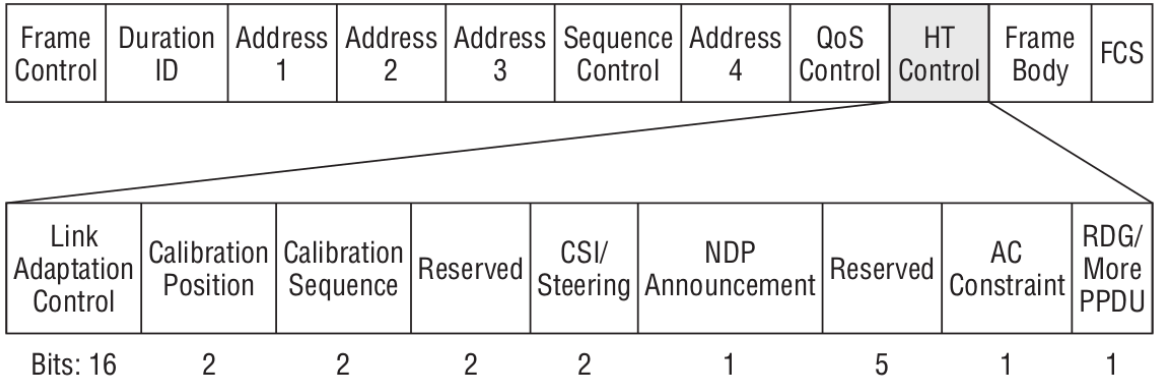

LLC or DS
MAC layer
1200 bytes
Sequence number = 542
Fragmentation threshold = 300 bytes
Physical layer


LLC or DS
300 bytes
CRC
112 bytes
MAC
CRC
272 bytes
MAC
Seq. # = 542; Fragment # = 4; More Frag. = 0
Seq. # = 542; Fragment # = 3; More Frag. = 1
Seq. # = 542; Fragment # = 2; More Frag. = 1
Seq. # = 542; Fragment # = 1; More Frag. = 1
Seq. # = 542; Fragment # = 0; More Frag. = 1
Physical layer



The 802.11-2007 standard states, “The **QoS Control** field is present in **all data frames** in which the **QoS subfield** of the **Subtype field** is set to **1**

Add in 802.11n



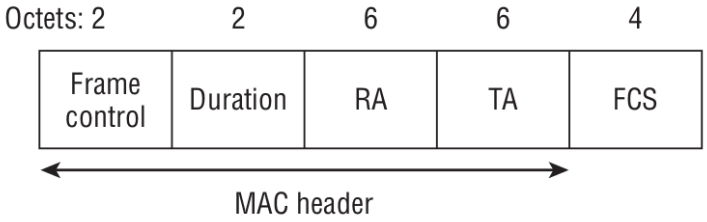
HT Control present, when

- MAC header -> FC.order = 1
- **QoS data & management frames**

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
01	Control	0000–0110	Reserved
01	Control	0111	Control wrapper
01	Control	1000	Block ack request (BlockAckReq)
01	Control	1001	Block ack (BlockAck)
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF-End
01	Control	1111	CF-End and CF-Ack

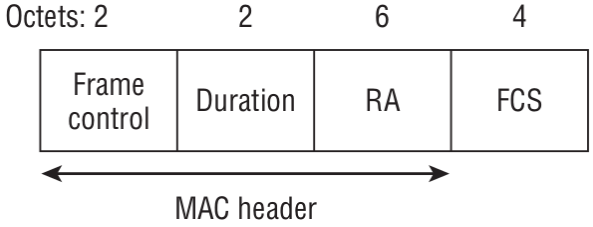
RTS frame

(Request to send)



CTS frame

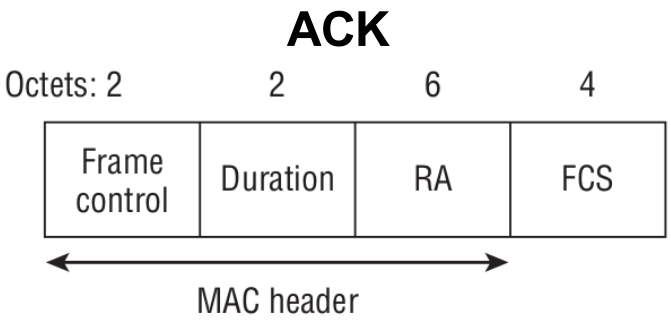
(Clear to send)



RA - receiver address

TA - transmitter address

Duration - the time needed for the subsequent frames in the transmit operation to be transmitted

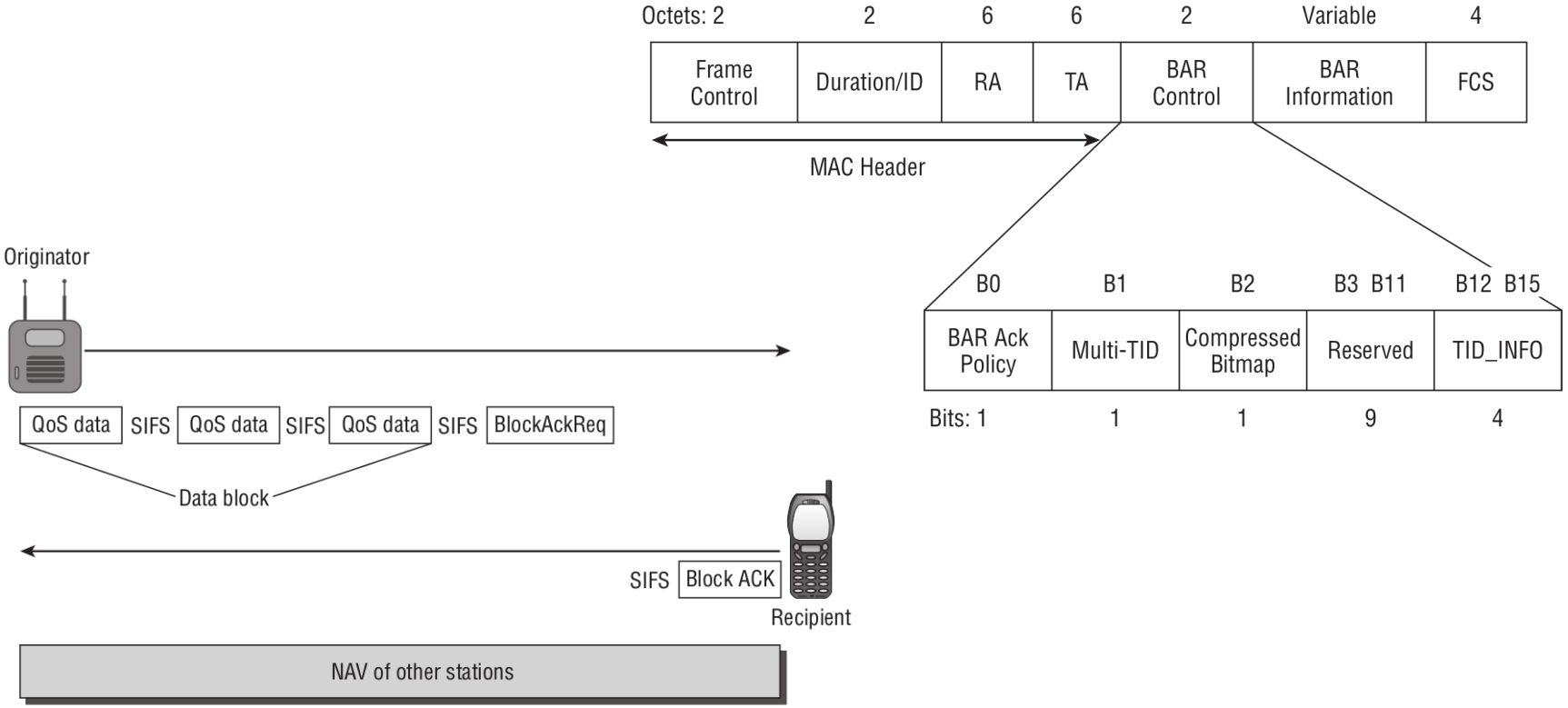


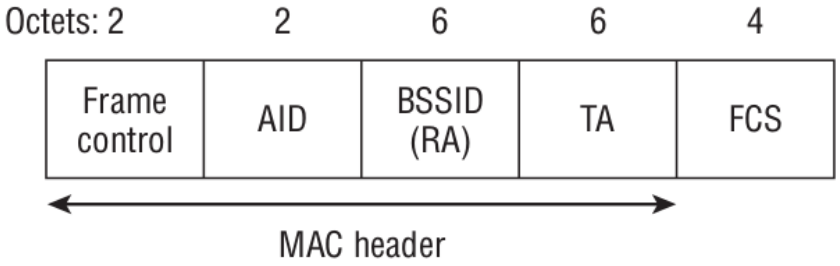
RA - receiver address,

is copied from the address 2 field of the frame that is being acknowledged

All unicast 802.11 frames must be acknowledged

BlockAck frame

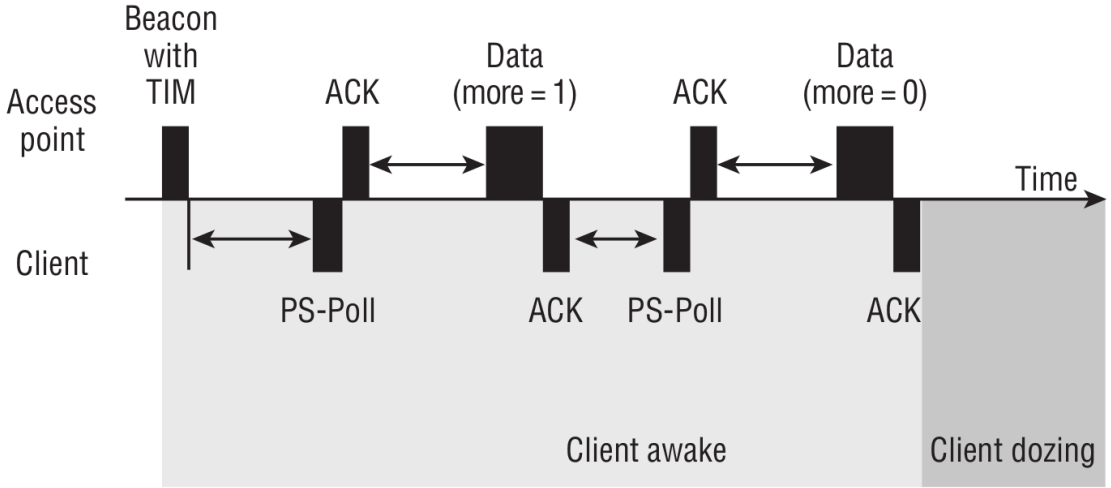




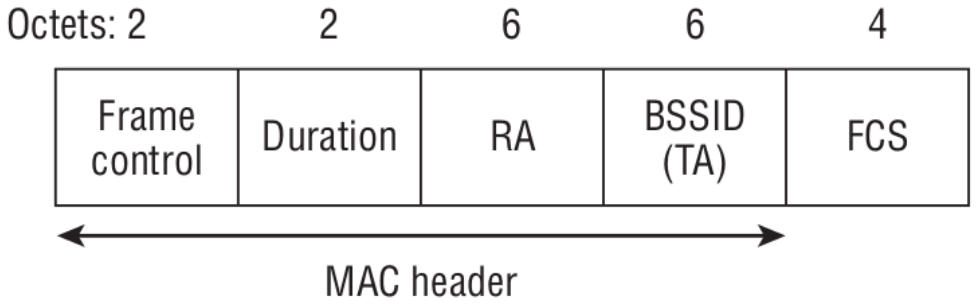
AID - association identifier

The **AP** uses this **AID** to keep track of the stations that are associated and the members of the BSS

PS-Poll frame

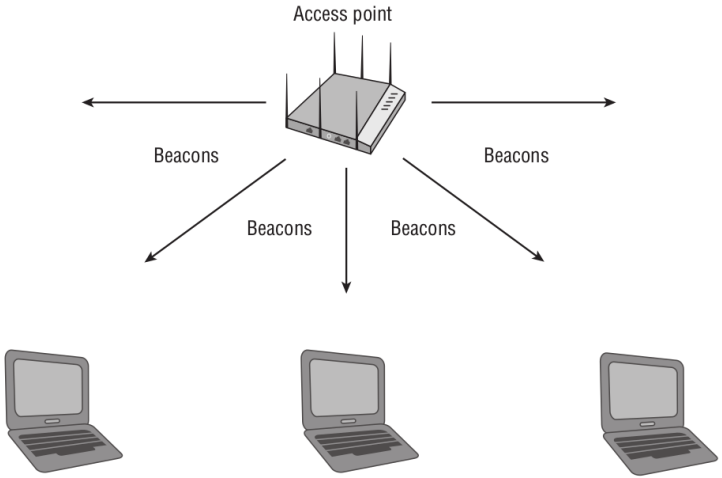


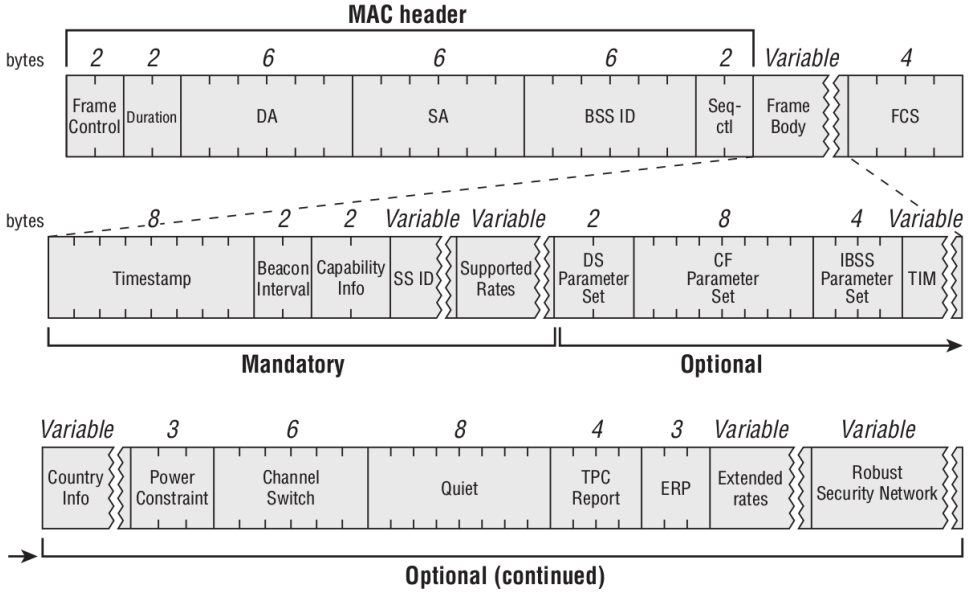
CF-End / CF-End + CF-Ack frame (Contention Free)



Subtype bits	Subtype description
0000	Association request
0001	Association response
0010	Reassociation request
0011	Reassociation response
0100	Probe request
0101	Probe response
1000	Beacon
1001	Announcement traffic indication message (ATIM)
1010	Disassociation
1011	Authentication
1100	Deauthentication
1101	Action
1110	Action no ack

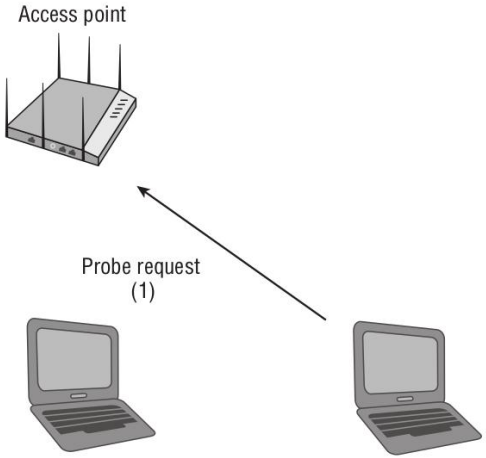
Beacon frame





Probe Request frame

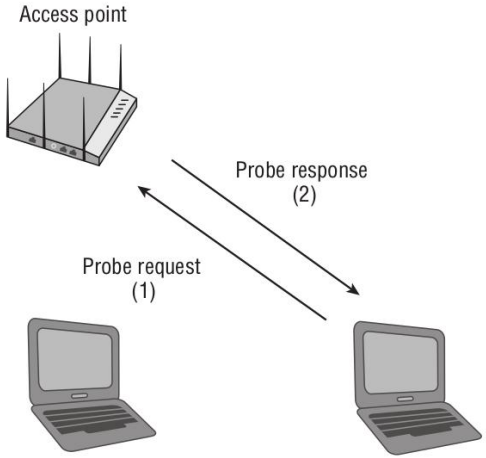
Order	Information	Note
1	Service Set Identifier (SSID)	
2	Supported Rates	
3	Request Information	Used with 802.11d.
4	Extended Supported Rates	The Extended Supported Rates element is present whenever there are more than eight supported rates; it is optional otherwise.
5	Vendor Specific	One or more vendor-specific information elements may appear in this frame. This information element follows all other information elements.

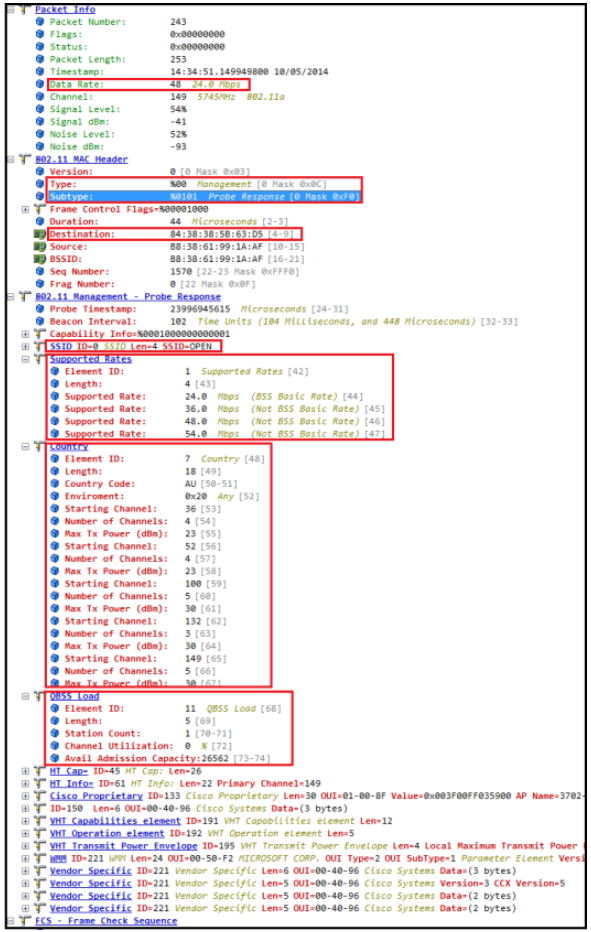


Probe Request are sent to the broadcast DA address (ff:ff:ff:ff:ff:ff)

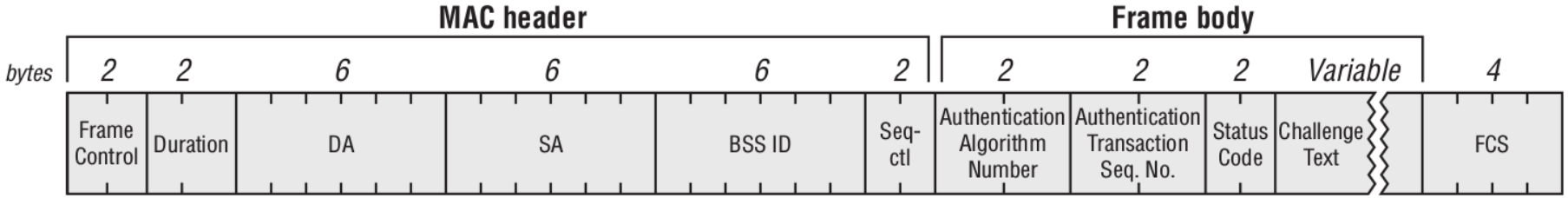
Probe Response frame

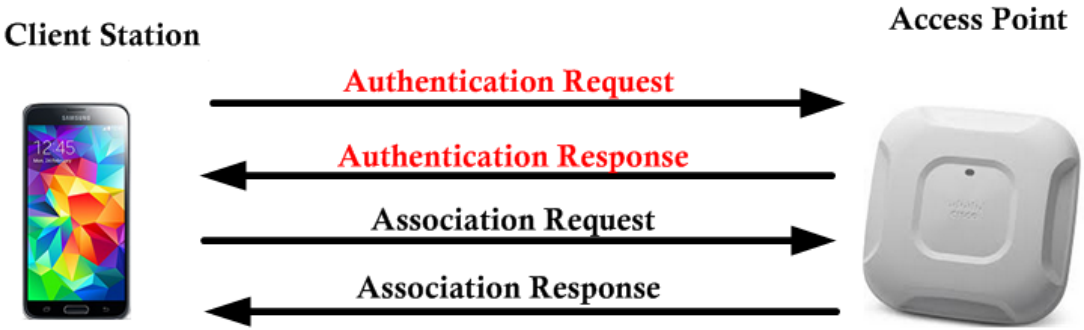
Upon receiving a probe request frame, a station in an IBSS or an AP will respond with a probe response frame, which contains information about itself and the cell



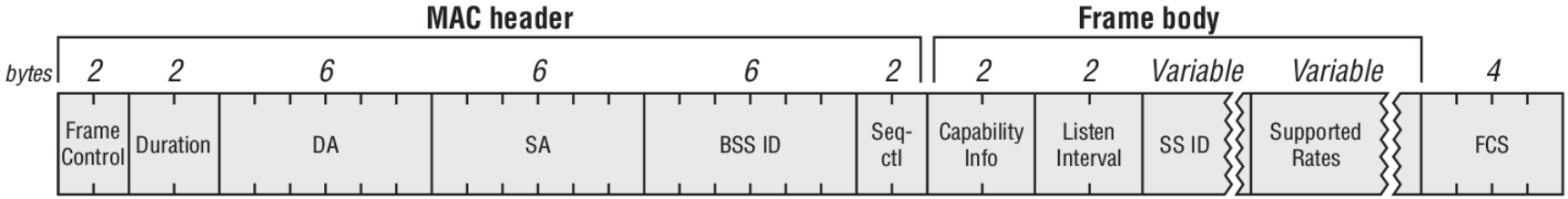


Authentication frame





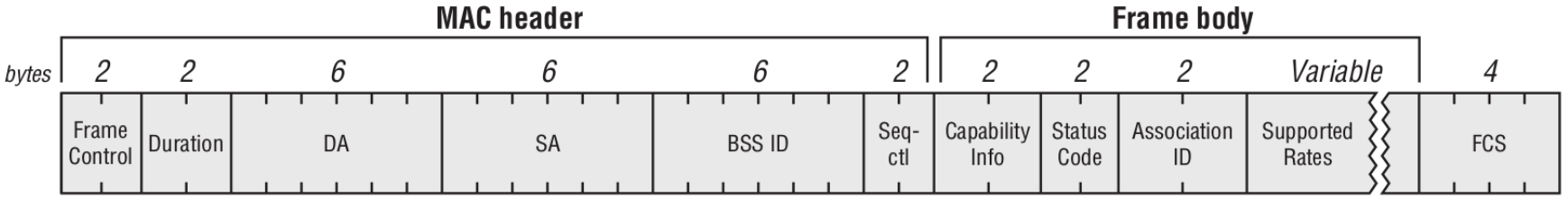
Association Request Frame



Order	Information	Notes
1	Capability Information	
2	Listen interval	
3	SSID	
4	Supported rates	
5	Extended Supported Rates	Present whenever there are more than eight supported rates; it is optional otherwise.
6	Power Capability	Used with 802.11h.
7	Supported Channels	Used with 802.11h.
8	RSN	Used with 802.11i.

Order	Information	Notes
9	QoS Capability	Used with 802.11e QoS.
10	RRM Enabled Capabilities	Used with 802.11k.
11	Mobility Domain	Used with 802.11r.
12	Supported Regulatory Classes	Used with 802.11r.
13	HT Capabilities	Used with 802.11n.
14	20/40 BSS Coexistence	Used with 802.11n.
15	Extended Capabilities	The Extended Capabilities element may be present if any of the fields in this element are nonzero.
Last	Vendor Specific	One or more vendor-specific information elements may appear in this frame. This information element follows all other information elements.

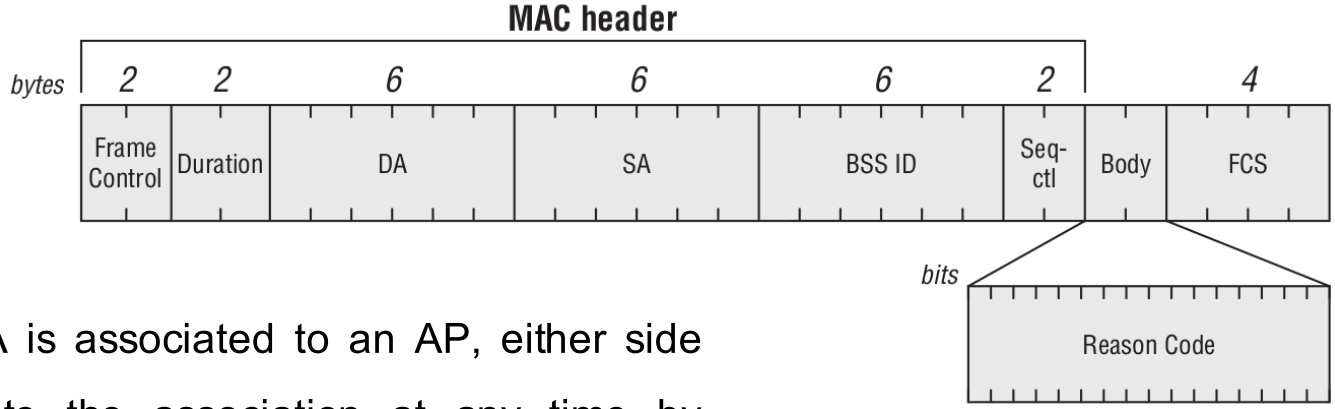
Association Response Frame



Order	Information	Notes
1	Capability Information	
2	Status Code	
3	Association ID	
4	Supported rates	
5	Extended Supported Rates	The Extended Supported Rates element is present whenever there are more than eight supported rates; it is optional otherwise.
6	EDCA Parameter Set	

Order	Information	Notes
7	RCPI	Used with 802.11k.
8	RSNI	Used with 802.11k.
9	RRM Enabled Capabilities	Used with 802.11k.
10	Mobility Domain	Used with 802.11r.
11	Fast BSS Transition	Used with 802.11r.
12	DSE Registered Location	Used with 802.11y.
13	Timeout Interval (association comeback time)	Used with 802.11w.
14	HT Capabilities	Used with 802.11n.
15	HT Operation	Used with 802.11n.
16	20/40 BSS Coexistence	Used with 802.11n.
17	Overlapping BSS Scan Parameters	Used with 802.11n.
18	Extended Capabilities	The Extended Capabilities element may be present if any of the fields in this element are nonzero.
Last	Vendor Specific	One or more vendor-specific information elements may appear in this frame. This information element follows all other information elements.

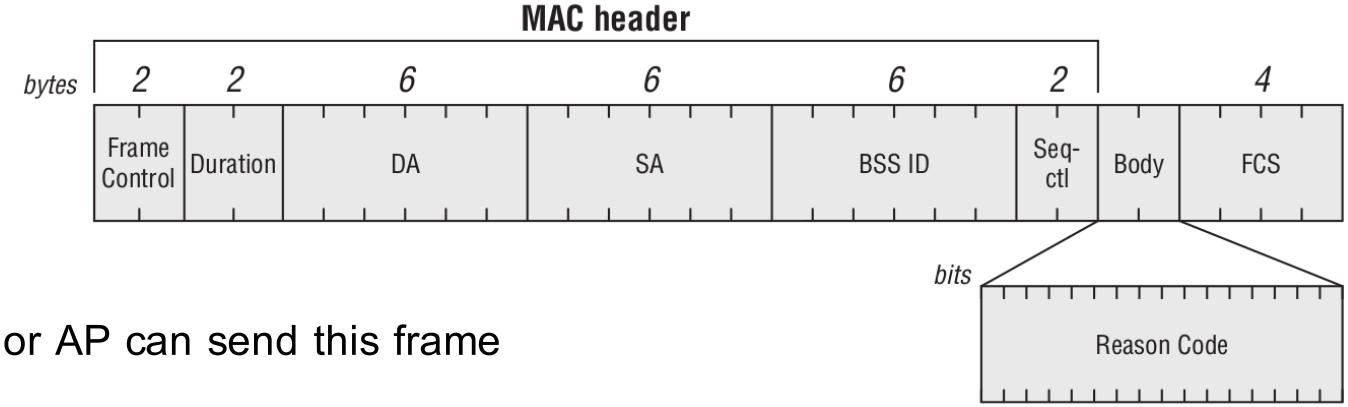
Disassociation Frame



Once a STA is associated to an AP, either side can terminate the association at any time by sending a disassociation frame

A disassociated station is still authenticated

Deauthentication Frame

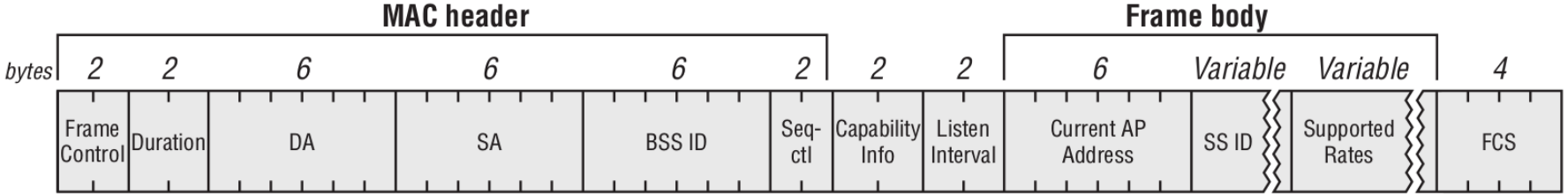


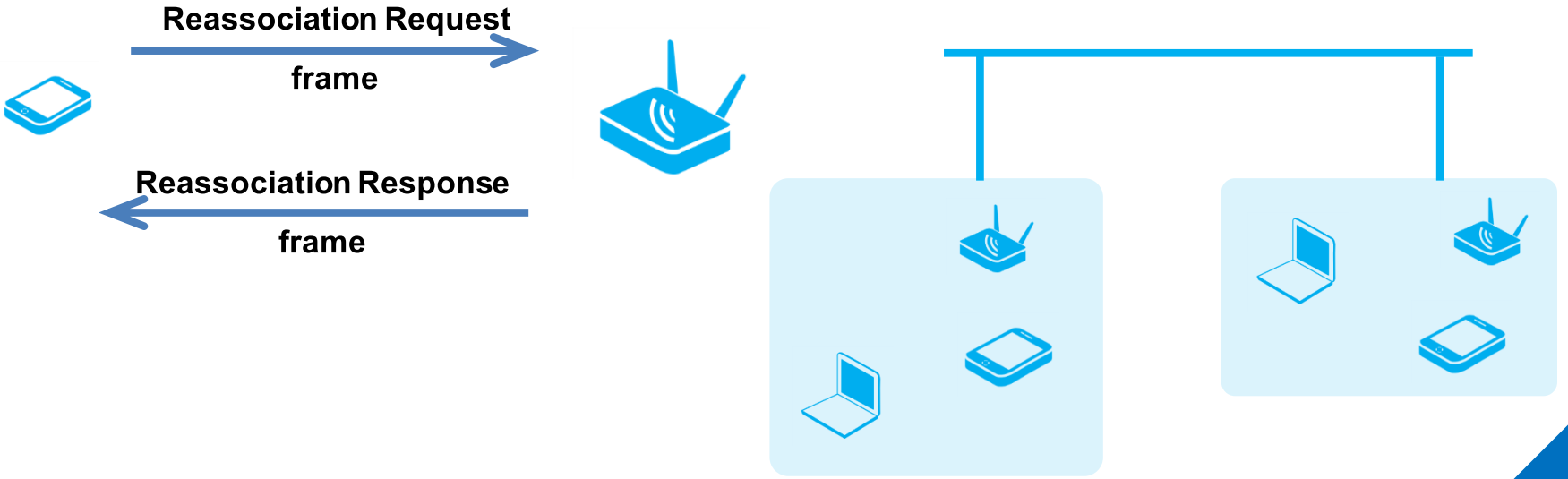
The station or AP can send this frame

This frame is used when all communications are terminated

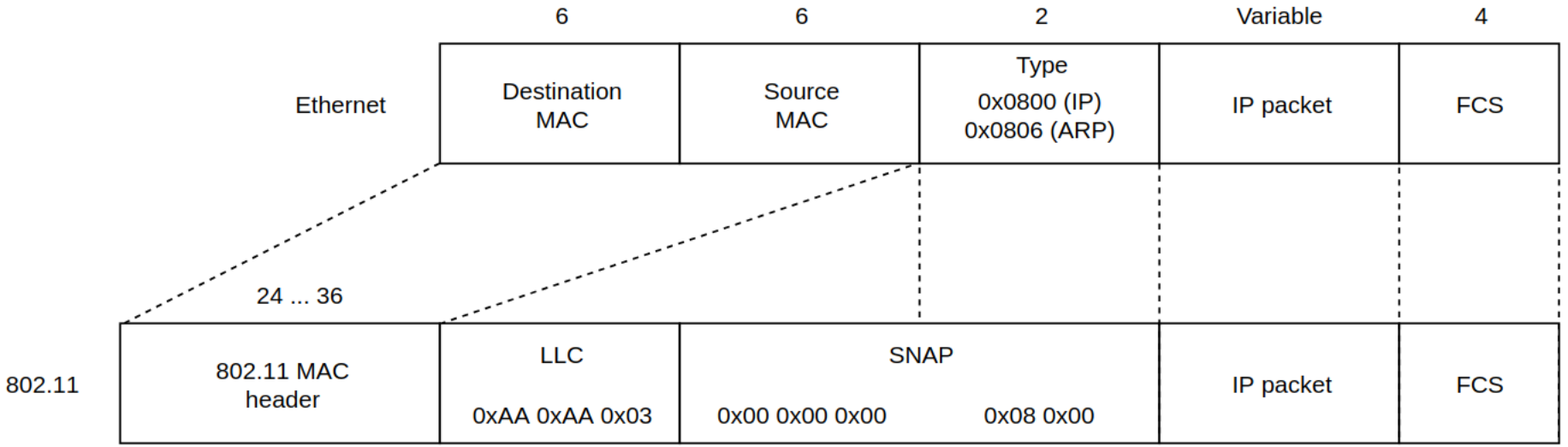
Type	Subtype	
00	1010	disassociation frame
00	1100	deauthentication frame

Reassociation Request/Response frame

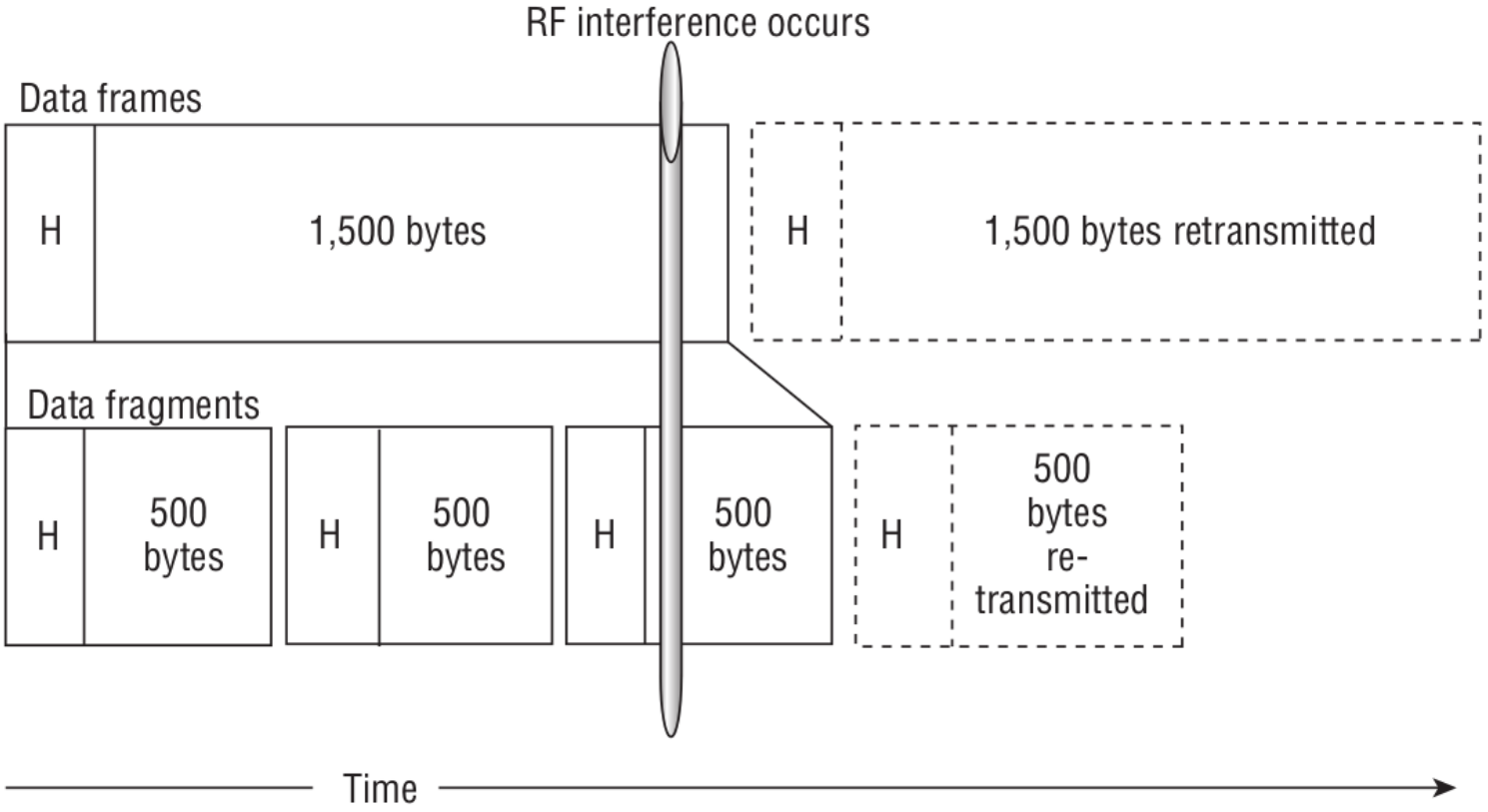




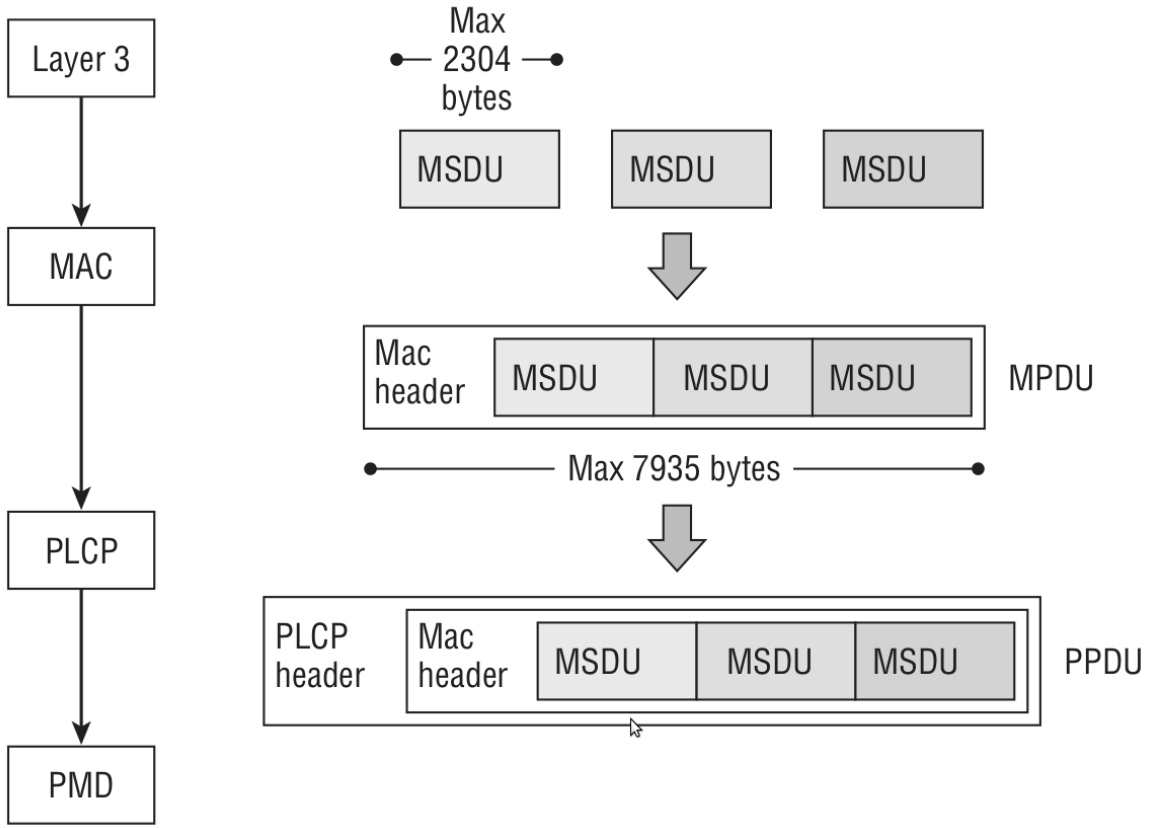
Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
10	Data	0000	Data
10	Data	0001	Data + CF-Ack [PCF only]
10	Data	0010	Data + CF-Poll [PCF only]
10	Data	0011	Data + CF-Ack + CF-Poll [PCF only]
10	Data	0100	Null (no data)
10	Data	0101	CF-Ack (no data) [PCF only]
10	Data	0110	CF-Poll (no data) [PCF only]
10	Data	0111	CF-Ack + CF-Poll (no data) [PCF only]
10	Data	1000	QoS Data [HCF]
10	Data	1001	QoS Data + CF-Ack [HCF]
10	Data	1010	QoS Data + CF-Poll [HCF]
10	Data	1011	QoS Data + CF-Ack + CF-Poll [HCF]
10	Data	1100	QoS Null (no data) [HCF]
10	Data	1101	Reserved
10	Data	1110	QoS CF-Poll (no data) [HCF]
10	Data	1111	QoS CF-Ack + CF-Poll (no data) [HCF]


6
6
2
Variable
4
Ethernet
Destination MAC
Source MAC
Type
0x0800 (IP)
0x0806 (ARP)
IP packet
FCS
24 ... 36
802.11
802.11 MAC header
LLC
0xAA 0xAA 0x03
SNAP
0x00 0x00 0x00
0x08 0x00
IP packet
FCS

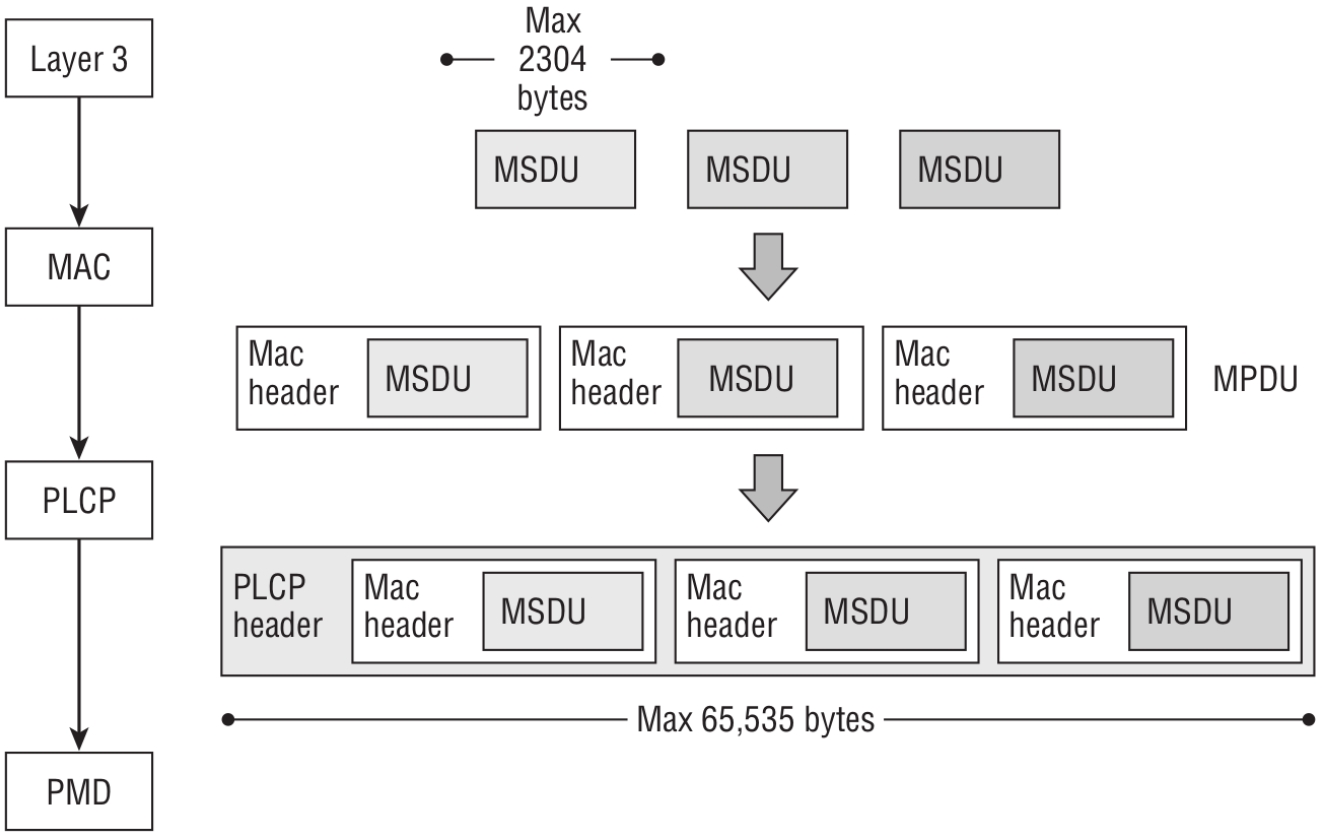
Fragmentation & Aggregation



Aggregate MAC service data unit (A-MSDU)

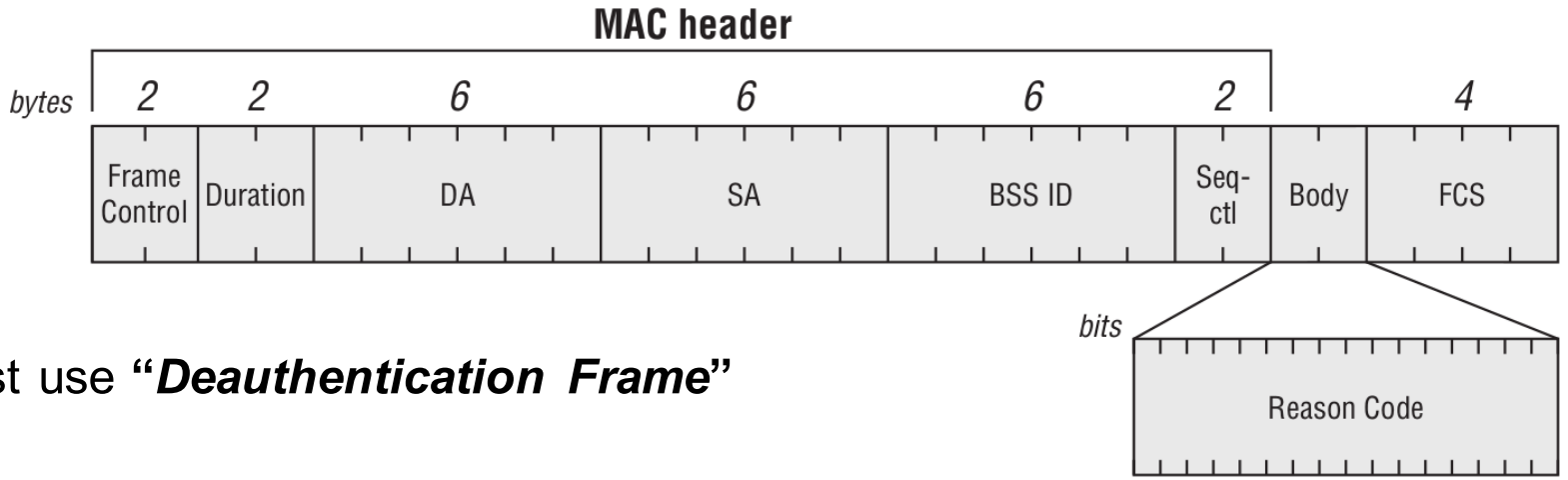


Aggregate MAC protocol data unit (A-MPDU)



	A-MSDU	A-MPDU
Encryption is enabled	all the MSDUs are encrypted together as a single payload	each MPDU is encrypted individually
	shall contain only MSDUs whose DA and SA parameter values map to the same RA and TA values	require the use of Block Ack

Wi-Fi Attack

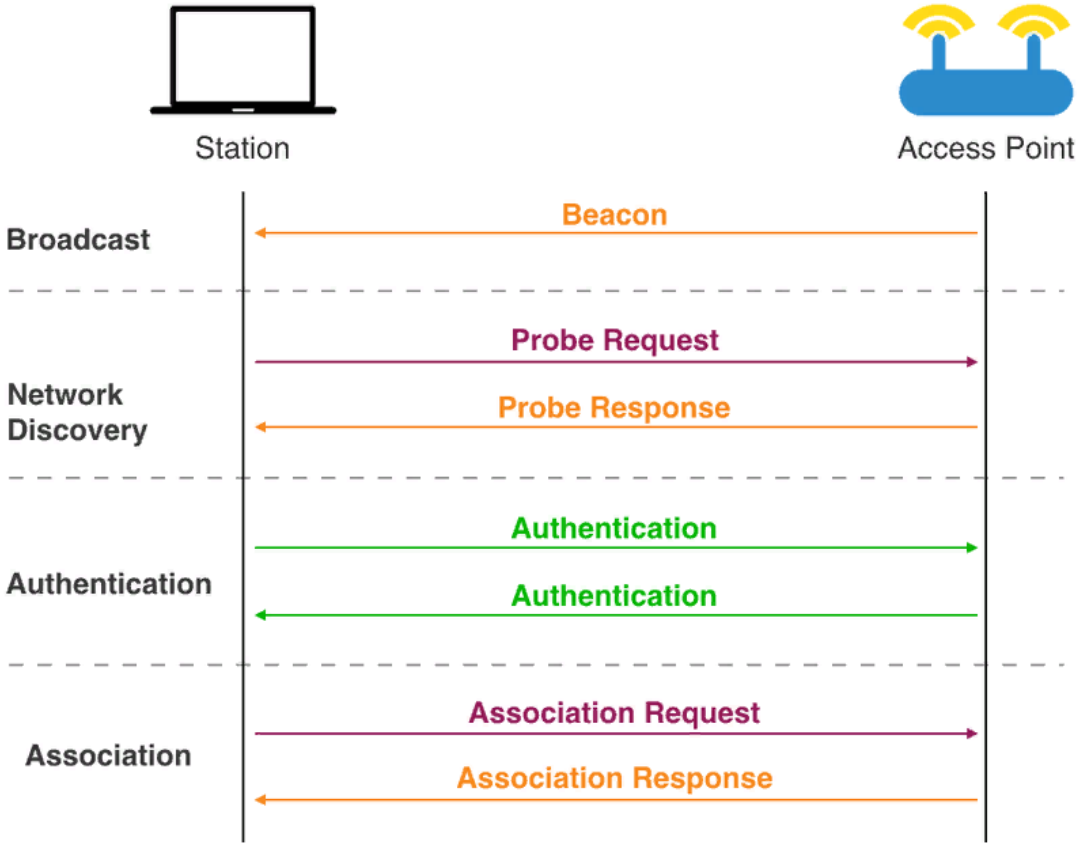


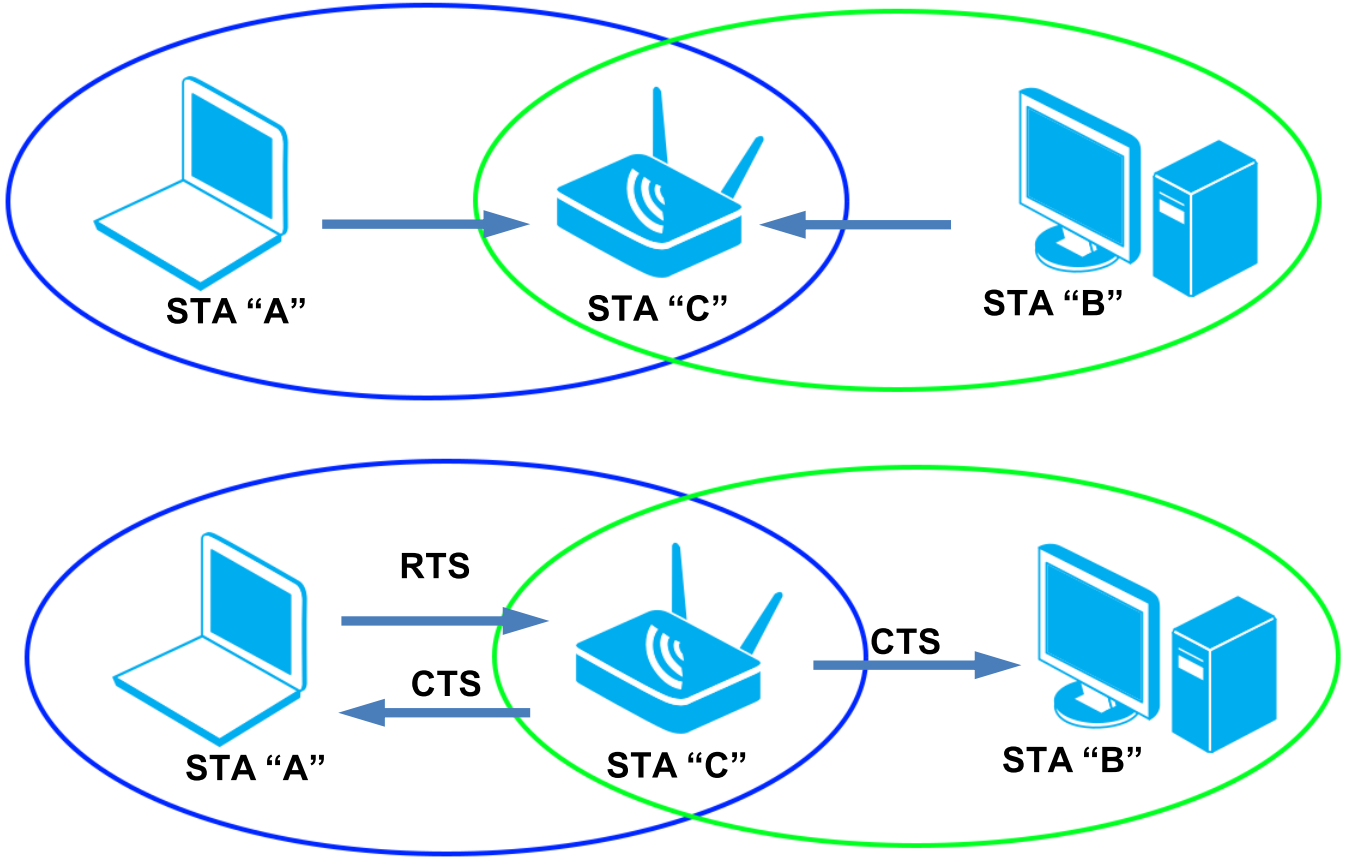
Just use "***Deauthentication Frame***"

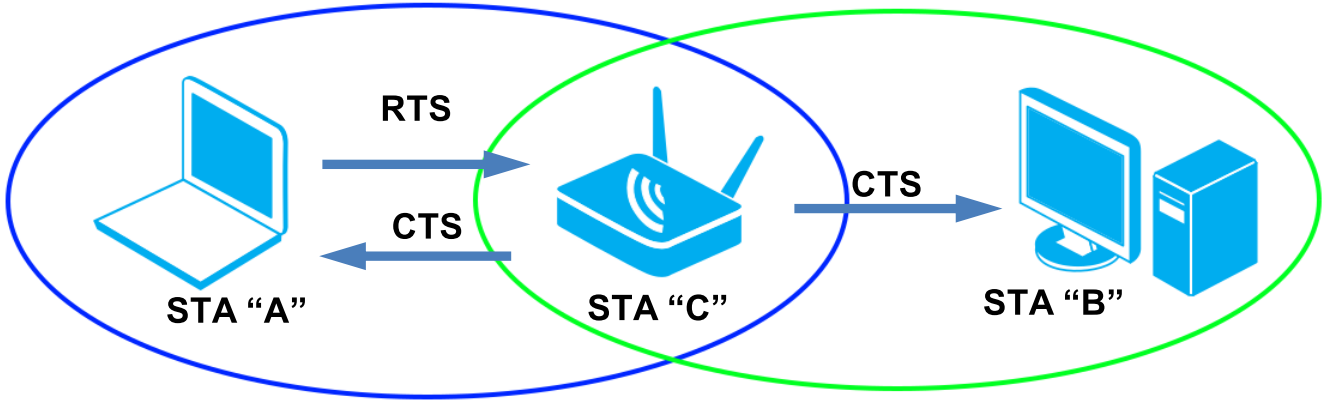
00-1010 disassociation frame

00-1100 deauthentication frame

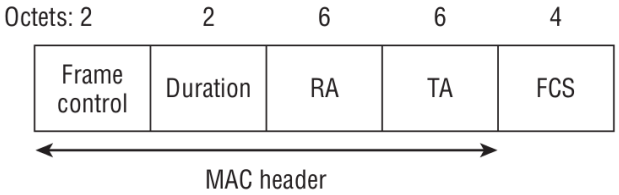
Order	Notes
1	Reason code.
2 – (Last – 1)	One or more vendor-specific information elements may appear in this frame.
Last	Used with 802.11w.


Station
Access Point
Broadcast
Beacon
Network Discovery
Probe Request
Probe Response
Authentication
Authentication
Authentication
Association
Association Request
Association Response

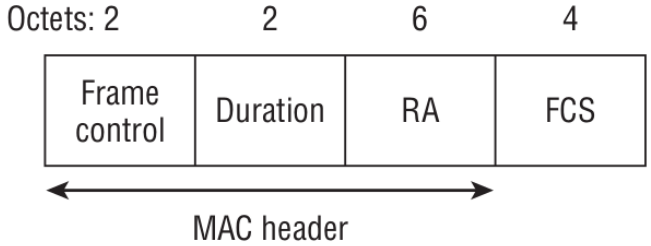

STA “A”
STA “C”
STA “B”
RTS
CTS
CTS
STA “A”
STA “C”
STA “B”

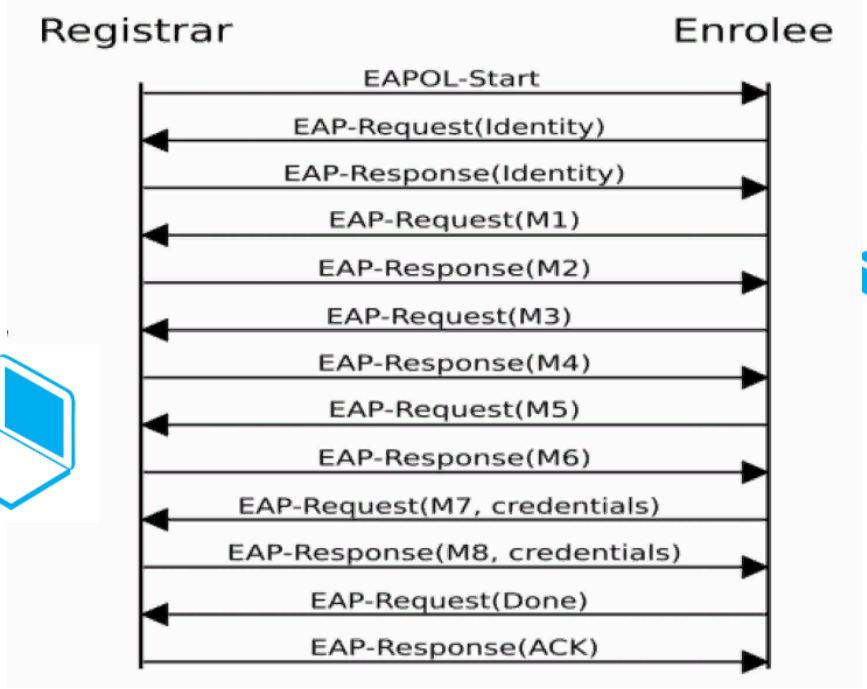


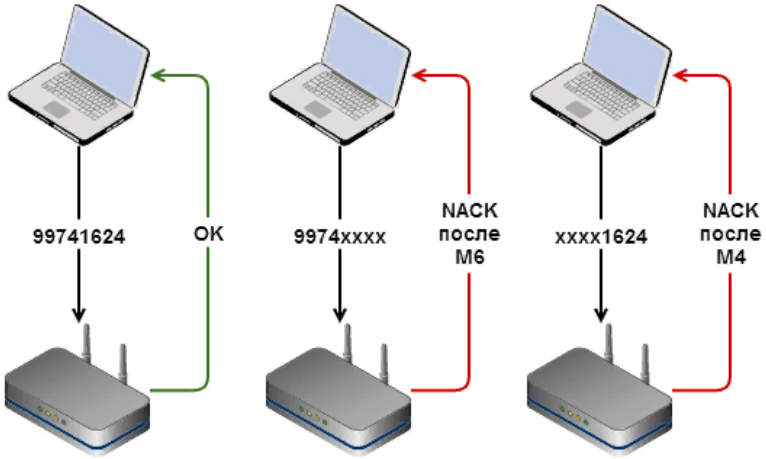
RTS frame



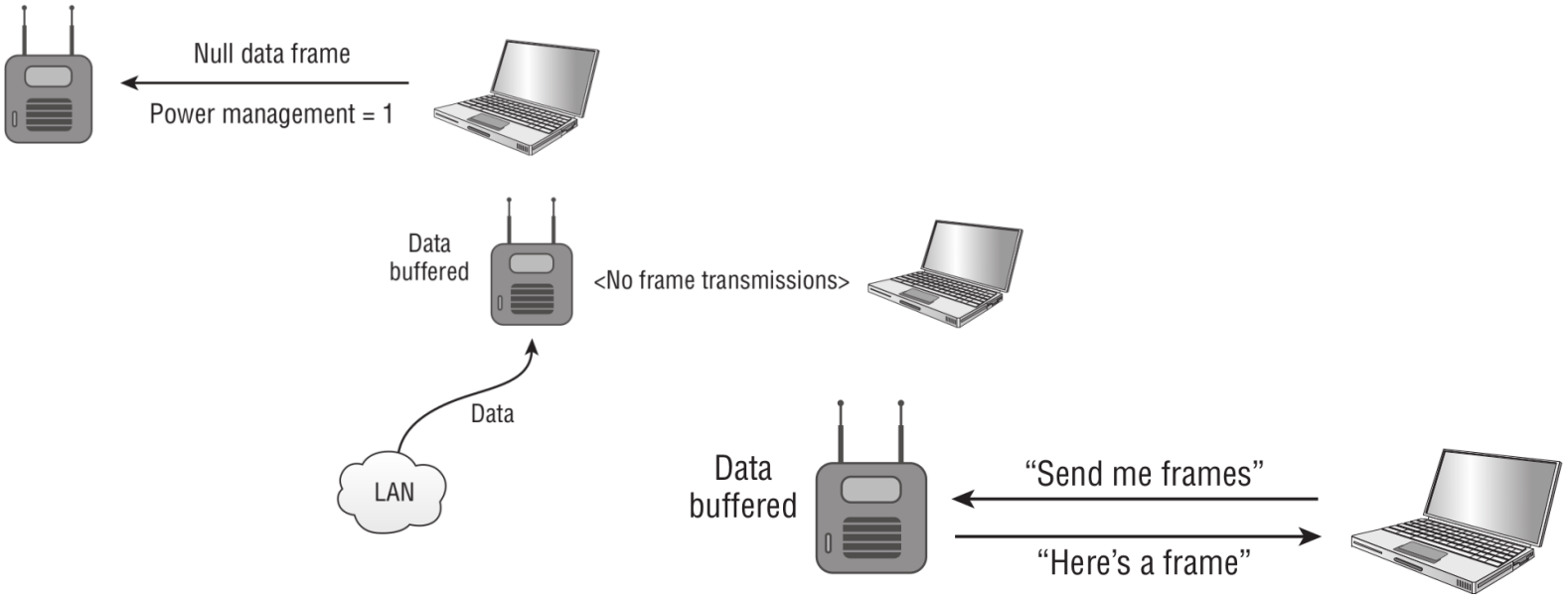
CTS frame




Registrar
Enrolee
EAPOL-Start
EAP-Request(Identity)
EAP-Response(Identity)
EAP-Request(M1)
EAP-Response(M2)
EAP-Request(M3)
EAP-Response(M4)
EAP-Request(M5)
EAP-Response(M6)
EAP-Request(M7, credentials)
EAP-Response(M8, credentials)
EAP-Request(Done)
EAP-Response(ACK)


99741624
OK
9974xxxx
NACK
после
M6
xxxx1624
NACK
после
M4

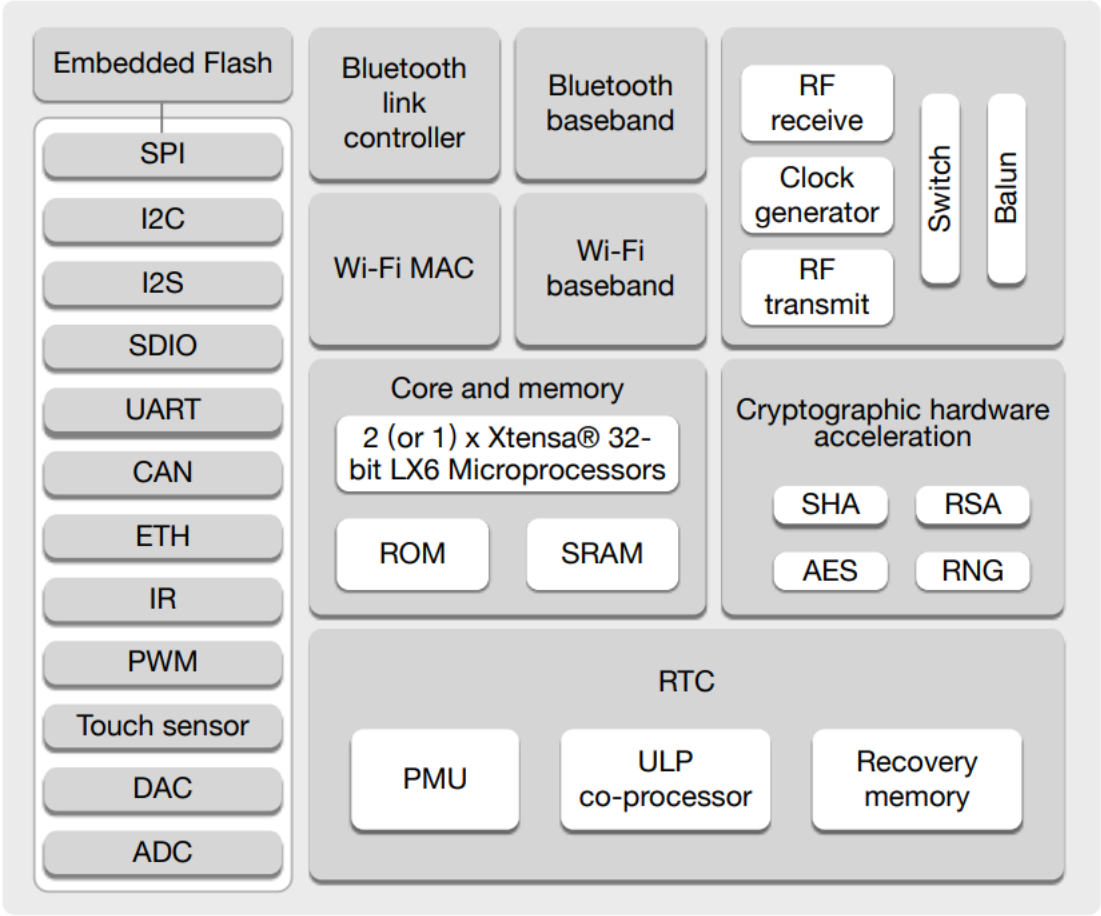
BSSID	Channel	RSSI	Auth Mode	B	G	N	LR	WPS	SSID
):10	2	-66	WPA|WPA2-PSK	0	1	1	0	0	Domashniy
:3C	10	-67	WPA2-PSK	1	1	1	0	0	WirelessNet
:D8	7	-69	WPA|WPA2-PSK	1	1	1	0	0	WiFi
:08	13	-77	WPA2-PSK	1	1	1	0	0	
:B8	13	-82	WPA2-PSK	1	1	1	0	0	Kain
:36	4	-83	WPA|WPA2-PSK	1	1	1	0	0	izet95
:28	13	-83	WPA2-PSK	1	1	1	0	0	Kain
:50	13	-84	WPA2-PSK	1	1	1	0	0	ASUS-B950
:A8	9	-85	WPA2-PSK	1	1	1	0	1	ASUS
:B8	6	-86	WPA2-PSK	1	1	1	0	1	wacheslav
:08	6	-94	WPA2-PSK	1	1	1	0	1	Room246



FC -> More Data bit

STA don't go to **Doze State**

ESP32

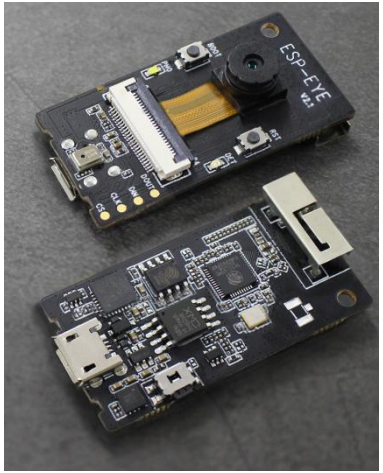

Embedded Flash
SPI
I2C
I2S
SDIO
UART
CAN
ETH
IR
PWM
Touch sensor
DAC
ADC
Bluetooth link controller
Bluetooth baseband
Wi-Fi MAC
Wi-Fi baseband
RF receive
Clock generator
RF transmit
Switch
Balun
Core and memory
2 (or 1) x Xtensa® 32-bit LX6 Microprocessors
ROM
SRAM
Cryptographic hardware acceleration
SHA
RSA
AES
RNG
RTC
PMU
ULP co-processor
Recovery memory

- **Processors:**

  Tensilica Xtensa 32-bit LX6 microprocessor

  Clock frequency: up to 240 MHz

  Performance: up to 600 DMIPS



- **Memory:**

  Internal memory:

  ROM: 448 KiB (for booting and core functions)

  SRAM: 520 KiB (for data and instruction)

  eFuse: 1 Kibit

  Embedded flash:

  0 … 4 MiB

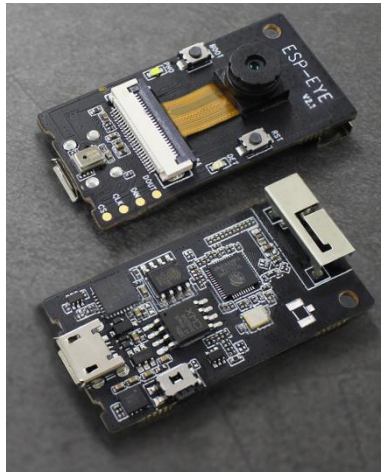
  External flash:

  Up to 16 MiB

- **Wireless connectivity:**

Wi-Fi

802.11 b/g/n
(802.11n @ 2.4 GHz up to 150 Mbit/s)



Bluetooth

v4.2 BR/EDR
Bluetooth Low Energy (BLE)

Scan Type

Mode	Description
Active Scan	Scan by sending a probe request. The default scan is an active scan.
Passive Scan	No probe request is sent out. Just switch to the specific channel and wait for a beacon. Application can enable it via the scan_type field of wifi_scan_config_t.
All-Channel Scan	It scans all of the channels. If the channel field of wifi_scan_config_t is set to 0, it is an all-channel scan.
Specific Channel Scan	It scans specific channels only. If the channel field of wifi_scan_config_t set to 1, it is a specific-channel scan

Sniffer Mode

ESP32 support* :

- 802.11 Management frame
- 802.11 Data frame, including MPDU, AMPDU, AMSDU, etc.
- 802.11 MIMO frame, for MIMO frame, the sniffer only dumps the length of the frame.
- 802.11 Control frame

ESP32 DON'T support* :

- 802.11 error frame, such as the frame with a CRC error, etc.

*** ESP-IDF SDK latest version**

Wi-Fi internal buffer

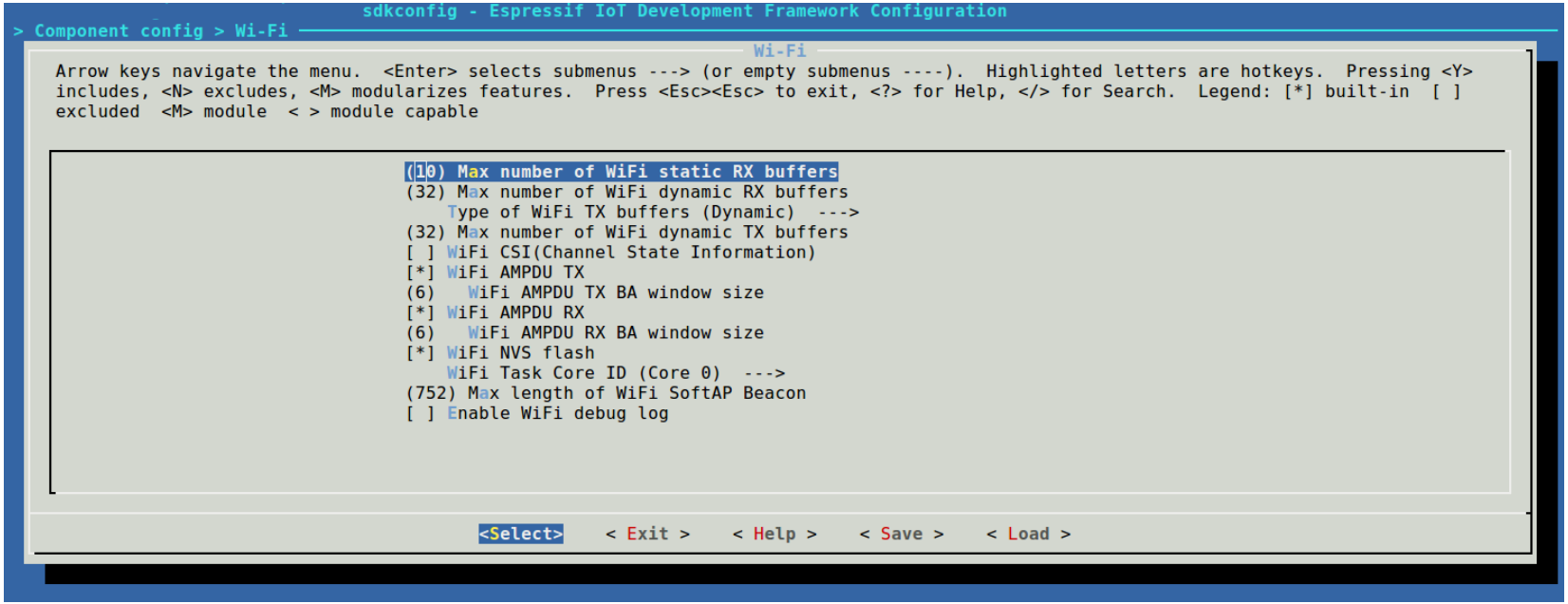
Buffer Type	Default value	Description
Static RX buf	10 x 1600 bytes	kind of DMA
Dynamic RX buf	32	the length is variable, depends on the Rx 802.11 frame
Static TX buf	16 x 1600 bytes	kind of DMA
Dynamic TX buf	32	This is a kind of DMA memory. It is allocated to the heap

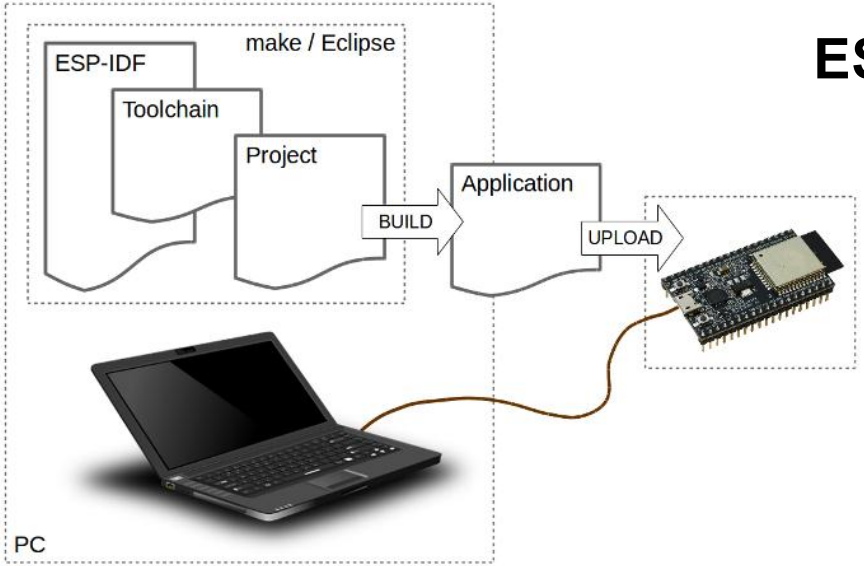
Wi-Fi internal buffer

To change configuration:

$ cd path/you/project

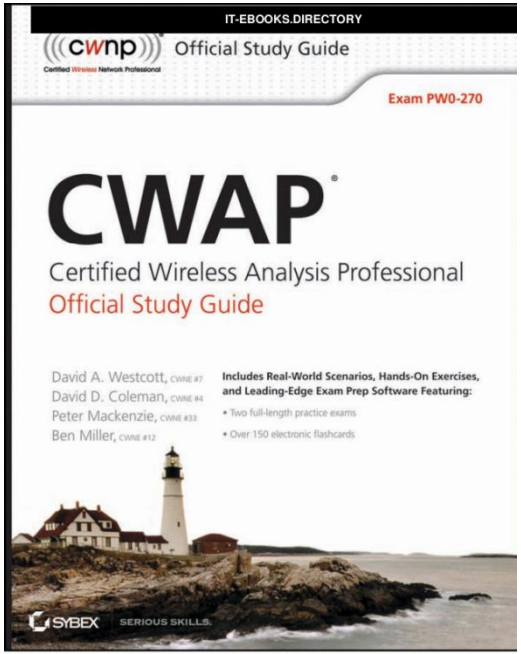
$ make menuconfig





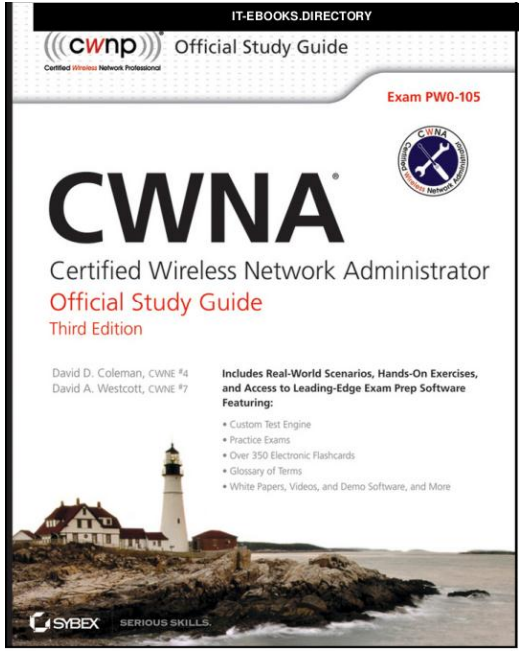
ESP-IDF Programming Guide

https://docs.espressif.com/projects/esp-idf/en/stable/index.html



Certified Wireless Analysis Professional

Exam PW0-270



Certified Wireless Network Administrator

Exam PW0-105

IEEE STANDARDS ASSOCIATION IEEE

IEEE Standard for Information technology—
Telecommunications and information exchange between systems
Local and metropolitan area networks—
Specific requirements

Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

https://mrncciew.com/2014/10/04/my-cwap-study-notes/

egor21@gmail.com

GS LABS
GS GROUP

egor.litvinov@gs-labs.ru

@Xarlan