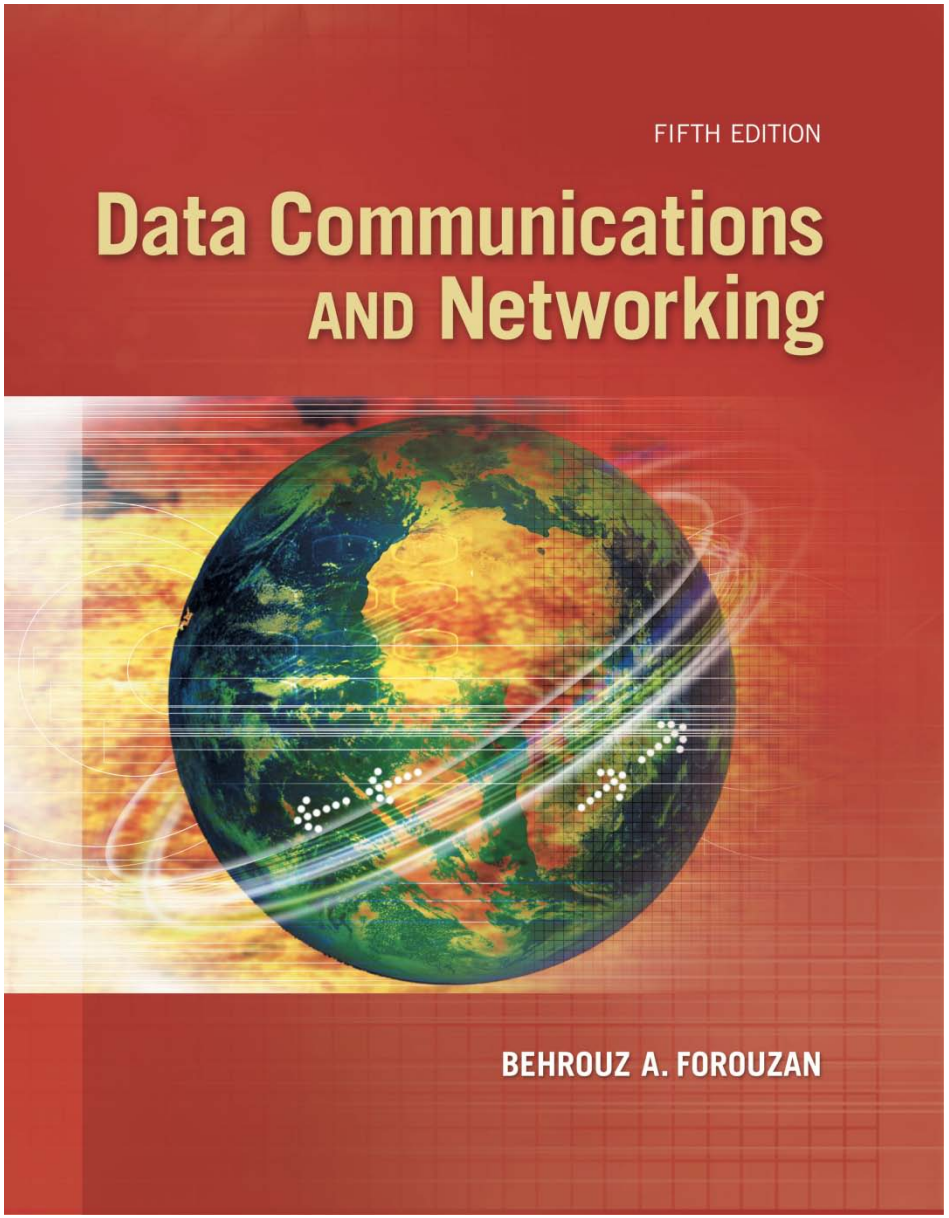
Chapter 15

Wireless LANs

Ref) 무선 LAN 보안프로토콜, 윤종호저 (교학사)

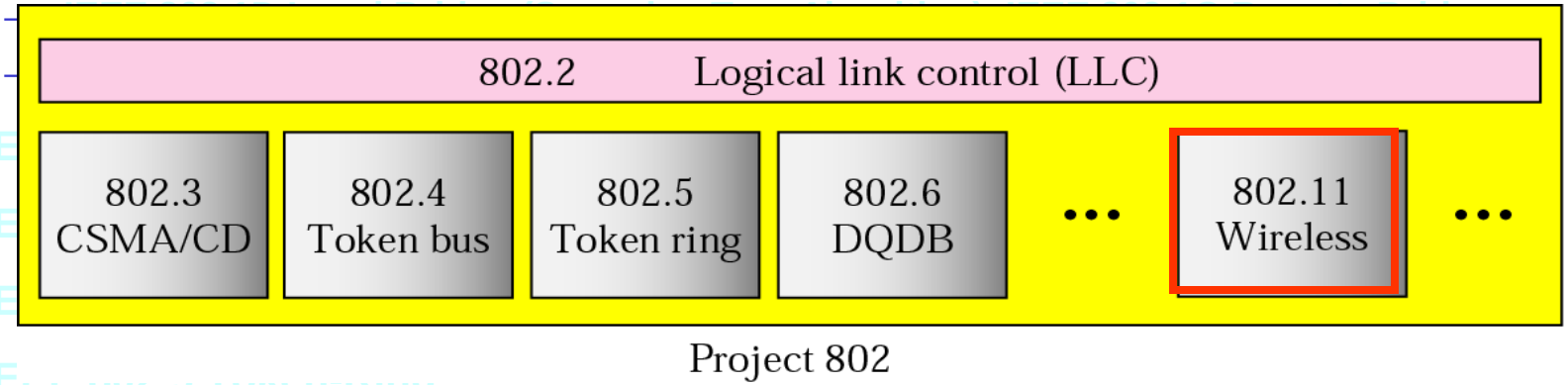


Chapter 15: Objective

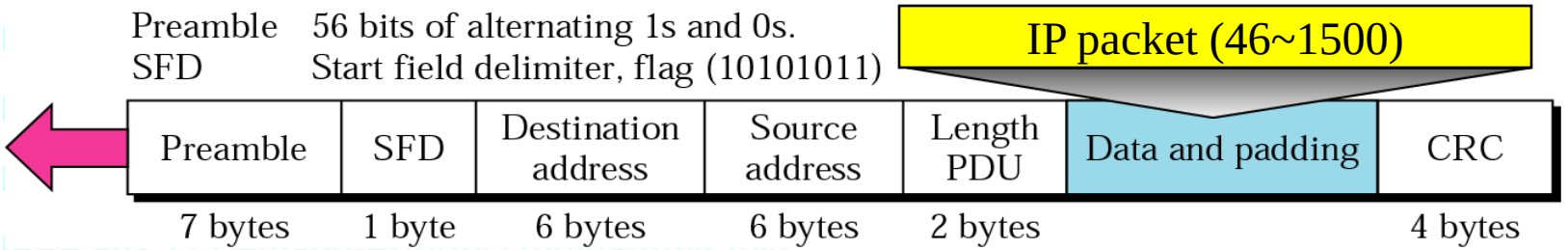
- The first section introduces the general issues behind wireless LANs and compares wired and wireless networks. The section describes the characteristics of the wireless networks and the way access is controlled in these types of networks.
- The second section discusses a wireless LAN defined by the IEEE 802.11 Project. This section defines the architecture of this type of LAN and describes the MAC sublayer.
- The third section discusses the Bluetooth technology as a personal area network (PAN). The section describes the architecture of the network, the addressing mechanism, and the packet format. Different layers used in this protocol are also briefly described and compared with the ones in the other wired and wireless LANs.

Review of IEEE Project 802 Standards

- IEEE 802.1 High Level Interface
- IE
- IE
- IE
- IEEE 802.5 Token Ring
- IEEE 802.6 DQDB (Distributed Queue Dual Bus)
- IEEE 802.7 Broadband Technical Advisory Group
- IEEE 802.8 Fiber Optic Technical Advisory Group
- I
- I
- I
- IEEE 802.12 Demand-Priority (100VG-AnyLAN)
- IEEE 802.14 CATV Networks (HFC)

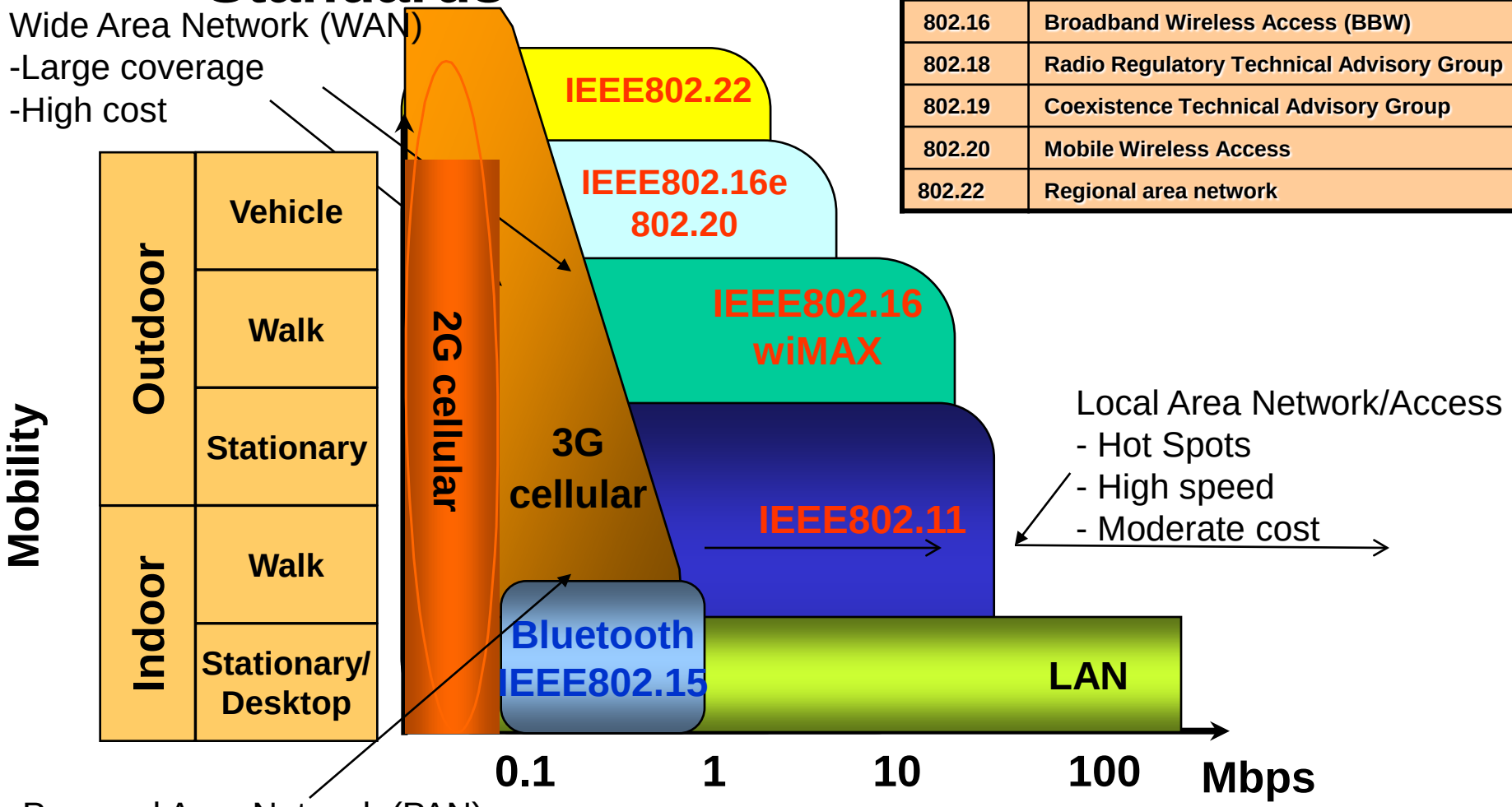


Project 802



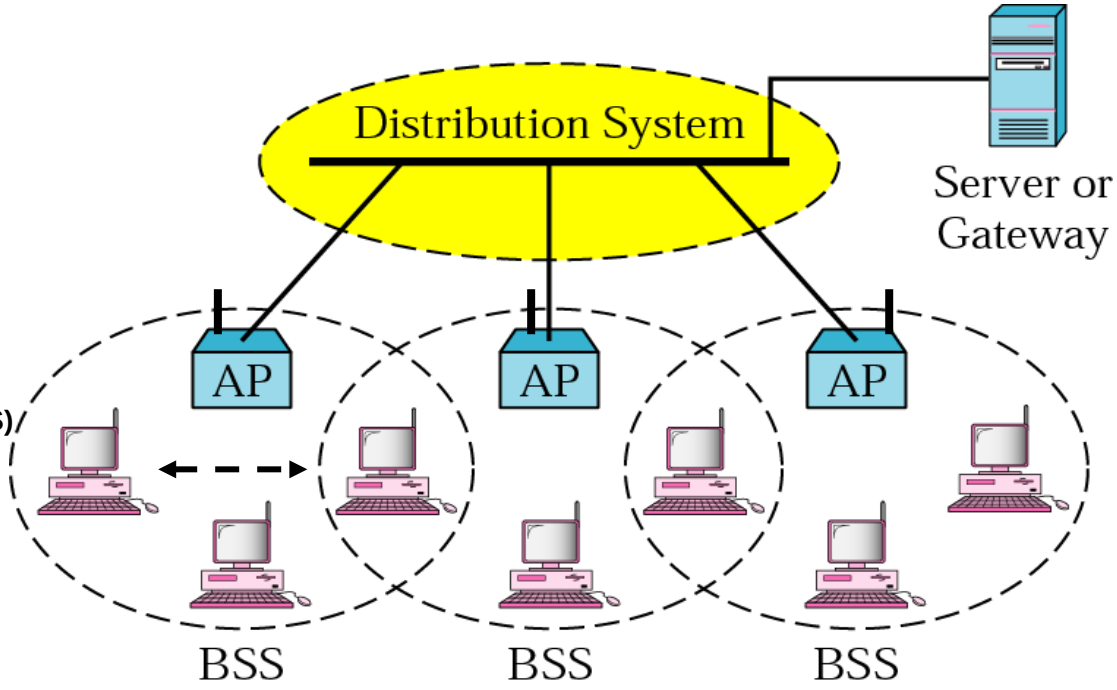
Wireless Standards

802.11	Wireless LAN (WLAN)
802.15	Wireless Personal Area Network (WPAN)
802.16	Broadband Wireless Access (BBW)
802.18	Radio Regulatory Technical Advisory Group
802.19	Coexistence Technical Advisory Group
802.20	Mobile Wireless Access
802.22	Regional area network



802.11 WLAN Architecture

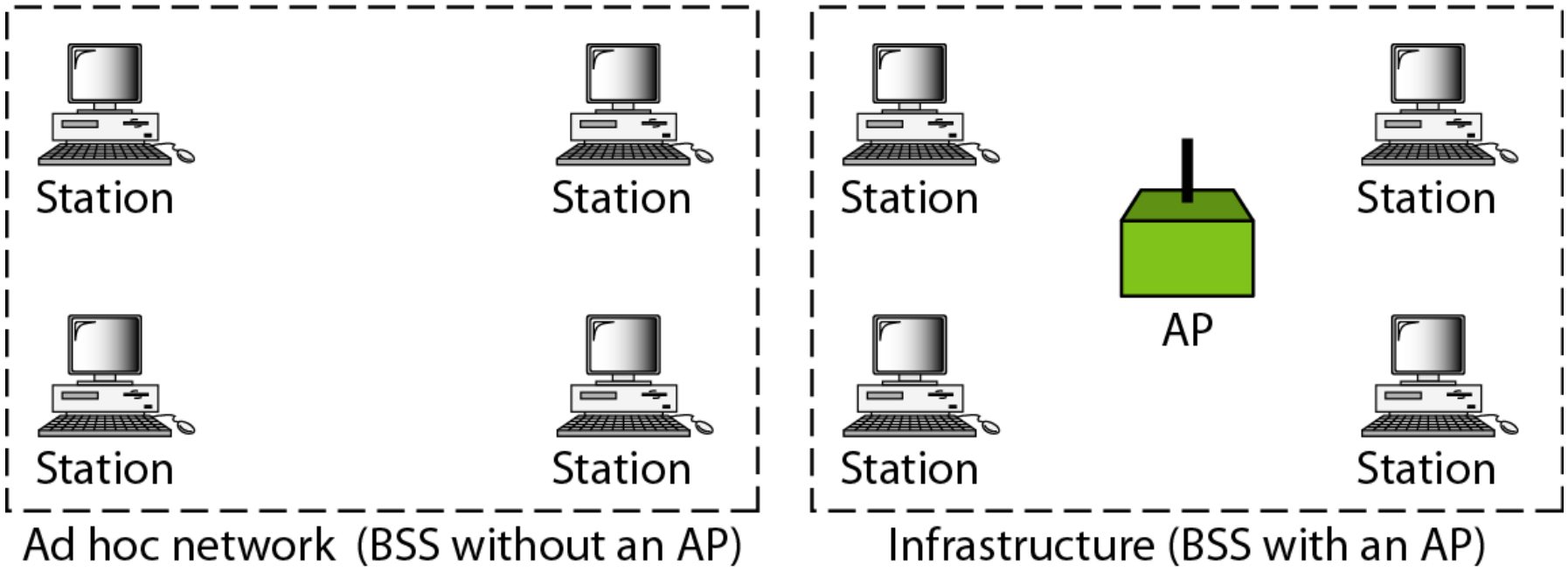
- **Basic Service Set (BSS) (a.k.a. "cell") contains:**
  - **wireless station (WS)**
  - **access point (AP): base station**
- **BSS-Two operation modes:**
  - **Infrastructure mode**
    - everything through AP
  - **Peer-to-peer mode**
    - called ad hoc network
- **BSS's combined to form distribution system (DS)**
- **Extended Service Set(ESS)**
  - **Two or more BSSs**



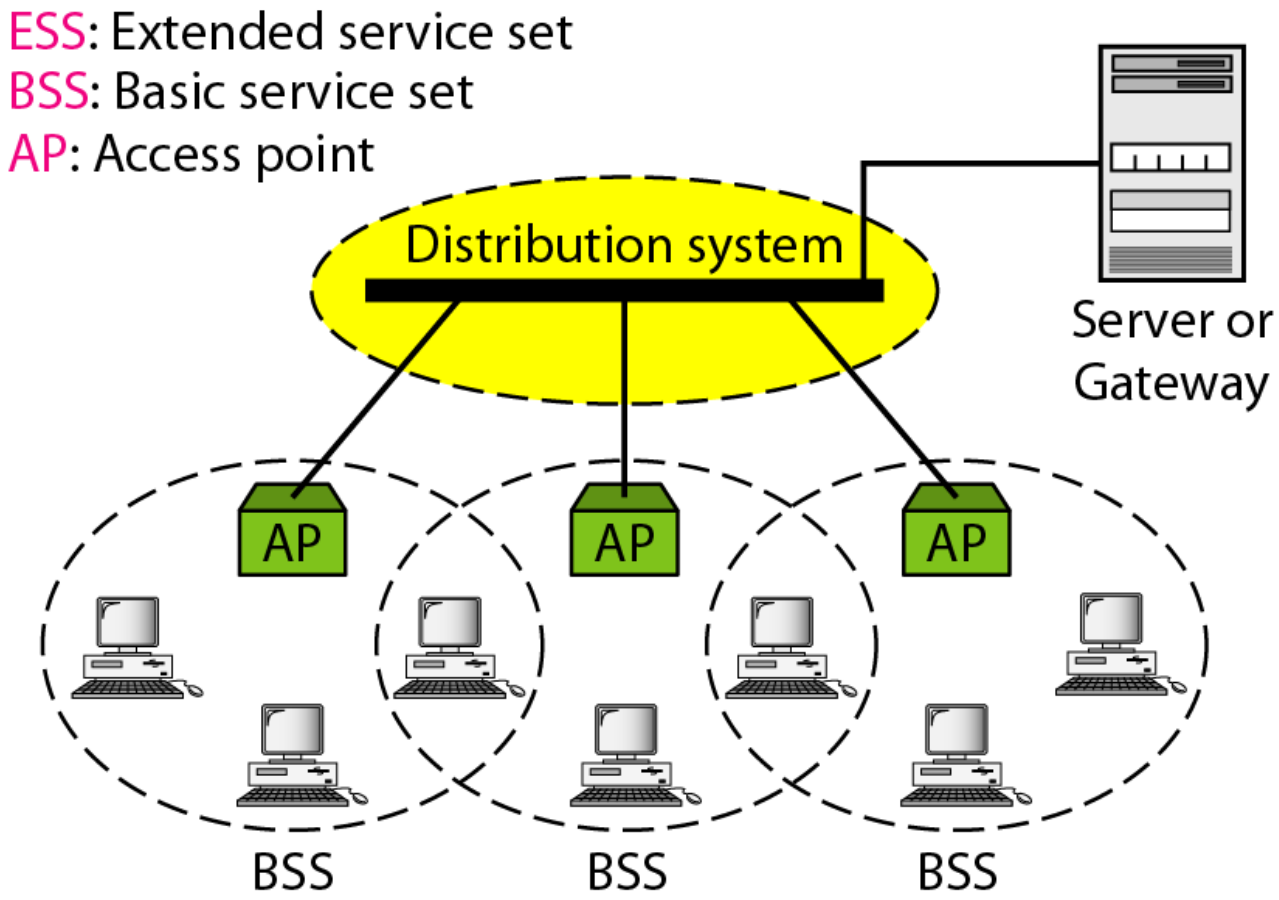
Basic Service Set (BSS)

- **A BSS without an AP is called an ad hoc network;**
- **a BSS with an AP is called an infrastructure network.**

BSS: Basic service set
AP: Access point



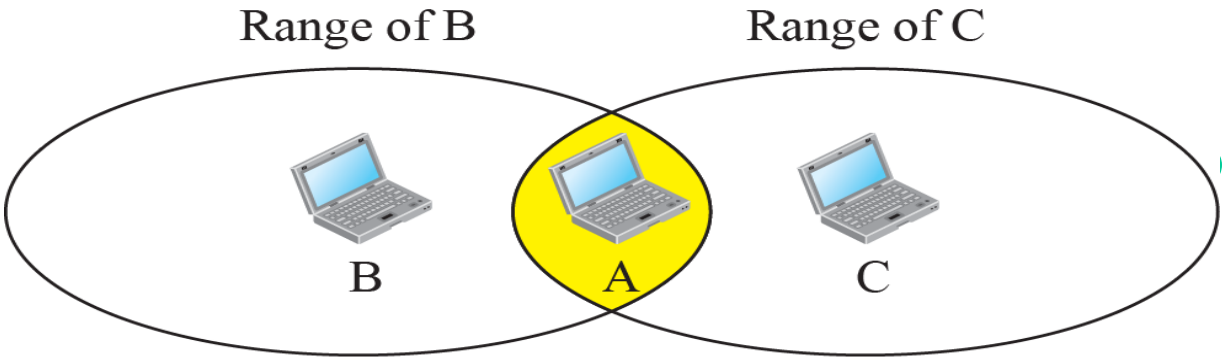
Extended Service Set (ESS)



Problems

The Hidden Terminal Problem

(A and C are hidden for each other with respect to B)



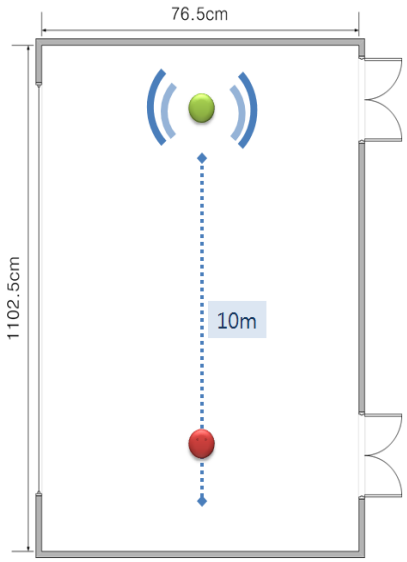
a. Stations B and C are not in each other's range.

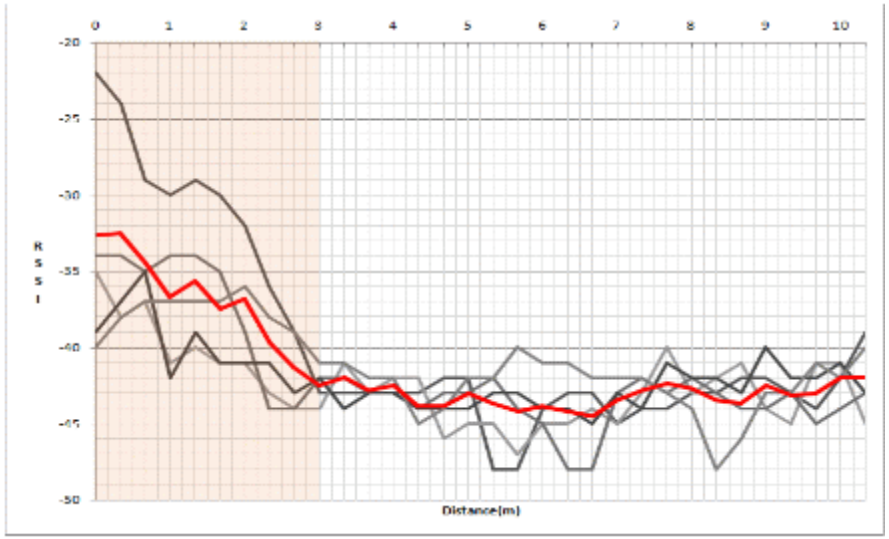
Figure 15.3: Hidden station problem

- **A is sending to B, but C cannot receive from A**
  - **Friis Law (power decay proportional to distance square)**
- **Therefore C sends to B, without detecting the transmission from A to B**
- **In summary, A is "hidden" for C in carrier sensing**
- **Implication: How to do carrier sense and collision detection?**

The reason of The Hidden Terminal Problem
Wireless Media Disperse Energy

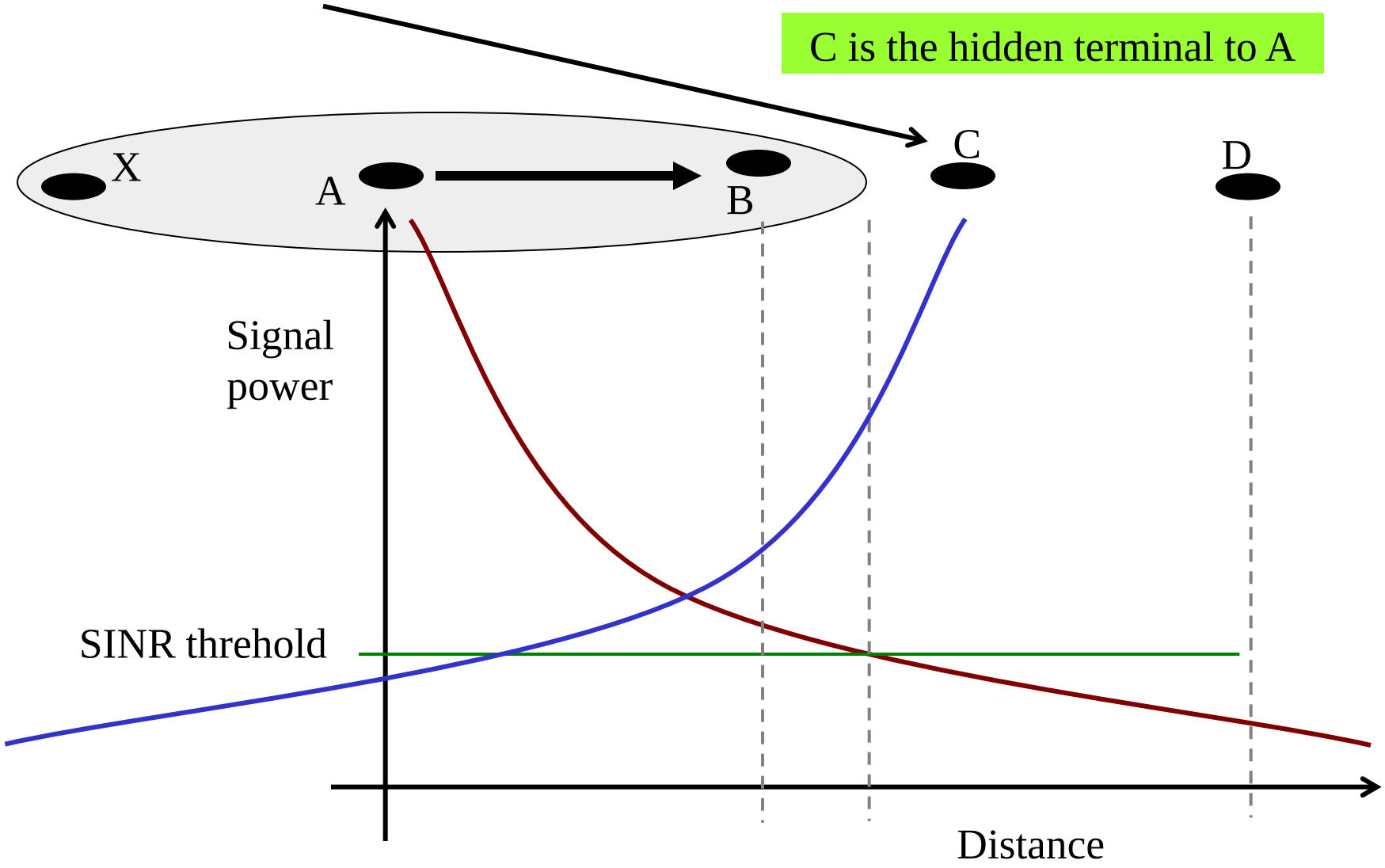
- **Signal not same at different locations**





Important: C has not heard A, but can interfere at receiver B

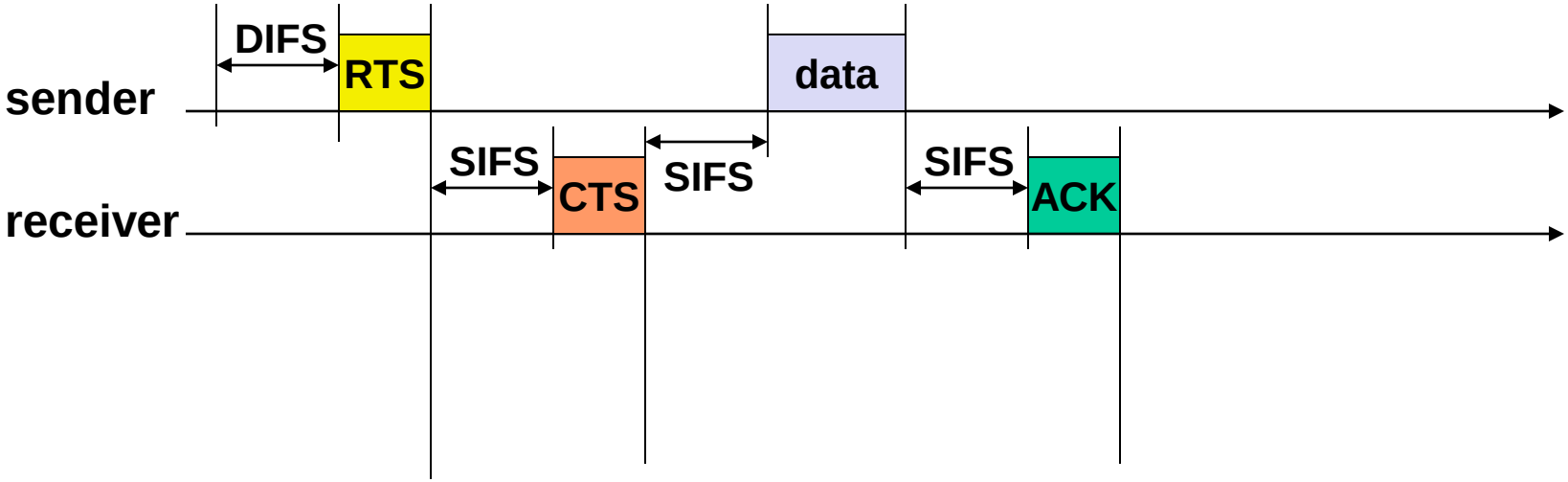
C is the hidden terminal to A



Solution: DCF with RTS/CTS

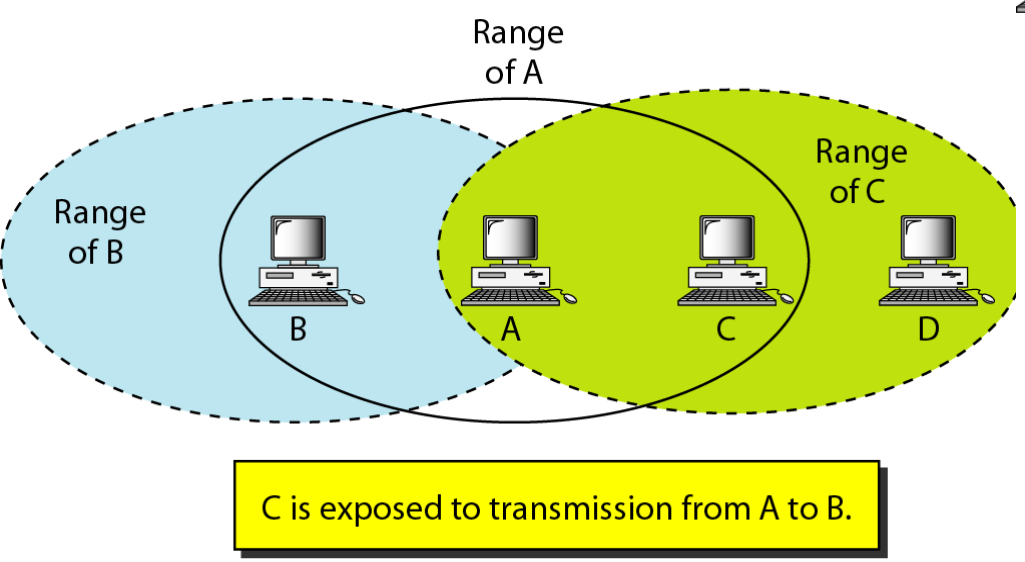
- Station can send RTS with reservation parameter after DIFS
- Acknowledgement via CTS after SIFS by receiver (if ready to receive)
- Sender can now send data at once, acknowledgement via ACK
- Other stations store medium reservations distributed via RTS/CTS

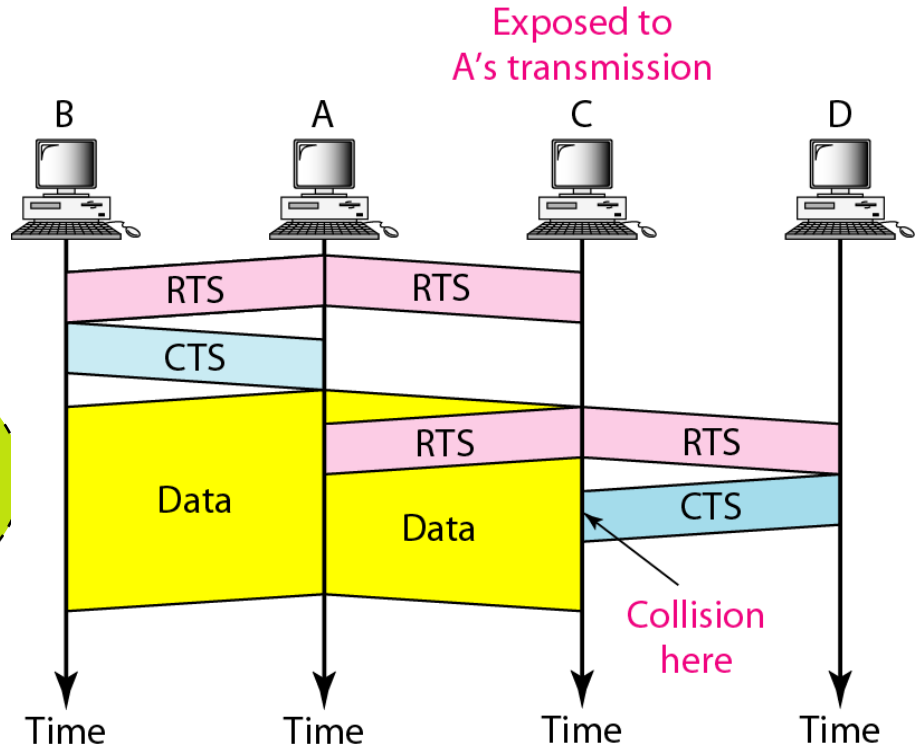
Solution of Hidden terminal problem



The Exposed Terminal Problem

- A is sending to B, C intends to send to D
- C senses an "in-use" medium, thus C waits (Since B is sending)
- But A is outside the radio range of D, therefore waiting is not necessary
- In summary, C is "exposed" to A
- Implication: false carrier sense

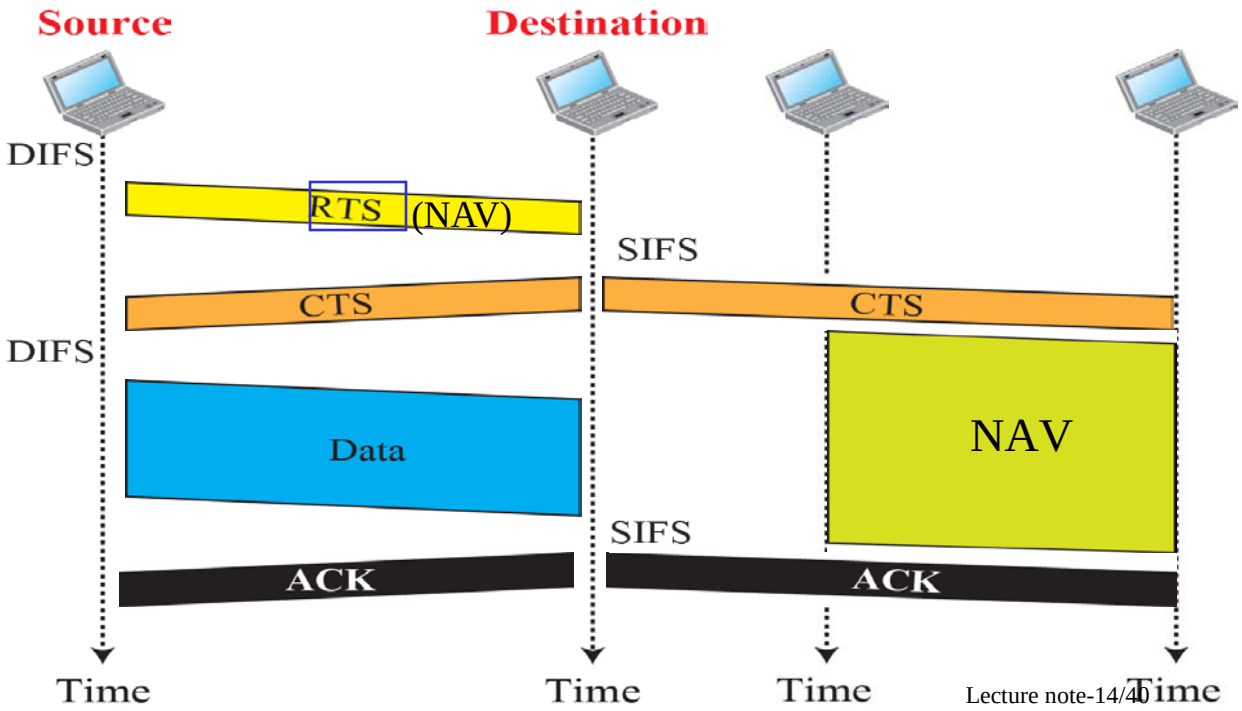




How is the Collision Avoidance?

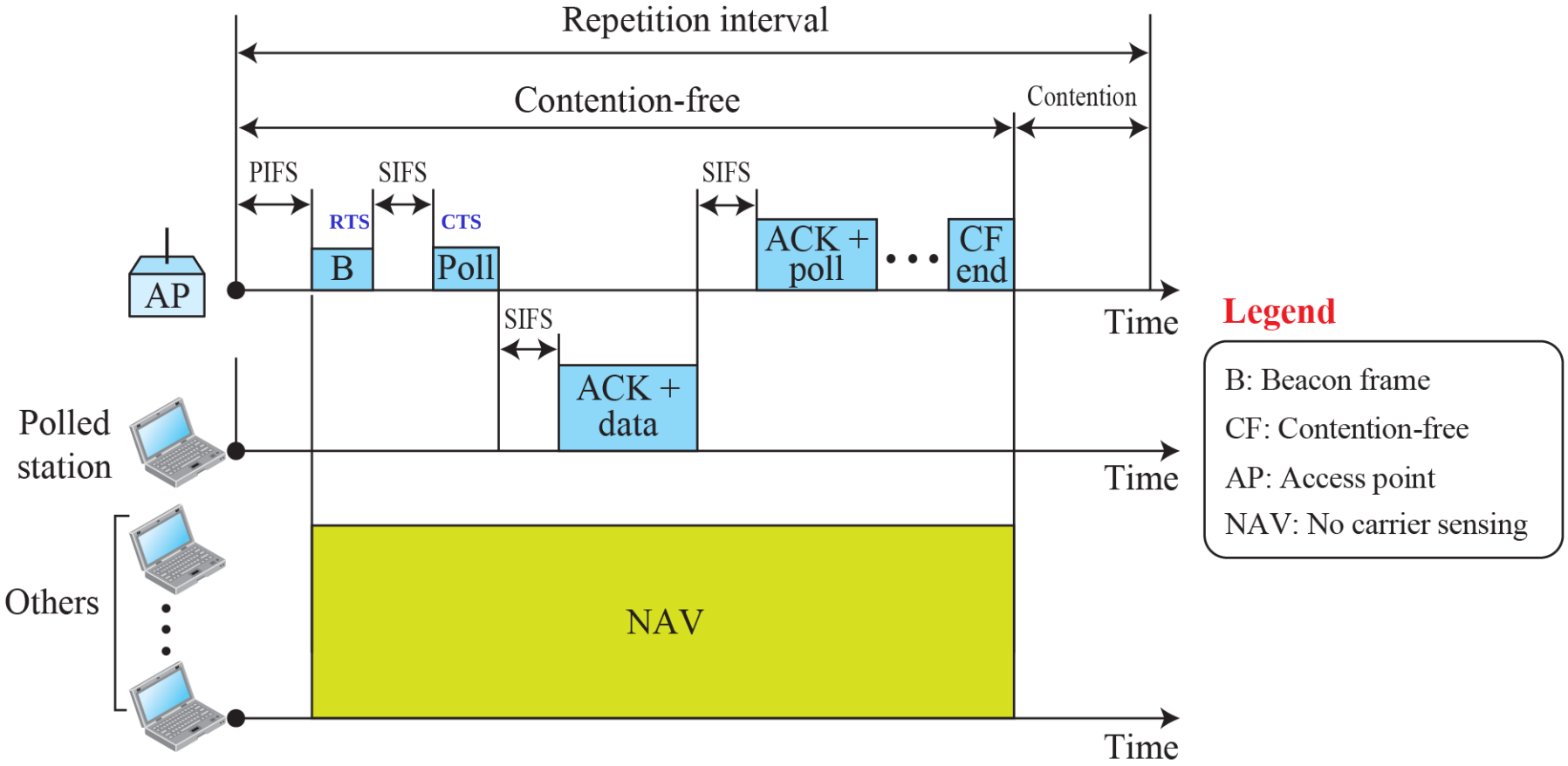
- How do other stations defer sending their data if one station acquires access? -> Network Allocation Vector
- RTS frame includes the duration of time that it needs to occupy the channel (=NAV).

Figure 15.7: CSMA/CA and NAV



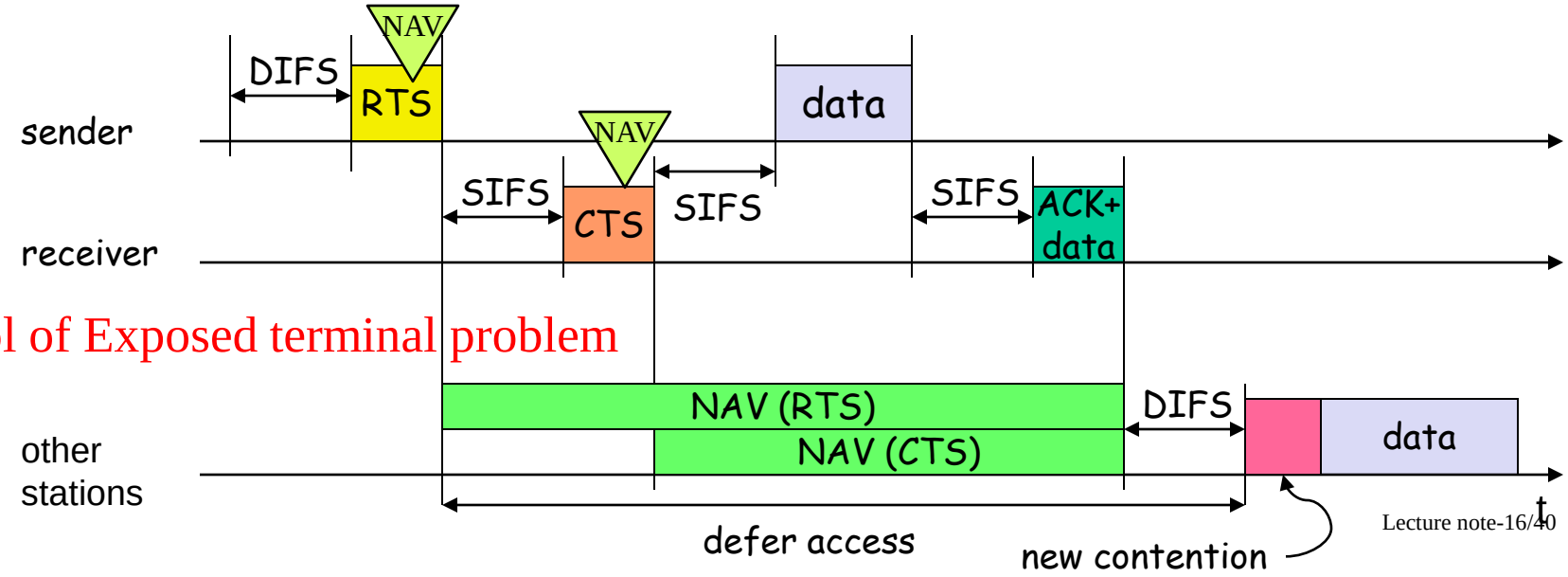
DIFS: Distributed Inter-Frame Spacing
SIFS: Short Inter-Frame Spacing

Figure 15.8: Example of repetition interval



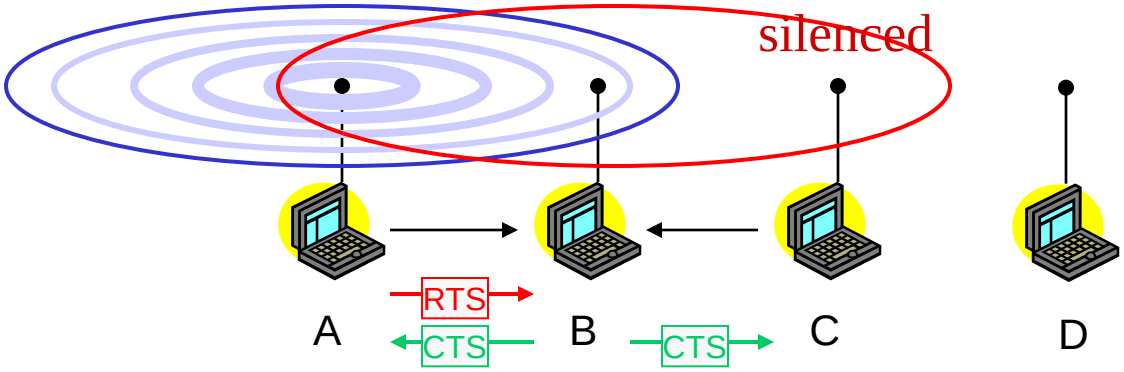
Solution: 802.11 – RTS/CTS + ACK

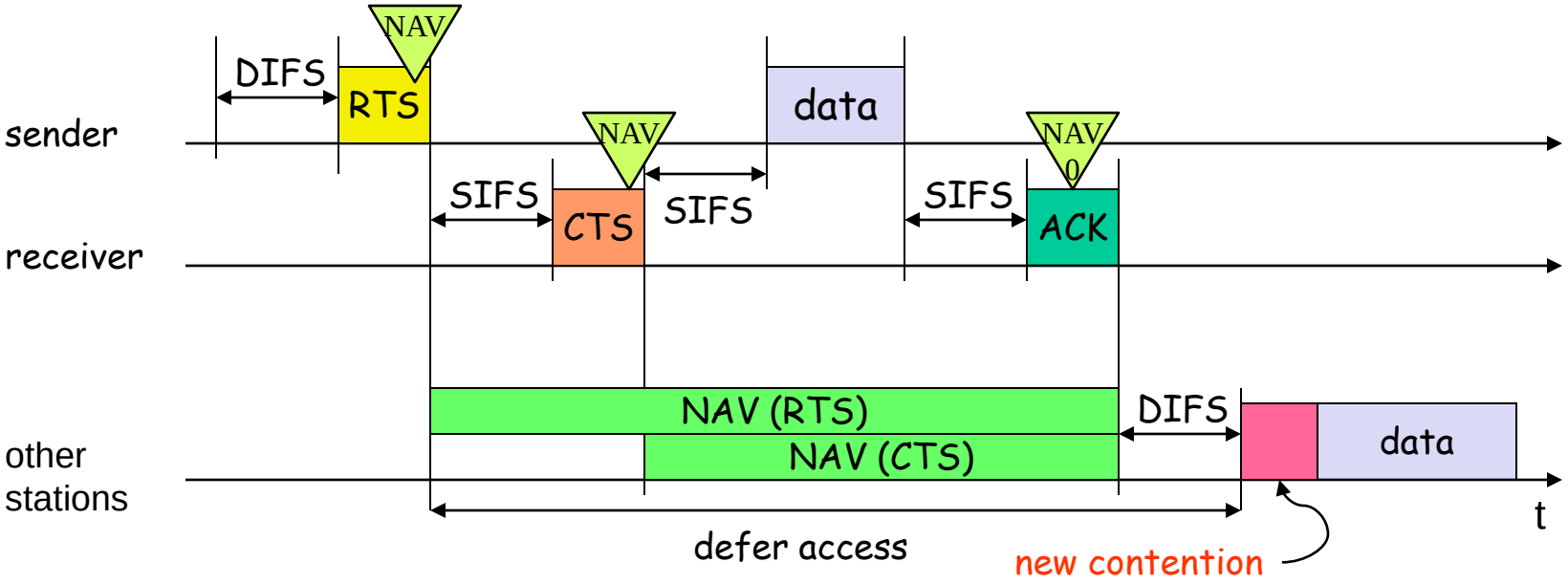
- Sender sends RTS with NAV (Network allocation Vector, i.e. reservation parameter that determines amount of time the data packet needs the medium) after waiting for DIFS
- Receiver acknowledges via CTS after SIFS (if ready to receive)
  - CTS reserves channel for sender, notifying possibly hidden stations
- Sender can now send data at once, acknowledgement via ACK
- Other stations store NAV distributed via RTS and CTS



Sol of Exposed terminal problem

Example: RTS-CTS





Thoughts !

- **802.11 does not solve HT/ET completely**
  - **Only alleviates the problem through RTS/CTS and recommends larger CS zone**

- **Large CS zone aggravates exposed terminals**
  - **Spatial reuse reduces → A tradeoff**
  - **RTS/CTS packets also consume bandwidth**
  - **Moreover, backing off mechanism is also wasteful**

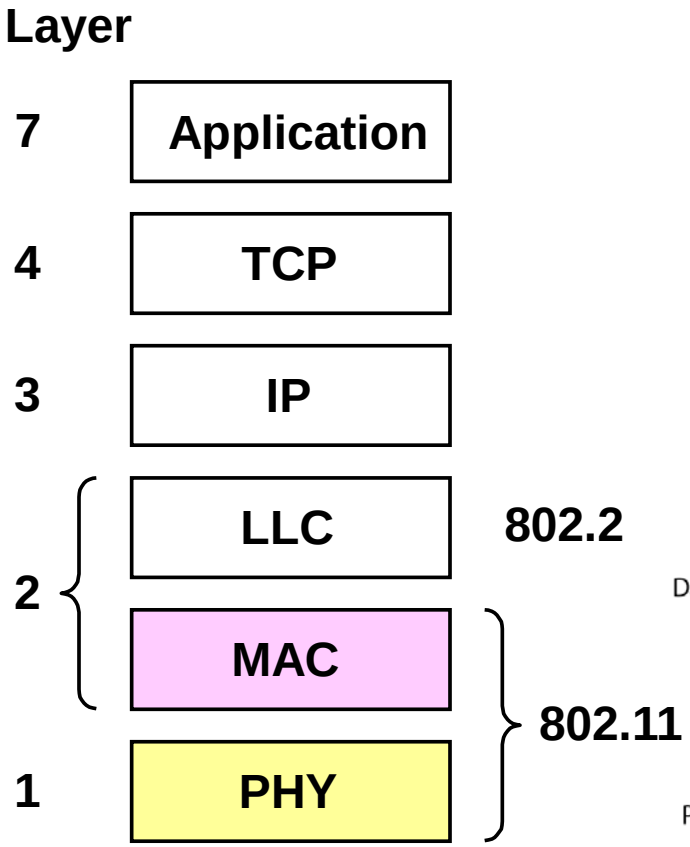
The search for the best MAC protocol is still on. However, 802.11 is being optimized too.

Thus, wireless MAC research still alive

Takes on 802.11 Wireless LAN Protocol

- **Role of RTS/CTS**
  - **Useful? No?**
  - **Is it a one-fit-all? Where does it not fit?**
- **Is ACK necessary?**
  - **MACA said no ACKs. Let TCP recover from losses**
- **Should Carrier Sensing replace RTS/CTS?**
- **New opportunities may not need RTS/CTS**
  - **Infratructured wireless networks (EWLAN)**

WLAN Protocol Architecture



- **Layers 1 and 2**
  - **One MAC and**
  - **multiple PHYs**

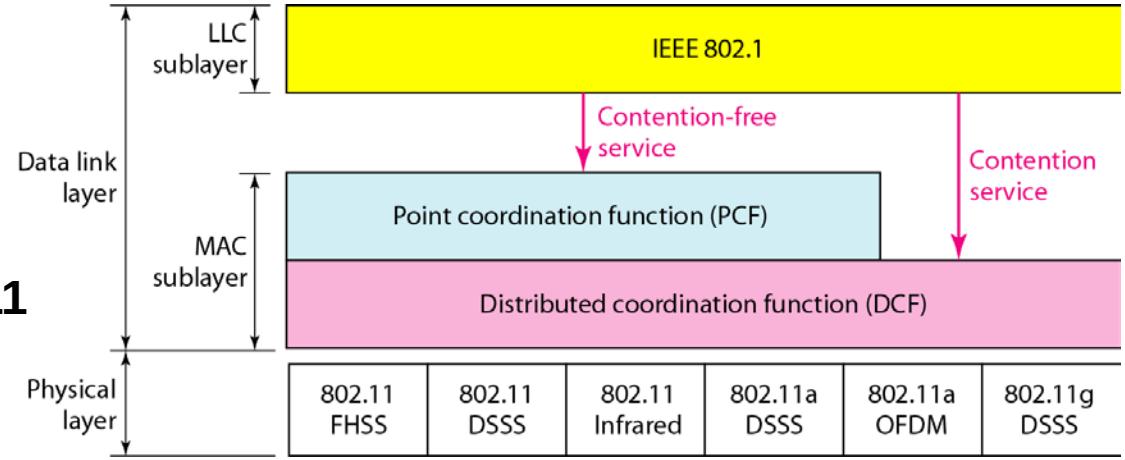


Table 1: IEEE 802.11 Specifications

	802.11b	*802.11a*	*802.11g*
Standard approved	July 1999	July 1999	June 2003
Maximum data rate	11 Mbps	54 Mbps	54 Mbps
Modulation	CCK	OFDM	OFDM and CCK
Data rates	1, 2, 5.5, 11 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	CCK: 1, 2, 5.5, 11 OFDM: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
Frequencies	2.4–2.497 GHz	5.15–5.35 GHz 5.425–5.675 GHz 5.725–5.875 GHz	2.4–2.497 GHz

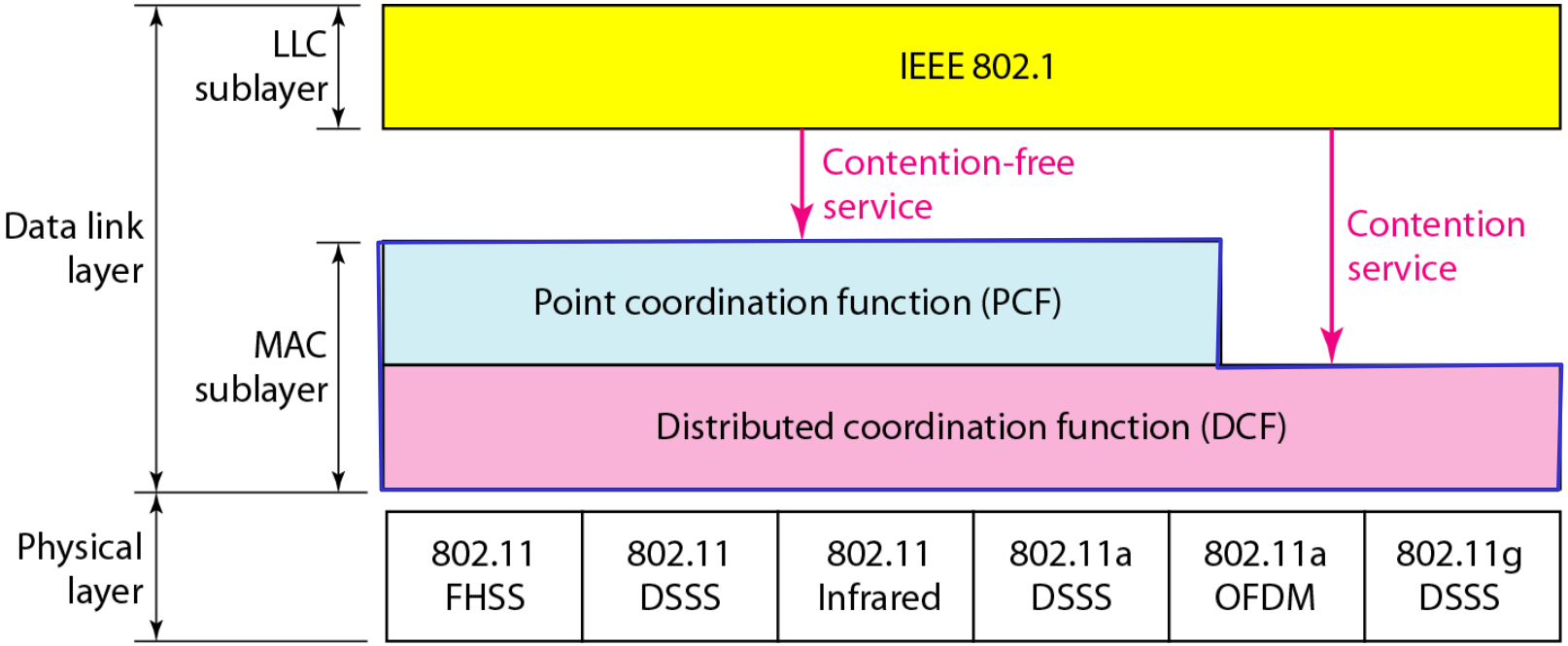
WLAN Media Access Control

- **Wireless LANs use** CSMA/CA **where CA = collision avoidance (CA). With CA, a station waits until another station is finished transmitting plus an additional random period of time before sending anything.**

similar to IEEE 802.3 Ethernet CSMA/CD

- **Why not CSMA/CD?**
  - Difficult to detect collision in a radio environment
  - Radio environment is not as well controlled as a wired broadcast medium, and transmissions from users in other LANs can interfere with the operation of CSMA/CD
  - Radio LANs are subject to the hidden-station problem

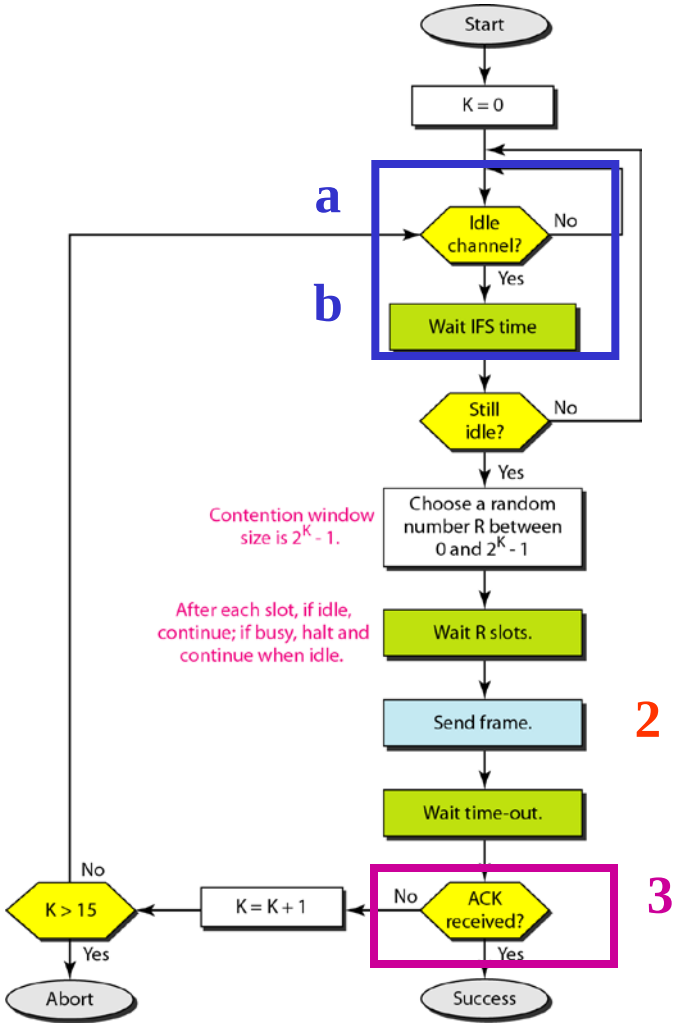
Two Coordination Functions



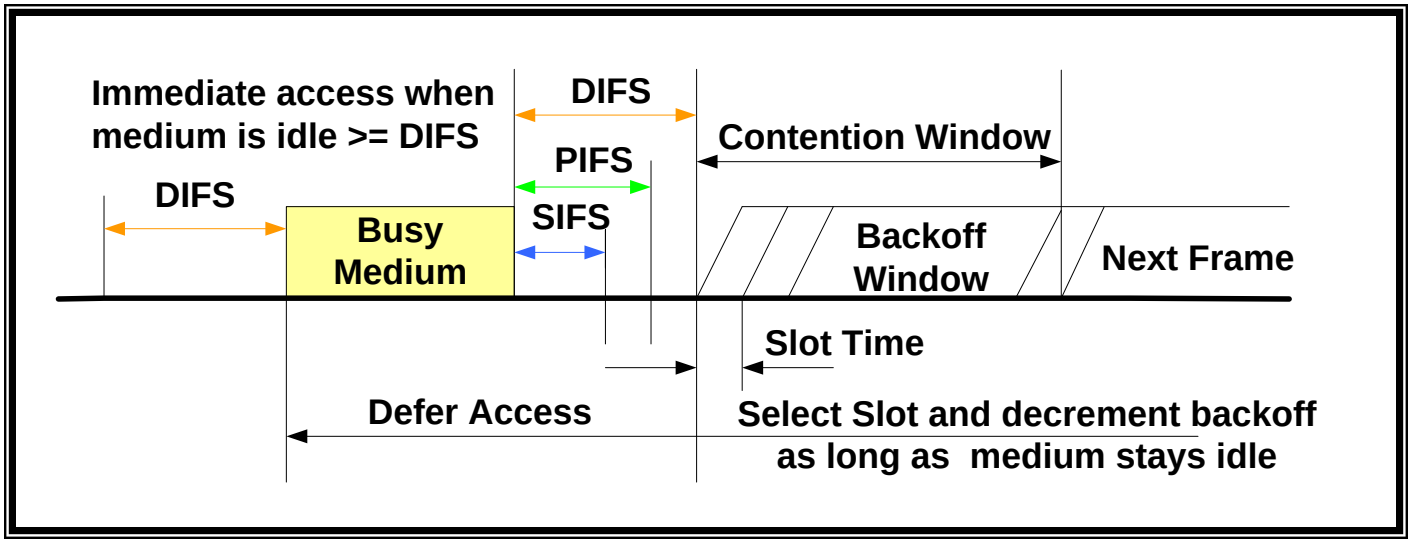
- ***Mandatory*** **Distributed Coordination Function (DCF)**
  - **For distributed contention-based channel access**
- ***Optional*** **Point Coordination Function (PCF)**
  - **For centralized contention-free channel access**

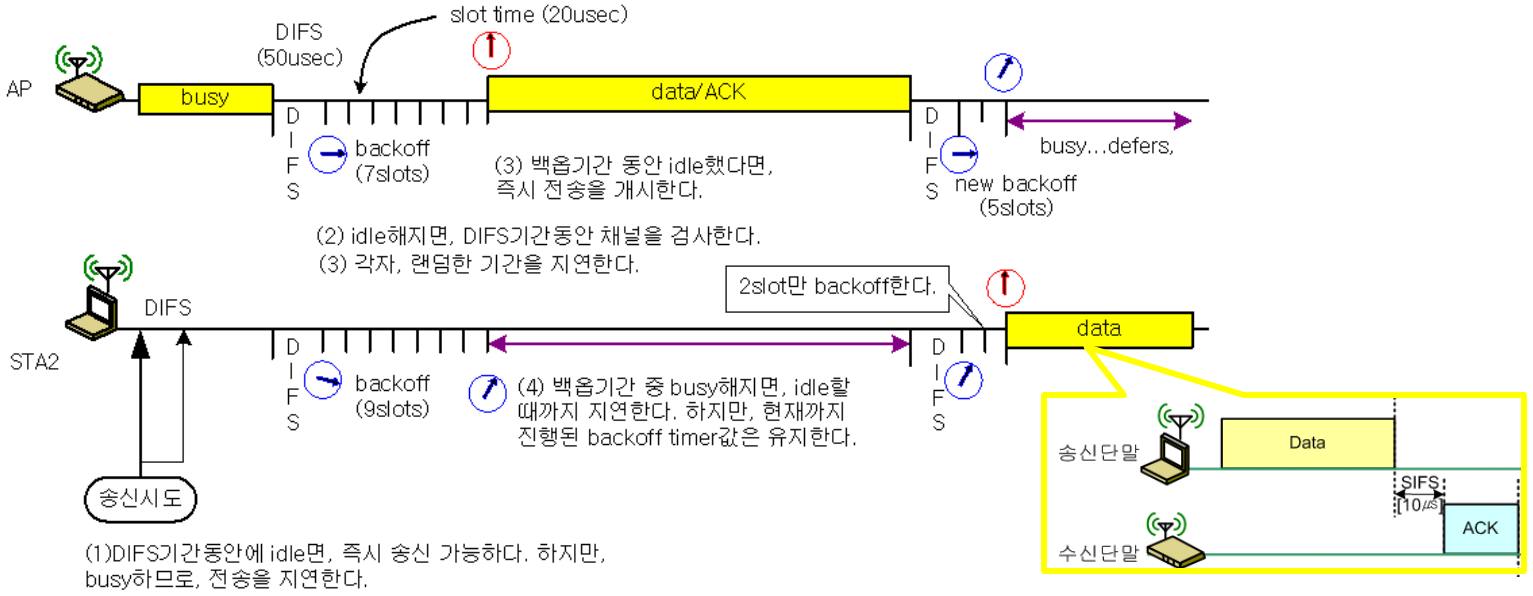
WLAN DCF MAC – CSMA/CA 1

1. Before sending a frame, senses the medium by checking the energy level
   a. **Persistence strategy**
   b. **Wait the interframe space (IFS=DIFS),**
2. Send data frame
3. **Receive acknowledgement after SIFS**



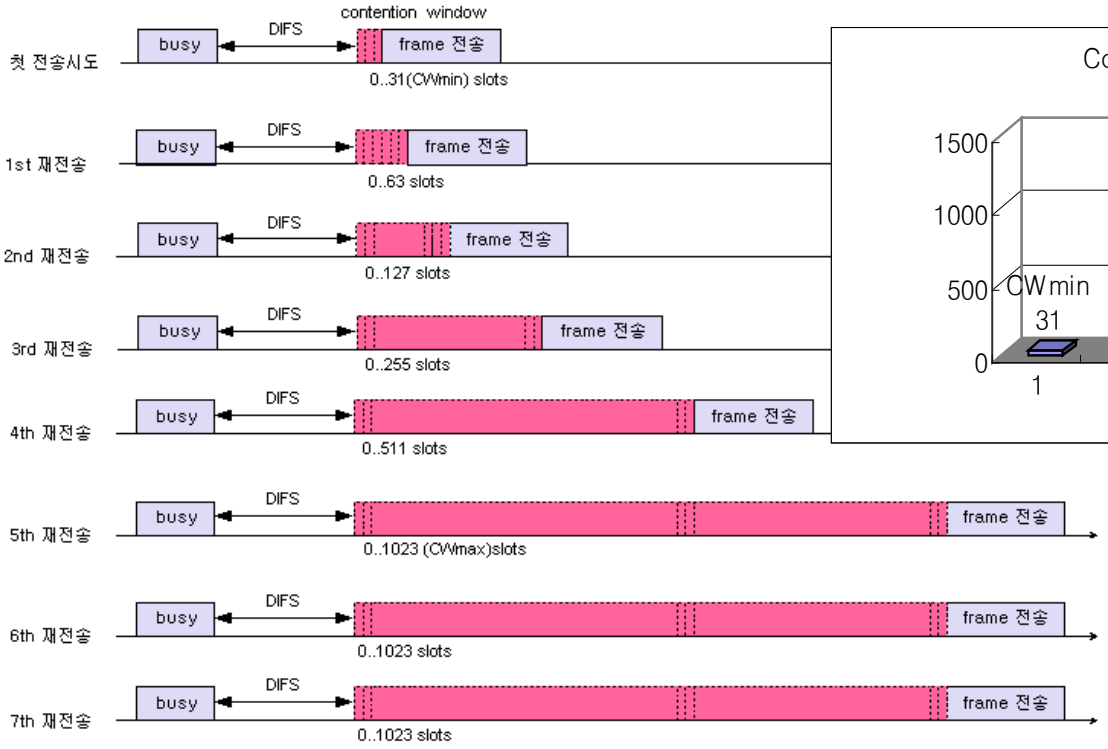
Distributed Coordination Function (DCF)

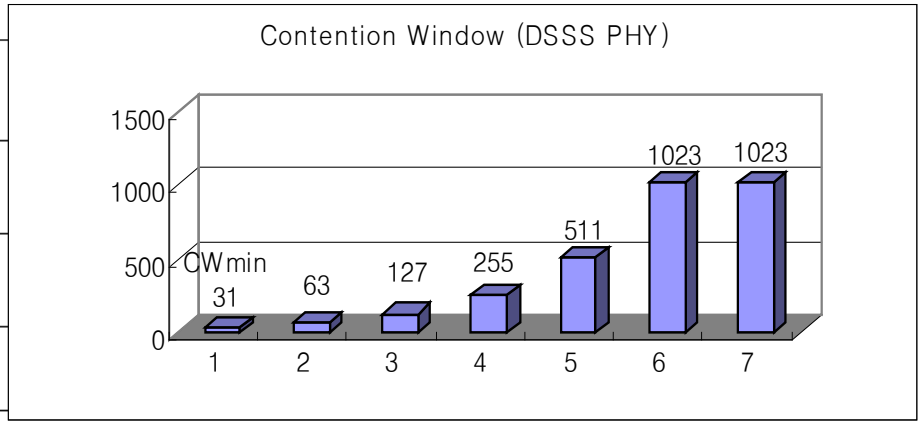




Exponential Backoff

- **Backoff Counter is randomly selected from [0,CW], where CW is contention window**
- **For each unsuccessful frame transmission, CW doubles (from CWmin to CWmax)**
  - **CW ← 2(CW+1)-1**
- **Reduces the collision probability**



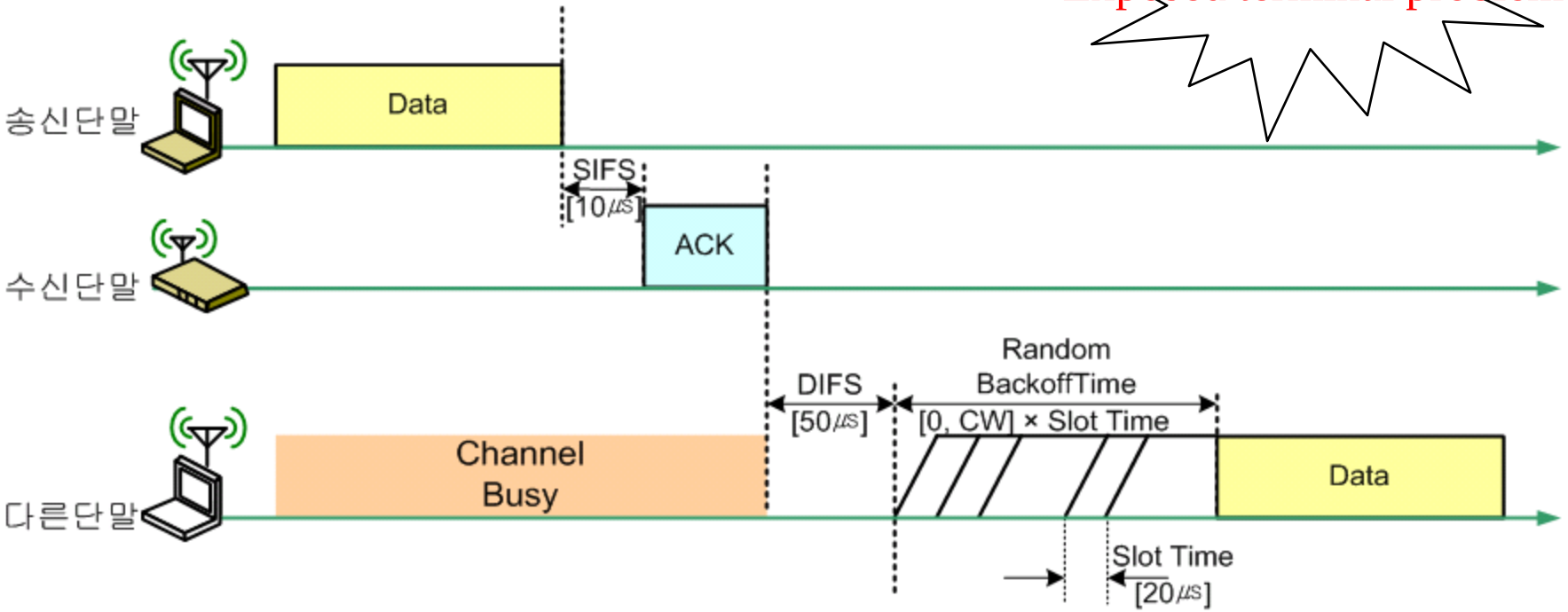


Basic DCF Access Method (2)

- **Station has to wait for DIFS before sending data**
- **Receivers acknowledge (after waiting for SIFS) if the packet was received correctly (CRC)**
- **Automatic retransmission of data packets in case of transmission errors**

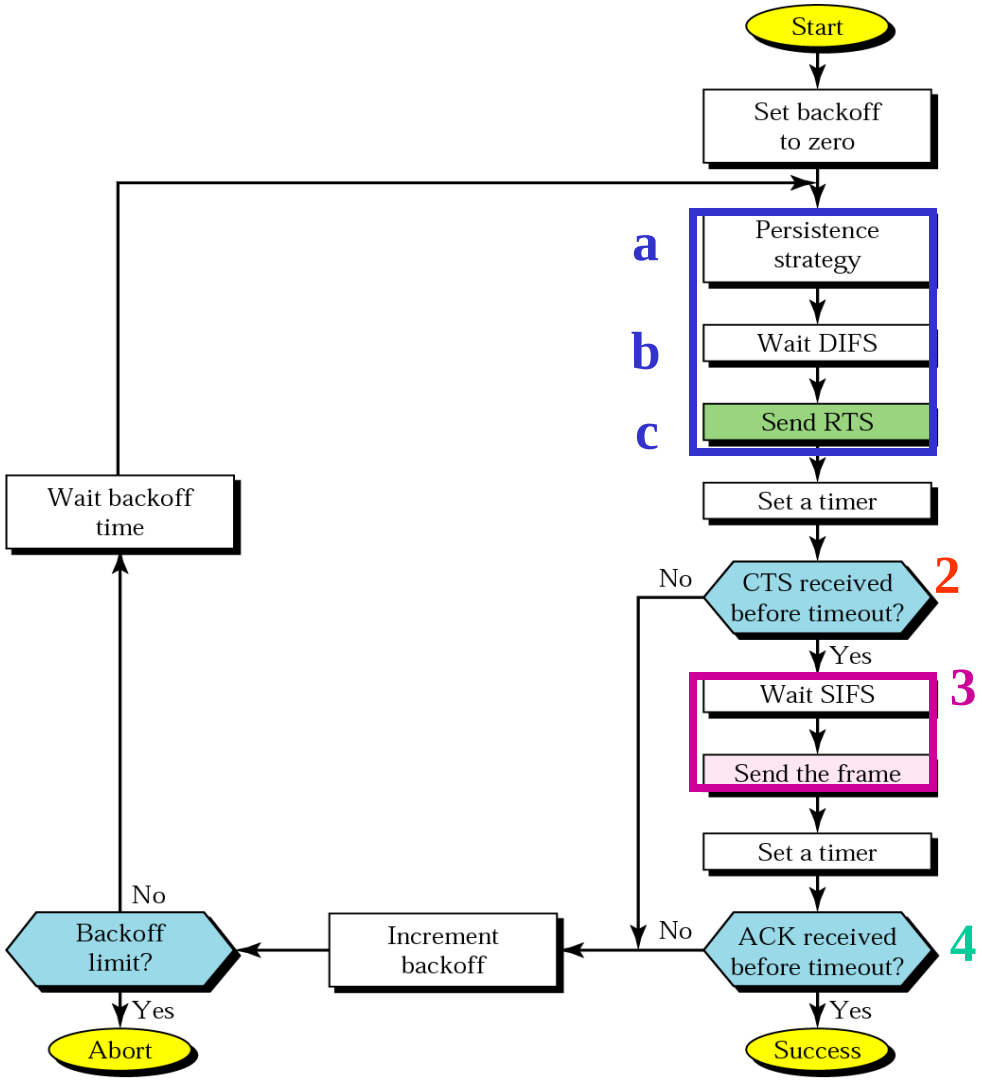
Hidden terminal problem

Exposed terminal problem



WLAN MAC – CSMA/CA 2

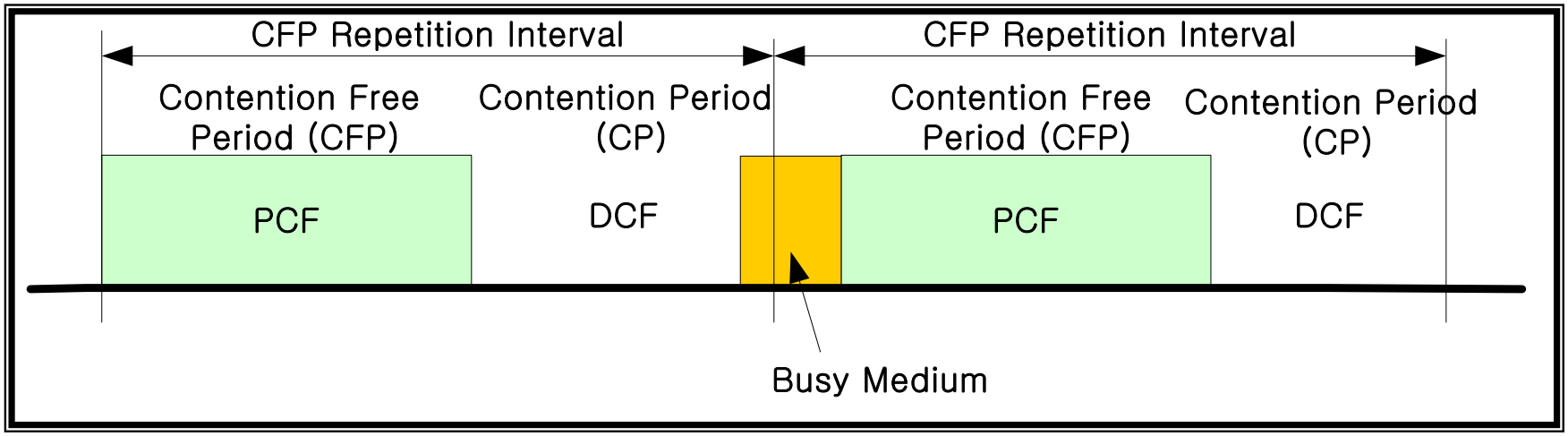
1. Before sending a frame, senses the medium by checking the energy level
   a. **Persistence strategy**
   b. **Wait the distributed interframe space (DIFS),**
   c. **Then, sends a control frame (RTS)**
2. **A**fter receiving the RTS and wait the short interframe space (SIFS), the destination sends a control frame (CTS)- ready to receive
3. Send data after SIFS
4. **Receive acknowledgement after SIFS**



PCF (Point Coordination Function)

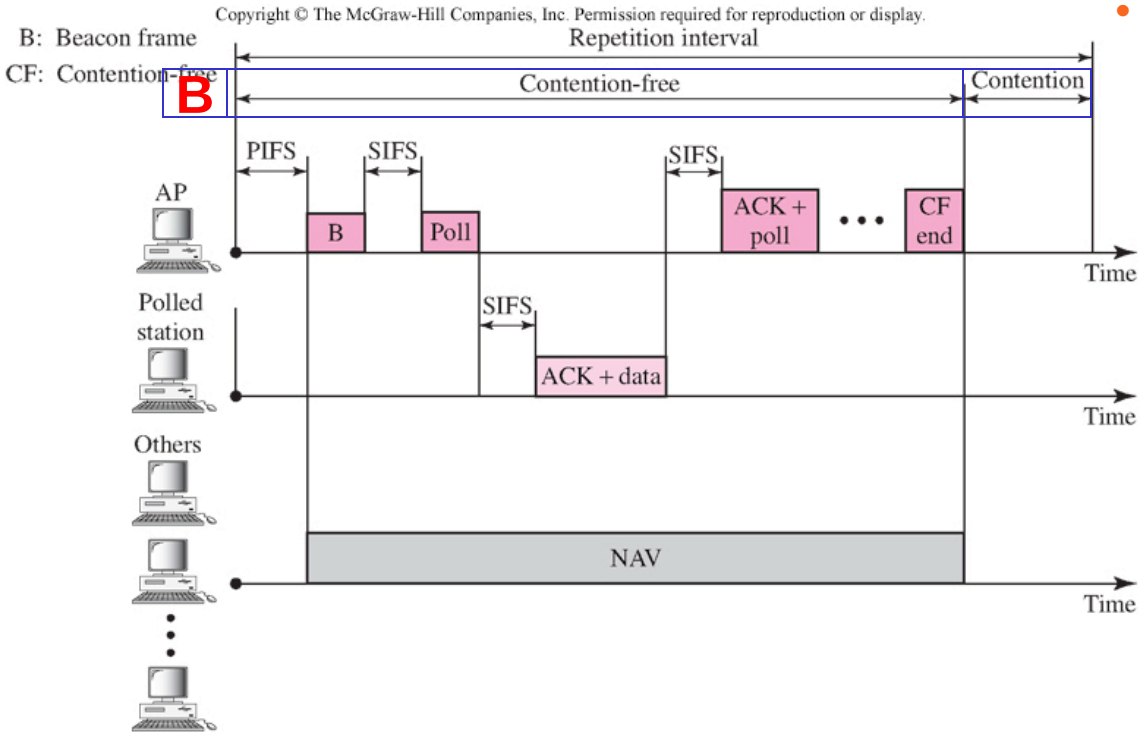
- **Optional function – used for time-sensitive transmission**
- **centralized Contention-free method by polling**

  ➡ **need Point Coordinator (PC), or AP**
- **Coexistence of the PCF and DCF**
- **Time-bounded Service**



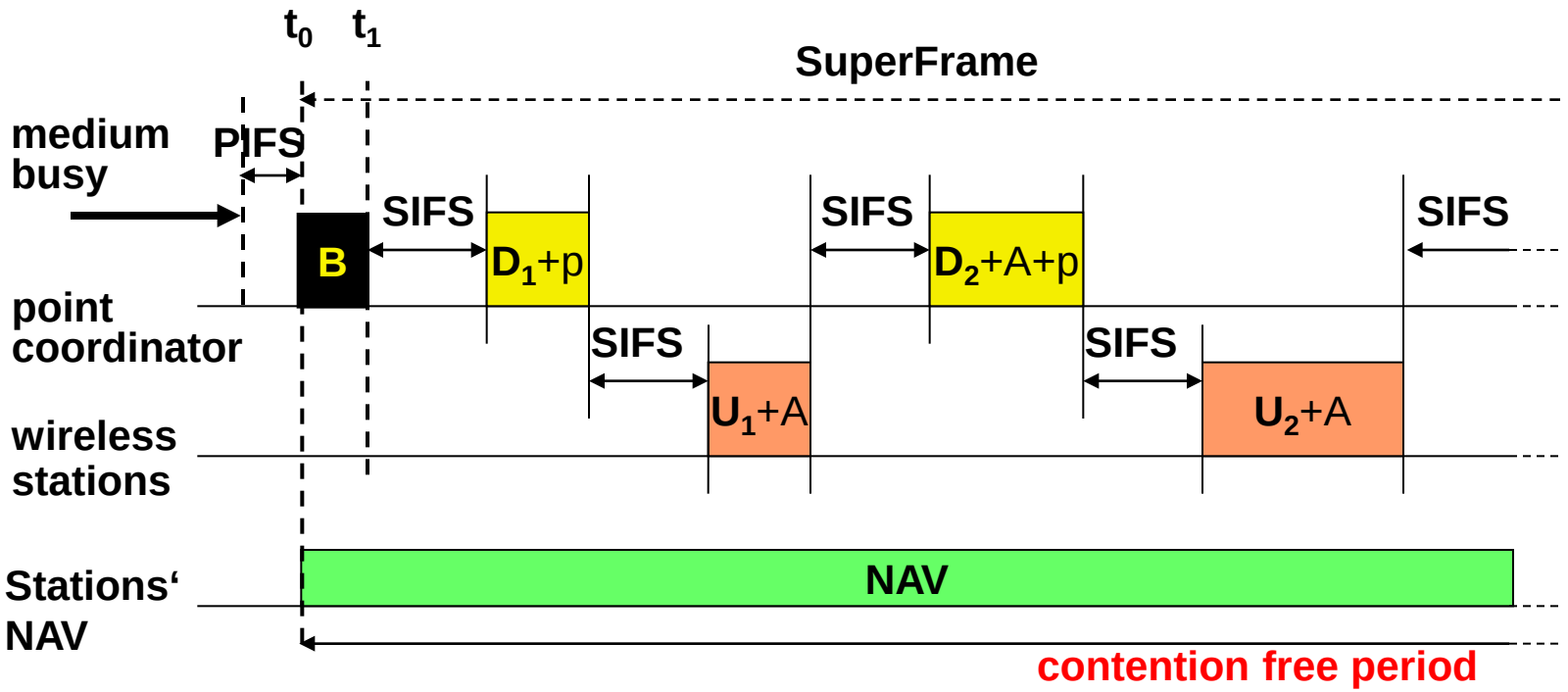
Point Coordination Function (PCF)

- **Poll-and-response MAC for nearly Isochronous service**
- **In infrastructure BSS only – Point Coordinator (PC) resides in AP**
- **Alternating Contention-Free Period (CFP) and Contention Period (CP)**



- Super frame structure
  Unit: TU(=1024us)

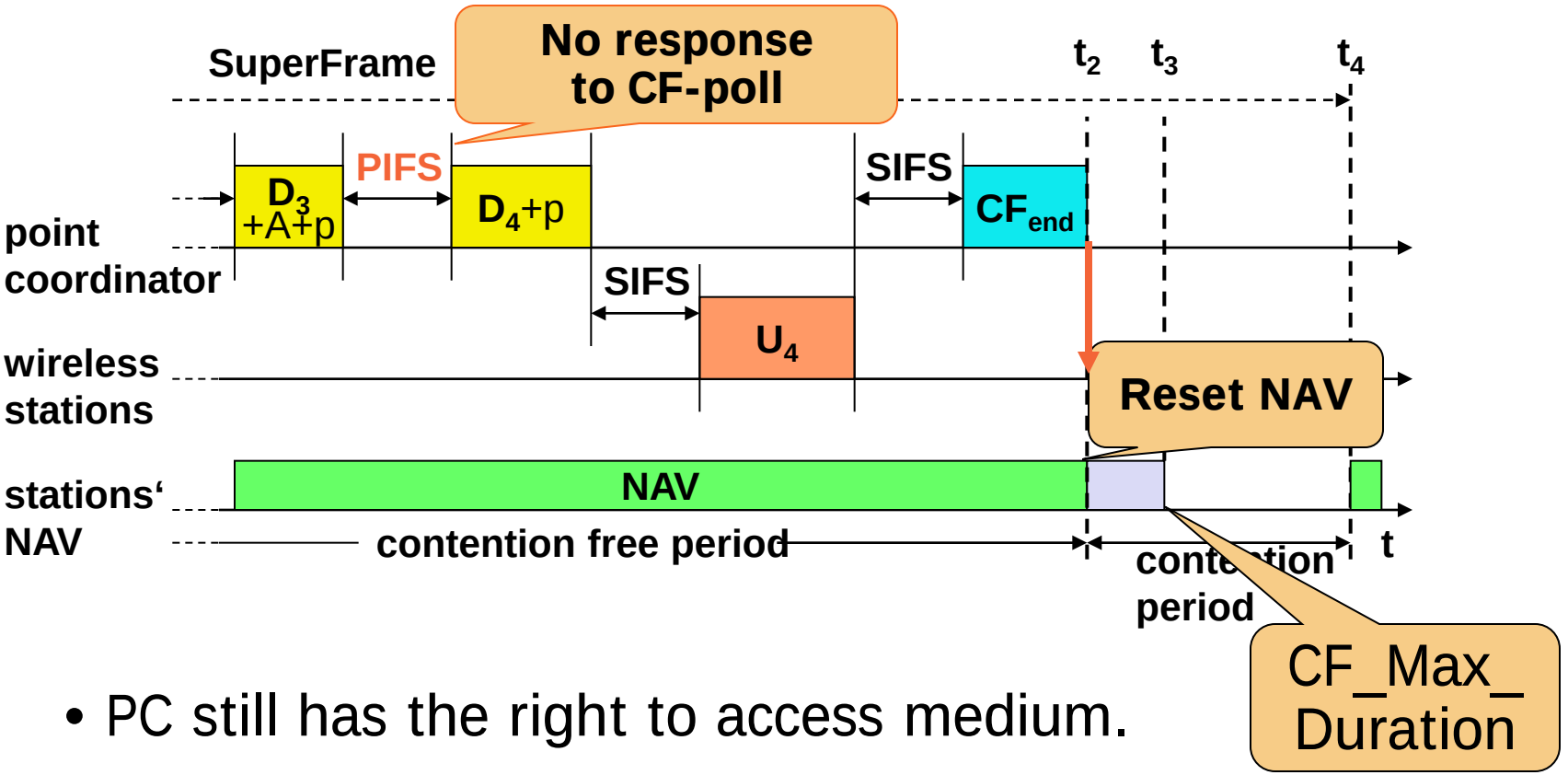
PCF Mechanism (1)



A : ACK

P : poll

PCF Mechanism (2)



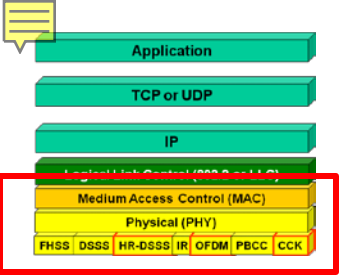
- PC still has the right to access medium.

  Because of SIFS < PIFS < DIFS

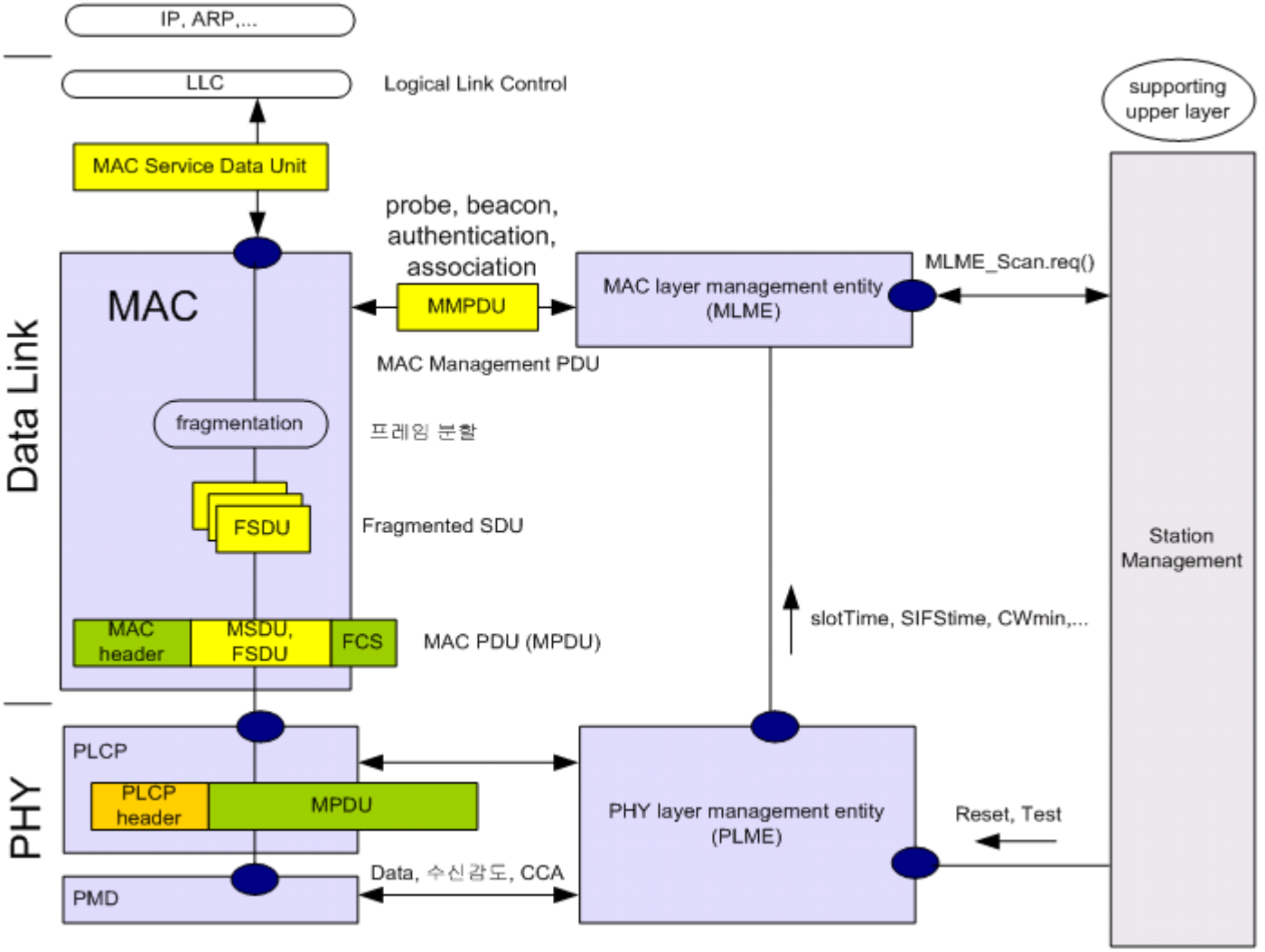
Polling in PCF

- **Polling list**
  - **used to force the polling of CF-Pollable STAs, where PC has traffic to transmit (or not)**
  - **a *logical* construct**
  - **Remainders are polled in next CFP**
- **When a polling cycle is finished**
  - **PC may send one or more CF-Polls to *any* STAs within CFP**
- **For efficiency, use piggyback**
- **During association, *polling list* is updated by checking Capability Information field**

Frame Format



802.11 MAC 계층 구조 및 PDU 종류

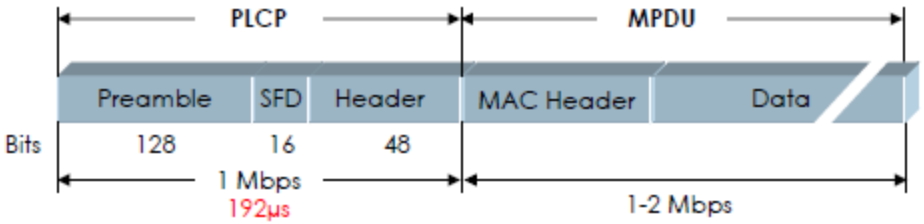


PLCP(Physical Layer Convergence protocol): 하부에 다양한 PMD가 있고 이들간의 동작을 정합시키는 역할을 수행한다. 상위 MAC 계층에서 전달된 MAC PDU에 프리앰블과 PLCP 헤더를 부착 후 PMD로 보낸다.
MAC: llc와 같은 상위 MAC SDU나 프로브, 비컨 등의 MAC Management 용 프레임을 수납하여 CSMA/CA 방식으로 전송과 재전송을 수행한다. 또한 필요 시 fragmented S여 들로 분할
(MLME)MAC layer management entity : 전원관리, 탐색, join, 인증, 결합, 시간 동기 등의 MAC 계층의 운영에 필요한 관리 기능을 특별한 MMPDU(probe, beacon, association, authentication 등)의 프레임을 사용해서 수행
(PLME)Physical sublayer management entity : 물리 계층의 리셋, 모뎀 동작값(슬롯타임, 송수신 전환 지연시간, 프리앰블 길이) 등을 설정하거나 읽는다.
Station Management: 상위 사용자로부터 reset, scan, assoication 요청 명령에 의해 MLME나 PLME의 작업을 지시하고 처리 결과를 상위계층에 전달하는 연결관리 기능의 총괄 모듈

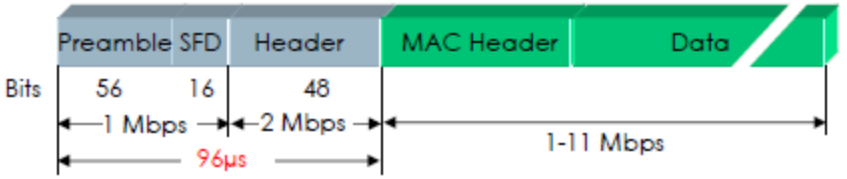
802.11 b/g PHY/MAC Frame Format

DSSS and OFDM packet formats are not compatible

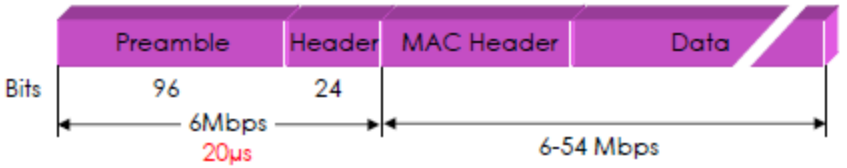
802.11 DSSS with
‚Long Preamble'
Barker Code



802.11b HR/DSSS with
‚Short Preamble'
Barker / CCK



802.11g (ERP)
Extended Rate PHY
new Frame Format
OFDM



PLCP = Physical Layer Convergence Protocol
MPDU = MAC Layer Protocol Data Unit

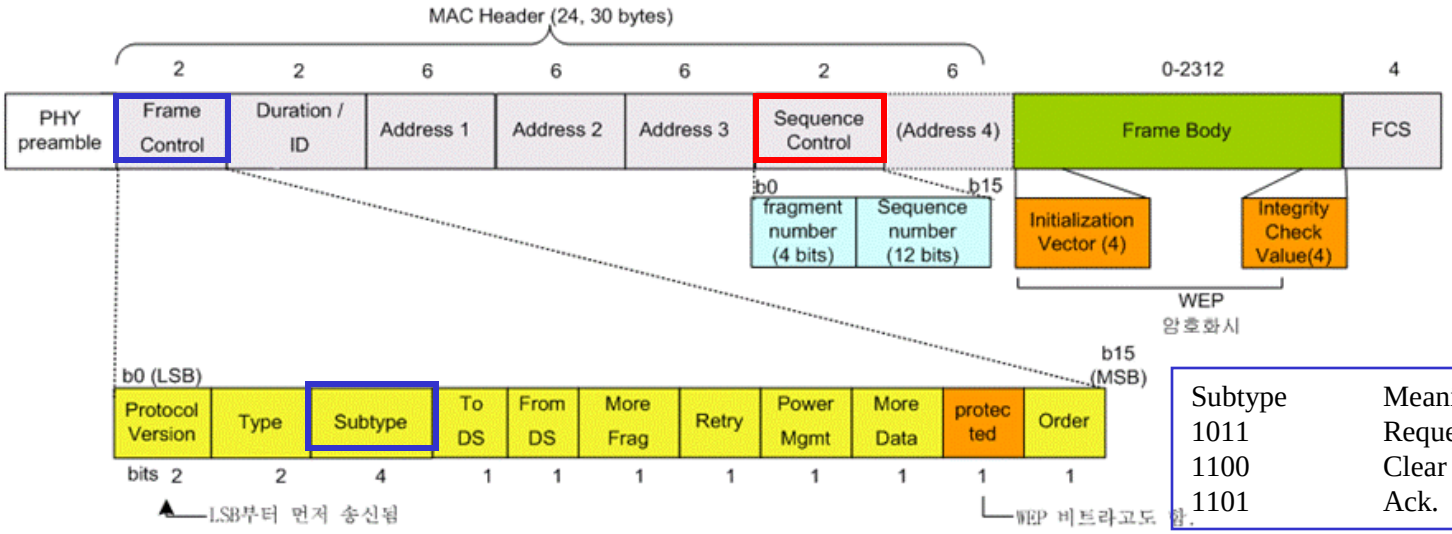
802.11 MAC Frame Format

Frame Control – management, control, data frame types

Duration – tells length of next frame (the value of NAV)

Addr *n* – cell ID, source, destination, transmitter, receiver

Sequence Control – fragmentation & sequence number



Subtype	Meaning
1011	Request to Send
1100	Clear to Send
1101	Ack.

그림 2.3 MAC 프레임의 기본형식

version – current version 0

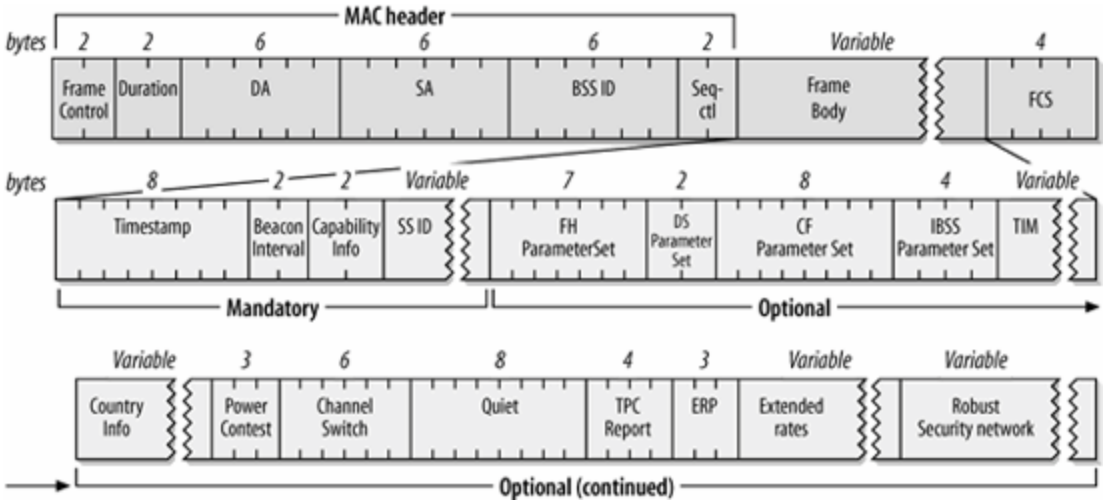
Type of information – management(00), control (01) or data (10)

Sub type – RTS, CTS, ACK

WEP – Wired equivalent privacy (encryption implemented)

Management frame format Example

Prove Request 프레임



Beacon프레임

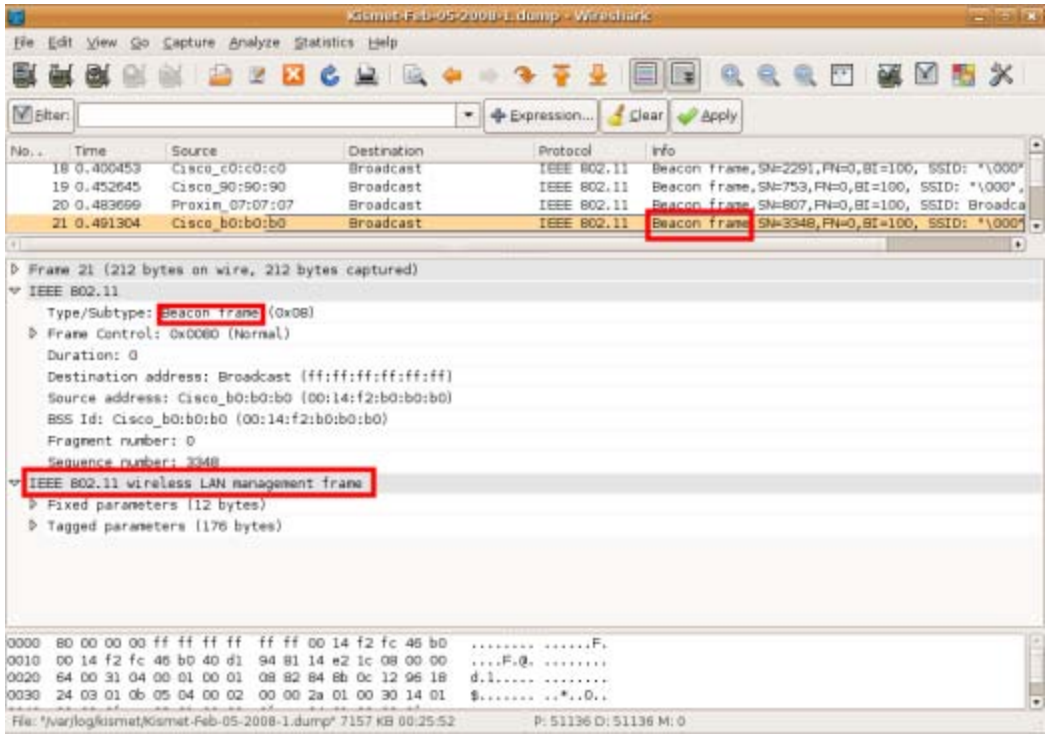
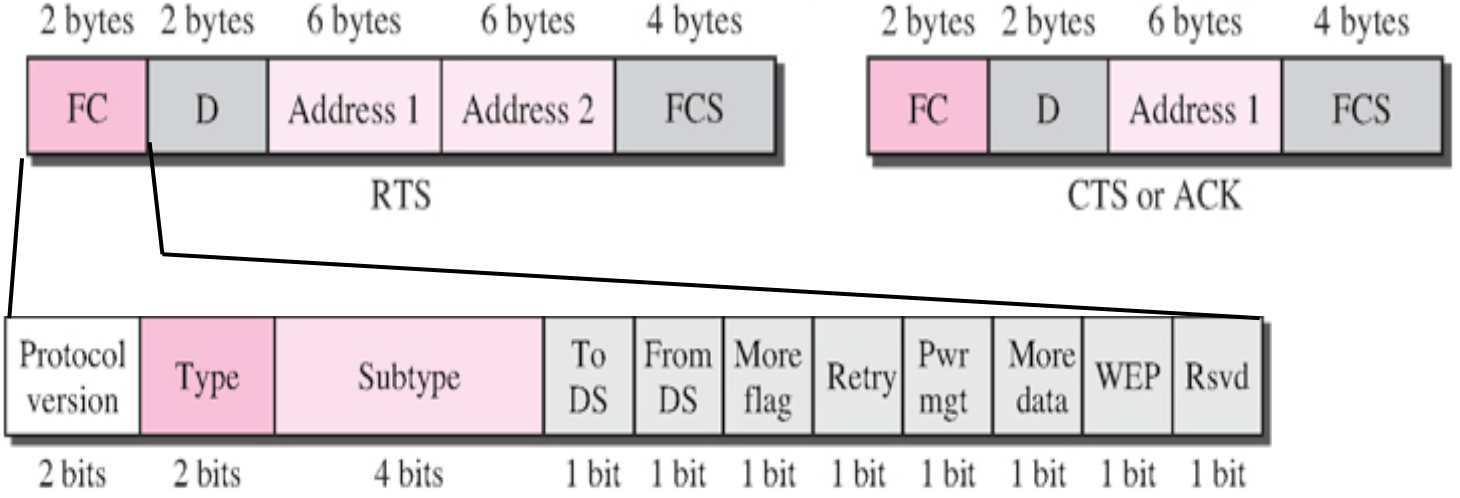
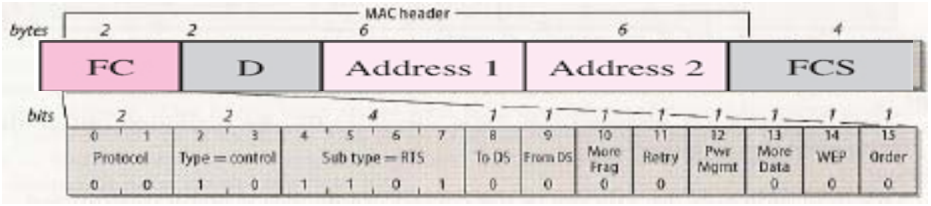

Kismet-Feb-05-2008-1.dump - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
18 0.400453 Cisco_c0:c0:c0 Broadcast IEEE 802.11 Beacon frame,SN=2291,FN=0,BI=100, SSID: *\000*
19 0.452645 Cisco_90:90:90 Broadcast IEEE 802.11 Beacon frame,SN=753,FN=0,BI=100, SSID: *\000*,
20 0.483699 Proxim_07:07:07 Broadcast IEEE 802.11 Beacon frame,SN=807,FN=0,BI=100, SSID: Broadca
21 0.491304 Cisco_b0:b0:b0 Broadcast IEEE 802.11 Beacon frame,SN=3348,FN=0,BI=100, SSID: *\000*
Frame 21 (212 bytes on wire, 212 bytes captured)
IEEE 802.11
Type/Subtype: Beacon frame (0x08)
Frame Control: 0x0080 (Normal)
Duration: 0
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Source address: Cisco_b0:b0:b0 (00:14:f2:b0:b0:b0)
BSS Id: Cisco_b0:b0:b0 (00:14:f2:b0:b0:b0)
Fragment number: 0
Sequence number: 3348
IEEE 802.11 wireless LAN management frame
Fixed parameters (12 bytes)
Tagged parameters (176 bytes)
0000 80 00 00 00 ff ff ff ff ff ff 00 14 f2 fc 46 b0 ....F.
0010 00 14 f2 fc 46 b0 40 d1 94 81 14 e2 1c 08 00 00 ....F.@. .....
0020 64 00 31 04 00 01 00 01 08 82 84 8b 0c 12 96 18 d.1..... .....
0030 24 03 01 0b 05 04 00 02 00 00 2a 01 00 30 14 01 $..... ..*..0..
File: "/var/log/kismet/Kismet-Feb-05-2008-1.dump" 7157 KB 00:25:52
P: 51136 D: 51136 M: 0

Figure 15.10: Control frame format Example



Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

RTS/CTS



RTS 프레임

	b0							b7	b8							b15	
Frame Control	0	0	1	0	1	1	0	1									2
Duration/AID	Duration = 0																2
Address 1	FF : FF : FF : FF : FF : FF (Broadcast)																6
Address 2	STA																6
	FCS																4

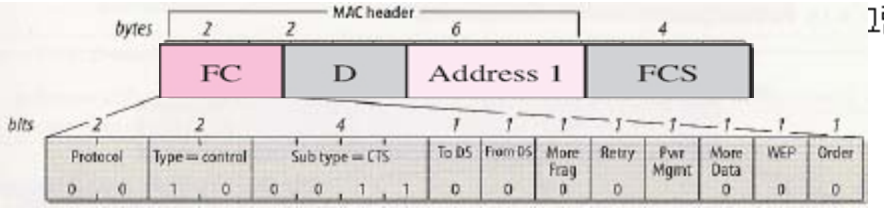


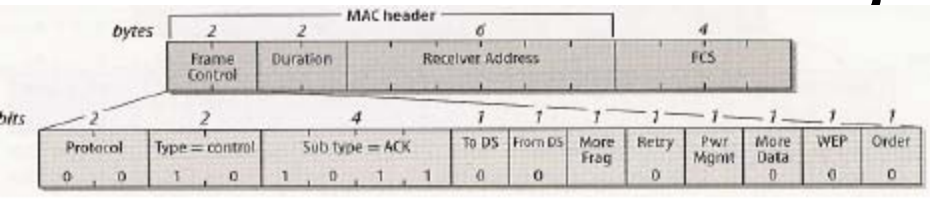
그림 2.27 Request To Send(RTS) 프레임 형식.

CTS 프레임

	b0							b7	b8							b15	
Frame Control	0	0	1	0	0	0	1	1									2
Duration/AID	Duration																2
Address 1	STA																6
	FCS																4

그림 2.28 Clear To Send(CTS) 프레임 형식.

ACK, PS-Poll



Acknowledgement프레임

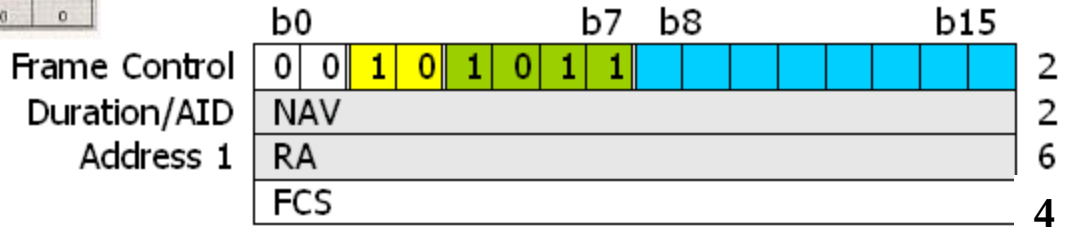
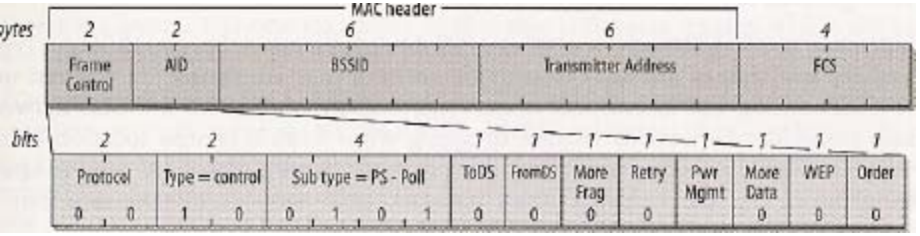


그림 2.29 Acknowledgment 프레임 형식.



Power-Save Poll 프레임

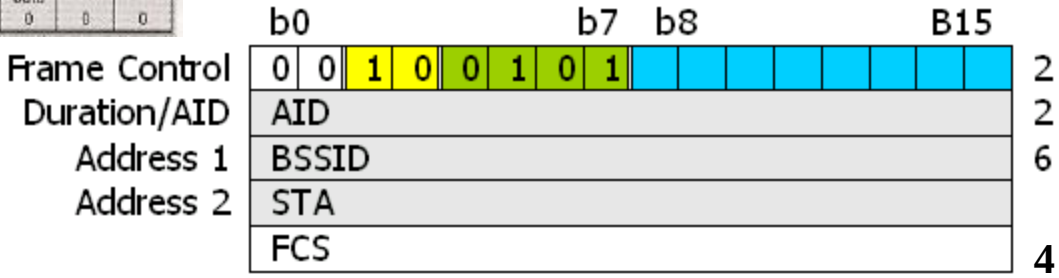
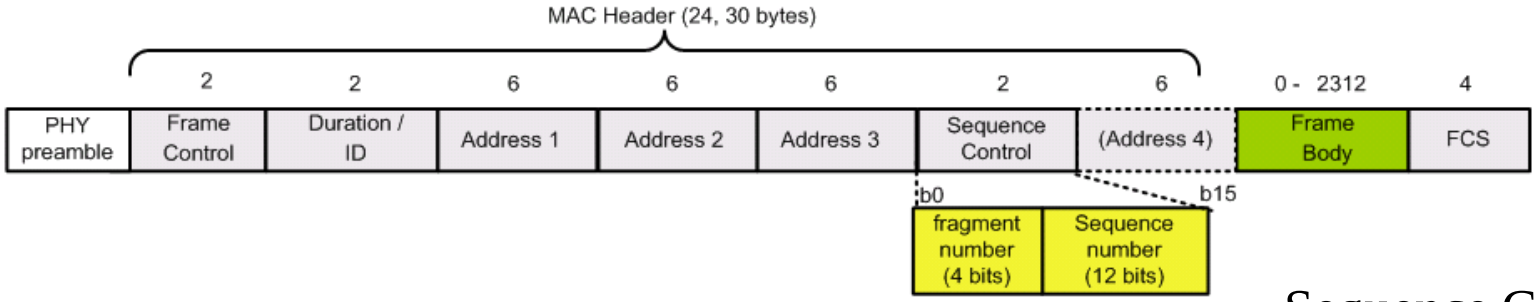


그림 2.30 PS-Poll 프레임 형식.

데이터 프레임 형식



Sequence Control

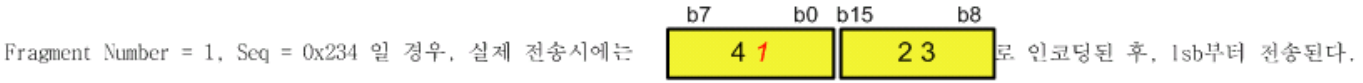


그림 2.8 시퀀스/분할번호 영역의 사용 예

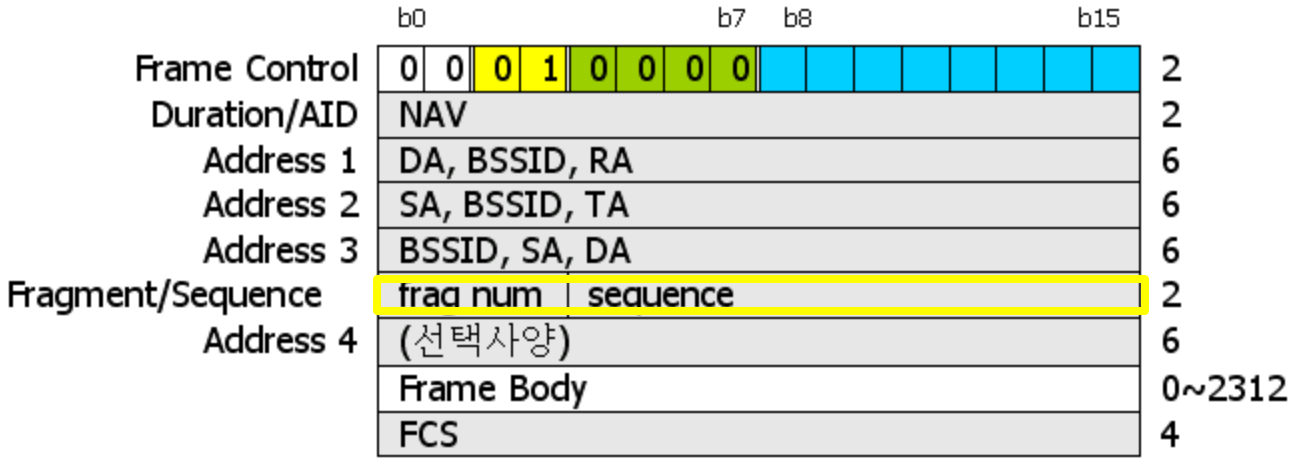
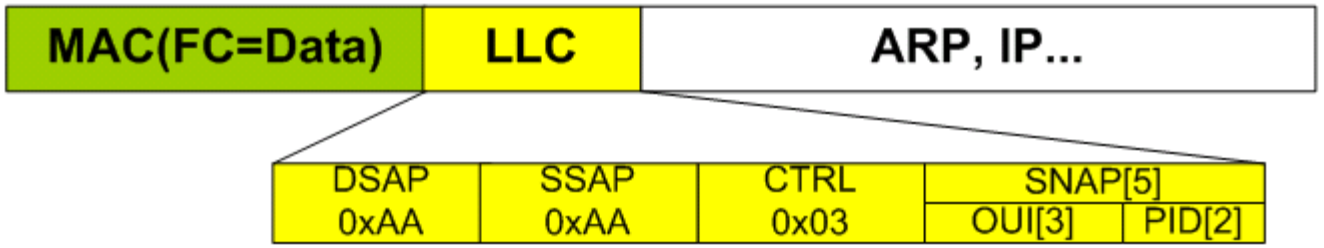


그림 2.31 데이터 프레임 형식.

Frame Body

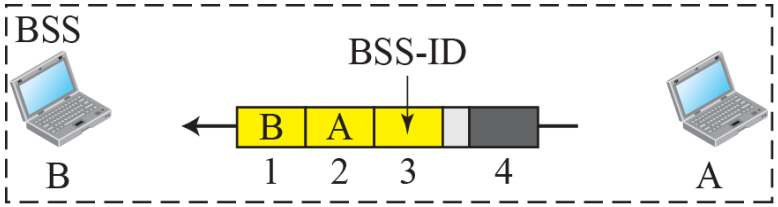


* DSAP = Destination Service Access Point (=0xAA)
* SSAP = Source SAP
* CTRL = Control Field (=0x03 = Unnumbered Information)
* SNAP = SubNetwork Access Protocol
* OUI = Organization Unique Identifier (000000 = IEEE802)
* PID = Protocol ID

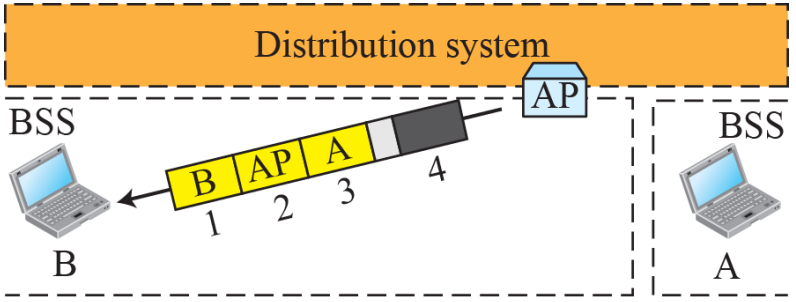
그림 2.9 데이터 프레임의 경우

802.11 Addressing Mechanisms

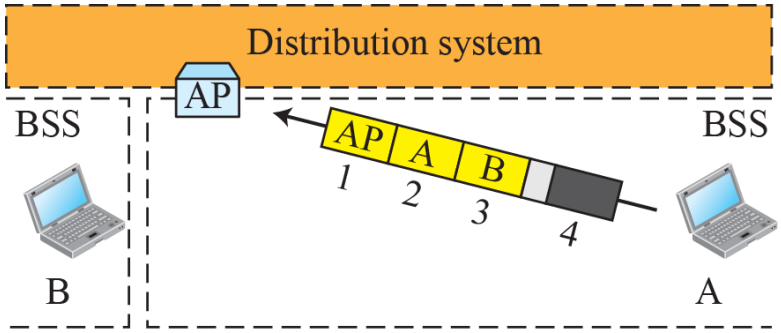
To DS	From DS	Add 1	ADD 2	Add 3	Add 4
0	0	Dest	Source	BSS ID	N/A
0	1	Dest	Sending AP	Source	N/A
1	0	Receiving AP	Source	Dest	N/A
1	1	Receiving AP	Sending AP	Dest	Source



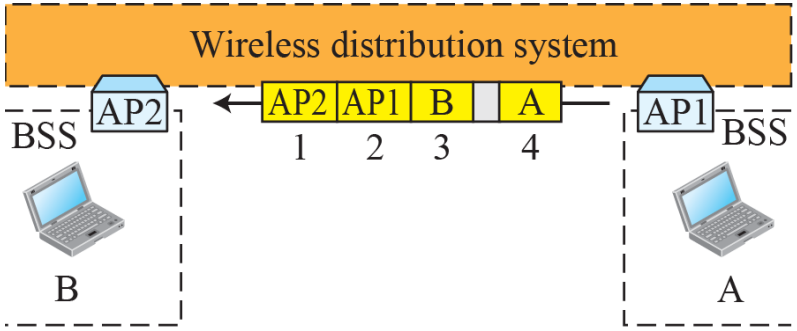
a. Case 1



b. Case 2



c. Case 3



d. Case 4

Example of Addressing mechanism

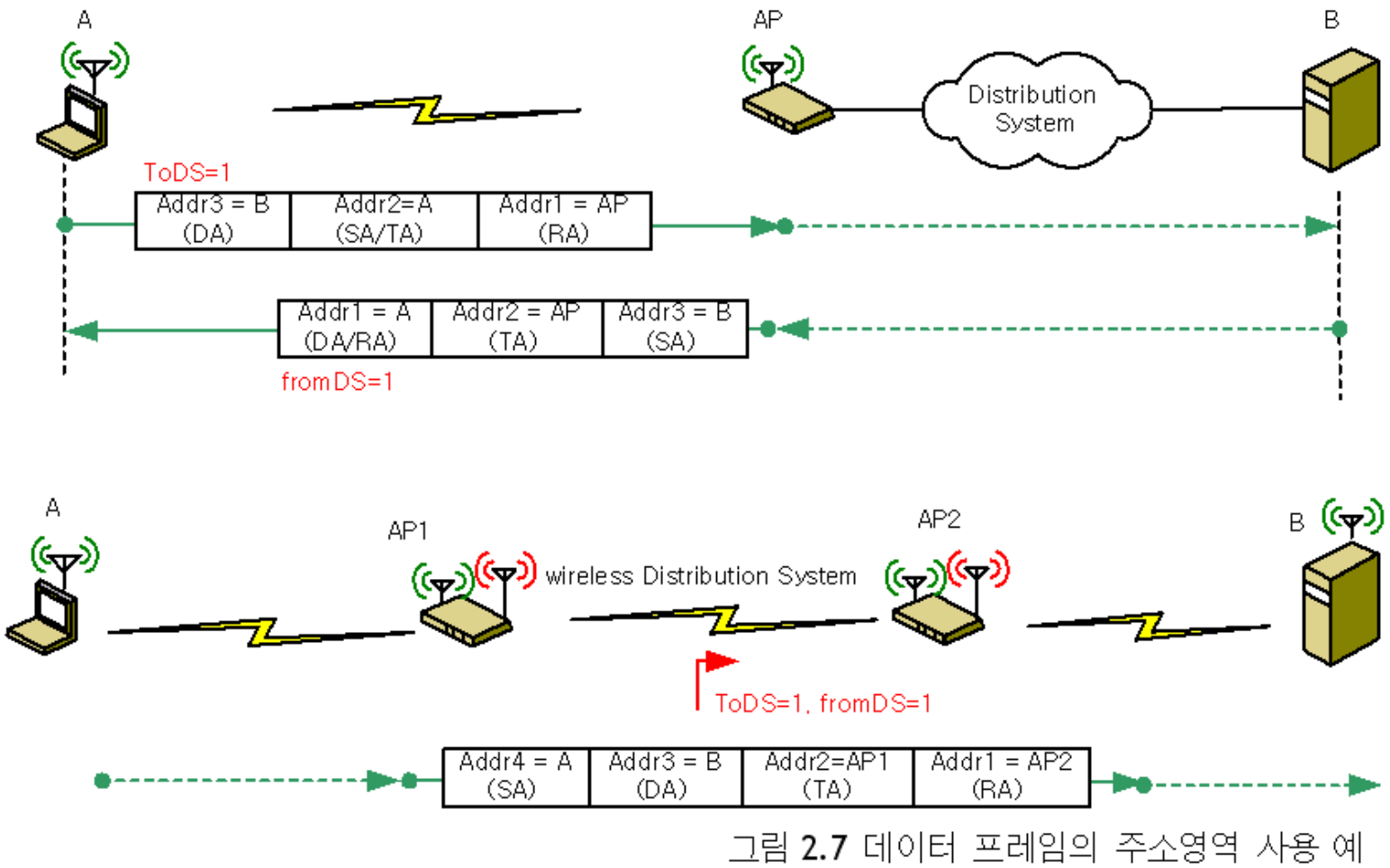
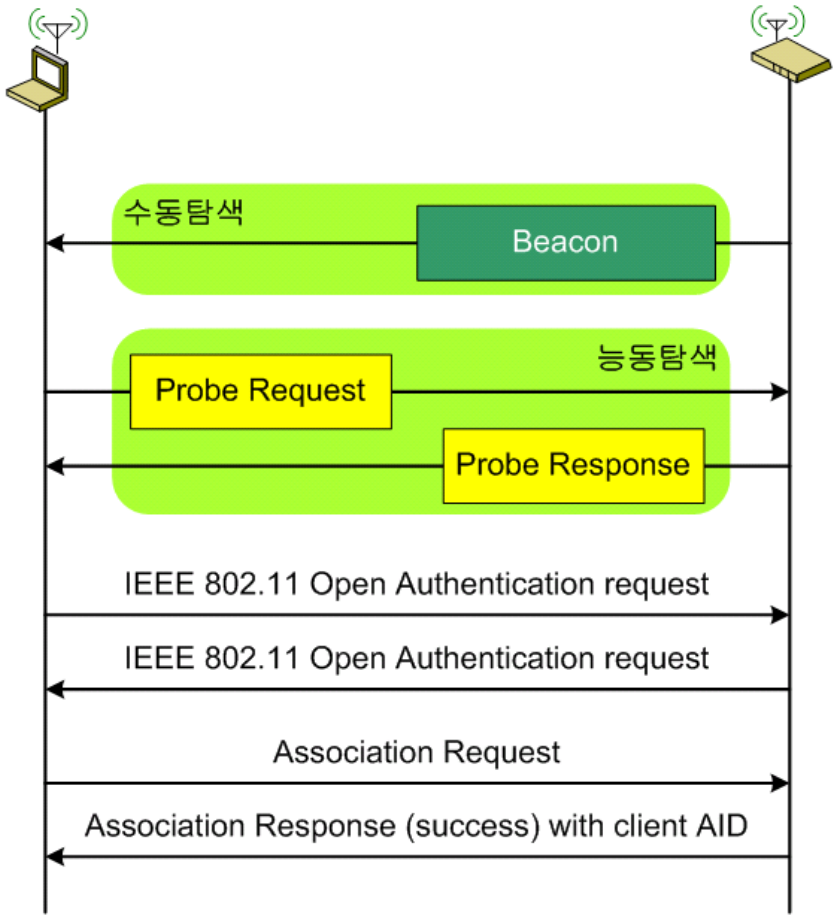


그림 2.7 데이터 프레임의 주소영역 사용 예

Operation

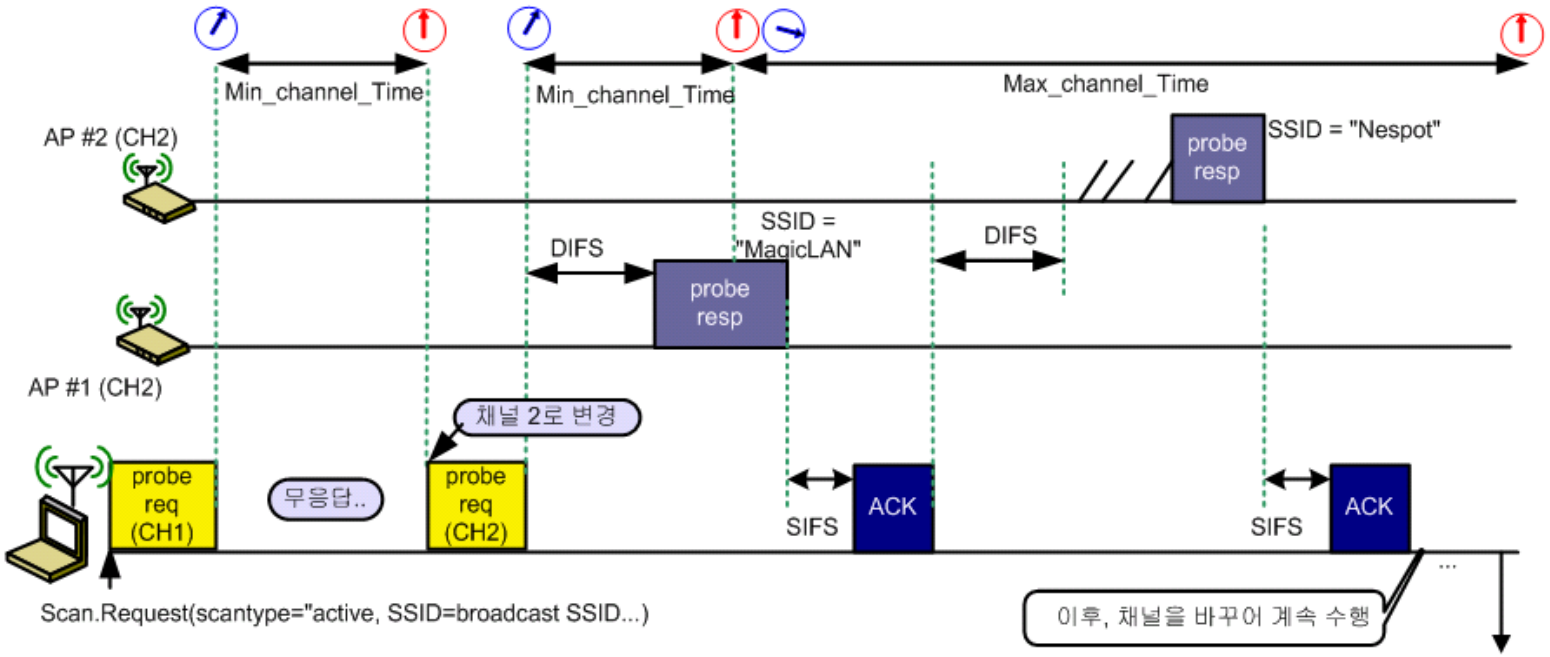
Network Access and Security

- 탐색
- **Join**
- 인증
- 결합



탐색 과정-능동탐색

MLME-SCANreq(BSSType = INFRASTRUCTURE, BSSID = 0xff..ff, SSID = “NULL”, ScanType = active,
프로브Delay= 5 usec, ChannelList = {1,2,3….14}, MinChannelTime = 1 TU, MaxChannelTime = 2 TU)



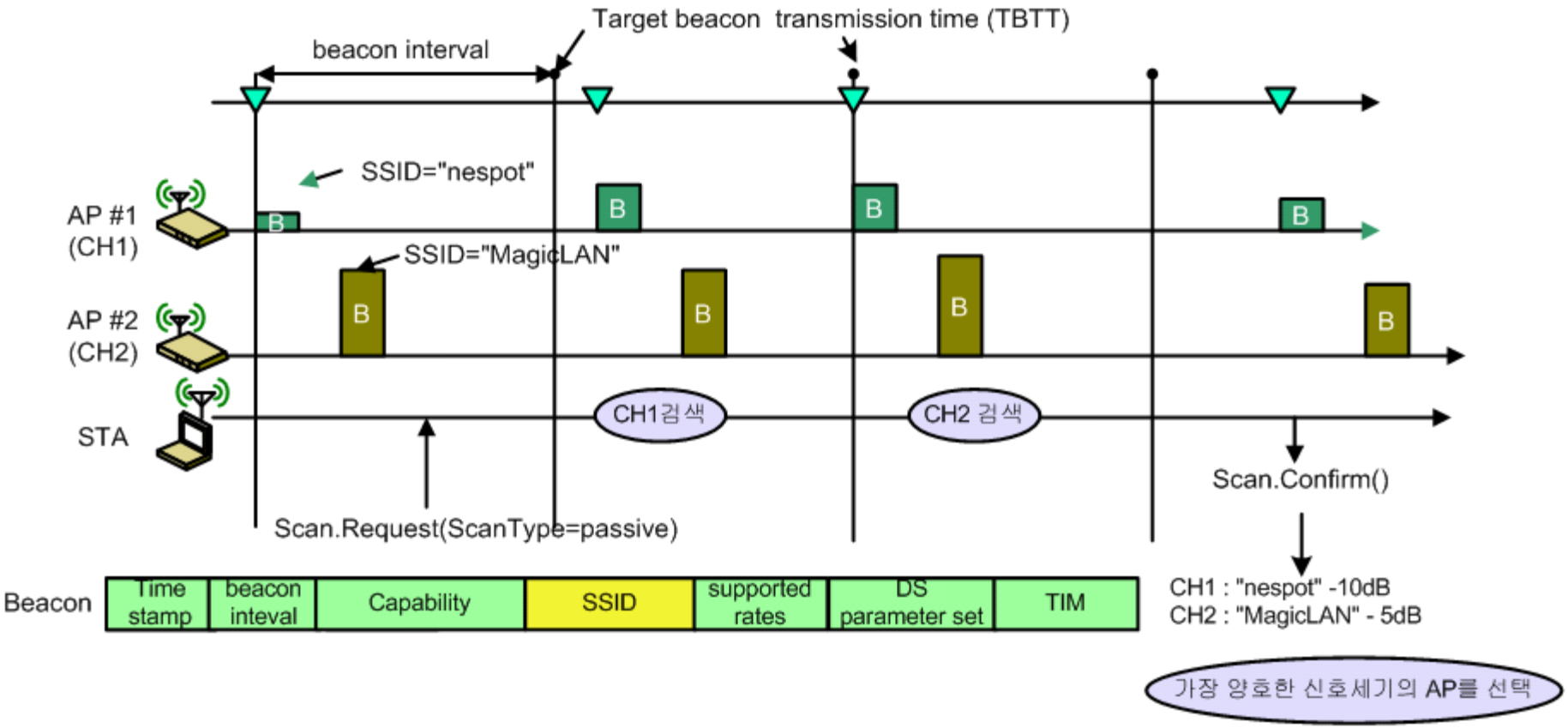
Probe

Frame Control	Duration	DA	SA	BSSID	Seq/ Frag	SSID	supported rates	FCS

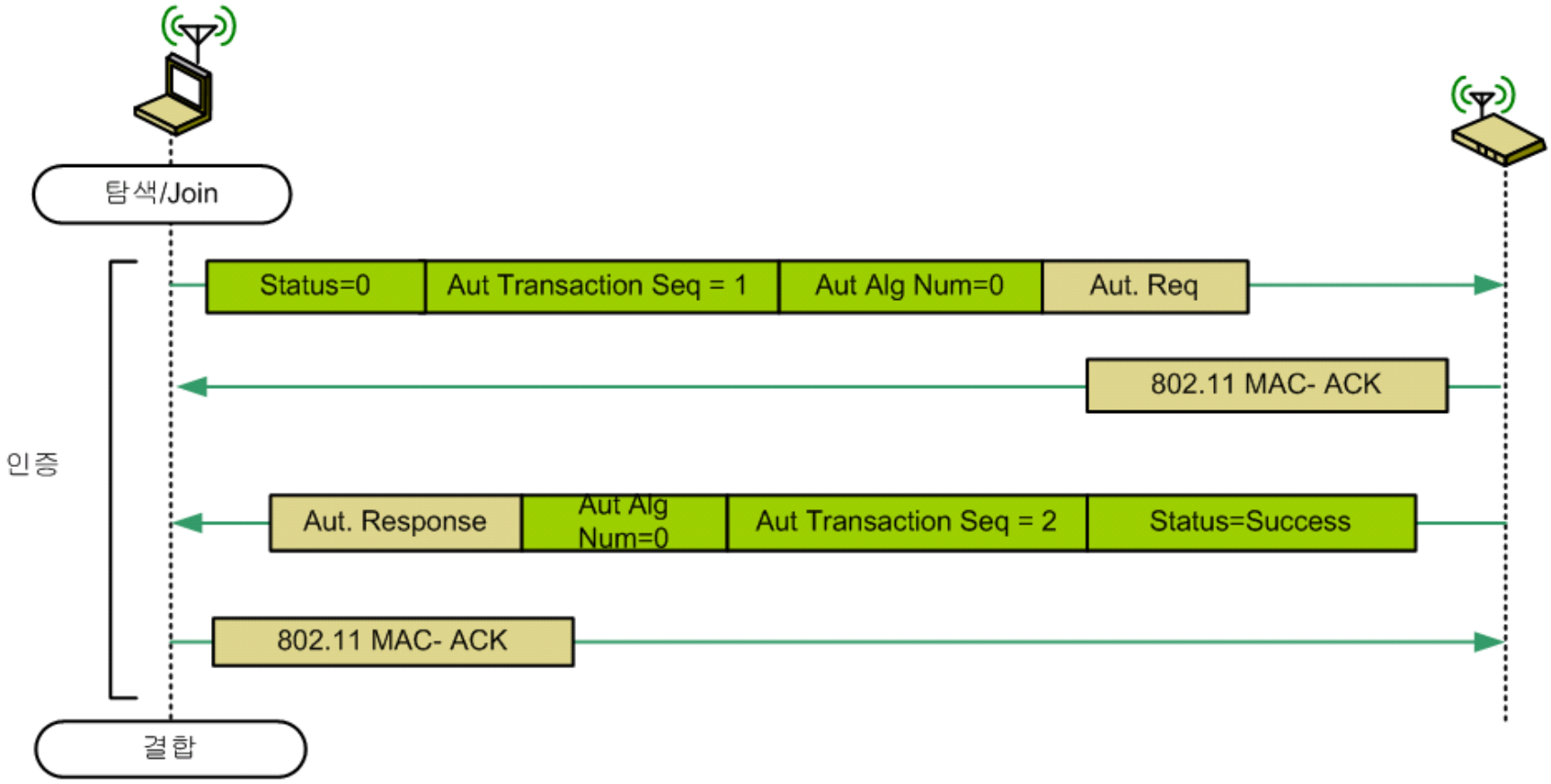
Probe Response

Frame Control	Duration	DA	SA	BSSID	Seq/ Frag	Time stamp	beacon interval	Capability	SSID	supported rates	DS parameter set	FCS

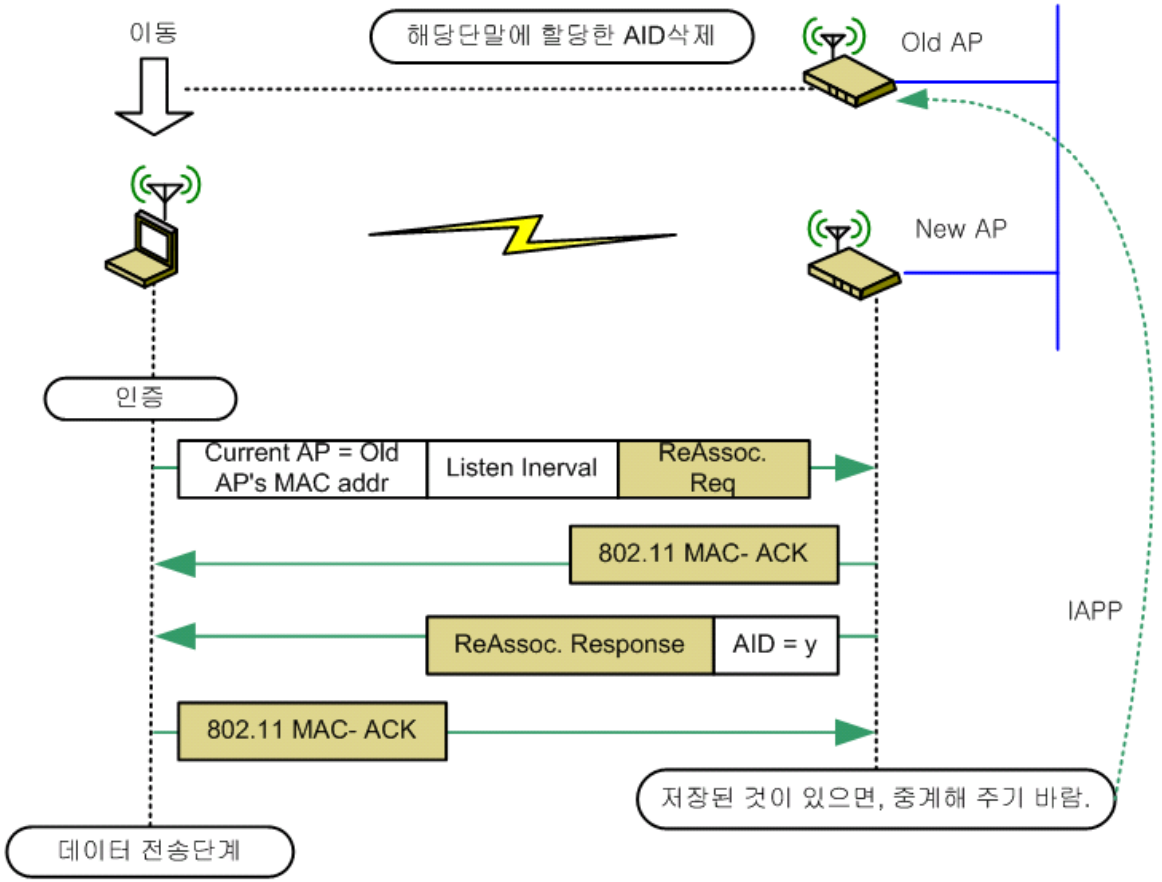
수동탐색


Target beacon transmission time (TBTT)
beacon interval
SSID="nespot"
AP #1
(CH1)
B
SSID="MagicLAN"
AP #2
(CH2)
STA
CH1검색
CH2 검색
Scan.Confirm()
Scan.Request(ScanType=passive)
Beacon
Time stamp
beacon inteval
Capability
SSID
supported rates
DS parameter set
TIM
CH1 : "nespot" -10dB
CH2 : "MagicLAN" - 5dB
가장 양호한 신호세기의 AP를 선택

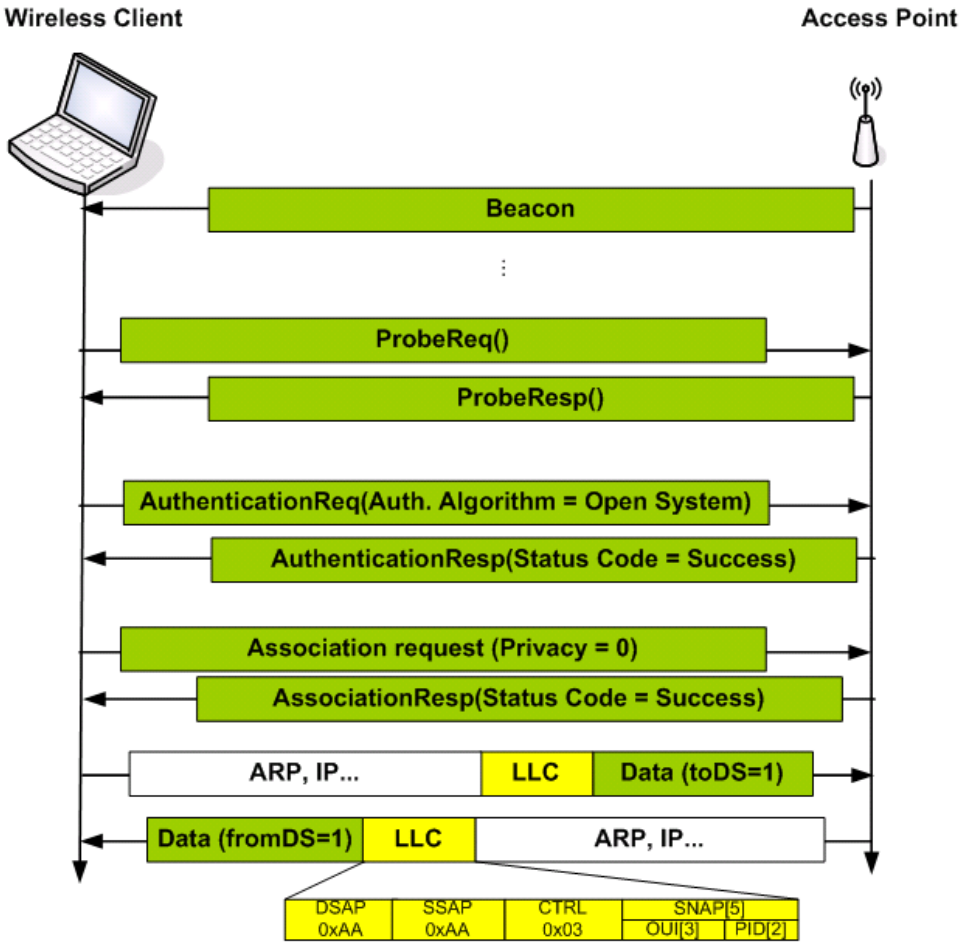
인증


탐색/Join
Status=0
Aut Transaction Seq = 1
Aut Alg Num=0
Aut. Req
802.11 MAC- ACK
인증
Aut. Response
Aut Alg Num=0
Aut Transaction Seq = 2
Status=Success
802.11 MAC- ACK
결합

결합

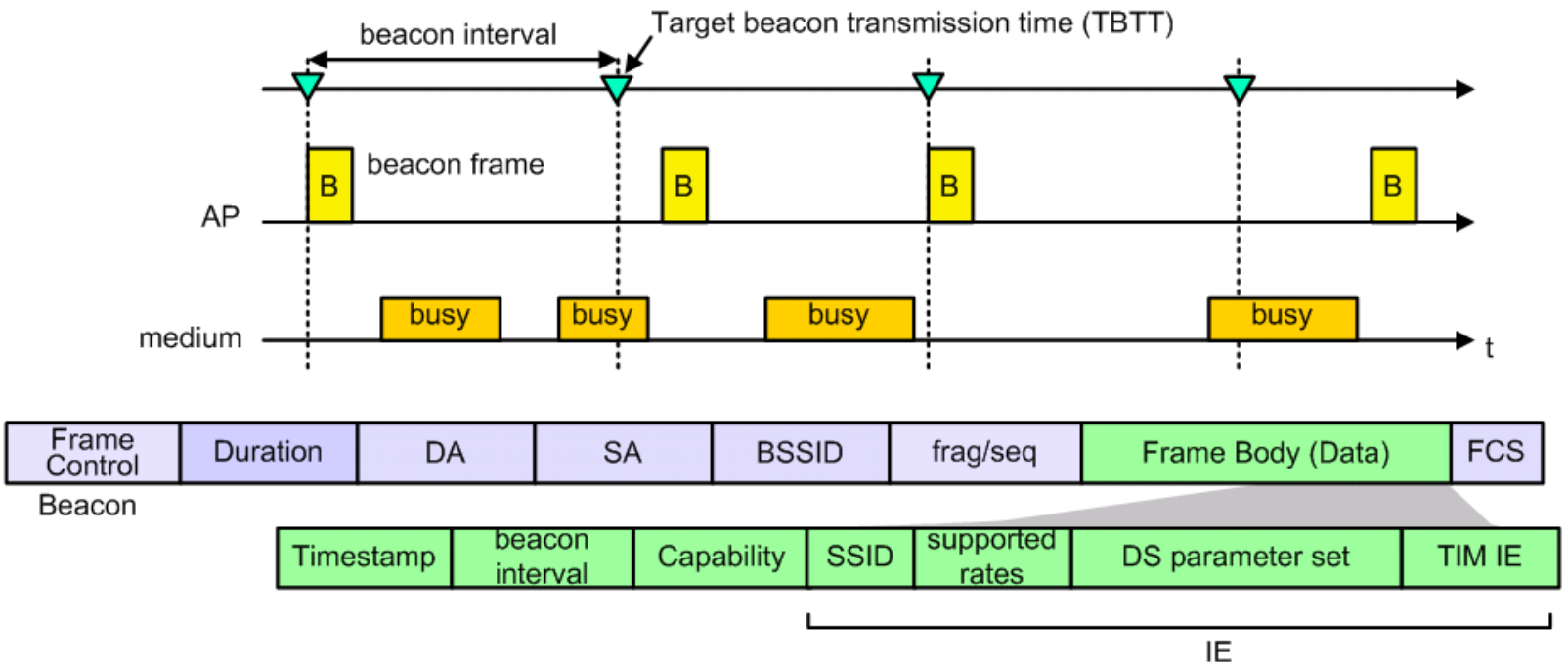

이동
해당단말에 할당한 AID삭제
Old AP
New AP
인증
Current AP = Old AP's MAC addr
Listen Inerval
ReAssoc. Req
802.11 MAC- ACK
ReAssoc. Response
AID = y
802.11 MAC- ACK
IAPP
저장된 것이 있으면, 중계해 주기 바람.
데이터 전송단계

절차분석

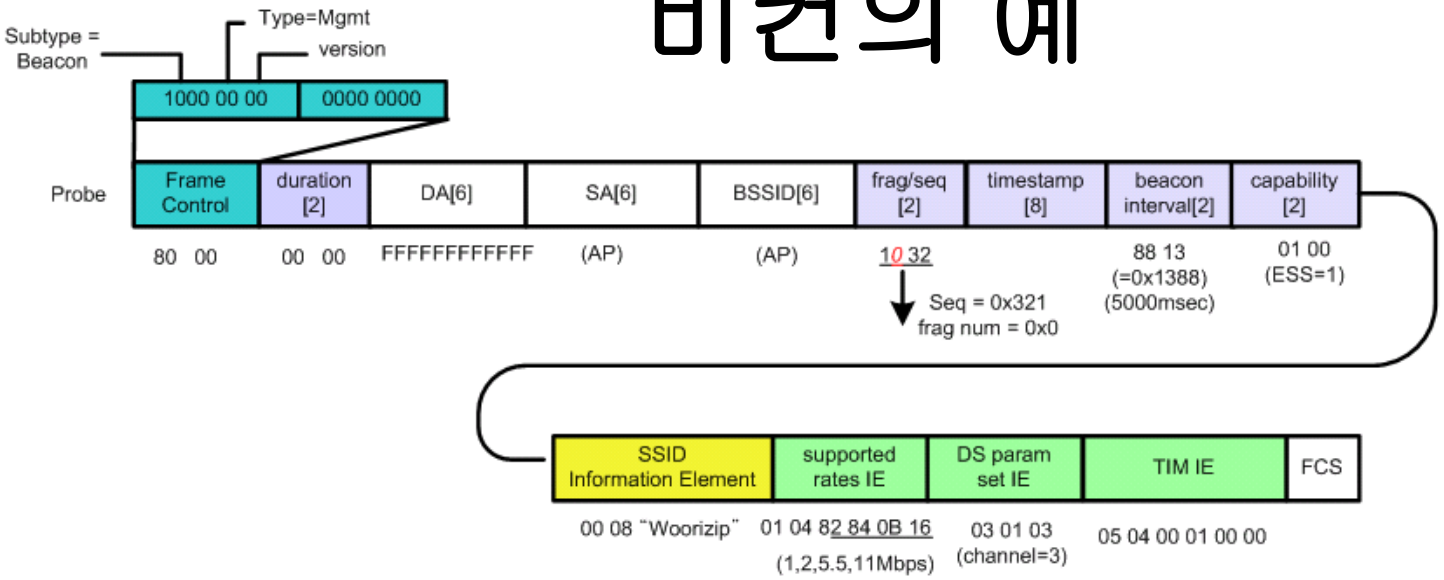


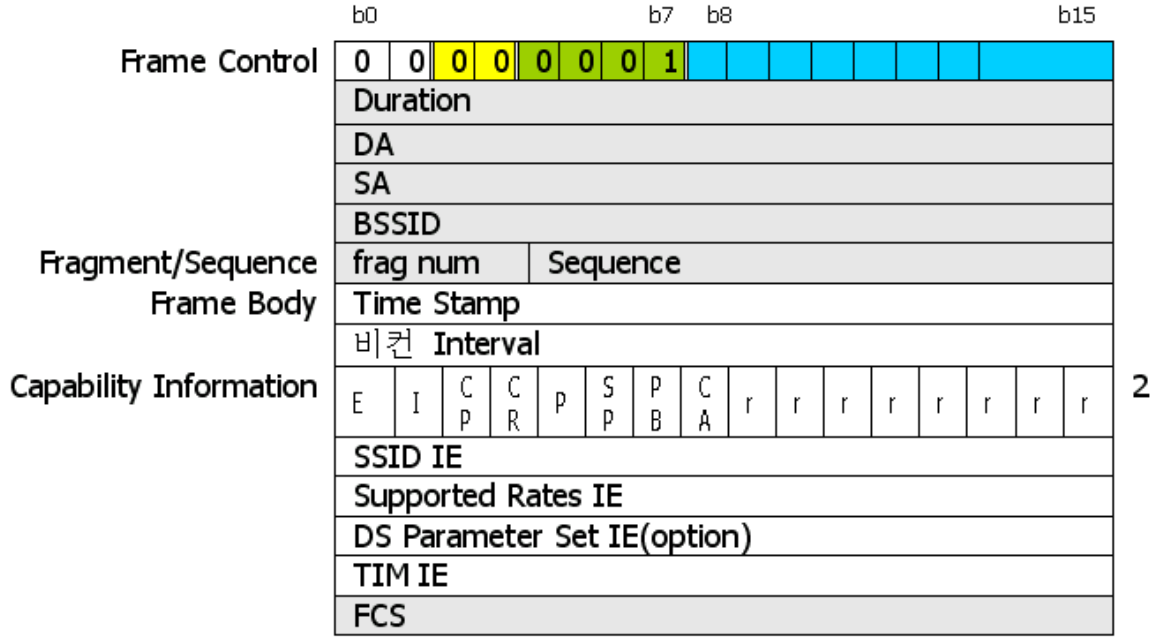
* DSAP = Destination Service Access Point (=0xAA)
* SSAP = Source SAP
* CTRL = Control Field (=0x03 = Unnumbered Information)
* SNAP = SubNetwork Access Protocol
* OUI = Organization Unique Identifier (000000 = IEEE802)
* PID = Protocol ID

비컨 프레임의 송신주기와 프레임의 구성의 예

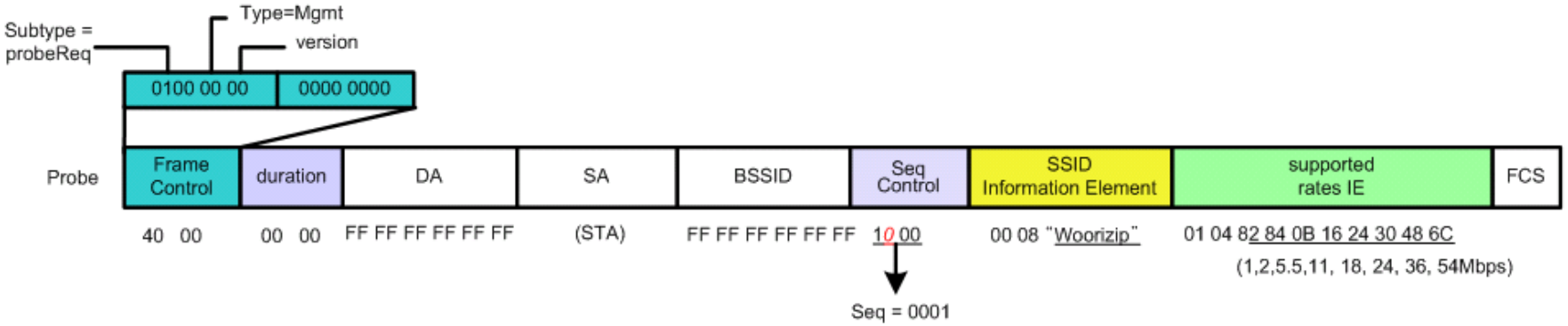


비컨의 예


Subtype = Beacon
Type=Mgmt
version
1000 00 00
0000 0000
Probe
Frame Control
duration [2]
DA[6]
SA[6]
BSSID[6]
frag/seq [2]
timestamp [8]
beacon interval[2]
capability [2]
80 00
00 00
FFFFFFFFFFFF
(AP)
(AP)
10 32
Seq = 0x321
frag num = 0x0
88 13
(=0x1388)
(5000msec)
01 00
(ESS=1)
SSID Information Element
supported rates IE
DS param set IE
TIM IE
FCS
00 08 "Woorizip"
01 04 82 84 0B 16
(1,2,5.5,11Mbps)
03 01 03
(channel=3)
05 04 00 01 00 00


b0
b7
b8
b15
Frame Control
0 0 0 0 0 0 0 1
Duration
DA
SA
BSSID
Fragment/Sequence
frag num
Sequence
Frame Body
Time Stamp
비컨 Interval
Capability Information
E I CP CR P SP PB CA r r r r r r r r
2
SSID IE
Supported Rates IE
DS Parameter Set IE(option)
TIM IE
FCS

프로브 요청 메시지의 예



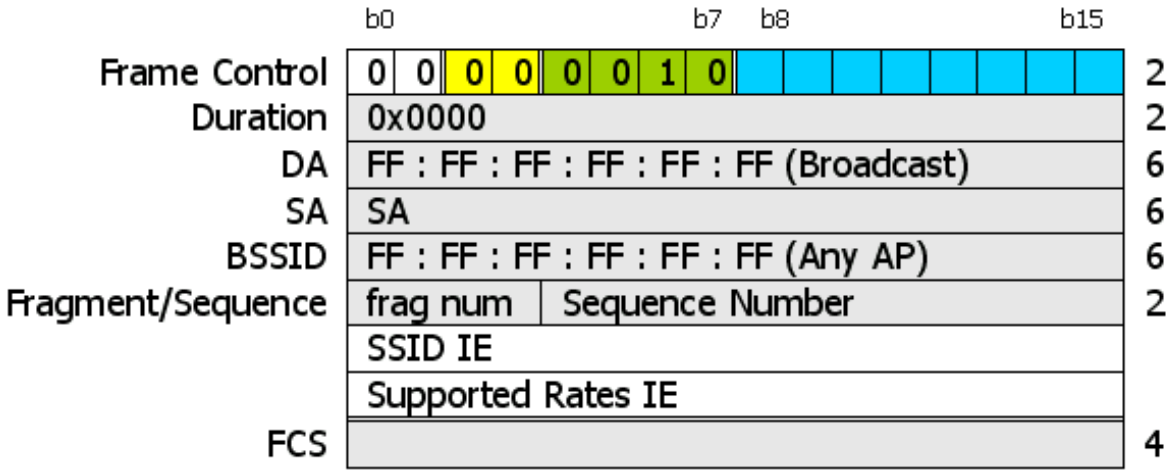
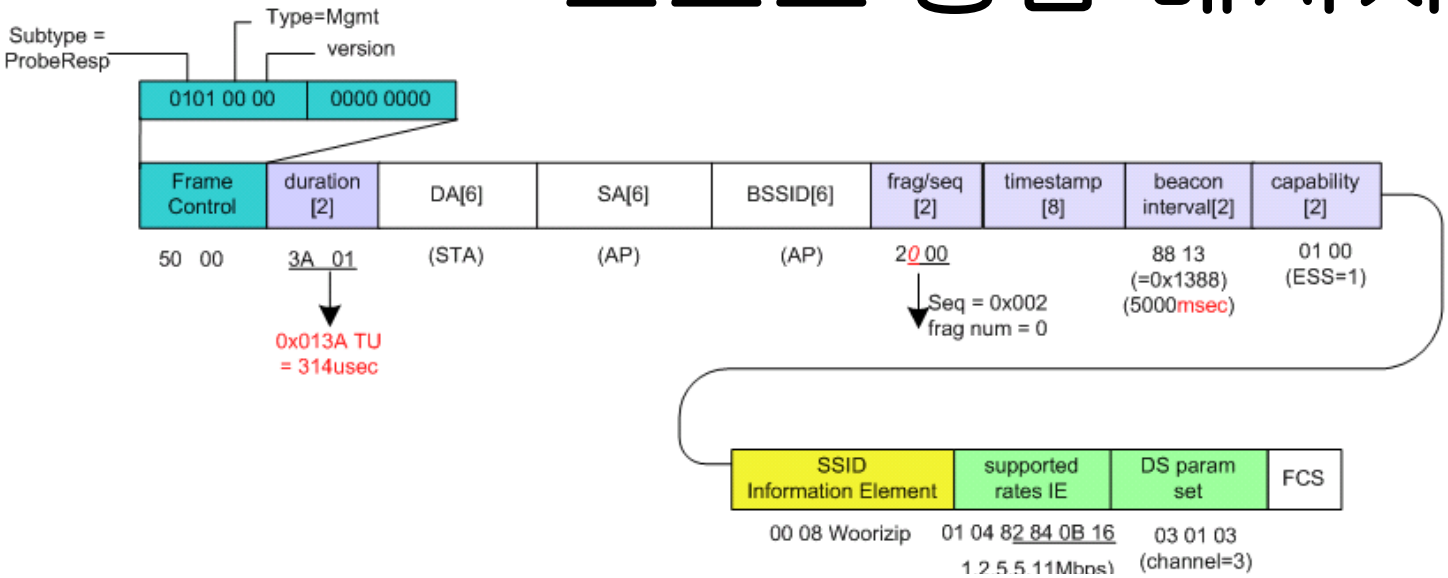


그림 2.36 프로브 요청 프레임의 구성

프로브 응답 메시지의 예



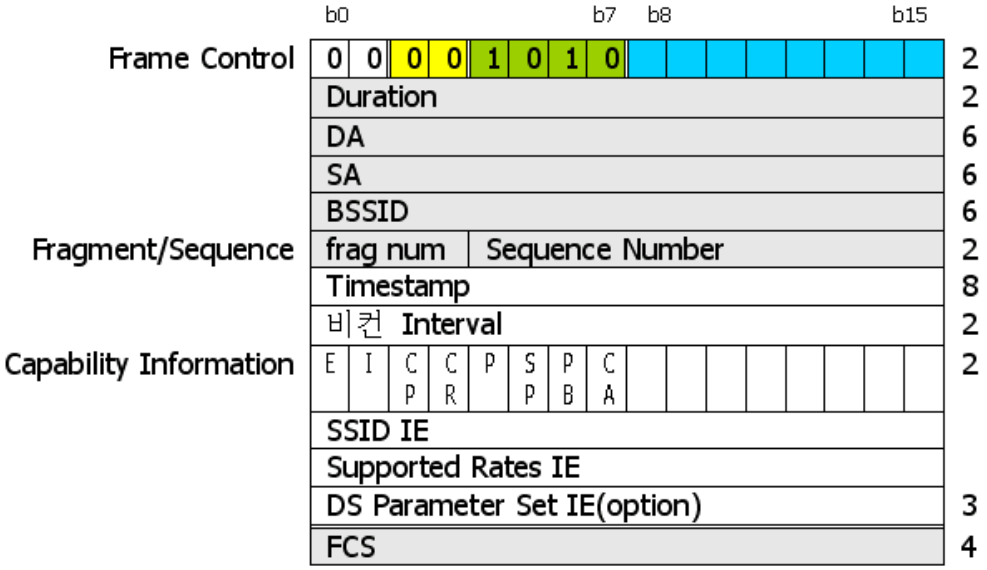


그림 2.37 프로브 응답 프레임의 구성

Authentication

- 요청/응답 복수용도

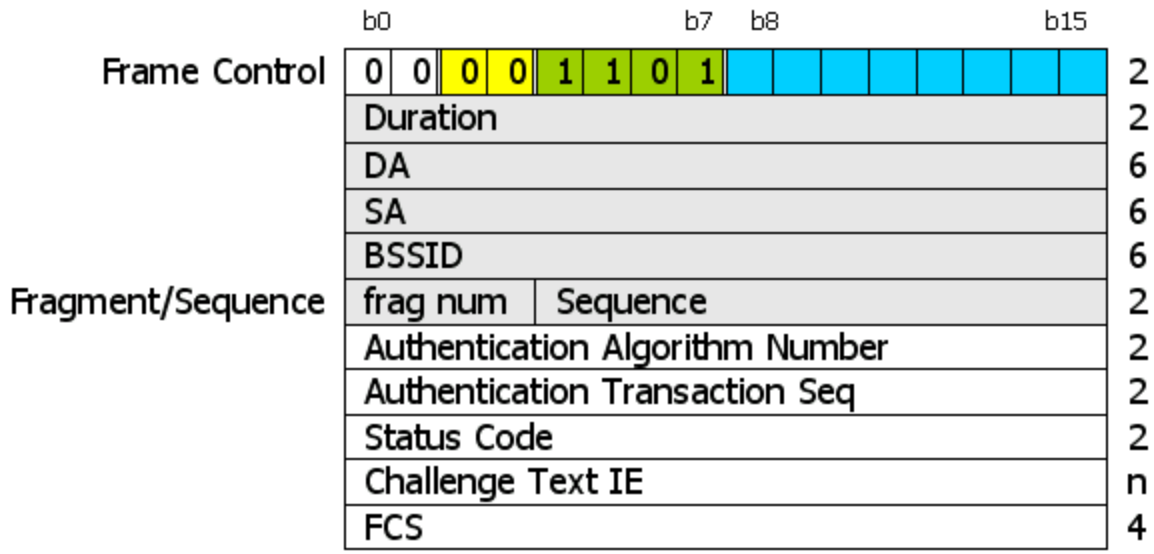


그림 2.38 인증 프레임의 구성

Assoc Req/Resp/Reassoc

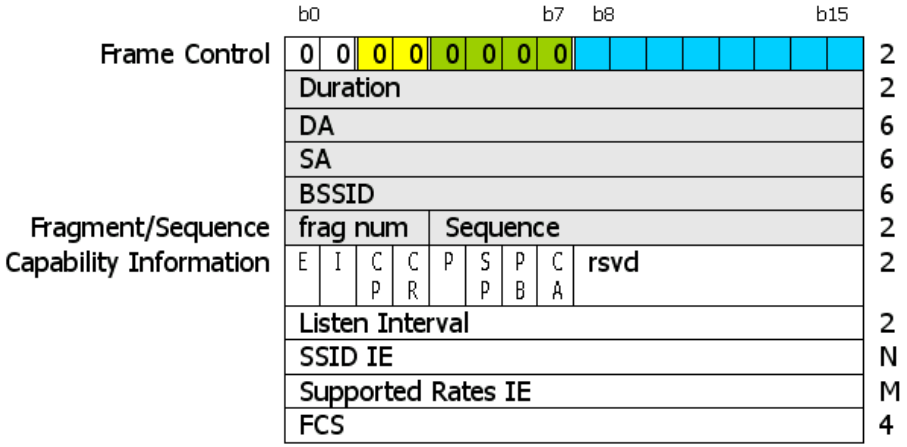


그림 2.39 결합 요청 프레임의 형식

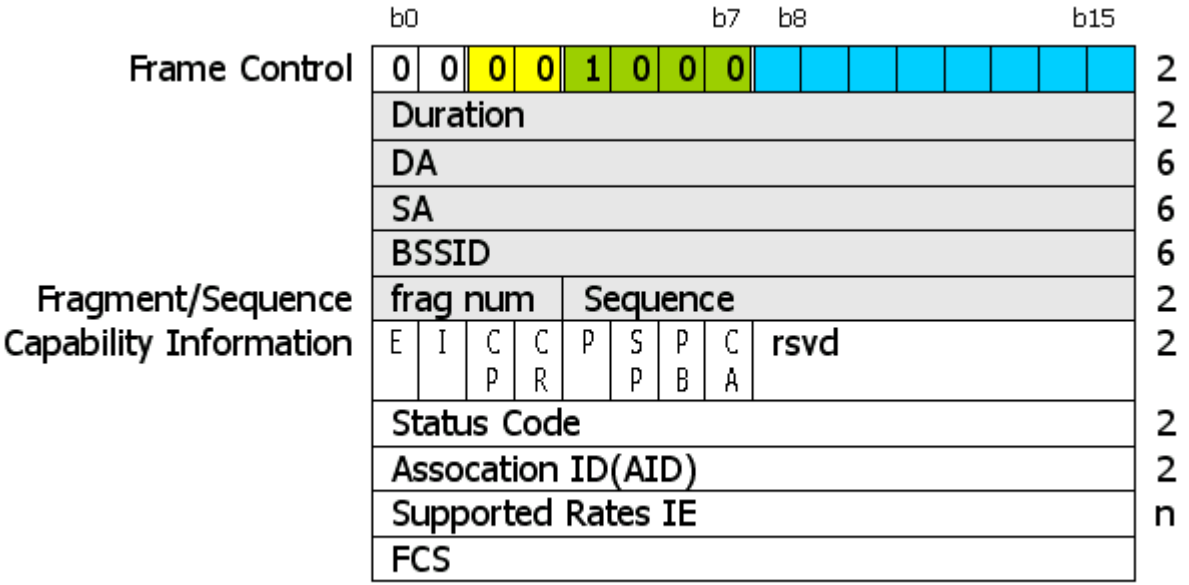
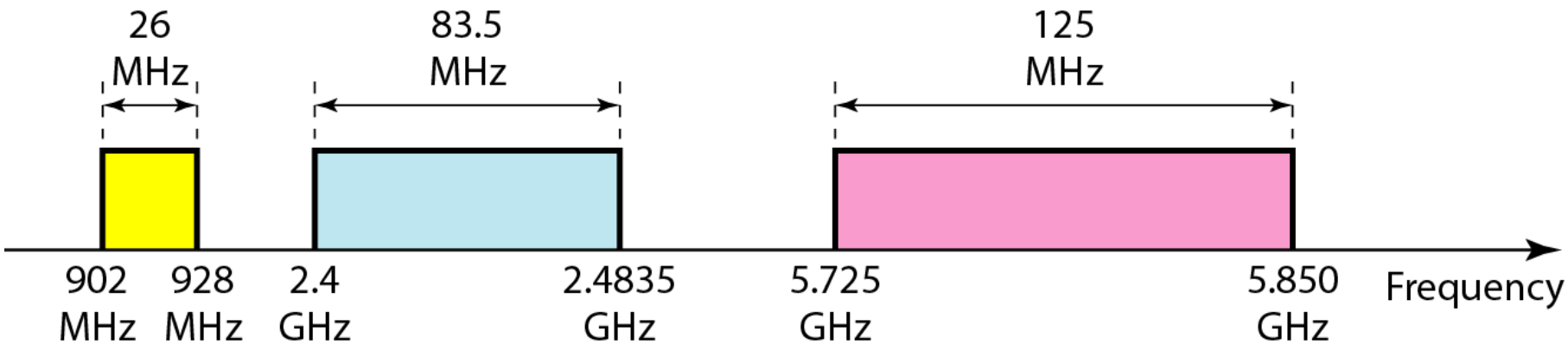


그림 2.40 결합/재결합 응답 프레임의 형식

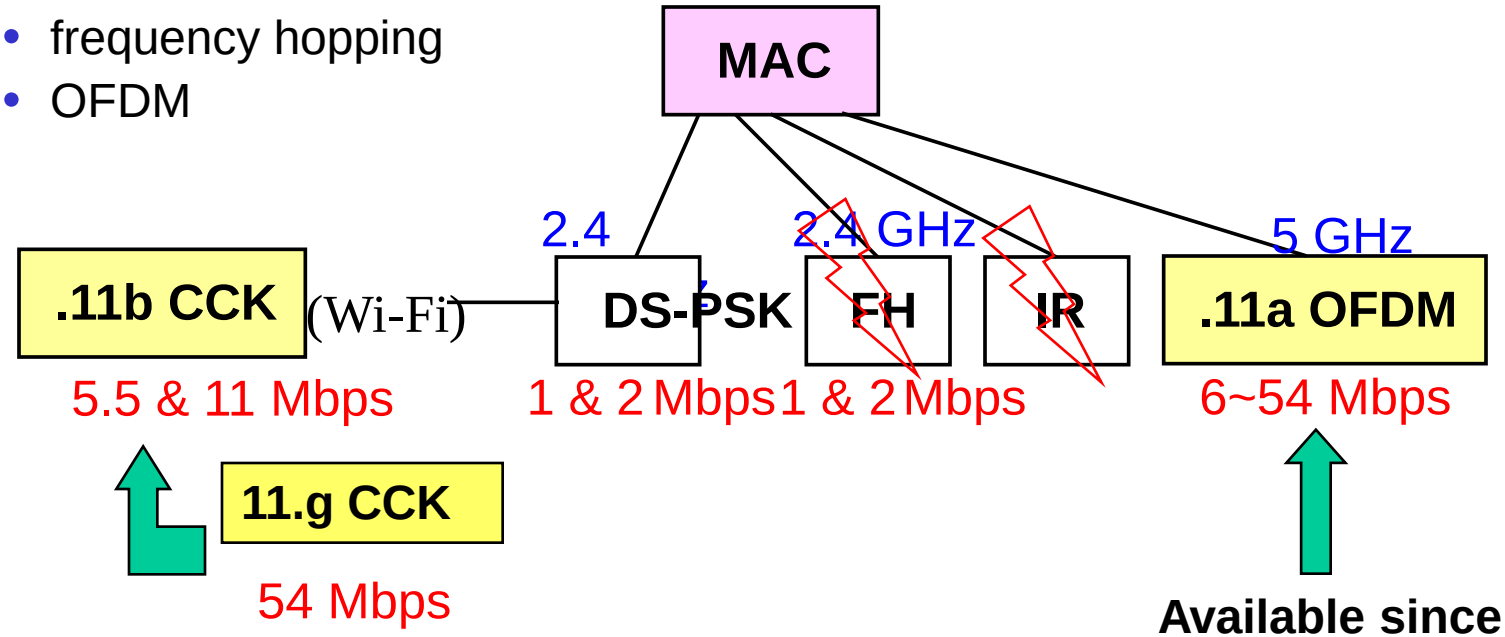
Physical Layer

Figure 14.14 *Industrial, scientific, and medical (ISM) band*



Transmission Mechanism

- **Radio frequency transmission**
  - **Spread spectrum transmission**
    - direct sequence
    - frequency hopping
    - OFDM



Cck: complementary code keying

- Infrared transmission
  - Laser diode sources
  - Light emitting diode sources

Figure 14.15 *Physical layer of IEEE 802.11 FHSS*

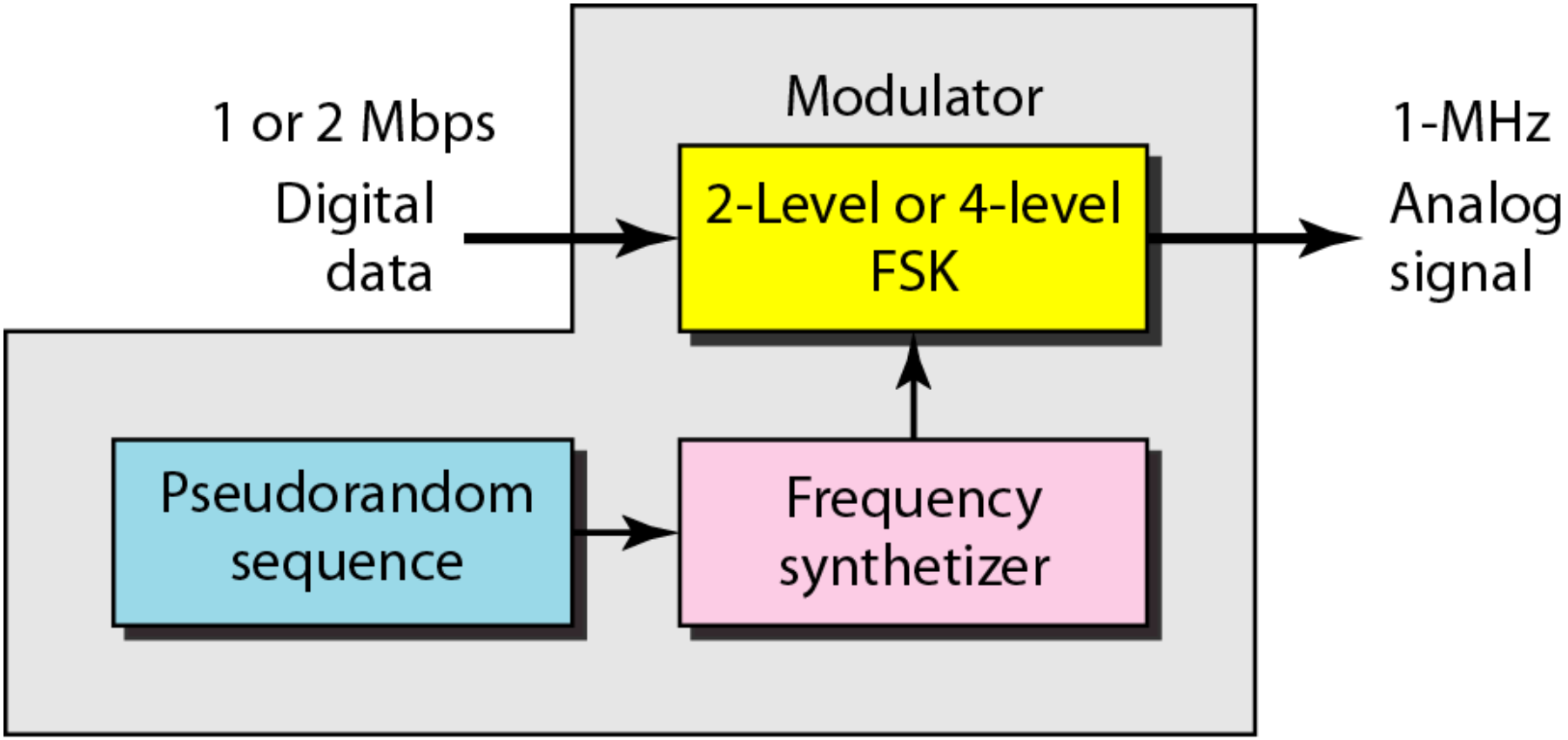


Figure 14.16 *Physical layer of IEEE 802.11 DSSS*

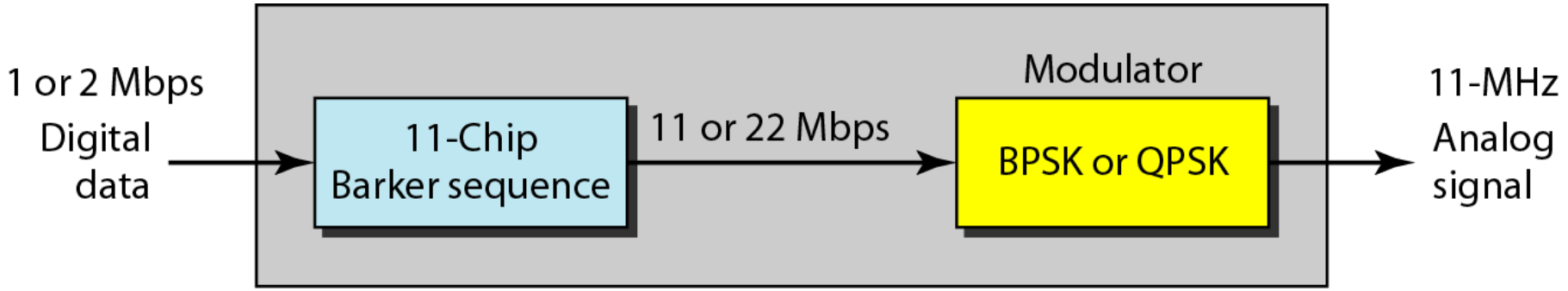


Figure 14.17 *Physical layer of IEEE 802.11 infrared*

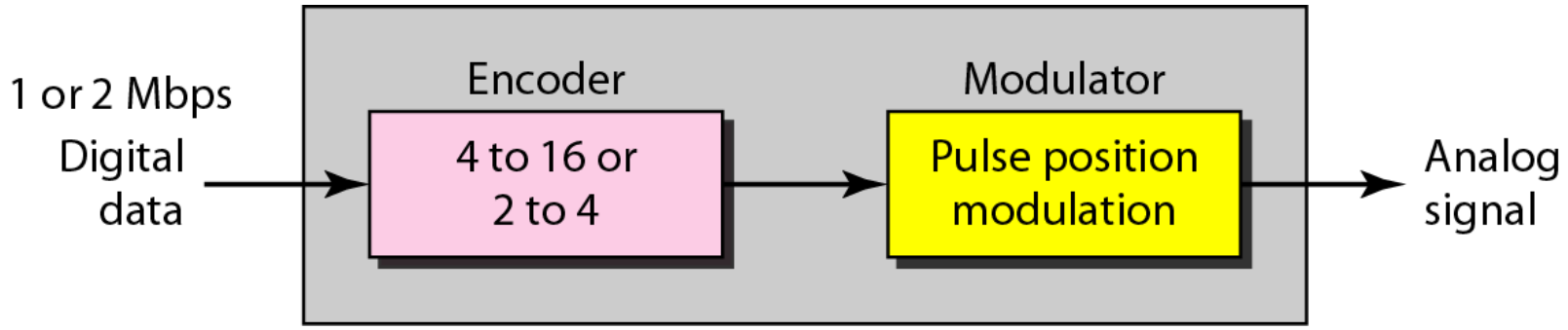
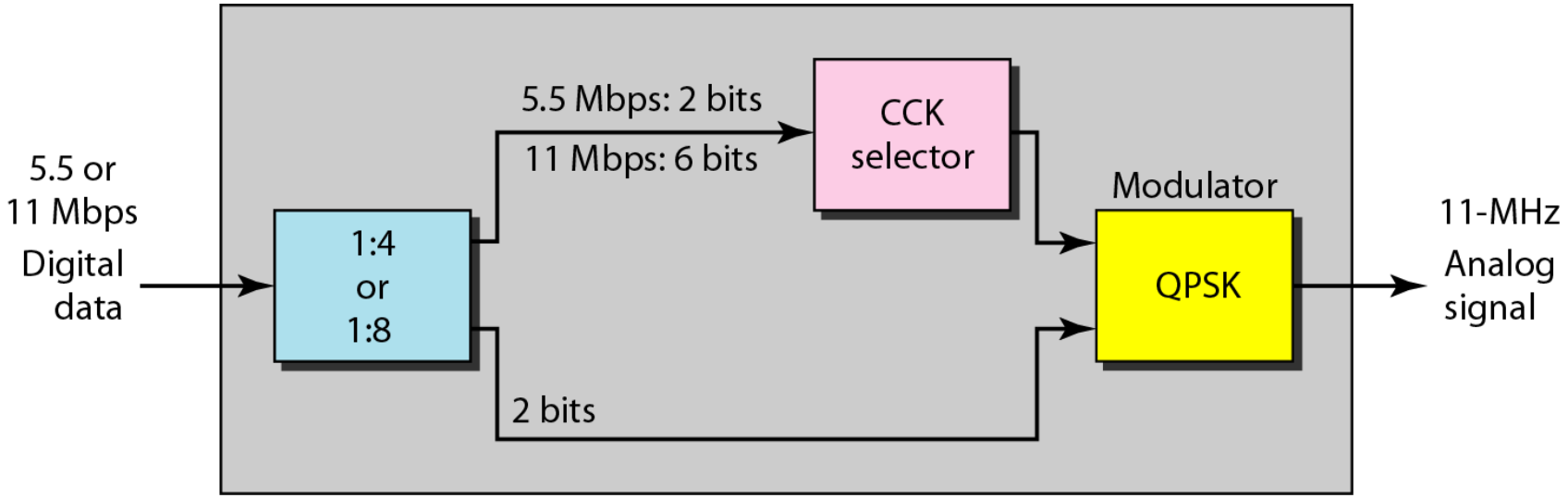


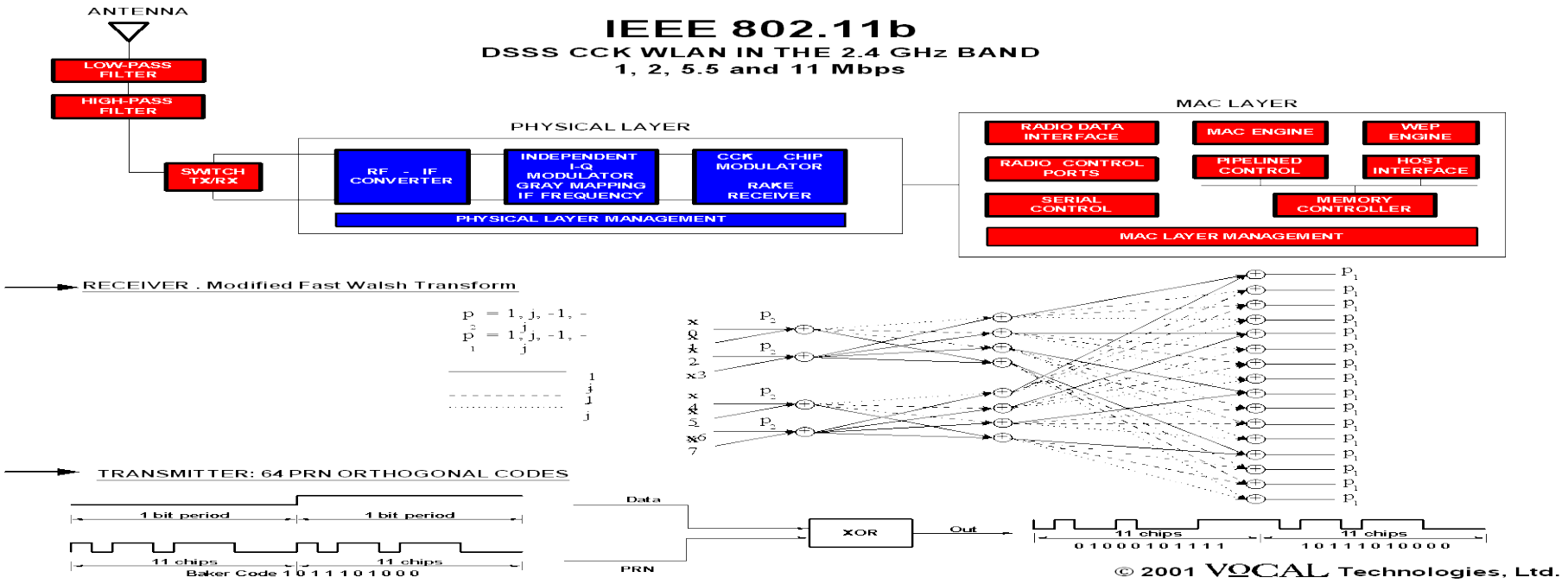
Figure 14.18 *Physical layer of IEEE 802.11b*



802.11 WLAN Physical layer Standards

	802.11b	802.11a	802.11g	802.11n
Standard Approved	Sept. 1999	Sept. 1999	June 2003	Dec 2009
Available Bandwidth	83.5 MHz	580 MHz	83.5 MHz	83.5/580 MHz
Frequency Band of Operation	2.4 GHz	5 GHz	2.4 GHz	2.4/5 GHz
# Non-Overlapping Channels (US)	3	24	3	3/24
Data Rate per Channel	1 – 11 Mbps	6 – 54 Mbps	1 – 54 Mbps	1 – 600 Mbps
Modulation Type	DSSS, CCK	OFDM	DSSS, CCK, OFDM	DSSS, CCK, OFDM, MIMO

802.11b System Model



Content of WLAN Technology

- **Spread Spectrum 원리**
  - **Direct Sequence SS**
  - **Frequency Hopping SS**
- **Medium access control technologies**
  - **PCF (point coordination function)**
    - Isochronous Traffic
  - **DCF (distributed coordination function)**
    - CSMA/CA
- **Physical layer technologies (802.11, 802.11a/b/g)**
  - **Architecture**
  - **Transmission Media & Signal**
  - **Frame Formats**

Spread Spectrum

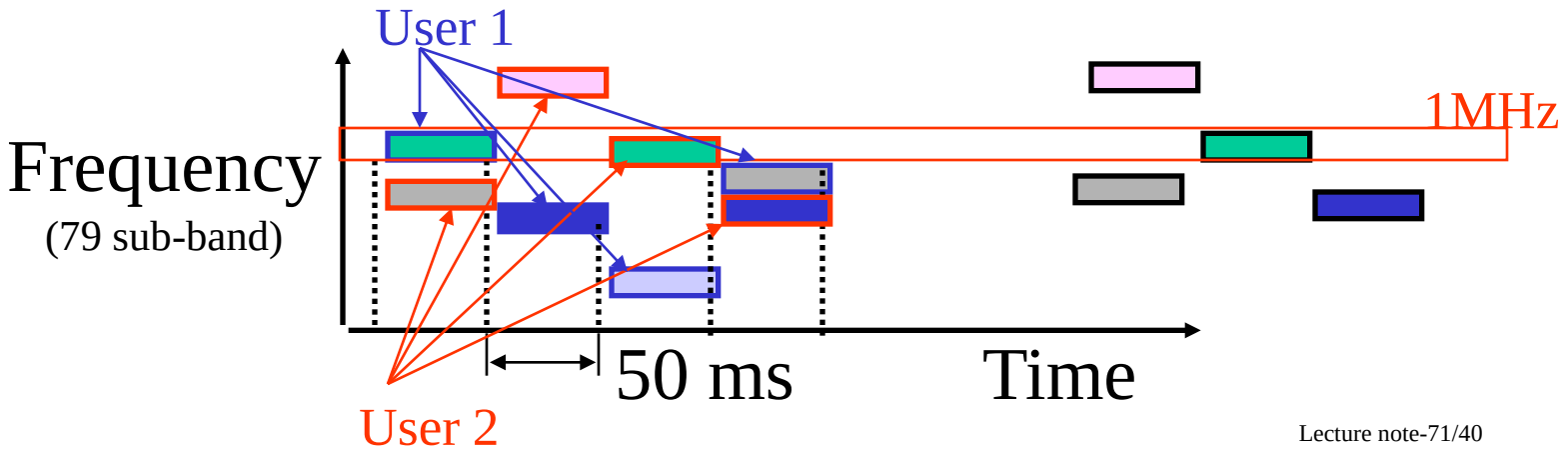
- **Modulates a wide band of frequencies**
- **Frequency hopping**
  - **Modulates a subband of the spectrum for a while then moves on and modulates another subband**
- **Direct sequence**
  - **Chipping sequence transmitted at a signaling rate much faster than the bit rate**

FH-SS

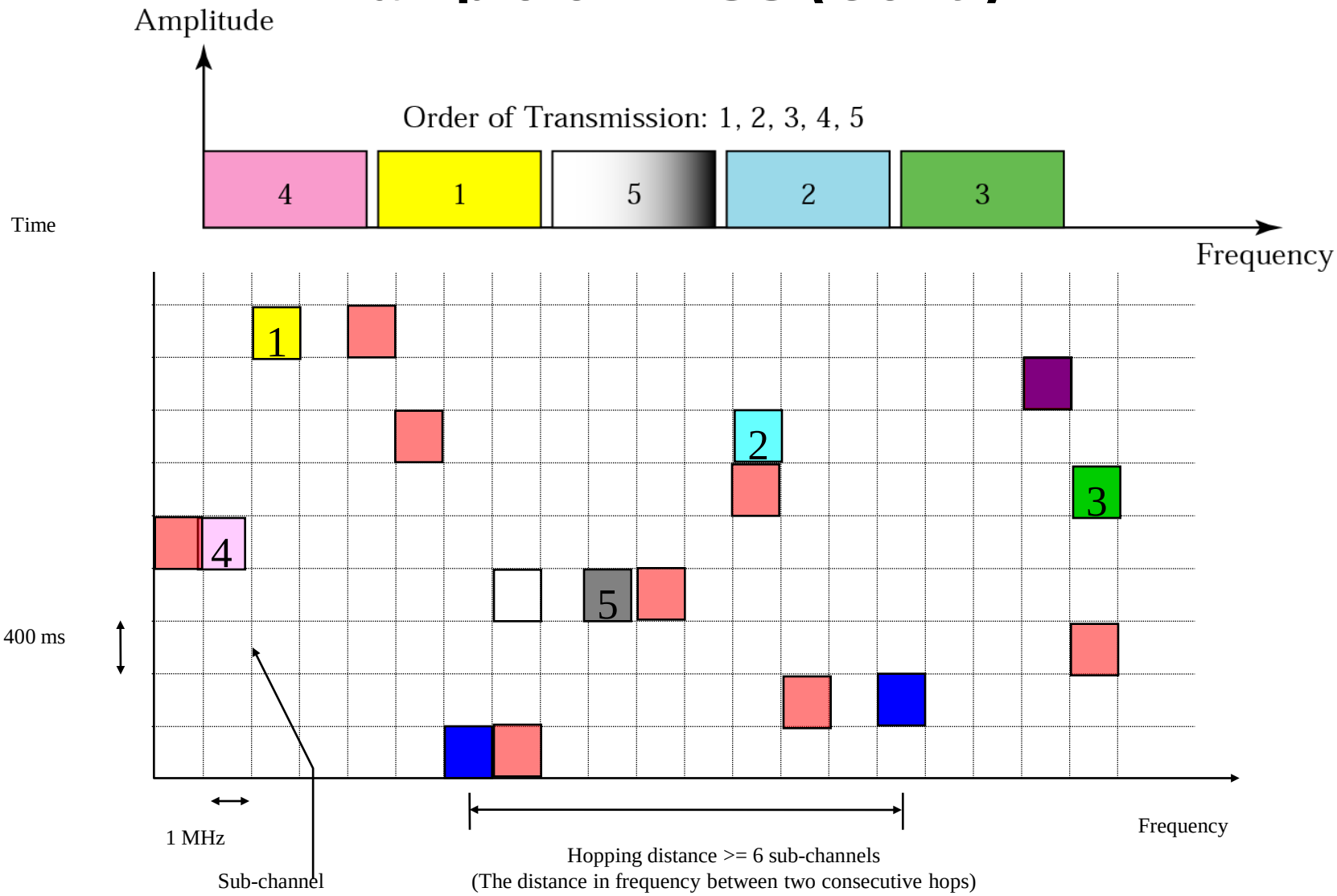
- **Transmitter uses pseudorandom sequence of carrier frequencies**
  - **Sequences are designed so that they interfere minimally with each other**
  - **Each frequency subband is 1 MHz wide**
  - **78 frequencies between 2.402 and 2.480 GHz**
  - **Minimum hop distance is 6 MHz**
- **Transmitter hops at rate of at least 2.5 hops per second**
- **2-level Gaussian Frequency Shift Keying (GFSK)**
  - **$F_c + f_d$ = logic 1**
  - **$F_c - f_d$ = logic 0**

FHSS

- Frequency-hopping Spread Spectrum (FHSS)
- Band 2400-2483.5 MHz: industrial, scientific, and medical
  - Divided into 79 sub-band channels of the 83 are used
  - Sub-channels of 1 MHz
- GFSK (Gaussian Frequency Shift Keying)
  - Two-level FSK or Four-level FSK : 1 or 2 bits/baud
- Slow hopping
- 3 main sets each with 26 different hopping sequences

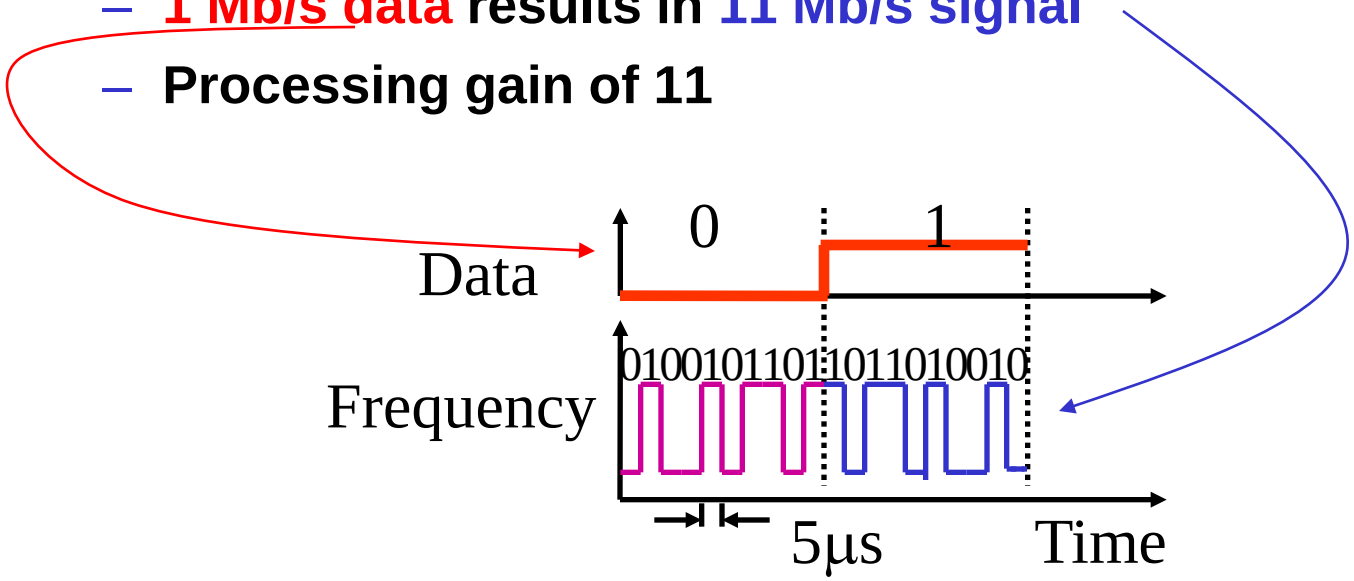


Example of FHSS (Cont.)

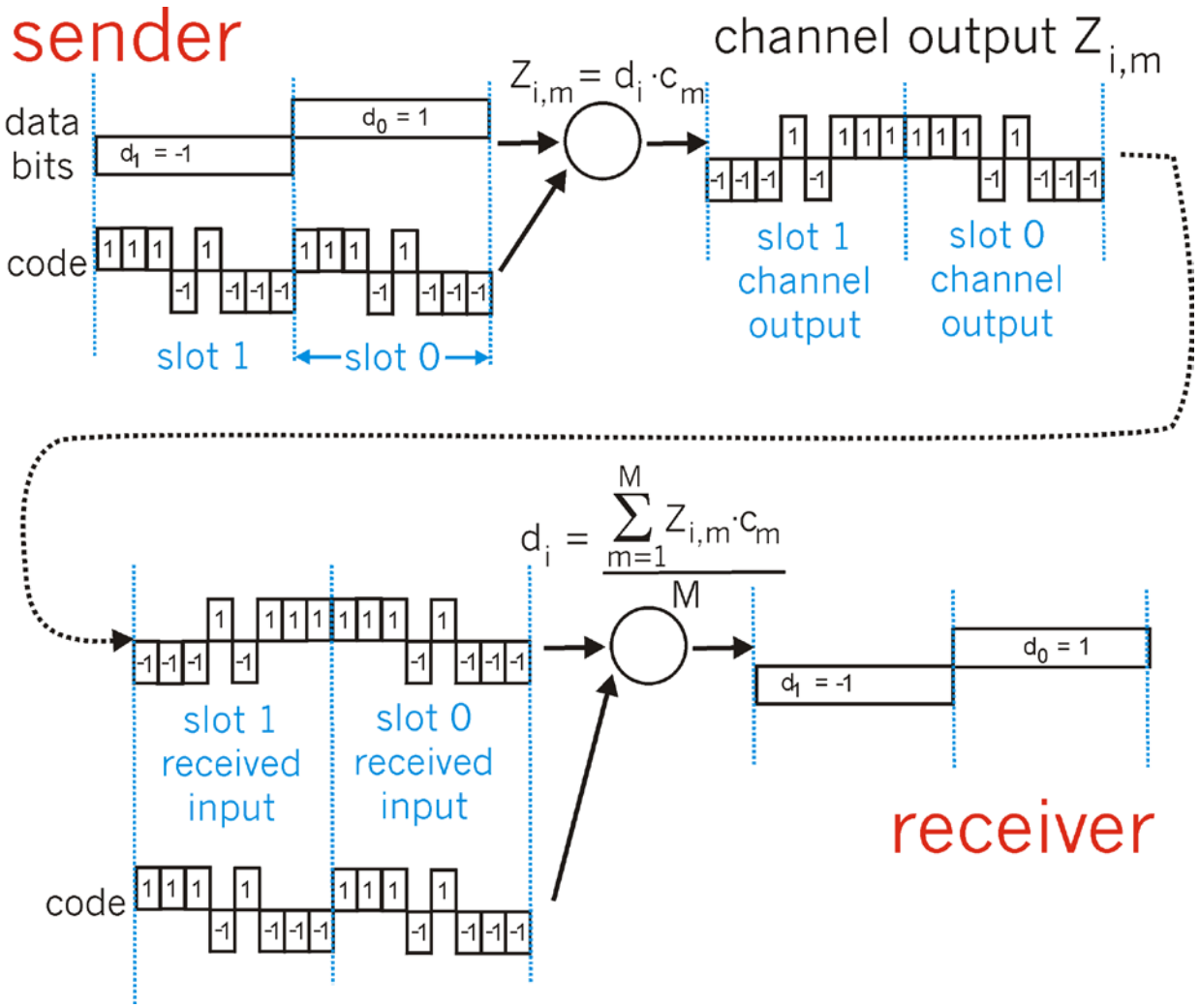


DS-SS

- Direct Sequence Spread Spectrum (DSSS)
- **Data stream is added (mod 2) to chipping (spreading) sequence of a higher rate**
- **Modulated data has much higher rate**
- **11-chip Barker sequence**
  - **+1,-1,+1,+1,-1,+1,+1,+1,-1,-1,-1**
  - **1 Mb/s data results in 11 Mb/s signal**
  - **Processing gain of 11**



Example of DS-SS Encode/Decode



IEEE 802.11a

- **OFDM (Orthogonal Freq. Div. Multiplexing)**
- **5 GHz (5.15-5.25, 5.25-5.35, 5.725-5.825GHz)**
- **52 Subcarriers**
  - 48 subbands for sending 48 groups of bits at a time
  - 4 subbands for control information
- **BPSK/QPSK(18 Mbps)/QAM(54Mbps)**
- **Forward Error Correction (Convolutional)**
- **Rates: 6, 9, 12, 18, 24, 36, 48, 54 Mbps**

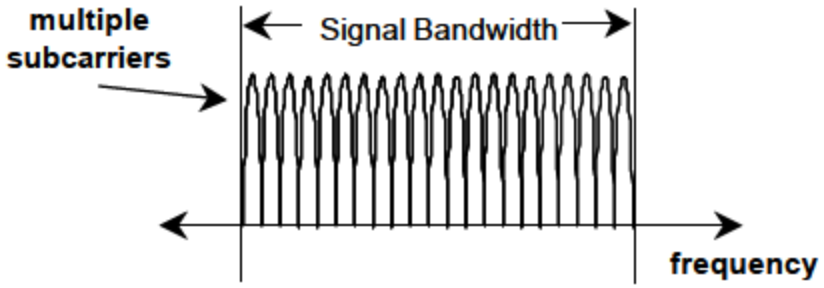
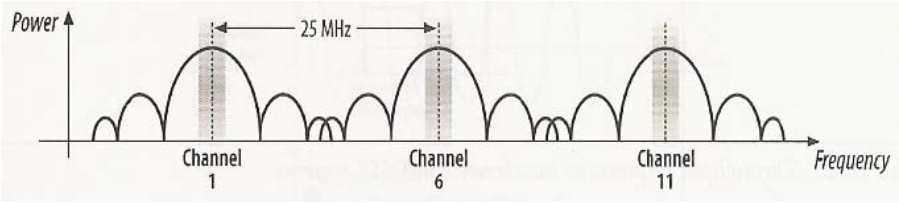
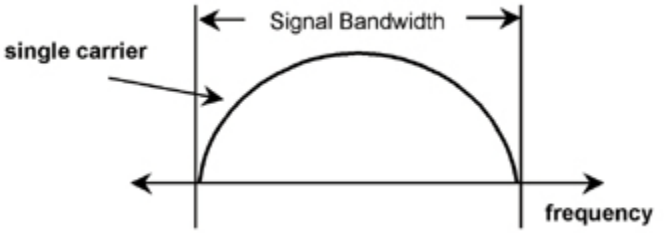


Figure 5 OFDM Systems Transmit Data on Multiple "Subcarriers"

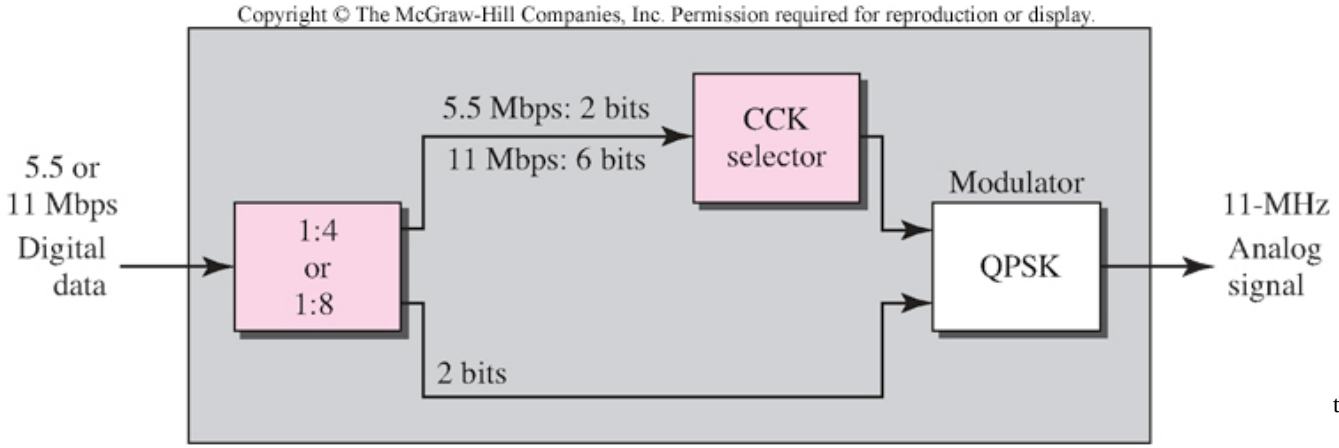
IEEE 802.11b

- **HR-DSSS: High rate DSSS (11-chip)**
- **2.4 GHZ band**
  - 11 22MHz channels
- **M-arry modulation.**
- **Convolutional Codes**
  - CCK (complementary Code Keying) encodes 4 or 8 bits to one CCK symbol
    - **5.5Mbps = 4bits*1.375Mbps (BPSK)**
    - **11Mbps = 8bits*1.375Mbps (QPSK)**
- **Rates 1, 2, 5.5 and 11 Mbps**
- **Shorter Preamble**





CCK is a 'single-carrier' modulation format

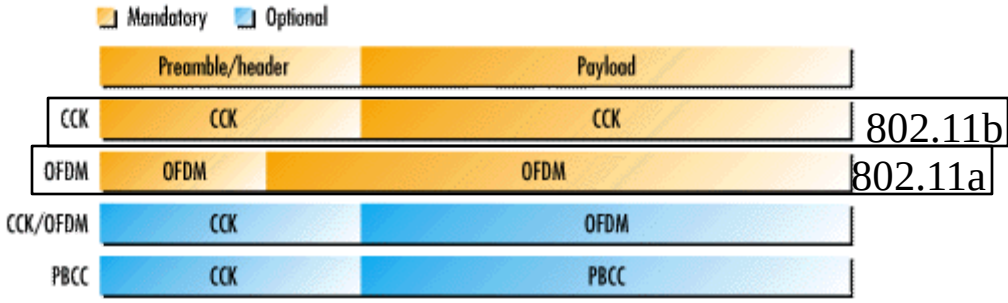


IEEE 802.11g

- **OFDM (Orthogonal Freq. Div. Multiplexing)**
- **2.4 GHz**
- **52 Subcarriers**
  - 48 subbands for sending 48 groups of bits at a time
  - 4 subbands for control information
- **BPSK/QPSK(18 Mbps)/QAM(54Mbps)**
- **Forward Error Correction (Convolutional)**
- **Rates: 6, 9, 12, 18, 24, 36, 48, 54 Mbps**

802.11g Data Rates, Transmission Types, and Modulation Schemes

Data Rate (Mbps)	Transmission Type	Modulation Scheme
54	OFDM	64 QAM
48	OFDM	64 QAM
36	OFDM	16 QAM
24	OFDM	16 QAM
18	OFDM	QPSK1
12	OFDM	QPSK
11	DSSS	CCK2
9	OFDM	BPSK3
6	OFDM	BPSK
5.5	DSSS	CCK
2	DSSS	QPSK
1	DSSS	BPSK



The elements of the IEEE 802.11g draft standard differ in packet format. The only mandatory modes are complementary code keying (CCK) for backward compatibility with existing 802.11b radios and orthogonal frequency division multiplexing (OFDM) for higher data rates. Developers can choose two optional elements, CCK/OFDM and packet binary convolutional coding (PBCC).

IEEE 802.11 etc

– http://www.cwnp.com/course/80211n/sample/

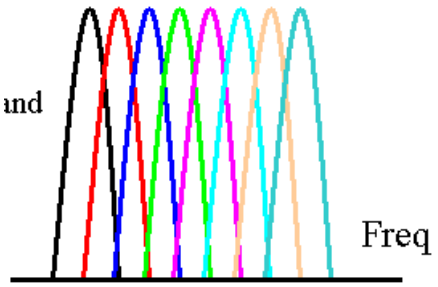
Project	Task Group	Chartered - Task	Target Date
802.11k	TGk	Radio Resource Management	Mar 08
802.11mb	TGmb	Maintainence	Mar 11
802.11n	TGn	High Throughput	Dec 09
802.11p	TGp	Wireless Access Vehicular Environment	Dec 09
802.11r	TGr	Fast Roaming	June 08
802.11s	TGs	ESS Mesh Networking	Dec 09
802.11t	TGt	Wireless Performance	Dec 09
802.11u	TGu	Interworking with Exterenal Networks	Sept 09
802.11v	TGv	Wireless Network Management	Dec 09
802.11w	TGw	Protected Management Frames	Mar 09
802.11y	TGy	3650-3700 Operation in US	June 08
TBD	DLS-SG	Direct Link Setup Study Group	TBD
TBD	VHT-SG	1Gbps Very High Throughput Study Group	TBD
TBD	QSE-SG	QoS Extensions Study Group	TBD
Ad-Hoc	WNG	Wireless Next Generation	-
TBD	IMT-AdHoc	International Mobile Communications Advanced	TBD

11n Technology

- **Uses multiple input multiple output antenna (MIMO)**
- **Data rate and range are enhanced by using spatial multiplexing (N antenna pairs) plus antenna diversity**
- **Occupies one WLAN channel, and in compliance with 802.11**
- **Backwards compatible with 802.11 a,b,g**
- **One access point supports both standard WLAN and MIMO devices**

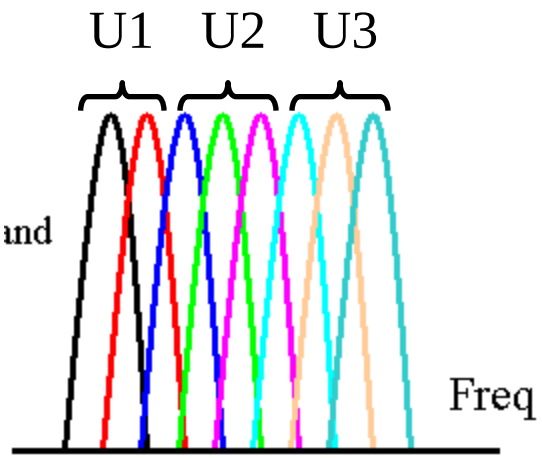
OFDM

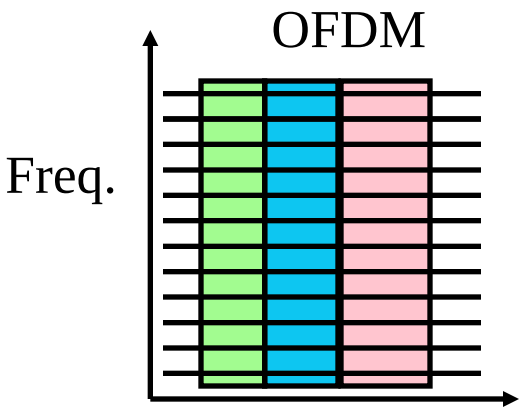
- **Orthogonal Frequency Division Multiplexing**
- **Ten 100 kHz channels are better than one 1 MHz Channel**
  ⇒ Multi-carrier modulation
- **Frequency band is divided into 256 or more sub-bands. Orthogonal ⇒ Peak of one at null of others**
- **Each carrier is modulated with a BPSK, QPSK, 16-QAM, 64-QAM etc depending on the noise (Frequency selective fading)**
- **Used in 802.11a/g, 802.16, Digital Video handheld (DVB-H)**



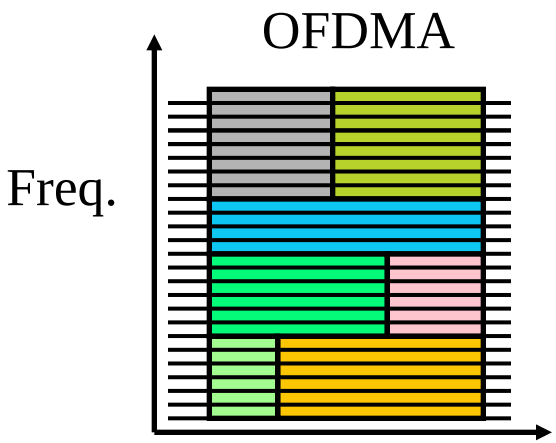
OFDMA

- **Orthogonal Frequency Division Multiple Access**
  - **OFDM is a modulation scheme OFDMA is a modulation and access scheme**
- **Each user has a subset of subcarriers for a few slots**
- **OFDM systems use TDMA**
- **OFDMA allows Time+Freq DMA ⇒ 2D Scheduling**





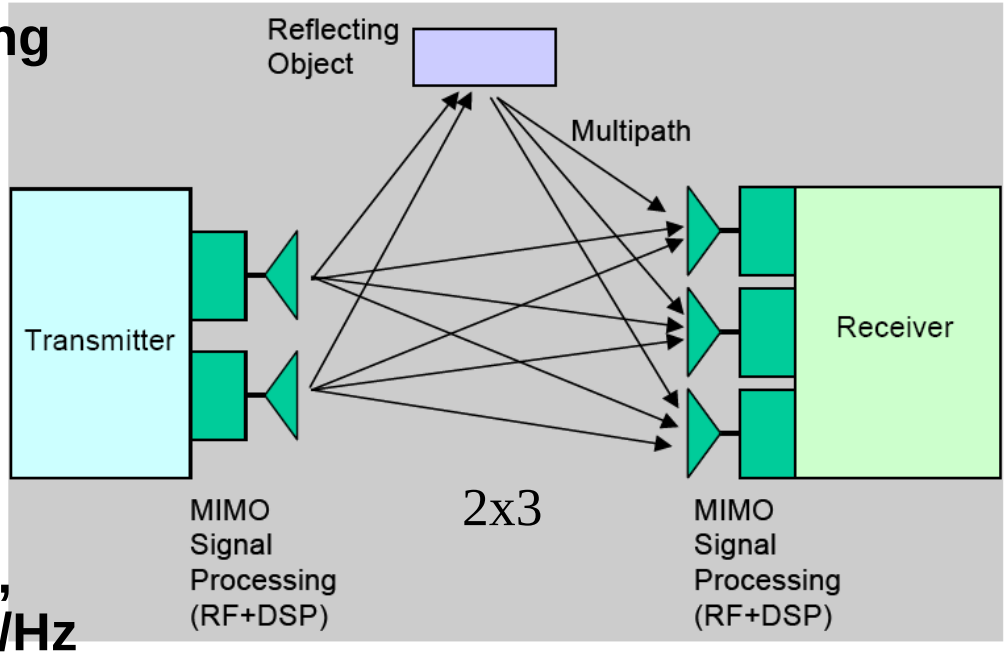
Frequency allocation per user is continuous vs. time



Frequency per user is dynamically allocated vs. time slots

MIMO← Multiple Antenna Techniques

- **Multiple Input Multiple Output →Simultaneous reception or transmission of multiple streams**
- **Multipath**
  - **Space-division multiplexing**
    - Split the data stream
    - – spatial stream
- **Four data streams**



- **54 Mbps/20 MHz = 2.7 bps/Hz, MIMO ⇒ 108 Mbps or 5.4 bps/Hz**

Issues with Wireless LANs

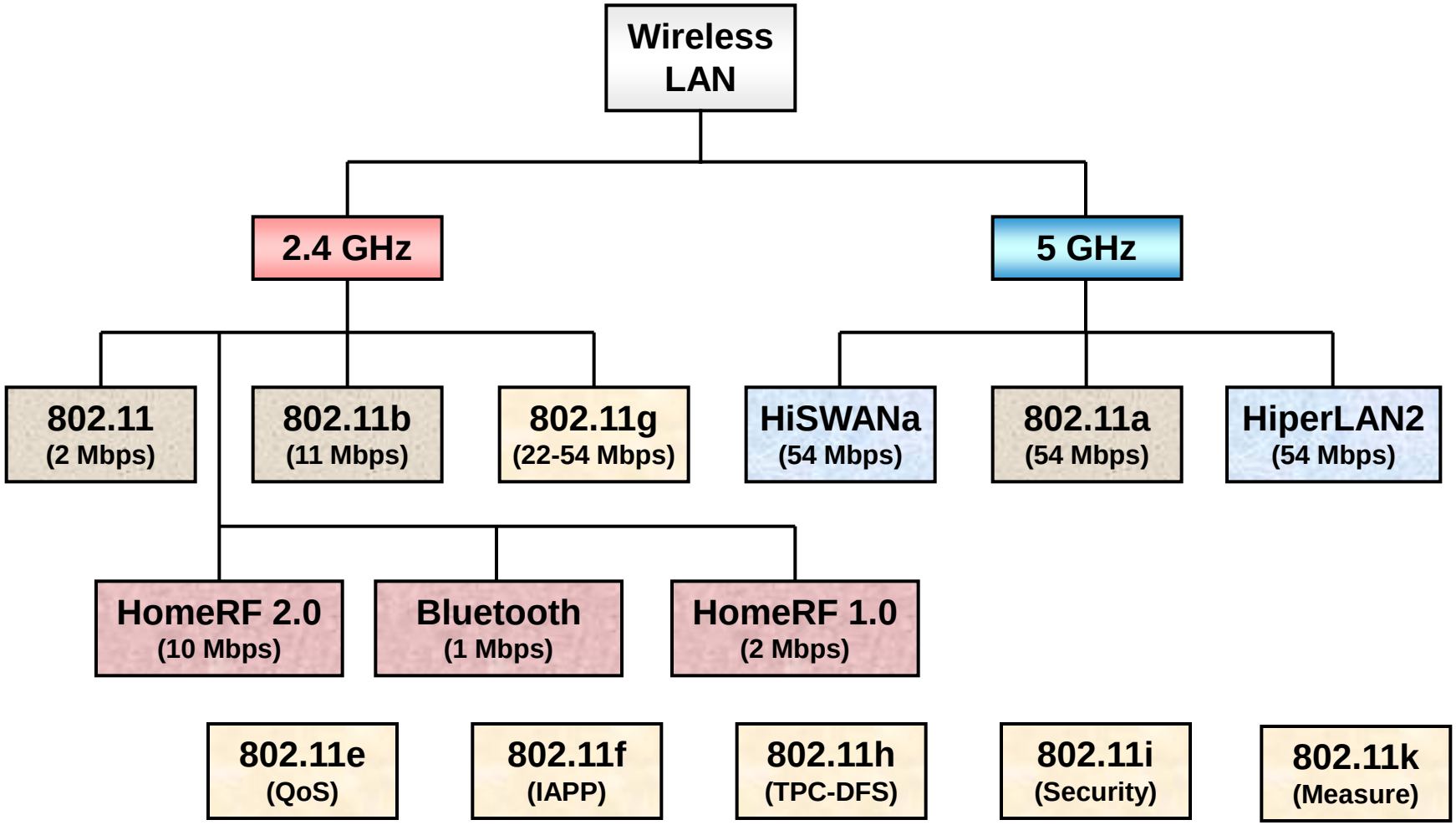
- IEEE 802.11 Standards
- Hidden Station Problem
- Spectrum management
- Access control and security
- Network Attachment (Mobility)

Hot Research Topics

- **Power control increases spatial reuse**
  - **Whisper in the room so that many people can talk**
- **Rate control based on channel quality**
- **Expolit channel diversity**
  - **Utilize multiple channels to parallelize dialogs**
- **Exploit spatial diversity**
  - **Use directional antennas to interfere over smaller region**

… and many more topics

Wireless Standards



IEEE 802.11

	802.11a	802.11b	802.11
Standard approved	Sep. 2002	Sep. 1999	July 1997
Available bandwidth	300 MHZ	83.5 MHZ	83.5 MHZ
Unlicensed freq. of operation	5.15-5.35G 5.725-5.825G	2.4-2.4835G	2.4-2.4835G
No. of non-overlapping Ch.	4	3	3
Rate per channel	6,9,12,18,24,36,48, 54 Mbps	1, 2, 5.5, 11 Mbps	1,2 Mbps
Range	225 feet	225 feet	??
Modulation	OFDM	DSSS	DSSS, FHSS

DSSS: direct sequence spread spectrum

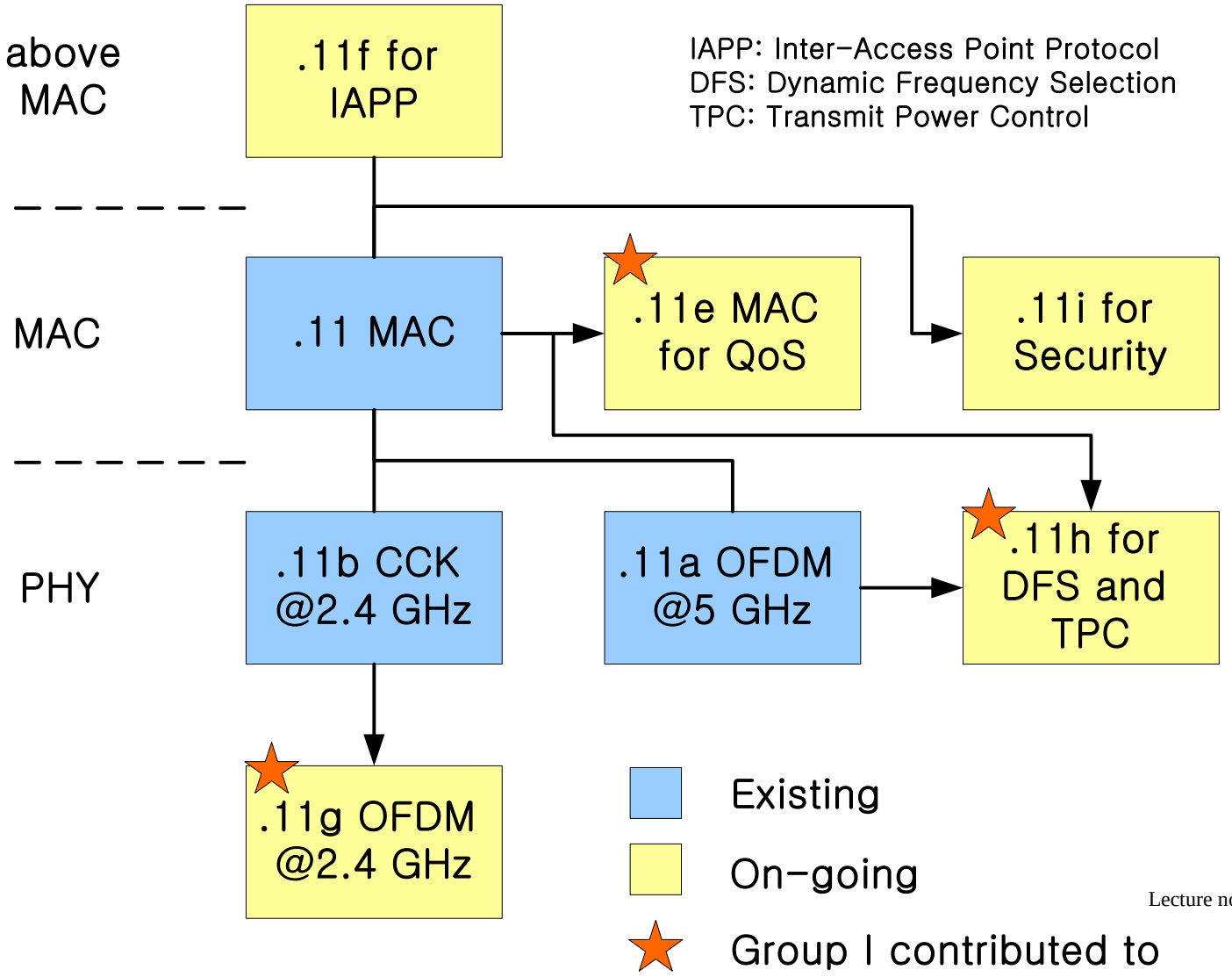
FHSS: frequency hopping spread spectrum

OFDM: orthogonal frequency division multiplexing

Higher Speeds?

- **IEEE 802.11a**
  - **compatible MAC, but now 5.8 GHz ISM band**
  - **transmission rates up to 50 Mbit/s**
  - **close cooperation with BRAN (ETSI Broadband Radio Access Network)**

802.11 Standards Expected in 2003



14-2 BLUETOOTH

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers, coffee makers, and so on. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously.

Topics discussed in this section:

Architecture
Bluetooth Layers
Baseband Layer
L2CAP

Figure 14.19 *Piconet*

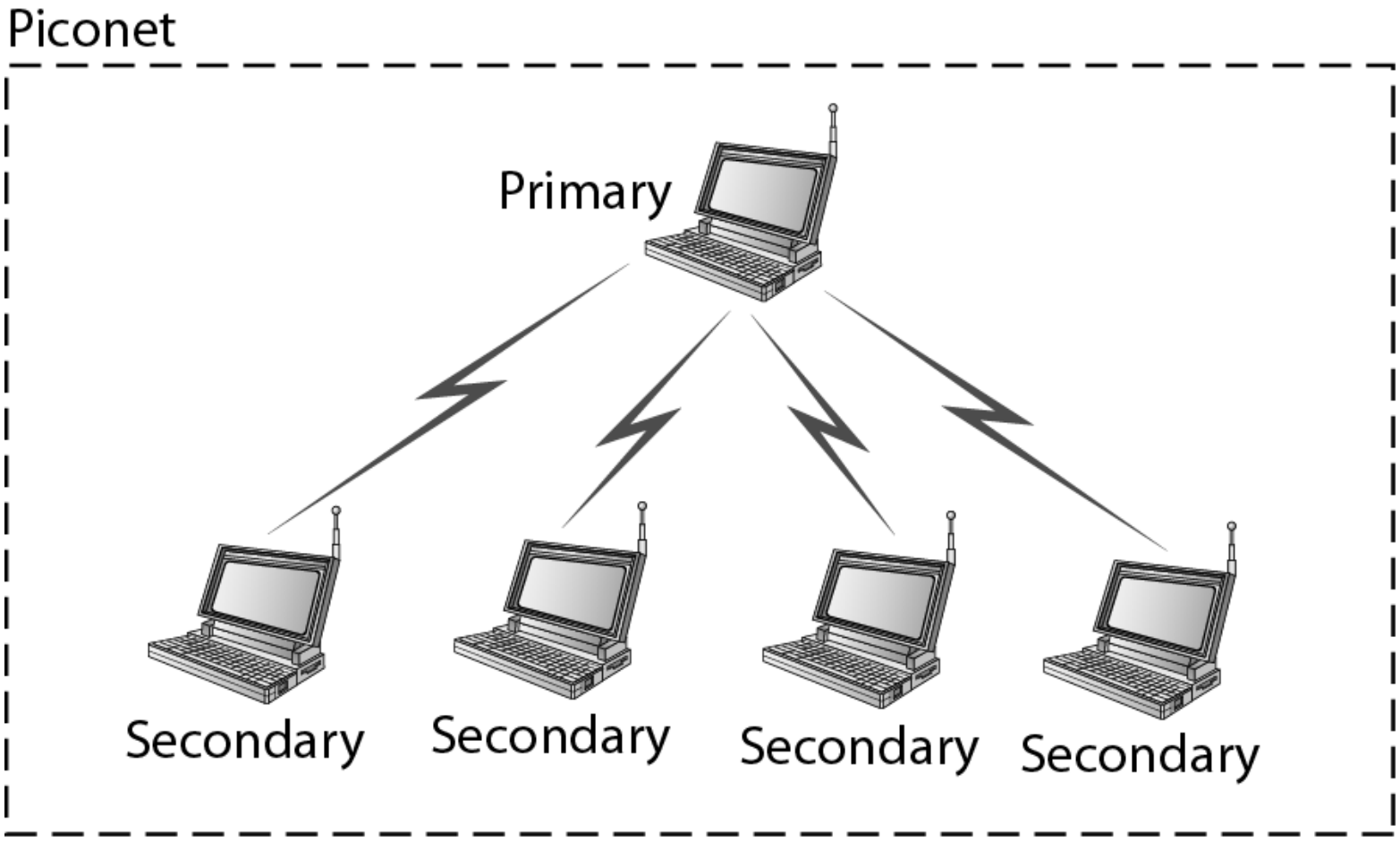


Figure 14.20 *Scatternet*

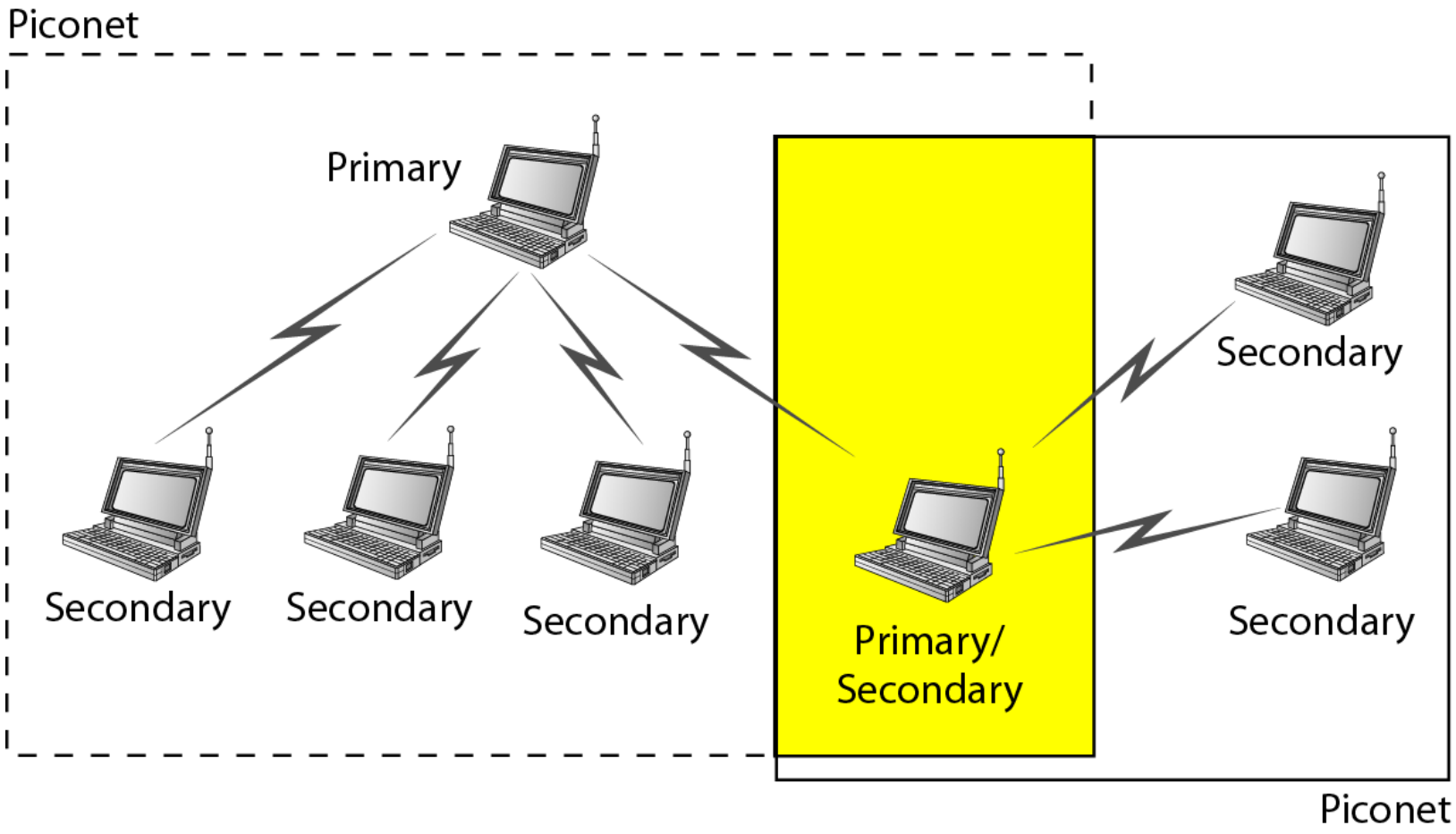


Figure 14.21 *Bluetooth layers*

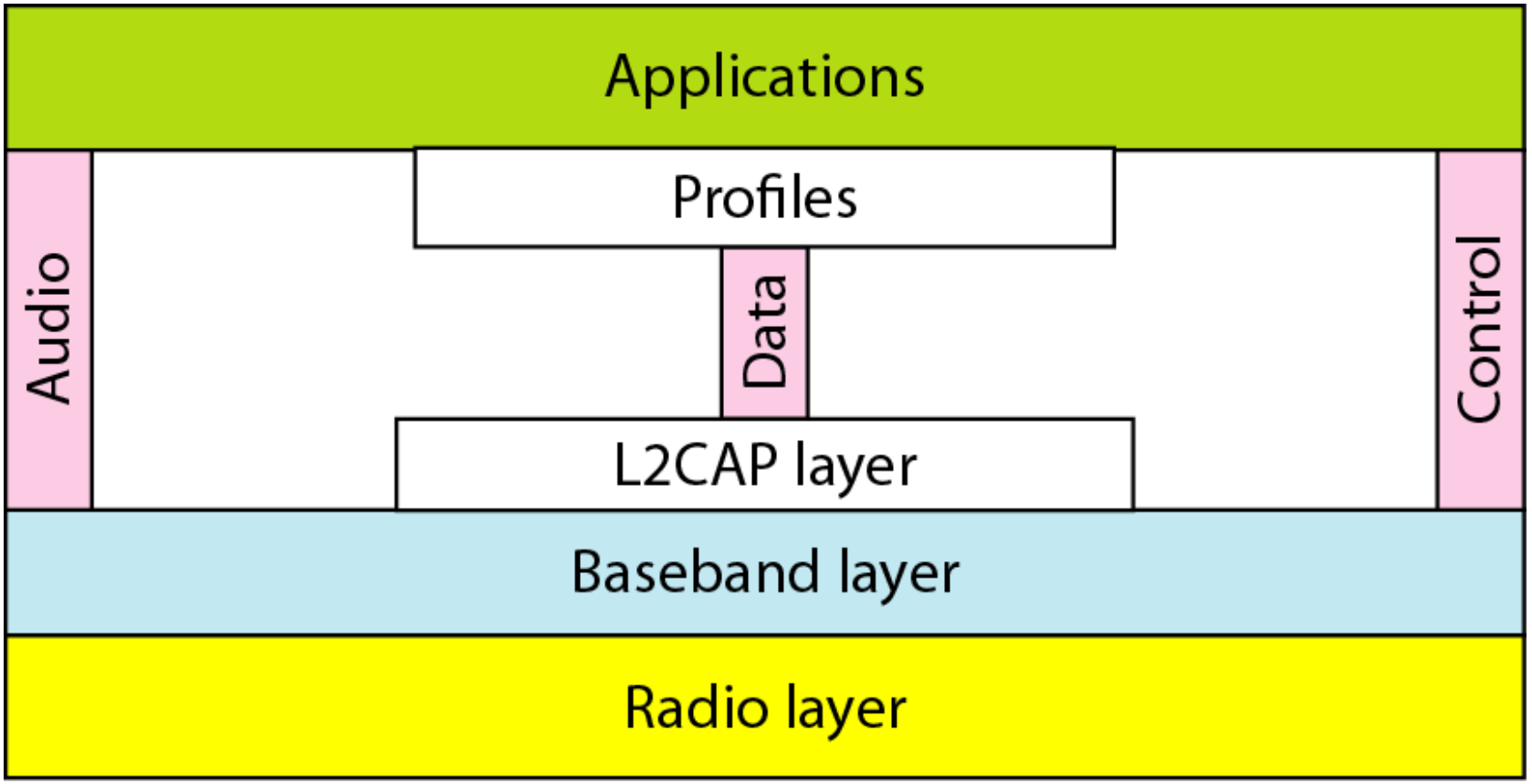


Figure 14.22 *Single-secondary communication*

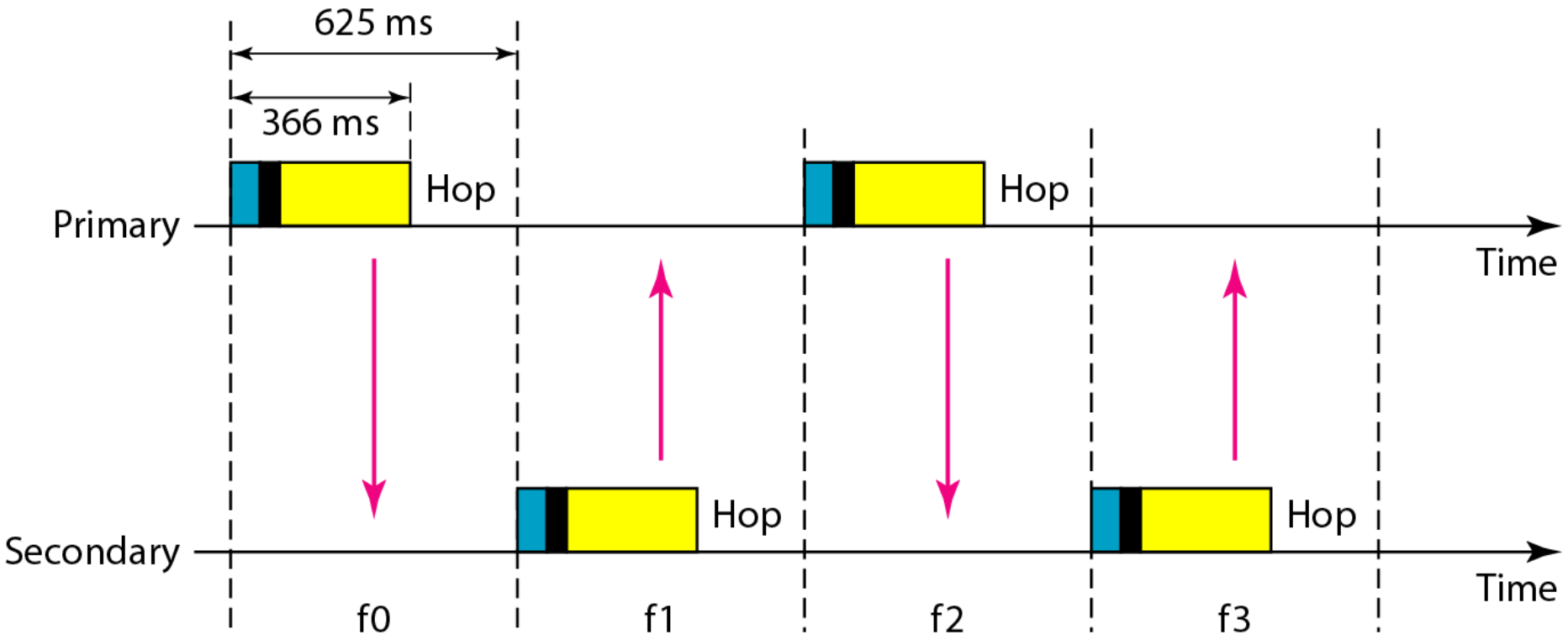


Figure 14.23 *Multiple-secondary communication*

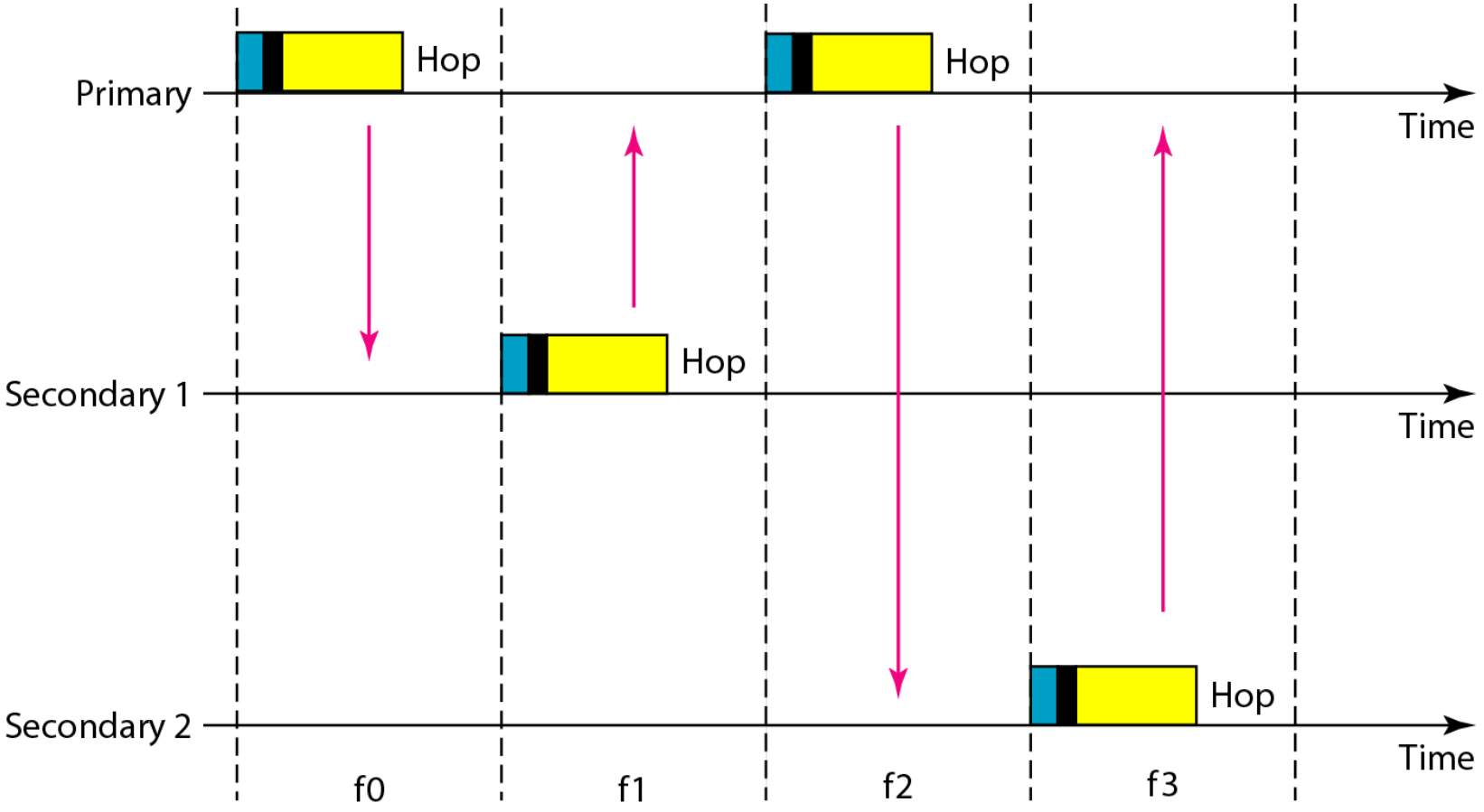
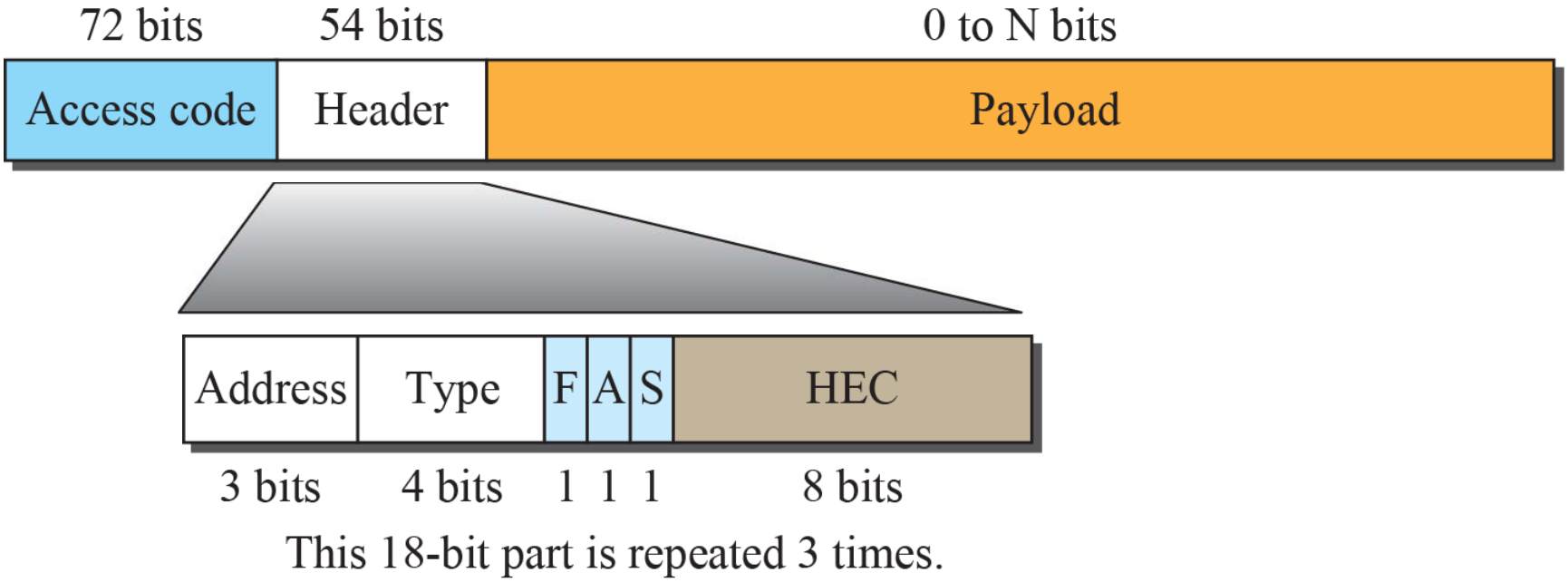


Figure 6.23: Frame format types



N = 240 for 1-slot frame

N = 1490 for 3-slot frame

N = 2740 for 5-slot frame

Figure 15.20: *L2CAP data packet format*